THE AFRICAN JOURNAL OF INFORMATION AND COMMUNICATION (AJIC)

ISSUE 28, 2021

Published by the LINK Centre
University of the Witwatersrand (Wits)
Johannesburg, South Africa
https://www.wits.ac.za/linkcentre

ISSN 2077-7213 (online version)
ISSN 2077-7205 (print version)

The African Journal of Information and Communication (AJIC)

Issue 28, 2021

Published by the LINK Centre, School of Literature, Language and Media (SLLM),
Faculty of Humanities, University of the Witwatersrand (Wits), Johannesburg, South Africa
https://www.wits.ac.za/linkcentre/ajic

The African Journal of Information and Communication (AJIC) is a peer-reviewed, interdisciplinary, open access academic journal focused on the myriad dimensions of electronic and digital ecosystems that facilitate information, communication, innovation and transformation in African economies and in the broader Global South. Accredited by the South African Department of Higher Education and Training (DHET), *AJIC* publishes online, free to the user, under a Creative Commons licence, and does not impose article processing charges. *AJIC* is indexed in Scientific Electronic Library Online (SciELO) SA, the Directory of Open Access Journals (DOAJ), Sabinet African Journals, and Wits University WIReDSpace.

Editors

Managing Editor: Tawana Kupe, Vice-Chancellor, University of Pretoria, tawana.kupe@up.ac.za
Corresponding Editor: Lucienne Abrahams, Director, LINK Centre, Faculty of Humanities, University of the Witwatersrand, PO Box 601, Wits 2050, Johannesburg, South Africa, ajic.submissions@gmail.com
Publishing Editor: Chris Armstrong, Research Associate, LINK Centre, University of the Witwatersrand, Johannesburg, South Africa, chris.armstrong@wits.ac.za

Peer-Reviewing

AJIC acknowledges with gratitude the following peer reviewers of submissions published in this issue: Mark Burke, Enrico Calandro, Barry Dwolatzky, Iginio Gagliardone, Shafika Isaacs, Geci Karuri-Sebina, Mike Klipin, Gillian Marcelle, Brett Van Niekerk, Nixon Muganda Ochara, Monica Singer, Damola Tolani and Chikezie Uzuegbunam.

Production

Sub-editing: LINK Centre
Proofreading: Linda Van de Vijver
Desktop-publishing: LINK Centre

AJIC is published by the LINK Centre, School of Literature, Language and Media (SLLM), Faculty of Humanities, University of the Witwatersrand (Wits), PO Box 601, Wits 2050, Johannesburg, South Africa. The LINK Centre is based at the Wits Tshimologong Digital Innovation Precinct, 41 Juta St., Braamfontein, Johannesburg, https://www.tshimologong.joburg

ISSN 2077-7213 (online version)
ISSN 2077-7205 (print version)

Past issues of *AJIC*, and its precursor *The Southern African Journal of Information and Communication (SAJIC)*, are available at https://www.wits.ac.za/linkcentre/ajic and https://www.wits.ac.za/linkcentre/sajic

CONTENTS

ARTICLES

Social Media Use, Disbelief and (Mis)information During a Pandemic: An Examination of Young Adult Nigerians' Interactions with COVID-19 Public Health Messaging

Olutobi Akingbade
Postdoctoral Research Fellow, Centre for the Advancement of Non-Racialism and Democracy (CANRAD), Nelson Mandela University, Port Elizabeth, South Africa
https://orcid.org/0000-0001-8536-9293

Abstract
This study contributes to transdisciplinary understanding of the COVID-19 pandemic through an examination of perceptions of public health messages as consumed primarily through social media by a purposively enlisted set of young adult Nigerians. The research used focus group discussions and in-depth interviews to elicit the views of 11 young adults, aged 21 to 24, resident in Ajegunle, a low-income community in Lagos, Nigeria's commercial capital. The study identifies the centrality of social media platforms to the respondents' processes of meaning-making, and draws on Hall's (1980) encoding/decoding model in order to bring to the fore their oppositional interpretations of public health messages. The study also identifies respondents' varying levels of disbelief about the realities of COVID-19, their mistrust of the government officials conveying and enforcing decisions to combat the pandemic, and the propensity for the social media messages they consume and propagate to serve as channels of misinformation.

Keywords
COVID-19, pandemic, public health, social media, media messages, codes, encoding, decoding, disbelief, misinformation, young adults, Nigeria, Lagos, Ajegunle

DOI: https://doi.org/10.23962/10539/32215

Recommended citation
Akingbade, O. (2021). Social media use, disbelief and (mis)information during a pandemic: An examination of young adult Nigerians' interactions with COVID-19 public health messaging. *The African Journal of Information and Communication (AJIC), 28*, 1-18. https://doi.org/10.23962/10539/32215

1. Introduction and context

The COVID-19 pandemic and its dangers are now public knowledge around the world. As of late June 2021, there were more than 180 million confirmed cases and more than 3.2 million deaths, spread across over 150 countries (WHO, n.d.). In order to contribute to the understanding of the varying responses to the pandemic across different communities and cultures, this study adopts a cultural and media studies perspective. The study focuses on the perceptions and understandings of young adults in a low-income community in Lagos, Nigeria's most populous city and the nation's commercial, financial, and industrial nerve centre (Statista, 2020).

Several social and behavioural researchers have argued that during pandemics and disasters, there must be consistent and targeted efforts aimed at gleaning how different demographics make sense of such episodes (see, for example, Flaherty, 2020; Holmes et al., 2020; Oksanen et al., 2020). It has also been argued that, in addition to making contributions to theorisations and postulations about the social impact of pandemics, understanding the lived experiences of individuals in specific cultures and age groups is useful in mitigating the conspiracy theories, misinformation, and mistrust that can contribute to the community transmission of a virus (Oksanen et al., 2020; Recchi et al., 2020).

This study examined perceptions of COVID-19 among a purposively enlisted set of 11 Nigerians aged 21 to 24 and resident in an urban low-income settlement in Lagos, with the aim of teasing out their perceptions of the pandemic information and the news reports they consume. This study was motivated by the need to provide insights into the actions, reactions, and nuances that underlie the reception of public health messages about the outbreak of COVID-19 on the African continent—in the context of various conspiracy theories and misleading rumours about the pandemic, and the pessimism expressed by stakeholders about the capacity and sincerity of politicians and government officials to mitigate and curb community transmission of the virus (see, for example, Amukele & Barbhuiya, 2020; Friedman, 2020; Harvey, 2020; Velavan & Meyer, 2020). More specifically, this study also sought to examine, within the context of the lived experiences of enlisted participants, the role of the mass media, including relatively recent forms of social media, in their self-understandings about COVID-19. This hinges on assertions in the extant literature (for example, Nicholas & O'Malley, 2013; Williams, 2013) which speak to the centrality of media to communication, perceptions, cultural beliefs, and understandings, and how the media has contributed, over the years, to the rapid spread of panic and misinformation during pandemic episodes and times of civil unrest.

Furthermore, the sampling of young Nigerians from amongst the residents in an urban low-income community stems from the steady increase, across several countries, in the numbers of confirmed COVID-19 cases amongst young adults, despite the original belief that they stand a better chance of not contracting COVID-19 (Grey,

2020; WHO, 2020). The tendency for young people to disobey the expected control measure of physical distancing as they perceive themselves to be at a lower risk of developing severe cases of COVID-19 (Andrews et al., 2020; Cummins, 2020; Lapin, 2020) thus proffers motivation for the purposive selection of the participants enlisted for this study. Young Nigerians were drawn from a low-income community (the community widely known as Ajegunle in Lagos) because physical distancing, personal hygiene, and other COVID-19 control measures have been a challenge in such communities, as alluded to by researchers, policy decision-makers, and other stakeholders in their efforts to mitigate the community transmission of COVID-19 (Hamann, 2020; Stringer et al., 2020).

2. Literature review

This study is grounded in conceptions of media consumption that emphasise the role of active audiences. Such audiences are not passive consumers of information about occurrences around them. They actively engage in a variety of ways with such information.

Media and audiences during epidemics and pandemics

Epidemics and pandemics are a recurring feature in human existence (Cunha, 2004; Hays, 2005; Lattanzi, 2008; Morganstein et al., 2017; Velavan & Meyer, 2020). Also, a recurring feature is the reality that the media shapes the perceptions and self-understandings of people during these episodes. During epidemic and pandemic episodes, the media play a central role in setting the public agenda and the tone of public discourse. The media also becomes the main source of information and knowledge relied on by residents in communities, cities, and countries where such severe outbreaks are recorded (Clarke & Everest, 2006; Riaz, 2008). Through media platforms, journalists in their various categories create awareness about pertinent issues in society and foster understanding of such issues through their disseminated messages—with the messages having the potential to create, shape, and maintain pictures of reality that are implicated in the actions, inactions, and overall behavioural patterns of the consumers of such messages (Croteau & Hoynes, 2014; McCombs, 2002).

A major aspect and component of the news stories and messages that shape public perceptions during epidemics and pandemics are the anxieties and fears embedded in the media messages that characterise these episodes, alongside other accompanying psychological stressors and behavioural responses. This is evidenced in studies that continuously point to the significant role that the media play as the main "conduit" through which ideas, news, and information that trigger these psychological stressors and behavioural responses flow (Akingbade, 2018; Croteau & Hoynes, 2014; Williams, 2013). This has seen the media in several countries described as being in the business of irrational fear-mongering through the dissemination of sensationalised headlines, news stories, and messages which have been proffered as the major source

of misinformation during pandemic episodes (Cantor, 2002; Goode & Ben-Yehuda, 2011; Hoekstra et al., 1999; Seale, 2002). The quick spread of misinformation, attributed to the media, which paves way for fears during the early stages of disease outbreaks has been suggested to result from the lack of immediate access by journalists and other communication executives to confirmed facts and scientific information from peer-reviewed literature, as these mostly lag behind during epidemic and pandemic episodes (Akingbade, 2017; Allgaier & Svalastog, 2015; Bursztyn et al., 2020).

Fears and other emotional responses that emanate from the continuous dissemination of misinformation during pandemics has the propensity to not only shape the self-understandings of the consumers of such messages but also to adversely affect their health as one's health status at any point in time is an outcome of complex interactions and interplays that operate over time (Akingbade, 2018; Seale, 2002). It is within such complex interactions and interplays that the media plays a crucial role during epidemics and pandemics, as residents who live through such outbreaks rely mainly on disseminated messages for information and knowledge. This was exemplified during the outbreak of Ebola, where sensationalised and exaggerated reporting created fears and widespread panic among consumers of such news stories in the affected West African states (Akingbade, 2017; Chan, 2014).

The implementation of physical distancing measures and various levels of lockdown around the world during the COVID-19 pandemic is also significantly enhancing and giving credence to the crucial role of the media as a means for individuals living through the pandemic to remain informed and educated about what is happening—and also as a means to reduce boredom and frustration.

At the same time, the various, and largely unregulated, social media platforms have been implicated in misinformation that circulates and shapes people's perceptions during epidemic and pandemic episodes. While misinformation predates the era of social media, these platforms create particularly significant complications during pandemics as they facilitate massive flows of exaggerated, manipulated, and conflicting stories that are widely viewed, liked, downloaded, and shared (Ciampaglia, 2018; Depoux et al., 2020; Farrell et al., 2020; Larson, 2018; Madrid-Morales et al., 2021). The lack of editorial gatekeeping (in comparison to traditional media) and the ability for users to generate and publicise content of their preference both enhance the viral nature of misinformation on social media platforms—phenomena that have been referred to as "digital pandemics" (Seymour et al., 2015). Additionally, social media platforms on smartphones, which create a confluence of interactivity, immediacy, and intimacy, transform users into active audiences (Larson, 2018; Willems, 2020) and immerse those who use these social media platforms in a deluge of opinions and stories during pandemics in ways that not only address boredom during lockdown, as alluded to earlier, but also aid and amplify the consumption and spread of misinformation. These and other similar dimensions have been examined in recent research

projects, such as the special issue edited by Ferrara et al. (2020), and this study adds to this body of knowledge.

Hall's (1980) encoding/decoding model of communication

There is a wide range of scholarship grounded in the assertion that while information disseminated through media is implicated in the behavioural patterns and self-understandings of recipients, the information serves as reference points that recipients actively use in evaluating their own lives. The recipients are not merely passive dupes who wholly consume and act on the received information (Kim, 2008; Takahashi, 2009). As researchers who draw on this theorising assert, media texts and information do not represent a set of explicit meanings but are polysemic, and the recipients of these texts and information critically interpret and "make sense" of these messages based on their social experiences, which are mostly contingent on the prevailing socio-economic and cultural factors within which these experiences are embedded (Barker & Jane, 2016; Hall, 1980).

This study draws on Hall's (1980) encoding/decoding model, which describes the audience/recipients of media messages and information as active meaning-makers who are capable of providing hegemonic, negotiated, or oppositional readings to these messages encoded according to the power structures and the professional and dominant ideologies of the message producers. Focused on the moments of *encoding* (production) and *decoding* (reception), the model conceptualises the process of communication as a complex circulation circuit. This model thereby posits that "meanings are open to wider ideological discourses" (Hall, 1980, p. 133) than assumed in the linear—sender, message, receiver—process that had been widely accepted up until the time of Hall's work (Schroder et al., 2003).

A hegemonic decoding/reading of an encoded media message—conceptualised in Hall's (1980) model as the "preferred" meaning that the producers of the disseminated message want the recipients and message consumers to decode and uphold—is considered as the dominant meaning as it offers patterns that reinforce the prevailing descriptions and ideological order encoded in the message. Recipients of media messages whose worldview aligns with the hegemonic reading will fully decode these messages in their entirety in the exact way they were intended by the producers. An oppositional decoding/reading, on the other hand, occurs when recipients of the encoded media message understand the intended and inherent substance of the message, but reject the hegemonic/preferred meaning in support of alternative readings. Although the audiences who adopt this oppositional reading can comprehend the hegemonic, dominant reading of the disseminated messages, they draw on their lived experiences in order to adopt an oppositional reading.

Negotiated reading of disseminated media messages, as theorised by Hall (1980), allows for recipients to both acknowledge the preferred meaning and, at the same time,

adapt and differently situate/decode the meaning to suit their personal preferences, circumstances, and contexts. While the recipients of media messages who operate within this position acknowledge the grand significations encoded in these messages, they "negotiate" their own meanings rather than fully accepting the hegemonic meaning. Although the encoding/decoding model has been critiqued by theorists (see, for example, Fiske, 1987; Murdock, 2017), it has remained relevant and useful in research projects on media consumption, youth subcultures, and audience reception studies, that require nuanced analyses of how the meanings of media messages are received, negotiated, and acted upon by recipients in the course of their everyday lives.

3. Research design

The research followed a qualitative design grounded in interpretative phenomenological analysis (IPA)—an approach that explores the lived experiences of research participants and emphasises that all human beings are in a "continual process of constructing, interpreting and making sense of their world" (Babbie & Mouton, 2001, pp. 28–29). The 11 young Nigerians enlisted for the study were born and brought up in the low-income community of Ajegunle. Their levels of education ranged from a high school certificate to a college diploma. They stated, at the time they were being enlisted for the study, that they had some form of paid employment that was inadequate to meet their basic needs. The deliberate focus on a small sample size stems from the IPA approach, whereby "small, purposively-selected and carefully situated samples" (Smith et al., 2009, p. 29) are focused on within a specific context with the aim of producing an in-depth examination of certain phenomena.

The data generated for this study emanated from semi-structured focus group discussions and individual in-depth interviews. Two focus group discussions were held in March 2020, which was after the first index case of COVID-19 in Nigeria had been announced, but prior to the commencement of the lockdown. The first focus group (FG1) had five participants (three males and two females), and the second (FG2) had six participants (four females and two males). In accordance with the position of qualitative research scholars (for example, Hansen et al., 1998; Krueger & Casey, 2014) who assert that focus group sessions are ideally best held in natural settings that are public spaces and not in a laboratory or artificial setting, the two focus group discussions were held in a local eatery that the participants were familiar with and had agreed was a convenient venue. FG1 lasted for 55 minutes, while FG2 lasted for about 64 minutes.

In the following month, April 2020, during the lockdown, follow-up individual in-depth interviews were conducted with all 11 participants through video calls on Facebook and WhatsApp. This approach was based on assertions in the literature

(for example, Drabble et al., 2016; Janghorban et al., 2014) which establish the usefulness of online interviews as a means of gathering data despite constraints in physical mobility. Although the researcher was back in South Africa when the follow-up interviews were conducted, the familiarity, rapport, and trust that the researcher had established with the participants during the focus group discussions mitigated the inhibition that comes with online interviews. The average duration of the interviews was 32 minutes.

During the focus group discussions, data were elicited from participants' conversations about their thoughts on COVID-19, where and how they got updates and news stories about the pandemic, with whom they shared and discussed the updates and news stories, alongside their thoughts about the function of government agencies in mitigating the spread of the pandemic. The individual interviews complemented the focus group sessions, as these provided clarity and further insights into the themes discussed during the focus group sessions—and also provided useful data on participants' experiences during the lockdown. The guiding questions for both the focus group discussions and the individual in-depth interviews are provided in the Appendix.

Research and ethics approval processes were completed at Lagos state's ministry of health, Ikeja. Written and verbal consent was obtained from each respondent before data collection began. Before this consent was sought, participants were provided with detailed information about the research project and informed of their right to withdraw from the project if at any point they felt uncomfortable or unwilling to continue.

4. Findings and analysis

The study results and discussion presented in the sub-sections below are based on thematic coding of the transcripts of the audio recordings from the focus group discussions and individual interviews. Pseudonyms are employed in the presentation of the data, because participants were guaranteed anonymity in order to allow them to speak as freely as possible and provide detailed narratives.

Centrality of social media

All the young adults enlisted for this study referred to social media platforms, specifically Facebook, Twitter, and WhatsApp, as being their primary sources for getting updated information about COVID-19 prior to the recording of the index case in Lagos state and also during the lockdown. This is evidenced in these excerpts from the focus group discussions and interview data:

> I get updates on all the happening stuffs on Facebook so there's nothing about COVID that I don't know […]. (Musa, in FG1)

> The only thing that gets me through this boring waste of time and propaganda called lockdown is the Facebook app on my Samsung where I get to catch up as usual on stuffs from my phone about every latest gist out there, including the lies we are being fed about this coro sickness […]. (Musa, interview)
>
> I follow *Vanguard* reports and other news agencies via my Facebook even before this coro thing started. See, I can bring out my phone and show you many stuff about coro on my WhatsApp and even on Facebook. (Adams, interview)

The data also show that social media had been an integral part of the everyday actions and activities of the participants prior to the outbreak of COVID-19. Thus, it was not out of character for this set of young Nigerians to turn to these platforms to make sense of the pandemic. These findings are consistent with those from studies indicating that youths are more active than other demographics in their participation in, and consumption of, social media (see Järvinen et al., 2012; Kannan & Hongshuang, 2017). The qualitative insight offered in this paper further exemplifies how young Africans engage daily with the world around them through social media, despite obvious constraints in internet access (such as expensive networks and internet subscription plans) in most states in sub-Saharan Africa. This also speaks to how the use of social media platforms has become a norm for this study's participants despite their low-income backgrounds.

It was found that eight of the 11 participants had maintained their paid access to internet despite losing their (low-paying) jobs during the mandated COVID-19 lockdown. These participants stated that they prioritise being able to reach out, and to receive communication, at all times through their social media accounts. All of the participants indicated that most of their social media engagements occurred through their smartphones, and that they would always prioritise owning a smartphone over owning cheaper models that could not access social media. This sentiment was strongly held even while the participants also complained of financial challenges, low-paying jobs, and—for the participants who had lost their jobs—unemployment. Study participants' narratives about how useful their smartphones have been, especially during the lockdown, which Musa, as cited above, refers to as a "boring waste of time and propaganda", speak to the theorising on the affordances of social media on smartphones and how it has the propensity to transform users into active audiences. This is useful in understanding the desire of this set of young Nigerians to always own a smartphone and to stay active on social media.

In the quotation above from the interview with Adams, in which he speaks of following reports from *Vanguard*, a daily newspaper, via its Facebook postings, we see social media serving as a conduit for content from traditional media outlets. Other study participants also referenced the social media channels of traditional media (print and

broadcast) as sources for some of the information they continuously access through their social media accounts. This is in consonance with the theorising, earlier highlighted, on how both traditional media and newer forms of social media do not only uphold the function of setting the public agenda and the tone of public discourse, but are main sources of information and knowledge. More specifically, this brings to the fore the unique and central position held by social media as the platforms through which this function is realised in the contemporary world.

Decodings of COVID-19 messages

During the two focus groups held in March 2020 before lockdown, all 11 participants rejected the reality of COVID-19. The detailed narratives they provided during the discussions indicated their disbelief as they asserted that the viral disease did not exist and was a mere distraction intended to create chaos. The study participants, throughout the duration of the focus group sessions, insisted that irrespective of the various news and reports about the viral disease that they had engaged with, COVID-19 precautionary measures were unnecessary since the disease was simply "propaganda".

In rejecting the reality of COVID-19, participants, during these focus group discussions, regarded it as something that should not be allowed to undermine their daily needs and activities. The words of Pam, a participant in FG2, were typical of the perspectives of the 11 participants:

> I was still saying it on one of the WhatsApp group chats this morning that we cannot allow ourselves to be fed and scammed with this distraction carefully packaged and labelled as "corona from China" and sent to us. The propaganda will get a lot of people but definitely not me. I just got a job as a receptionist and office assistant after almost three years of completing my diploma, so this job plus my other daily hustling is what I am concerned with. […] all-round poverty cannot be staring you in the face every day and you will still be believing some funny charade rather than focusing on your hustle […]. (Pam, in FG2)

Drawing on Hall's (1980) encoding/decoding model, the stance of this set of young adults indicates their refusal to accept the preferred and dominant meaning encoded in COVID-19 messages—despite their ability to fully grasp and decode the dominant and intended information inherent in the messages. They dismiss the hegemonic decoding/readings as "distraction". This is consistent with the theorising on active audiences, as these young Nigerians refuse to passively receive reportage on COVID-19. Instead, they draw on the COVID-19 messages as reference points as they evaluate their lives, and have decided that an undivided focus on their "daily hustling" is more worthy of their attention than the "distraction carefully packaged and labelled as 'corona from China'".

This disposition of these young adults during the focus group discussions aligns with the view that active audiences make sense of the messages they receive within the context of their social experiences, which mostly hinge on the prevailing socio-economic and cultural factors within which these experiences are embedded. The young adults who participated in this study were raised and presently live in Ajegunle, a community regarded as crime-ridden and one of the most disadvantaged in Lagos state. Accordingly, they interpret the reports about COVID-19 within the context of their everyday socio-economic challenges—summarised by Pam, in the quotation above, as "all round poverty". In the words of a FG1 participant, Lizzy:

> There's no need to listen to the plenty fake stories about this corona thing while I have so many disturbing things I need to sort out in my life and in this ghetto. Adding their silly propaganda to the list will be a senseless thing for me to do. […] I've already shared my opinion and stand about this Chinese *wahala*[1] on my WhatsApp stories yesterday, and I also did that while sharing, on my Facebook timeline, one of the corona stories on *Tribune*'s [*Nigerian Tribune* newspaper's] Facebook page. (Lizzy, in FG1)

However, during the individual interviews conducted during the lockdown in April 2020, seven of the participants somewhat accepted the possibility of the existence of COVID-19, while at the same time expressing their scepticism. Even though these seven participants acknowledged the existence of COVID-19, unlike the other four who insisted that the viral disease was a myth and upheld their disbelief, their scepticism was evident in how they downplayed the seriousness attached to the pandemic by the various news, media reports, and relevant government authorities. Despite the shift in COVID-19 perceptions of these seven young Nigerians who now stated that the viral disease does exist—in Lagos state, the epicentre of the pandemic in Nigeria, as well as in other parts of the country and in other countries in the world—they asserted that it was really nothing to be afraid of and regarded the lockdown as an exaggerated response. One of the seven, Eddi, drew comparisons to malaria and Ebola:

> Yes, I now accept that this China corona is real, but then it's not rocket science […]. Locking us all down because of something just like malaria that those of us in this 'hood are so, so used to does not make sense to me. Check social media or your TV, you'll see the debates on chloroquine, a malaria drug, being used in some isolation centres, [so] isn't that malaria? We defeated Ebola without locking up everywhere, so why must we foolishly copy other nations and lock everywhere down because of this overhyped propaganda? (Eddi, interview)

Eddi's mention of Ebola is a reference to the 2014 Ebola outbreak in Lagos. Lockdown was not enforced during this outbreak, and the epidemic was combated.

1 A Yoruba word meaning "trouble" or "problem".

In the words of another interviewee, Shai:

> Even though we are told it is real and I'm now in agreement with that, the truth is that I do not bother myself to use the face mask because I know that this coro thingy is not for people like us who almost never leave this 'hood, not to talk of travelling outside *naija* [Nigeria]. Go check your social media and see those infected. They're the rich people who are always on the move. […] have you seen any struggling person from this place have it? I don't know of a single person from this area that has tested positive […]. So you see what I'm saying. It is these rich people and politicians that are at risk and they're saying we should stay at home when they know that lockdown and social distancing cannot work in an overpopulated place like this where over 30 people are sharing bathroom and toilet with no regular water […]. (Shai, interview)

These quotations provide examples from the data which usefully show the perceptions of the young adults who have come to accept the reality of COVID-19, but still hold on to their doubts about the scope of the pandemic which, contrary to their assertions, is not similar to malaria and is not bound to the confines of a specific demographic group or societal classification. These statements indicate how recipients of information about a pandemic can negotiate their own meanings by situating and then adapting the decoded meaning to suit their personal preferences, biases, experiences, and contexts. This phenomenon was also evident in other statements shared by the young adults during the interviews, including narratives pointing out that hunger is deadlier than COVID-19 and that they have been exposed to severe hunger as a result of the lockdown—due to their monthly wages being reduced by their employers, due to losing their jobs, and due to them not being able to pursue other "daily hustling" which ordinarily serves as a source of income.

The interview respondents were apparently engaged in a process where they continually "make sense" of the pandemic and the messages they were being exposed to—in consonance with assertions that disseminated texts and information do not have explicit meanings but are polysemic and can therefore be interpreted in different ways.

Misinformation

Statements from study participants, in both the focus groups and the individual interviews, also demonstrate their consumption of, and participation in the spread of, misinformation about COVID-19—and the degree to which social media channels are often implicated in these patterns. Othering COVID-19 on social media as "Chinese *wahala*" or as a "distraction carefully packaged and labelled as 'corona from China'" reveals a propensity to shift the attention of those they interact with online—towards misinformation, and away from pertinent compliance measures that should be practised and upheld to mitigate the spread of the viral disease.

We saw above the false assertions that COVID-19 is similar to malaria, that chloroquine is an effective treatment for the disease, and that the disease does not spread among the poor. Such misinformation spreads rapidly when virtual friends and followers pass along the oppositional stance through their respective social media platforms. This underscores how the circulation of misinformation during outbreaks of viral diseases is amplified through the varying forms of user-generated content on social media. Such content, according to Murdock (2017), has repositioned audiences as productive agents engaged in a continuous process of interpreting and responding to messages, goods, and services by circulating their own materials and resources, which can range from simple "likes" or "shares" to uploading videos, posting photos, posting comments, and other forms of social media engagement or behaviour.

The more this set of young adults, or others with similar worldviews, hold on to their disbelief about COVID-19 and discuss it amongst themselves, in-person and virtually, the more the tendency for these perceptions to engender the spread of misinformation which, as stated above, is further complicated by social media. The more the seeming logic in the arguments presented by these young Nigerians in support of their scepticism is raised and discussed amongst their peers, the more there is the tendency for this misinformation to encourage them to neglect and abandon the measures intended to mitigate the spread of COVID-19.

State illegitimacy

Participants frequently referred to the COVID-19 outbreak as "propaganda"—an assertion that was further qualified, at times, with the claim that the government's response was "silly", "overhyped", or a "silly charade". Here we see evidence of respondents' mistrust of those in power, at various levels of governance in Nigeria, who are leading the efforts to combat the pandemic. This perception was sharply exemplified in the claim by one of the participants who, in reacting to the information about the outbreak of COVID-19, asserted that he and his peers "are all being scammed by these politicians", thereby resulting in his refusal to wear a face mask or obey physical distancing rules. This assertion, and others like it in the data, proffers insight into how study participants' lack of trust in the intentions of their democratically elected leaders feeds into their reluctance to wholly embrace the reality of COVID-19.

The experiences shared by participants show that they are far from being oblivious to the inequalities and marginalisation that have long plagued Nigeria. They have seen the continued neglect of their community despite the low standard of living and the clear need for developmental intervention by the state. The violations of human rights, the corruption, and the continued abuse of other democratic principles and values by most political office holders in Nigeria have persistently undermined social solidarity, and have engraved mistrust for politicians in the subconscious of these young adults—and such profound disillusionment cannot suddenly be erased at the instance of an outbreak of a disease such as COVID-19. These young residents of Ajegunle understandably find it difficult to wholly accept that political office holders

are suddenly interested in their welfare and that a total lockdown that keeps them not just in their impoverished community for weeks but also in a state of hunger without palliative measures is in their best interest.

6. Conclusions

This study has demonstrated how a purposively enlisted set of young Nigerians relies on social media for public health information during a pandemic. The study has highlighted their interpretation of public health messages within the context of their socio-economic realities, and how they draw on these interpretations to reject the dominant meanings encoded in such messages and negotiate their own meanings. The study has also identified the propensity for people who feel a sense of socio-economic marginalisation to neglect, and/or refuse to participate in, efforts intended to combat a pandemic if the efforts are spearheaded by political leaders whom they do not trust.

Among other remedies, there is a need for consistent effort by relevant stakeholders to contribute to the maturation of democratic institutions in Nigeria, because the more democratic values are entrenched, the more trust can be established between citizens in various demographic groupings and political leaders. The more such trust exists, the more political leaders can rely on citizens, irrespective of their socio-economic status, to cooperate with measures aimed at mitigating the spread of a viral disease during a pandemic episode. In the case of young adults, it will also be advisable to incorporate, as stakeholders during pandemic episodes, local artistes who are active in social media spaces and whom young adults hold in high esteem. Such artistes can reach out to young people, through social media, and emphasise the need to comply with safety and preventive measures.

References

Akingbade, O. (2017). *Negotiating the line between information and panic: A case study of Vanguard's coverage of the Ebola outbreak in Nigeria.* Master's dissertation, Rhodes University, Grahamstown, South Africa. http://vital.seals.ac.za:8080/vital/access/manager/Repository/vital:20986?site_name=GlobalView

Akingbade, O. (2018). Epidemics, fears and the mass media: An analysis of the 2014 Ebola virus disease outbreak in Nigeria. *Journal of Communication and Media Research*, *10*(2), 139–148.

Allgaier, J., & Svalastog, A. L. (2015). The communication aspects of the Ebola virus disease outbreak in Western Africa – Do we need to counter one, two, or many epidemics? *Croatian Medical Journal*, *56*(5), 496–499. https://doi.org/10.3325/cmj.2015.56.496

Amukele, T., & Barbhuiya, M. (2020, July 12). African countries need cheaper COVID-19 tests: Here's how to get them. https://theconversation.com/african-countries-need-cheaper-covid-19-tests-heres-how-to-get-them-141315

Andrews, J. L., Foulkes, L., & Blakemore, S. J. (2020). Peer influence in adolescence: Public-health implications for COVID-19. *Trends in Cognitive Sciences*, *24(8)*, 585–587. https://doi.org/10.1016/j.tics.2020.05.001

Babbie, E., & Mouton, J. (2001). *The practices of social research*. Oxford University Press.

Barker, C., & Jane, E. A. (2016). *Cultural studies: Theory and practice*. Sage.

Bursztyn, L., Rao, A., Roth, C., & Yanagizawa-Drott, D. (2020). *Misinformation during a pandemic.* Becker Friedman Institute for Economics Working Paper (2020-44), University of Chicago. https://doi.org/10.3386/w27417

Cantor, J. (2002). Fright reactions to mass media. *Media effects: Advances in theory and research*, *2*(2), 287–306.

Chan, M. (2014). Ebola virus disease in West Africa—no early end to the outbreak. *New England Journal of Medicine*, *371*(13), 1183–1185. https://doi.org/10.1056/NEJMp1409859

Ciampaglia, G. L. (2018). Fighting fake news: A role for computational social science in the fight against digital misinformation. *Journal of Computational Social Science*, *1*(1), 147–153. https://doi.org/10.1007/s42001-017-0005-6

Clarke, J. N., & Everest, M. M. (2006). Cancer in the mass print media: Fear, uncertainty and the medical model. *Social Science & Medicine*, *62*(10), 2591–2600.

Croteau, D., & Hoynes, W. (2014). *Media/society: Industries, images, and audiences* (5th ed.). Sage.

Cummins, E. (2020, March 24). A likely culprit in Covid-19 surges: People hell-bent on ignoring social distancing orders. https://www.vox.com/the-highlight/2020/3/24/21191184/coronavirus-masks-social-distancing-memorial-day-pandemic-keep-calm-carry-on-fauci

Cunha, B. A. (2004). Influenza: Historical aspects of epidemics and pandemics. *Infectious Disease Clinics*, *18*(1), 141–155. https://doi.org/10.1016/S0891-5520(03)00095-3

Deacon, D., Pickering, M., Murdock, A., & Golding, P. (1999). *Researching communications: A practical guide to methods in media and cultural analysis*. Arnold.

Depoux, A., Martin, S., Karafillakis, E., Preet, R., Wilder-Smith, A., & Larson, H. (2020). The pandemic of social media panic travels faster than the COVID-19 outbreak. *Journal of Travel Medicine*, *27*(3), 1–2. https://doi.org/10.1093/jtm/taaa031

Drabble, L., Trocki, K. F., Salcedo, B., Walker, P. C., & Korcha, R. A. (2016). Conducting qualitative interviews by telephone: Lessons learned from a study of alcohol use among sexual minority and heterosexual women. *Qualitative Social Work*, *15*(1), 118–133. https://doi.org/10.1177/1473325015585613

Farrell, T., Gorrell, G., & Bontcheva, K. (2020). Vindication, virtue and vitriol: A study of online engagement and abuse toward British MPs during the COVID-19 pandemic. *Journal of Computational Social Science*, *3*, 401–443. https://doi.org/10.1007/s42001-020-00090-9

Ferrara, E., Cresci, S., & Luceri, L. (2020). Misinformation, manipulation, and abuse on social media in the era of COVID-19. *Journal of Computational Social Science*, *3*(2), 271–277. https://doi.org/10.1007/s42001-020-00094-5

Fiske, J. (1987). *Television culture.* Routledge.

Flaherty, C. (2020, May 26). Social scientists on COVID-19. *Inside Higher Ed.* https://www.insidehighered.com/news/2020/05/26/social-scientists-covid-19

Friedman, S. (2020, July 16). South Africa is failing on COVID-19 because its leaders want to emulate the First World. https://theconversation.com/south-africa-is-failing-on-covid-19-because-its-leaders-want-to-emulate-the-first-world-142732

Gautret, P., Lagier, J. C., Parola, P., Meddeb, L., Mailhe, M., Doudier, B., Courjon, J., Giordanengo, V., Vieira, V. E., Dupont, H. T., & Honoré, S. (2020). Hydroxychloroquine and azithromycin as a treatment of COVID-19: Results of an open-label non-randomized clinical trial. *International Journal of Antimicrobial Agents*, p. 105949. https://doi.org/10.1101/2020.03.16.20037135

Goode, E., & Ben-Yehuda, N. (2011). Grounding and defending the sociology of moral panic. In S. P. Hier (Ed.), *Moral panic and the politics of anxiety* (pp. 20–36). Routledge.

Grey, H. (2020, June 24). More young people are getting COVID-19: What that means for the outbreak. *Healthline*. https://www.healthline.com/health-news/more-young-people-are-getting-covid-19-what-that-means-for-the-outbreak

Guo, Y. R., Cao, Q. D., Hong, Z. S., Tan, Y. Y., Chen, S. D., Jin, H. J., Tan, K. S., Wang, D. Y., & Yan, Y. (2020). The origin, transmission and clinical therapies on coronavirus disease 2019 (COVID-19) outbreak – An update on the status. *Military Medical Research*, *7*(1), 1–10. https://doi.org/10.1186/s40779-020-00240-0

Hall, S. (1980). Encoding/decoding. In S. Hall, D. Hobson, A. Lowe, & P. Willis (Eds.), *Culture, media, language* (pp. 128–138). Hutchinson.

Hamann, R. (2020, July 3). Civil society groups that mobilised around COVID-19 face important choices. *The Conversation*. https://theconversation.com/civil-society-groups-that-mobilised-around-covid-19-face-important-choices-140989.

Hansen, A., Cottle, S., Negrine, R., Newbold, C. & Halloran, J. (1998). *Mass communication research methods.* Macmillan.

Harvey, R. (2020, July 9). How COVID-19 is putting the rule of law to the test across Africa. *The Conversation*. https://theconversation.com/how-covid-19-is-putting-the-rule-of-law-to-the-test-across-africa-142080

Hays, J. N. (2005). *Epidemics and pandemics: Their impacts on human history*. ABC-Clio.

Hoekstra, S. J., Harris, R. J., & Helmick, A. L. (1999). Autobiographical memories about the experience of seeing frightening movies in childhood. *Media Psychology*, *1*(2), 117–140. https://doi.org/10.1207/s1532785xmep0102_2

Holmes, E. A., O'Connor, R. C., Perry, V. H., Tracey, I., Wessely, S., Arseneault, L., Ballard, C., Christensen, H., Silver, R.C., Everall, I., & Ford, T. (2020). Multidisciplinary research priorities for the COVID-19 pandemic: A call for action for mental health science. *The Lancet Psychiatry*, *7*(6), 547–560. https://doi.org/10.1016/S2215-0366(20)30168-1

Janghorban, R., Roudsari, R. L., & Taghipour, A. (2014). Skype interviewing: The new generation of online synchronous interview in qualitative research. *International Journal of Qualitative Studies on Health and Well-being*, *9*(1), 24152. https://doi.org/10.3402/qhw.v9.24152

Järvinen, J., Tollinen, A., Karjaluoto, H., & Jayawardhena, C. (2012). Digital and social media marketing usage in B2B industrial section. *Marketing Management Journal*, *22*(2), 102–117.

Jordan, R. E., Adab, P., & Cheng, K. K. (2020). COVID-19: Risk factors for severe disease and death. *BMJ*. https://doi.org/10.1136/bmj.m1198

Kannan, K., & Hongshuang, A. L. (2017). Digital marketing: A framework, review and research agenda. *International Journal of Research in Marketing*, *34*(1), 22–45. https://doi.org/10.1016/j.ijresmar.2016.11.006

Kapitan, S., & Silvera, D. H. (2016). From digital media influencers to celebrity endorsers: Attributions drive endorser effectiveness. *Marketing Letters*, *27*(3), 553–567. https://doi.org/10.1007/s11002-015-9363-0

Kim, Y. (Ed.). (2008). *Media consumption and everyday life in Asia.* Routledge. https://doi.org/10.4324/9780203892480

Krueger, R. A., & Casey, M. A. (2014). *Focus groups: A practical guide for applied research*. Sage.

Lapin, T. (2020, June 30). Alabama students partied despite knowing they had coronavirus, officials say. *New York Post.*

Larson, H. J. (2018). The biggest pandemic risk? Viral misinformation. *Nature*, *562*(7726), 309–310. https://doi.org/10.1038/d41586-018-07034-4

Lattanzi, M. (2008). Non-recent history of influenza pandemics, vaccines, and adjuvants. In R. Rappuoli, & G. Del Giudice (Eds.), *Influenza vaccines for the future* (pp. 245–259). Birkhäuser Basel. https://doi.org/10.1007/978-3-7643-8371-8_11

Madrid-Morales, D., Wasserman, H., Gondwe, G., Ndlovu, K., Sikanku, E., Tulley, M., Umejei, E., & Uzuegbunam, C. (2021). Motivations for sharing misinformation: A comparative study in six sub-Saharan African countries. *International Journal of Communication*, *15*, 1200–1219.

McCombs, M. (2002). The agenda-setting role of the mass media in the shaping of public opinion. Paper presented at London School of Economics and Political Science. http://sticerd.lse.ac.uk/dps/extra/McCombs.pdf

Metzler, K. (2020, April 18). What social science can offer us in a time of Covid-19 [Blog post]. *Times Higher Education*.

Morganstein, J. C., Fullerton, C. S., Ursano, R. J., Donato, D., & Holloway, H. C. (2017). Pandemics: Health care emergencies. In R. J. Ursano, C. S. Fullerton, L. Weisaeth, & B. Raphael (Eds.), *Textbook of disaster psychiatry* (2nd ed.) (pp. 270–283). Cambridge University Press. https://doi.org/10.1017/9781316481424.019

Murdock, G. (2017). Mediatisation and the transformation of capitalism: The elephant in the room. *Javnost - The Public*, *Journal of the European Institute for Communication and Culture, 24*(2), 119-135.

Nicholas, S., & O'Malley, T. (Eds.) (2013). *Moral panics, social fears, and the media: Historical perspectives*. Routledge. https://doi.org/10.4324/9780203386231

Oksanen, A., Kaakinen, M., Latikka, R., Savolainen, I., Savela, N., & Koivula, A. (2020). Regulation and trust: 3-month follow-up study on COVID-19 mortality in 25 European countries. *JMIR Public Health and Surveillance*, *6*(2), e19218. https://doi.org/10.2196/19218

Recchi, E., Ferragina, E., Helmeid, E., Pauly, S., Safi, M., Sauger, N., & Schradie, J. (2020). The "eye of the hurricane" paradox: An unexpected and unequal rise of well-being during the Covid-19 lockdown in France. *Research in Social Stratification and Mobility*, *68*, 100508. https://doi.org/10.1016/j.rssm.2020.100508

Riaz, S. (2008). Agenda setting role of mass media. *Global Media Journal*, *1*(2), 2070–2469.

Rothan, H. A., & Byrareddy, S. N. (2020). The epidemiology and pathogenesis of coronavirus disease (COVID-19) outbreak. *Journal of Autoimmunity*, *109*, 1–4. https://doi.org/10.1016/j.jaut.2020.102433

Schroder, K., Drotner, K., Kline, S., & Murray, C. (2003). *Researching audiences*. Arnold.

Seale, C. (2002). *Media and health*. Sage.

Seymour, B., Getman, R., Saraf, A., Zhang, L. H., & Kalenderian, E. (2015). When advocacy obscures accuracy online: Digital pandemics of public health misinformation through an antifluoride case study. *American Journal of Public Health*, *105*(3), 517–523. https://doi.org/10.2105/AJPH.2014.302437

Smith, J. A., Flower, P., Tindall, L., & Larkin, M. (2009). *Interpretative phenomenological analysis: Theory, method and research.* Sage.

Singhal, T. (2020). A review of coronavirus disease-2019 (COVID-19). *The Indian Journal of Pediatrics*, *87*, 1–6. https://doi.org/10.1007/s12098-020-03263-6

Statista. (2020). *Demographics of Nigeria.*

Stringer, B., Alcayna, T., Caleo, G., Carrion-Martin, I., Froud, A., Gray, N., Keating, P., Kuehne, A., Lenglet, A., Stellmach, D., & De Jong, A. (2020). Exploring the perceptions of communities toward the impact novel Coronavirus-2 (SARS-CoV-2), COVID-19 outbreak and response can have on their lives and security. Multisite qualitative assessment protocol. Médecins Sans Frontières.

Takahashi, T. (2009). *Audience studies: A Japanese perspective* (Vol. 5). Routledge. https://doi.org/10.4324/9780203871980

Thompson, J. B. (1995). *The media and modernity: A social theory of the media*. Polity Press.

Velavan, T. P., & Meyer, C. G. (2020). The COVID-19 epidemic. *Tropical Medicine & International Health*, *25*(3), 278–280. https://doi.org/10.1111/tmi.13383

World Health Organisation (WHO) (n.d.). WHO coronavirus disease (COVID-19) dashboard. https://covid19.who.int/

WHO. (2020). Key messages and actions for COVID-19 prevention and control in schools. https://www.who.int/docs/default-source/coronaviruse/key-messages-and-actions-for-covid-19-prevention-and-control-in-schools-march-2020.pdf?sfvrsn=baf81d52_4

Willems, W. (2020). Beyond platform-centrism and digital universalism: The relational affordances of mobile social media publics. *Information, Communication & Society*, *24*(12), 1–17. https://doi.org/10.1080/1369118X.2020.1718177

Williams, K. (2013). Moral panics, emotion and newspaper history. In S. Nicholas, & T. O'Malley (Eds.), *Moral panics, social fears, and the media: Historical perspectives* (pp. 28–45). Routledge.

Xu, X., & Pratt, S. (2018). Social media influencers as endorsers to promote travel destinations: An application of self-congruence theory to the Chinese Generation Y. *Journal of Travel & Tourism Marketing*, *35*(7), 958–972. https://doi.org/10.1080/10548408.2018.1468851

Appendix: Focus group and interview protocols

The questions below guided the facilitation of the focus group discussions and the individual interviews. The themes discussed emanated from these guiding questions which, in no specific order, were adapted to suit each session.

Guiding questions for the semi-structured focus group discussions

1. Can you please share with me when, where and how you first learnt about COVID-19?
2. Please share with me your thoughts about COVID-19, in terms of what you think it is. Are there other people you have discussed these thoughts with?
3. Where specifically (in terms of media) do you get news or updates about COVID-19 or other events happening around here in the country and who do you discuss these with? Is there a reason for these choices? If yes, please share the reasons.
4. Looking at the large population in this neighbourhood and in Lagos state alongside COVID-19's mode of transmission, what are your thoughts?
5. Some countries have implemented lockdown measures to slow down the spread of COVID-19. Please share your thoughts about this especially with regard to the news of a similar lockdown in Nigeria. In more specific terms, are you in support of a lockdown in Nigeria or not? Please share the reason(s) for your response.
6. What are your thoughts about the role of the Nigeria Centre for Disease Control (NCDC) and other government agencies responsible for combating pandemics such as COVID-19?

Guiding questions for the semi-structured individual interviews

1. You expressed your disbelief about COVID-19 during the focus group session. What are your thoughts now that there are more cases of COVID-19 and lockdown regulations are in place?
2. Can you please share more about your experience so far since the commencement of the lockdown regulations?
3. During the focus group session, reference was made to social media platforms as a means of getting updates and also sharing and discussing your thoughts about COVID-19 and other issues. Is this still the case? If yes, when was the last time you did this, what were the updates you got, and what were the thoughts you shared and discussed?
4. Looking back again to the conversation we had during the focus group session, do you have a different opinion from what you shared about the role of the NCDC and other relevant government agencies in the country?

User Perceptions of Mobile Banking Apps in Tanzania: Impact of Information Systems (IS) Factors and Customer Personality Traits

Daniel Ntabagi Koloseni
Lecturer, Faculty of Computing, Information Systems and Mathematics, Institute of Finance Management, Dar es Salaam
https://orcid.org/0000-0002-4104-2704

Abstract
This study probes the roles that information systems (IS) success factors and user personality traits play in Tanzanian users' perceptions of their experiences with mobile banking apps. Based on a survey of 249 mobile banking customers, the study finds that users are being positively influenced by the apps' *system quality* and *system service*, but not by the apps' *information quality*. The study also finds that, with respect to user personality traits, *openness*, *agreeableness*, *conscientiousness* and *extraversion* are all traits that have a positive impact on customers' use of, and satisfaction with, mobile banking apps. The findings suggest that developers of mobile banking apps for the Tanzanian market need to both improve the quality of the information in the apps and continue to target a range of personality traits.

Keywords
mobile banking apps, adoption, personality traits, information systems (IS), IS success model, Tanzania

DOI: https://doi.org/10.23962/10539/32214

Recommended citation
Koloseni, D. N. (2021). User perceptions of mobile banking apps in Tanzania: Impact of information systems (IS) factors and customer personality traits. *The African Journal of Information and Communication (AJIC), 28*, 1-26.
https://doi.org/10.23962/10539/32214

1. Introduction

Banks and financial institutions are investing heavily in the development of mobile applications (apps) to enhance their mobile banking service provision capacity. Mobile banking apps allow customers to use mobile devices (e.g., a smartphone or a tablet) to make money transfers within banks, across banks, and to/from mobile money platforms (e.g., M-Pesa and Tigo Pesa in Tanzania); to make in-app purchases; and to view balances and bank statements.

The mobile app provides a scalable platform for the provision of banking services and also serves as an advertisement platform through which banks can advertise their services and products. With mobile apps, banks can tailor their services based on the personal needs and/or locations of customers to retain them (Floh & Treiblmaier, 2006). Furthermore, mobile apps enable banks to reduce operational costs by changing the traditional service model to one of self-service, which also enhances customer engagement.

Mobile apps are mostly accessed via smartphones, and thus the proliferation of mobile apps has gone hand in hand with the exponential growth in smartphone usage. However, the use of mobile banking apps can be hampered by several factors, including security, privacy, reliability, information quality, e-services quality, and design issues such as response speed linked to sensor capabilities and small screens (Dukic et al., 2015; Fife & Orjuela, 2012; Gilbert et al., 2011; Godwin-Jones, 2011; Inukollu et al., 2014; Jain & Shanbhag, 2012; Zwass, 2003).

Furthermore, the use of mobile banking apps is affected by the personal characteristics of the user (Barnett et al., 2014; Bennett & Perrewé, 2002), as those personal characteristics interact with an app's system characteristics (Hong et al., 2002; Pituch & Lee, 2006; Ramayah et al., 2012). Because of the growing importance of user personal characteristics in the functioning of technologies, Bennett and Perrewé (2002) suggest incorporating personality traits into research frameworks to better understand technology adoption behaviour, specifically technology usage. There have been numerous studies of the adoption of mobile apps (see Alavi & Ahuja, 2016; Chmielarz & Łuczak, 2015; Hepola et al., 2016; Kumar et al., 2018; Manuel & Veríssimo, 2016; Muñoz-Leiva et al., 2017; Sampaio et al., 2017; Sangar & Rastari, 2015; Vedadi & Warkentin, 2016; Yang, 2013). However, these studies have not given significant attention to the potential roles played by personality traits in the use of mobile banking apps, creating a knowledge gap for banks and their app developers.

Accordingly, the purpose of this study was to investigate the roles played by information systems (IS) factors and customers' personality traits in influencing customers' perceptions of the use of mobile banking apps in Tanzania. The study's data, generated via a survey questionnaire completed by Tanzanian mobile banking users, was analysed using the DeLone and McLean (2003) IS success model and the five factor model (FFM) of personality (Digman, 1990).

2. Context: Use of mobile banking apps

The Tanzanian financial services industry is growing exponentially(Were et al., 2021), triggering an increased need for easy, reliable, timely, and trustworthy access to financial services. To cope with this need, banks in Tanzania are, among other approaches, deploying mobile banking apps. The goal of such apps is to imitate the functions that are carried out by web-based mobile banking applications and make them accessible in a mobile setting, in an interactive and personalised manner, on a smartphone or tablet. Furthermore, mobile banking apps are used to enhance service reachability, position brands in the highly competitive market, and encourage impulse-buying behaviour among consumers (Alavi & Ahuja, 2016). Mobile banking apps add a new set of tools for marketing in the digital age (Alavi & Ahuja, 2016). The owners of the apps (i.e., banks) can easily map consumers' preferences and easily plan how best to meet consumers' preferences through personalised services and suggestions.

Recently, the functionality of mobile payment apps in Tanzania was extended through the integration of quick response (QR) codes. This integration allows customers to scan merchants' QR codes and make payments in real-time (ClickPesa, 2019). It is now common for QR codes, along with other mobile payment channels, to be made available by merchants in major stores in Tanzania. Therefore, due to the benefits offered by mobile financial apps, it is no surprise that banks are heavily and rapidly investing in using mobile apps to deliver selected banking services.

Meanwhile, user adoption of mobile banking apps is rapidly increasing. Several factors have been found to contribute to the adoption of such apps. For instance, Hepola et al. (2016) and Sampaio et al. (2017) find that cognitive processing, activation, perceived risks, and affection have a positive influence on the adoption of mobile banking apps, while Muñoz-Leiva et al. (2017) find that attitude is a strong predictor of intention to use mobile banking apps. Satisfaction and perceived usefulness (performance expectancy) have also featured in several studies as key predictors of the adoption of mobile banking apps, such as the studies by Vedadi and Warkentin (2016), Kumar et al. (2018) and Ahuja and Alavi (2016). Other factors found to influence the adoption of mobile banking apps are intrinsic regulation, identified regulation, external regulation and integrated regulation, perceived ease of use, perceived risk and cost, and need for information (Ahuja & Alavi, 2016; Kumar et al., 2018). Prominent theories used in previous studies investigating the adoption of mobile banking apps include the technology acceptance model (TAM) (Muñoz-Leiva et al., 2017), the expectation–confirmation theory (ECT) (Vedadi & Warkentin, 2016), the self-determination theory (Kumar et al., 2018), and service-dominant logic (Hepola et al., 2016).

3. Hypothesis development and research framework

IS success model

For measuring users' perceptions of the success or effectiveness of an information system, the DeLone and McLean (2003) IS success model is one of the dominant models. However, as seen in the previous section of this article, the IS success model is not prominent in published studies of the adoption of mobile banking apps. The model focuses on how three quality measures—*system quality*, *service quality*, and *information quality*—interact with system *use* (or *intention to use*) and *user satisfaction* in ways that, if the influences are positive, will generate *net benefits* for the user (DeLone & McLean, 2003).

Previous studies, such as those by Barnett et al. (2014), Camadan et al. (2018), Devaraj et al. (2008), Krishnan et al. (2010), McElroy et al. (2007), Panda and Jain (2018) and Svendsen et al. (2013), have already examined the influence of personal characteristics on technology use in various contexts. However, studies of the influence of personality elements on technology adoption through the lens of the DeLone and McLean (2003) information systems (IS) success model are limited, thus presenting another knowledge gap that this study seeks to address.

Relationships between the IS success model's three quality measures and *use* have been empirically validated in previous studies. For example, Mohammadi (2015) finds that all three quality measures influence the use of e-learning; and Rana et al. (2015) find that the three quality measures influence the use of online public grievance redress systems. Accordingly, for this study, it was expected that each of the three quality measures would influence the use of the mobile banking app. Hence, the following hypotheses were tested:

> **H1**: System quality has a positive influence on the use of mobile banking apps.
> **H2**: Service quality has a positive influence on the use of mobile banking apps.
> **H3**: Information quality has a positive influence on the use of mobile banking apps.

Relationships between the IS success model's three quality measures and *user satisfaction* are also well-documented in previous studies, including the aforementioned

Mohammadi (2015) and Rana et al. (2015) studies, and in the work of Freeze et al. (2019) and Gao and Park (2017). In connection with the above findings, the following hypotheses emerged:

> **H4**: System quality has a positive influence on user satisfaction with mobile banking apps.
> **H5**: Service quality has a positive influence on user satisfaction with mobile banking apps.
> **H6**: Information quality has a positive influence on user satisfaction with mobile banking apps.

Furthermore, the consequent effects of both actual use and user satisfaction could ultimately impact user individual performance based on the net benefits of using mobile banking apps. The user could continue using the mobile banking app if the net benefits are positive or, in other words, if the mobile banking app continues to help the customer or user to achieve individual performance.

User satisfaction is defined as a sum of feelings or an affective response regarding the effectiveness of a particular technology to accomplish a given task (Gatian, 1994; Melone, 1990). In the context of this study, user satisfaction is achieved if the user feels that the mobile banking apps have effectively helped him or her to accomplish banking-related tasks. The relationship between user satisfaction and individual performance is also demonstrated in previous studies such as those of Gelderman (1998) and Isaac et al. (2017). The influence of a user's actual use of information systems on individual performance is reported in studies such as Tam and Oliveira (2016). Furthermore, literature strikes a close relationship between perceived user satisfaction and actual use of information systems or ICT in general. It has been demonstrated that as the perceived satisfaction of using information systems increases, the desire to use mobile banking apps could also shoot up. Examples of empirical findings demonstrating this relationship include those generated by AL Athmay et al. (2016) and Byun and Finnie (2011). Based on the findings of previous studies, the following hypotheses were developed:

> **H7**: User satisfaction with mobile banking apps has a positive influence on individual performance.
> **H8**: Use of the mobile banking apps has a positive influence on individual performance.
> **H9**: User satisfaction with mobile banking apps has a positive influence on the use of the apps.

The five-factor model

Personality characteristics refer to cognitive behaviour patterns in facets of general tendencies that govern an individual's thoughts, feelings, and actions (Krishnan et al., 2010; Maddi, 1996). These personality traits play an important role in IS adoption as they affect how information systems are used (Halko & Kientz, 2010; Rosen & Kluemper, 2008). There are many personal characteristics in the psychology literature, however, the current study investigates the direct effects of the "big five" personality traits on the use of mobile banking apps. These five traits are: *conscientiousness*, *openness*, *extraversion*, *neuroticism*, and *agreeableness* (taken from Digman, 1990). Previous studies suggest that the five-factor model (FFM) is effective in explorations of the effects of personal characteristics, with a good predictive ability (Chang et al., 2012). The influence of the big five personality traits has been rarely studied in the mobile banking apps context, despite their potential importance in understanding differences in user behaviour.

Conscientiousness encompasses an individual's predisposition to be cautious, organised, hardworking, abiding by rules, and reliable. Thus, conscientious individuals organise themselves to perform tasks with a high level of discipline, and do so cautiously and reliably. Since this group of individuals is self-disciplined, cautious and reliable, they are likely to use mobile banking apps productively to perform banking-related tasks. The empirical finding also indicates that conscientiousness influences the productive use of internet resources (Landers & Lounsbury, 2006) and IT system usage (Barnett et al., 2014). Therefore, the resulting hypothesis was:

> **H10**: Conscientiousness has a positive influence on the use of mobile banking apps.

Openness includes an individual's inquisitiveness, willingness to experiment, and inclination to engage and to explore new ideas and the surrounding world (McCrae, 1993; McCrae & Terracciano, 2005). These individuals are likely to try new technology in pursuit of a better way to accomplish the tasks at hand. Similarly, it is expected that open-minded individuals are likely to use mobile banking apps in an attempt to explore the bank-related functions and services offered through mobile banking apps. The association between an individual's openness and eagerness to use technology is reported in various IS studies such as Tuten and Bosnjak (2001) and Kim and Jeong (2015). Hence, consistent with such previous studies, it was hypothesised that:

> **H11**: Openness has a positive influence on the use of mobile banking apps.

Extraversion refers to individuals who are social, affectionate, cheerful, and optimistic. They easily get themselves involved in seeking affiliation in the social environment in a quest to achieve a particular goal. Hence, they are more likely to use technology that will help them to achieve goals (Shambare, 2013). For this reason, extroverts are likely to use mobile banking apps to achieve socially related goals. The connection between extraversion and technology use is well reported in the works of Loiacono (2015) and Leonidas et al. (2019). Therefore, it was hypothesised that:

> **H12**: Extraversion has a positive influence on the use of mobile banking apps.

Neuroticism reflects emotional instability, negativity, sadness, and difficulty with dealing with all sorts of stress. Since neurotic individuals are inclined to negative perceptions and emotional instability, they tend to perceive technology as stressful and difficult to use, and as a result they tend to avoid and oppose using it (Rosen & Kluemper, 2008). Similar findings which support the relationship between neuroticism and information systems usage include those of Loiacono (2015) and Barnett et al. (2014). Hence, it was hypothesised that:

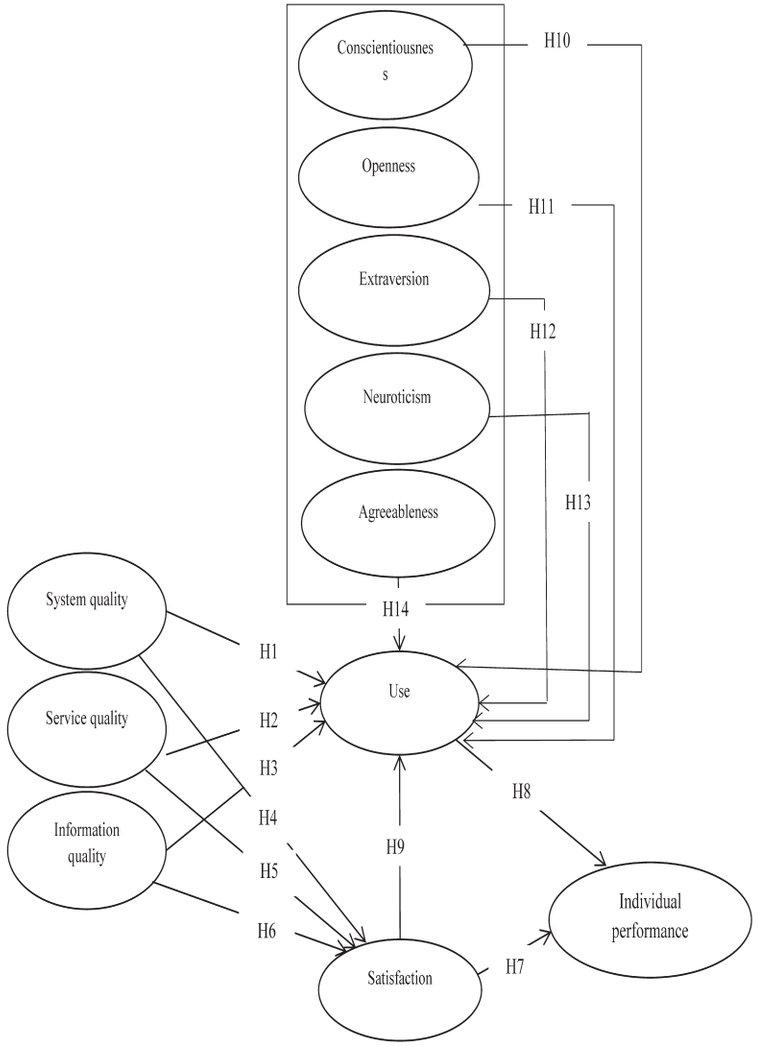
> **H13**: Neuroticism has a negative influence on the use of mobile banking apps.

Agreeableness embodies the tendency of individuals to be compassionate, tolerant, good-natured, forgiving, and cooperative. IS literature indicates that agreeableness is positively linked to technology use. It has been found that agreeable individuals patiently use technology that is slightly difficult to use, such as a website that is onerous to navigate (Landers & Lounsbury, 2006). Loiacono (2015) reports that agreeable people are more likely to use the internet and social networking sites. Accordingly, it was hypothesised that:

> **H14**: Agreeableness has a positive influence on the use of mobile banking apps.

The research framework for the study, based on the 14 hypotheses, is illustrated in Figure 1.

Figure 1: Research framework



4. Methodology

Instrument development

The data collection questionnaire had two parts. The first part consisted of items for measuring respondent perceptions of the use of mobile banking apps, and the second part consisted of items aimed at gathering demographic information. Items on the perceptions of respondents (see Appendix) were borrowed from previous studies and adjusted to match the setting of this study. Items for measuring user perceptions of system quality, service quality, information quality and use were based on those used by Urbach et al. (2010); items for measuring a user's performance were based on those used by Goodhue and Thompson (1995); items for measuring user satisfaction were based on those used by Bhattacherjee (2001), and items for measuring conscientiousness, openness, agreeableness, extraversion, and neuroticism were based on those used by Donnellan et al. (2006) and Goldberg (1999).

All the items for measuring respondent perceptions consisted of statements (see Appendix), each of which respondents rated via a five-point Likert scale ranging from 1 (strongly disagree) to 5 (strongly agree). Prior to its use with respondents, the questionnaire was sent to five information system experts and five experienced banking services personnel to check content validity. The comments provided by these individuals informed the finalisation of the questionnaire.

Study sample, data collection

The study sample consisted of Tanzanian users of mobile banking apps from five regions: Dar es Salaam, Arusha, Mwanza, Dodoma, and Kilimanjaro. These regions host the majority of the country's bank branches. A judgmental sampling method was employed during the selection of respondents. Respondents were selected based on two criteria: (1) experience of using mobile banking apps for six months or more; and (2) habit of using mobile banking apps at least once per week.

The population of respondents who met the selection criteria for this study is large and unknown. In this situation, it is recommended that the Cochran formula for the unknown population be applied to determine the appropriate sample size for the study (Cochran, 1977). Using the Cochran formula, $n_0 = Z^2 p(1-p)/e^2$ $n_0 = Z^2 p(1-p)/e^2$ (where Z is the confidence level, p = expected proportion, and e = margin error), the sample size of the study was 384 respondents. This study set Z = 1.96 at 95% confidence level, margin error in a proportion of one, if 5%, e = 0.05 and expected proportion in a proportion of one, p = 0.5.

The questionnaire was self-administered to the targeted respondents. Out of 384 questionnaires, 249 questionnaires were completed. Before data analysis, the collected questionnaires were checked for missing data using the missing completely at random (MCAR) test (Little, 1988). The test result was not significant ($x^2 = 178.733$, $df = 160$, $p = 0.148$), indicating that there were randomly missing data. Missing data were replaced by estimating maximum likelihood using the expectation-maximisation (EM) approach.

5. Results

Descriptive findings

Table 1 provides demographic information—gender, age, years of experience using mobile banking apps, and frequency per week of use of the apps—for the 249 respondents.

Table 1: Respondent demographics ($N = 249$)

Variable	Category	Frequency	Percentage
Gender	Male	172	69.1
	Female	77	30.9
Age	18–25	72	28.9
	26–45	116	46.5
	46 or older	61	24.5
Years of experience using mobile banking apps	less than 1 year	62	24.9
	1–3 years	68	27.3
	more than 3 years	119	47.8
Frequency per week of use of mobile banking apps	1–3 times	37	14.9
	4–6 times	72	28.9
	7–9 times	64	25.7
	more than 10 times	76	30.5

Assessment of the measurement and structural models

The study used covariance-based structural equation modelling (CB-SEM) to assess both the measurement model and the structural model. The study followed a two-stage approach, as recommended by Anderson and Gerbing (1988): (1) assessment of the measurement model; and (2) assessment of the structural model.

Assessment of the measurement model

To assess the measurement model, the study used model fit indices from each category of model fit indices as defined by Hair et al. (2010). Specifically, the study used Root Mean Square of Error Approximation (RAMSEA) and Goodness of Fit Index (GFI) from the absolute fit category, Comparative Fit Index (CFI) and Tucker-Lewis index (TLI) from the incremental fit category, and x^2/df (Chi-square/df) from the parsimonious fit category. In the first stage, the study found that the measurement model demonstrated adequate psychometric properties after dropping INFOQ3 and INFOQ5 from information quality and EXT2 from extraversion constructs due to low factor loadings. The results of the goodness of fit for the entire model and acceptable thresholds are reported in Table 2.

Table 2: Measures of goodness of fit

Model fit Index	Values in this study	Recommended threshold values	Source
x^2/df	2.275	≤ 3.0	Bentler and Bonett (1980)
GFI	0.871	≥ 0.90	Joreskog and Sorbom (1984)
RAMSEA	0.081	≤ 0.08	Hair et al. (2010)
CFI	0.942	≥ 0.90	Byrne (2009)
TLI	0.978	≥ 0.90	Byrne (2009)

Convergent and discriminant validity was used to assess the measurement model and composite reliability (CR) was used to assess reliability. Table 3 indicates the results of convergent validity and reliability assessment. The results of convergent validity indicate that the average variance extracted (AVE) values for the constructs are great than 0.5, implying that the measurement items for each construct are theoretically related to each other (Fornell & Larcker, 1981) and the values for composite reliability are all above 0.7, implying that the measurement items have met the reliability threshold (Nunnally & Bernstein, 1994).

Table 3: Convergent validity and reliability assessment

Construct	AVE	CR
Use	0.652	0.878
Service quality	0.703	0.904
Conscientiousness	0.647	0.793
Agreeableness	0.562	0.771
System quality	0.649	0.902
Extraversion	0.519	0.801
Neuroticism	0.685	0.771
Openness	0.891	0.824
Information quality	0.788	0.907
Satisfaction	0.845	0.956
Individual performance	0.811	0.928

Concerning discriminant validity, the results confirm that the constructs of the study were distinct from each other since the intercorrelations of the constructs did not exceed the square root of the AVE of the constructs. Results of discriminant validity are reported in Table 4.

Table 4: Discriminant validity assessment

	USE	SEQ	CONS	AGR	SYQ	EXT	NEU	OPN	INFQ	SAT	PER
USE	**0.807**										
SEQ	0.661	**0.838**									
CONS	0.688	0.721	**0.804**								
AGR	0.566	0.458	0.686	**0.750**							
SYQ	0.791	0.774	0.705	0.676	**0.806**						
EXT	0.638	0.658	0.715	0.702	0.714	**0.720**					
NEU	0.265	0.104	0.418	0.427	0.271	0.382	**0.828**				
OPN	0.838	0.862	0.910	0.924	0.917	0.916	0.456	**0.943**			
INFQ	0.860	0.714	0.711	0.657	0.766	0.769	0.217	0.741	**0.887**		
SAT	0.850	0.694	0.772	0.599	0.866	0.791	0.215	0.826	0.842	**0.919**	
PER	0.856	0.749	0.807	0.591	0.851	0.733	0.280	0.825	0.896	0.861	**0.901**

Legend

USE: Use *SEQ: Service Quality* *CONS: Conscientiousness* *AGR: Agreeableness*
SYQ: System Quality *EXT: Extraversion* *NEU: Neuroticism* *OPN: Openness*
INFQ: Information Quality *SAT: Satisfaction* *PER: Performance*

***Note**: Bolded diagonal values are the square root of AVE, and correlational values are significant at $p < 0.001$.*

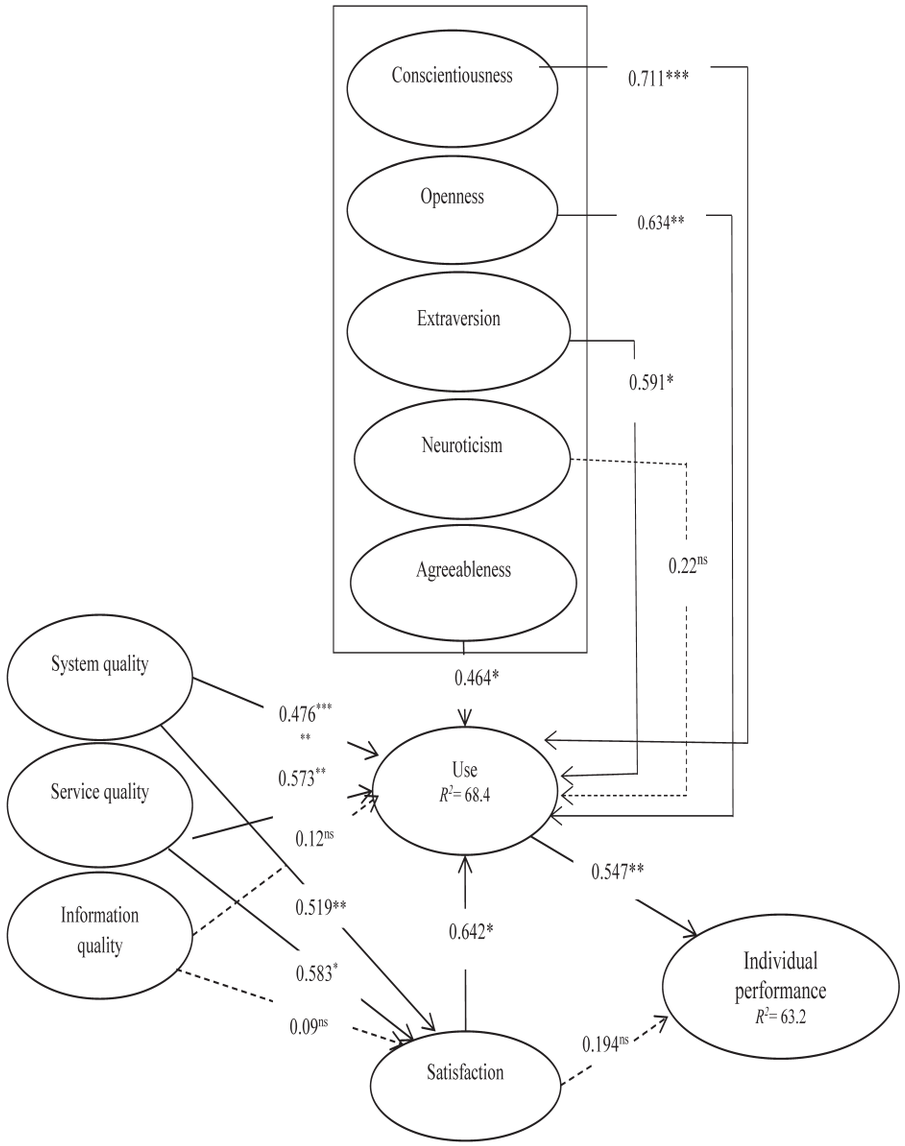
Assessment of the structural model, and hypothesis testing

In the second stage, the study assessed the structural model using the same model fit indices used in the assessment of the measurement model. The assessment of the structural model yielded the following goodness of fit: $x^2/df = 2.267$, RAMSEA = 0.083, GFI = 0.870, CFI = 0.940, and TLI = 0.976. The model fit indices indicate that there is an adequate structural fit between the hypothesised model and the observed data. The explained variance (R^2) in use is 63.2% and in individual performance is 68.4%, suggesting that the model has good explanatory power as compared to similar studies and is good enough to produce substantial effects (Cohen, 1988). Results of hypothesis testing and the resulting path diagram are provided in Table 5 and Figure 2, respectively.

Table 5: Results of hypothesis testing

Hypothesis	Relationship			t- values	β-values	Result
H1	SYQ	→	USE	1.981	0.476	Supported
H2	SEQ	→	USE	2.191	0.573	Supported
H3	INFQ	→	USE	0.743	0.12	Not supported
H4	SYQ	→	SAT	2.133	0.519	Supported
H5	SEQ	→	SAT	2.217	0.583	Supported
H6	INFQ	→	SAT	0.409	0.09	Not supported
H7	SAT	→	PER	0.916	0.194	Not supported
H8	USE	→	PER	2.052	0.547	Supported
H9	SAT	→	USE	3.257	0.642	Supported
H10	CONS	→	USE	4.078	0.711	Supported
H11	OPN	→	USE	3.211	0.634	Supported
H12	EXT	→	USE	2.571	0.591	Supported
H13	NEU	→	USE	1.221	0.221	Not supported
H14	AGR	→	USE	1.971	0.464	Supported

Figure 2: Path diagram



***Note**: * p ≤ 0.05, ** p ≤ 0.01, *** p ≤ 0.001, ns: Not significant*

6. Discussion

Unsupported hypotheses

Four of the 10 hypotheses were *not* supported by the findings:

- H3: Information quality positively influences the use of mobile banking apps.
- H6: Information quality positively influences user satisfaction with mobile banking apps.
- H7: User satisfaction with mobile banking apps has a positive influence on individual performance.
- H13: Neuroticism has a negative influence on the use of mobile banking apps.

Information quality and use (H3), information quality and user satisfaction (H6)

One of the three DeLone and McLean (2003) quality measures—*information quality*—was found to not have a positive influence on either *use* or *user satisfaction* with the use of mobile banking apps. (Under *information quality*, the survey (see Appendix) probed the extent to which users found the information in the apps *useful, understandable*, *interesting*, *reliable*, *complete*, and *up to date*). This finding, which suggests that the surveyed users perceived the quality of the information provided by the mobile banking apps as being unsatisfactory and thus a disincentive to using the apps, appears to resonate with the findings of Chiu et al. (2016) on the adoption of mobile banking services in Philippines. Also, the study by Franque et al. (2021) in Mozambique finds that information quality had a positive influence on the *use* of mobile banking services, and the study by Kumar and Sharma (2019) in Oman finds that information quality had a positive influence on *user satisfaction* with such services.

User satisfaction and individual performance (H7)

Contrary to the study's expectations and the literature, user satisfaction was not found to positively influence *individual performance*—though it does, as seen later in this section, positively influence the *use* of mobile banking apps.

Neuroticism and use (H13)

Neuroticism was found to have no significant influence on the respondents' use of mobile banking apps. This finding appears to contrast with findings from several other studies. For example, studies by Loiacono (2015) in Italy and Ashraf (2019) in Lebanon find that neuroticism had a significant influence on, respectively, the intention to use social networking websites and the intention to use mobile banking. An earlier study, by Rosen and Kluemper (2008) in the US, finds that neurotics often perceive new technology negatively.

Supported hypotheses

Ten of the hypotheses—all except the four hypotheses discussed in the previous sub-section—were supported by the research findings.

Openness

The study found that openness has a positive influence on the use of Tanzanian mobile banking apps. It is plausible that mobile banking users consider the use of the apps to be a new experience and therefore they are attracted to using them. This finding would appear to be consistent with findings in studies by Kim and Jeong (2015) in South Korea and by McElroy et al. (2007) in the US, which find openness to be positively related to internet use, but the finding appears to contrast with the Barnett et al. (2014) finding that openness is unrelated to technology acceptance.

Conscientiousness

Similar to findings by Moslehpour et al. (2018) on the intention of Taiwanese to purchase goods and services online, this study found that conscientiousness positively influences Tanzanians' use of mobile banking apps. It is possible that this finding stems from a belief that using mobile banking apps can improve financial management discipline and offer greater reliability in making business transactions.

Extraversion

Extraversion was also found to have a positive influence on the use of mobile banking apps, a finding that appears to be consistent with findings from several previous studies, such as the Panda and Jain (2018) study of the obsessive use of smartphones among young Indians, and the Lissitsa and Kol (2021) study of mobile shopping among members of the so-called "generation Y" (i.e., people reaching adulthood at the turn of the millennium) in Israel. Devaraj et al. (2008) find that because extraverts are socially inclined, outgoing, and like to create connections, they are amenable to the use of advanced technology to achieve socially oriented goals.

Agreeableness

The core of agreeableness behaviour is maintaining a positive relationship with others (Graziano & Eisenberg, 1997). Given the importance of one's relationship with one's bank, the respondents could reasonably be expected to choose to use the mobile banking apps, upon being introduced to them by their respective banks, to maintain their relationship with their banks. This finding appears to be consistent with that of Khan et al. (2019) on the use of mobile payment systems in China.

System quality and use, service quality and use

Two of the three DeLone and McLean (2003) IS quality measures—*system quality* and *service quality*—were found to positively influence the *use* of mobile banking

apps. These findings appear to be in line with previous studies in technology acceptance literature. For example, Mohammadi (2015) finds that these two factors influenced the use of e-learning in Iran.

System quality and user satisfaction, service quality and user satisfaction

Two of the three DeLone and McLean (2003) IS quality measures—*system quality* and *service quality*—were also found to positively influence *user satisfaction* with the use of mobile banking apps. This finding apparently aligns with that of Veeramootoo et al. (2018) on the use of e-government services in Mauritius.

User satisfaction and use

Unsurprisingly, user satisfaction was found to positively influence use, a finding that appears to be consistent with the findings of Shim and Jo (2020), who investigated the use of health informatics sites in South Korea.

Limitations and further studies

This study was conducted with respondents living in a single country, Tanzania. Future studies would benefit from involving respondents from more than one country, so as to account for the effects of national and cultural differences on the final results. Also, some of the studied constructs, particularly those used to measure personality traits, may have been perceived by some respondents as carrying a negative meaning. Hence, their responses could have been influenced by notions of social acceptability. Future studies could supplement questionnaire data with an additional data source in using a combination of data collection methods to overcome the potential common methods biases.

7. Conclusions

The study offers a research framework which combines the consideration of personality traits and IS success factors in influencing Tanzanians' *use* of, and *satisfaction* with, mobile banking apps. This model enhances our understanding of the influence of personality traits on the acceptance of mobile banking apps. Studies which have studied these traits in the context of the IS success model, particularly in the African context, are limited. This study's identification of strong positive relationships between four personality traits—*openness*, *agreeableness*, *conscientiousness*, and *extraversion*—and both use and user satisfaction suggests that banks can benefit from ensuring that users can give full expression to their personalities when using the apps. If developers can design mobile banking apps which allow each customer to have a sense of expressing their unique personality traits, the customer's use and user satisfaction can be expected to increase.

Also of potential value to developers is the finding that one of the three IS success factors—*information quality*—is not at present positively influencing Tanzanian mobile banking users. This is an apparent indication that developers of mobile banking

apps for the Tanzanian market need to place greater emphasis on ensuring that the information provided is, according to the terms used in the survey, *useful*, *understandable*, *interesting*, *reliable*, *complete*, and *up to date*.

References

AL Athmay, A. A. A., Fantazy, K., & Kumar, V. (2016). E-government adoption and user's satisfaction: An empirical investigation. *EuroMed Journal of Business*, *11*(1), 57–83. https://doi.org/10.1108/EMJB-05-2014-0016

Alavi, S., & Ahuja, V. (2016). An empirical segmentation of users of mobile banking apps. *Journal of Internet Commerce*, *15*(4), 390–407. https://doi.org/10.1080/15332861.2016.1252653

Anderson, J. C., & Gerbing, D. W. (1988). Structural equation modelling in practice: A review and recommended two-step approach. *Psychological Bulletin*, *103*(3), 411–423. https://doi.org/10.1037/0033-2909.103.3.411

Ashraf, H. (2019). *Factors that Influence the use of Mobile Banking in Lebanon: Integration of UTAUT2 and 3M Model*. Universidade de Santiago de Compostela.

Barnett, T., Allison, W., Pearson, R., & Kellermanns, F. W. (2014). Five-factor model personality traits as predictors of perceived and actual usage of technology. *European Journal of Information Systems*, *24*(4), 374–390. https://doi.org/10.1057/ejis.2014.10

Bennett, J., & Perrewé, P. L. (2002). An empirical examination of individual traits as antecedents to computer anxiety and computer self-efficacy. *MIS Quarterly*, *26*(4), 381–396. https://doi.org/10.2307/4132314

Bentler, P. M., & Bonett, D. G. (1980). Significance tests and goodness of fit in the analysis of covariance structures. *Psychological Bulletin*, *88*(3), 588–606. https://doi.org/10.1037/0033-2909.88.3.588

Bhattacherjee, A. (2001). Understanding information systems continuance: An expectation-confirmation model. *MIS Quarterly*, *25*(3), 351–370. https://doi.org/10.2307/3250921

Bond, M. H. (1983). Linking person perception dimensions to behavioral intention dimensions: The Chinese connection. *Journal of Cross-Cultural Psychology*, *14*(1), 41–63. https://doi.org/10.1177/0022002183014001004

Bond, M. H., & Forgas, J. P. (1984). Linking person perception to behavior intention across cultures: The role of cultural collectivism. *Journal of Cross-Cultural Psychology*, *15*(3), 337–352. https://doi.org/10.1177/0022002184015003006

Byrne, B. M. (2009). *Structural equation modeling with AMOS: Basic concepts, applications, and programming* (2nd ed.). Routledge.

Byun, D. H., & Finnie, G. (2011). Evaluating usability, user satisfaction and intention to revisit for successful e-government websites. *Electronic Government*, *8*(1), 1–19. https://doi.org/10.1504/EG.2011.037694

Camadan, F., Reisoglu, I., Faruk, U. Ö., & Mcilroy, D. (2018). How teachers[’] personality affect on their behavioral intention to use tablet PC. *The International Journal of Information and Learning Technology Article Information*, *35*(1), 12–28. https://doi.org/10.1108/IJILT-06-2017-0055

Chang, L., Connelly, B. S., & Geeza, A. A. (2012). Separating method factors and higher order traits of the big five: A meta-analytic multitrait-multimethod approach. *Journal of Personality and Social Psychology*, *102*(2), 408–427. https://doi.org/10.1037/a0025559

Chiu, P. S., Chao, I. C., Kao, C. C., Pu, Y. H., & Huang, Y. M. (2016). Implementation and evaluation of mobile e-books in a cloud bookcase using the information system success model. *Library Hi Tech*, *34*(2), 207–223. https://doi.org/10.1108/LHT-12-2015-0113

Chmielarz, W., & Łuczak, K. (2015). Mobile banking in the opinion of users of banking applications in Poland. *Applied Mechanics and Materials*, *795*, 31–38. https://doi.org/10.4028/www.scientific.net/AMM.795.31

Clickpesa. (2019). An overview of Consumer Financial Apps in Tanzania. https://clickpesa.com/financial-apps-tanzania/

Cochran, W. (1977). *Sampling techniques* (3rd ed.). John Wiley & Sons.

Cohen, J. (1988). *Statistical power analysis for the behavioral sciences* (2nd ed.). Hillsdale.

DeLone, W. H., & McLean, E. R. (2003). The DeLone and McLean model of information systems success: A ten-year update. *Journal of Management Information Systems*, *19*(4), 9–30. https://doi.org/10.1080/07421222.2003.11045748

Devaraj, S., Easley, R. F., & Crant, J. M. (2008). How does personality matter? Relating the five-factor model to technology acceptance and use. *Information Systems Research*, *19*(1), 93–105. https://doi.org/10.1287/isre.1070.0153

Digman, J. M. (1990). Personality structure: Emergence of the five-factor model. *Annual Review of Psychology*, *41*(1), 417–440. https://doi.org/10.1146/annurev.ps.41.020190.002221

Donnellan, M. B., Oswald, F. L., Baird, B. M., & Lucas, R. E. (2006). The mini-IPIP scales: Tiny-yet-effective measures of the big five factors of personality. *Psychological Assessment*, *18*(2), 192–203. https://doi.org/10.1037/1040-3590.18.2.192

Dudley, N. M., Orvis, K. A., Lebiecki, J. E., & Cortina, J. M. (2006). A meta-analytic investigation of conscientiousness in the prediction of job performance: Examining the intercorrelations and the incremental validity of narrow traits. *Journal of Applied Psychology*, *91*(1), 40–57. https://doi.org/10.1037/0021-9010.91.1.40

Dukic, Z., Chiu, D., & Lo, P. (2015). How useful are smartphones for learning? Perceptions and practices of Library and Information Science students from Hong Kong and Japan. *Library Hi Tech*, *33*(4), 545–561. https://doi.org/10.1108/LHT-02-2015-0015

Fife, E., & Orjuela, J. (2012). The privacy calculus: Mobile apps and user perceptions of privacy and security regular paper. *International Journal of Engineering Business*, *4*(11), 1–10. https://doi.org/10.5772/51645

Floh, A., & Treiblmaier, H. (2006). What keeps the e-banking customer loyal? A multigroup analysis of the moderating role of consumer characteristics on e-loyalty in the financial service industry. *Journal of Electronic Commerce Research*, *7*(2), 97–110. https://doi.org/10.2139/ssrn.2585491

Fornell, C., & Larcker, D. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, *18*(1), 39–50. https://doi.org/10.1177/002224378101800104

Franque, F. B., Oliveira, T., & Tam, C. (2021). Understanding the factors of mobile payment continuance intention: empirical test in an African context. *Heliyon*, *7*(8), 1–12.

Freeze, R. D., Lane, P. L., & Wen, H. J. (2019). IS success model in e-learning context based on students' perceptions. *Journal of Information Systems Education*, *21*(2), 173–185.

Gaardboe, R., Nyvang, T., & Sandalgaard, N. (2017). Business intelligence success applied to healthcare information systems. *Procedia Computer Science*, *121*, 483–490. https://doi.org/10.1016/j.procs.2017.11.065

Gao, L., & Park, A. T. (2017). Understanding sustained participation in virtual travel communities from the perspectives of IS success model and flow theory. *Journal of Hospitality and Tourism Research*, *41*(4), 475–509. https://doi.org/10.1177/1096348014563397

Gatian, A. W. (1994). Is user satisfaction a valid measure of system effectiveness? *Information & Management*, *26*(3), 119–131. https://doi.org/10.1016/0378-7206(94)90036-1

Gelderman, M. (1998). The relation between user satisfaction, usage of information systems and performance. *Information & Management*, *34*(1), 11–18. https://doi.org/10.1016/S0378-7206(98)00044-5

Gilbert, P., Cox, L. P., Chun, B.-G., & Jung, J. (2011). Vision: Automated security validation of mobile apps at app markets. In *Proceedings of the Second International Workshop on Mobile Cloud Computing and Services* (pp. 21–26). https://doi.org/10.1145/1999732.1999740

Godwin-Jones, R. (2011). Emerging technologies mobile apps for language learning. *Language Learning & Technology*, *15*(2), 2–11.

Goldberg, L. (1999). A broad-bandwidth, public-domain, personality inventory measuring the lower-level facets of several five-factor models. In I. Mervielde, I. Deary, F. De Fruyt, & F. Ostendorf (Eds.), *Personality psychology in Europe* (Vol. 7) (pp. 7-28). Tilburg University Press.

Goodhue, D. L., & Thompson, R. L. (1995). Task-technology fit and individual. *MIS Quarterly*, *19*(2), 213–236. https://doi.org/10.2307/249689

Graziano, W. G., & Eisenberg, N. (1997). Agreeableness: A dimension of personality. In R. Hogan, J. Johnson, & S. Briggs (Eds.), *Handbook of personality psychology* (pp. 795–824). Elsevier. https://doi.org/10.1016/B978-012134645-4/50031-7

GSMA. (2021). *The mobile economy 2021*. https://www.gsma.com/mobileeconomy/wp-content/uploads/2021/07/GSMA_MobileEconomy2021_3.pdf

Hair, J., Black, W. C., Babin, B. J., & Anderson, R. E. (2010). *Multivariate data analysis: A global perspective* (7th ed.). Prentice-Hall.

Halko, S., & Kientz, J. A. (2010). Personality and persuasive technology: An exploratory study on health-promoting mobile applications. In T. Ploug, P. Hasle, & H. Oinas-Kukkonen (Eds.), *Persuasive technology: 5th International Conference, PERSUASIVE 2010, Copenhagen, Denmark, June 7-10, 2010: Proceedings* (pp. 150–161). https://doi.org/10.1007/978-3-642-13226-1_16

Hepola, J., Karjaluoto, H., & Shaikh, A. A. (2016). Consumer engagement and behavioral intention toward continuous use of innovative mobile banking applications—A case study of Finland. In *Thirty Seventh International Conference on Information Systems, Dublin* (pp. 1–20).

Hong, W., Thong, J. Y. L., & Wai-Man Wong, K.-Y. T. (2002). Determinants of user acceptance of digital libraries: An empirical examination of individual differences and system characteristics. *Journal of Management Information Systems*, *18*(3), 97–124. https://doi.org/10.1080/07421222.2002.11045692

Hu, P.-H. (2003). Evaluating telemedicine systems success: A revised model. In *36th Annual Hawaii International Conference on System Sciences, 2003.* https://doi.org/10.1109/HICSS.2003.1174379

Inukollu, V. N., Keshamoni, D. D., Kang, T., & Inukollu, M. (2014). Factors influencing quality of mobile apps: Role of mobile app development life cycle. *International Journal of Software Engineering & Applications (IJSEA)*, *5*(5), 15–34. https://doi.org/10.5121/ijsea.2014.5502

Isaac, O., Abdullah, Z., Ramayah, T., & Mutahar, A. M. (2017). Internet usage, user satisfaction, task-technology fit, and performance impact among public sector employees in Yemen. *The International Journal of Information and Learning Technology*, *34*(3), 210–241. https://doi.org/10.1108/IJILT-11-2016-0051

Jain, A. K., & Shanbhag, D. (2012). Addressing security and privacy risks in mobile applications. *IT Professional*, *14*(5), 28–33. https://doi.org/10.1109/MITP.2012.72

Joreskog, K., & Sorbom, D. (1984). *LISREL VI user's guide* (3rd ed.). Scientific Software.

Keyes, D. (2019, July 2). WhatsApp Pay is on the verge of launching in India. *Business Insider*. https://www.businessinsider.com/whatsapp-pay-ready-for-india-launch-2019-7?IR=T

Khan, A. N., Xiongfei, C. & Pitafi, H. (2019). Personality traits as predictor of m-payment systems: A SEM-neural networks approach. *Journal of Organizational and End User Computing*, *31*(4), 89–110. https://doi.org/10.4018/JOEUC.2019100105

Kim, M., Chang, Y., Park, M., & Lee, J. (2015). The effects of quality on the satisfaction and the loyalty of smartphone users. *Telematics and Informatics*, *32*(4), 949–960. https://doi.org/10.1016/j.tele.2015.05.003

Kim, Y., & Jeong, J. S. (2015). Personality predictors for the use of multiple internet functions. *Internet Research*, *25*(3), 399–415. https://doi.org/10.1108/IntR-11-2013-0250

Krishnan, S., Lim, V. K. G., & Tao, T. S. H. (2010). How does personality matter? Investigating the impact of big-five personality traits on cyberloafing. In *International Conference on Information Systems* (pp. 1–16). https://scholarbank.nus.edu.sg/handle/10635/44246

Kumar, R. R., Israel, D., & Malik, G. (2018). Explaining customer's continuance intention to use mobile banking apps with an integrative perspective of ECT and self-determination theory. *Pacific Asia Journal of the Association for Information Systems*, *10*(2). https://doi.org/10.17705/1pais.10204

Kumar, S., & Sharma, M. (2019). Examining the role of trust and quality dimensions in the actual usage of mobile banking services : An empirical investigation. *International Journal of Information Management*, *44*, 65–75. https://doi.org/10.1016/j.ijinfomgt.2018.09.013

Landers, R. N., & Lounsbury, J. W. (2006). An investigation of big five and narrow personality traits in relation to internet usage. *Computers in Human Behavior*, *22*(2), 283–293. https://doi.org/10.1016/j.chb.2004.06.001

Leonidas, H., Misirlis, N., Arnhem, H., Boutsouki, C., & Vlachopoulou, M. (2019). Understanding the role of personality traits on Facebook intensity. *International Journal of Internet Marketing and Advertising*, *13*(2), 99–119. https://doi.org/10.1504/IJIMA.2019.099494

Lissitsa, S., & Kol, O. (2021). Four generational cohorts and hedonic m-shopping: association between personality traits and purchase intention. *Electronic Commerce Research*, *21*(2), 545–570.

Little, R. J. A. (1988). A test of missing completely at random for multivariate data with missing values. *Journal of the American Statistical Association*, *83*(404), 1198–1202. https://doi.org/10.1080/01621459.1988.10478722

Loiacono, E. T. (2015). Self-disclosure behavior on social networking web sites. *International Journal of Electronic Commerce*, *19*(2), 66–94.

Luo, X., Li, H., Zhang, J., & Shim, J. P. (2010). Examining multi-dimensional trust and multi-faceted risk in initial acceptance of emerging technologies: An empirical study of mobile banking services. *Decision Support Systems*, *49*, 222–234. https://doi.org/10.1016/j.dss.2010.02.008

Maddi, S. R. (1996). *Personality theories: A comparative analysis*. Brooks/Cole.

Manuel, J., & Veríssimo, C. (2016). Enablers and restrictors of mobile banking app use: A fuzzy set qualitative comparative analysis (fsQCA). *Journal of Business Research*, *69*(11), 5456–5460. https://doi.org/10.1016/j.jbusres.2016.04.155

McCrae, R. R. (1993). Openness to experience as a basic dimension of personality. *Imagination, Cognition and Personality*, *13*(1), 39–55. https://doi.org/10.2190/H8H6-QYKR-KEU8-GAQ0

McCrae, R. R., & Terracciano, A. (2005). Universal features of personality traits from the observer's perspective: Data from 50 cultures. *Journal of Personality and Social Psychology*, *88*(3), 547. https://doi.org/10.1037/0022-3514.88.3.547

McElroy, J. C., Hendrickson, A. R., Townsend, A. M., & DeMarie, S. M. (2007). Dispositional factors in internet use: Personality versus cognitive style. *MIS Quarterly*, *31*(4), 809–820. https://doi.org/10.2307/25148821

Melone, N. P. (1990). A theoretical assessment of the user-satisfaction construct in information systems research. *Management Science*, *36*(1), 76–91. https://doi.org/10.1287/mnsc.36.1.76

Mohammadi, H. (2015). Investigating users' perspectives on e-learning: An integration of TAM and IS success model. *Computers in Human Behavior*, *45*, 359–374. https://doi.org/10.1016/j.chb.2014.07.044

Moslehpour, M., Thi Thanh, H. Le, & Van Kien, P. (2018). Technology perception, personality traits and online purchase intention of Taiwanese consumers. In *International Conference of the Thailand Econometrics Society* (pp. 392–407). https://doi.org/10.1007/978-3-319-70942-0_28

Muñoz-Leiva, F., Climent-Climent, S., & Liébana-Cabanillas, F. (2017). Determinants of intention to use the mobile banking apps: An extension of the classic TAM model. *Spanish Journal of Marketing*, *21*(1), 25–38. https://doi.org/10.1016/j.sjme.2016.12.001

Njoroge, C. N., & Koloseni, D. (2015). Adoption of social media as full-fledged banking channel: An analysis of retail banking customers in Kenya. *International Journal of Information and Communication Technology Research*, *5*(2), 1–12.

Nunnally, J. C., & Bernstein, I. (1994). *Psychometric theory*. McGraw-Hill.

Ones, D. S., & Viswesvaran, C. (1996). Bandwidth–fidelity dilemma in personality measurement for personnel selection. *Journal of Organizational Behavior*, *17*(6), 609–626.https://doi.org/10.1002/(SICI)1099-1379(199611)17:6<609::AID-JOB1828>3.0.CO;2-K

Panda, A., & Jain, N. K. (2018). Compulsive smartphone usage and users' ill-being among young Indians: Does personality matter? *Telematics and Informatics*, *35*(5), 1355–1372. https://doi.org/10.1016/j.tele.2018.03.006

Pituch, K. A., & Lee, Y. (2006). The influence of system characteristics on e-learning use. *Computers & Education*, *47*, 222–244. https://doi.org/10.1016/j.compedu.2004.10.007

Podsakoff, P. M., MacKenzie, S. B., & Podsakoff, N. P. (2012). Sources of method bias in social science research and recommendations on how to control it. *Annual Review of Psychology*, *63*, 539–569. https://doi.org/10.1146/annurev-psych-120710-100452

Ramayah, T., Wai, J., & Lee, C. (2012). System characteristics, satisfaction and e-learning usage: A structural equation model. *The Turkish Online Journal of Educational Technology*, *11*(2), 26–28.

Rana, N., Dwivedi, Y., Williams, M., & Weerakkody, V. (2015). Investigating success of an e-government initiative: Validation of an integrated IS success model. *Information Systems Frontiers*, *17*(1), 127–142. https://doi.org/10.1007/s10796-014-9504-7

Rosen, P. A., & Kluemper, D. H. (2008). The impact of the big five personality traits on the acceptance of social networking website. In *AMCIS 2008 Proceedings* (pp. 1–10). https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.909.2632&rep=rep1&type=pdf

Sampaio, C. H., Ladeira, W. J., & Santini, F. D. O. (2017). Apps for mobile banking and customer satisfaction: A cross-cultural study. *International Journal of Bank Marketing*, *35*(7), 1133–1153. https://doi.org/10.1108/IJBM-09-2015-0146

Sangar, A. B., & Rastari, S. (2015). A model for increasing usability of mobile banking apps on smart phones. *Indian Journal of Science and Technology*, *8*(30), 1–9. https://doi.org/10.17485/ijst/2015/v8i30/85690

Shambare, N. (2013). *Examining the influence of personality traits on intranet portal adoption by faculty in higher education*. PhD dissertation, Northcentral University, San Diego, CA.

Shim, M., & Jo, H. S. (2020). What quality factors matter in enhancing the perceived benefits of online health information sites? Application of the updated DeLone and McLean information systems success model. *International Journal of Medical Informatics*, *137*. https://doi.org/10.1016/j.ijmedinf.2020.104093

Svendsen, G. B., Johnsen, J. A. K., Almås-Sørensen, L., & Vittersø, J. (2013). Personality and technology acceptance: The influence of personality factors on the core constructs of the technology acceptance model. *Behaviour and Information Technology*, *32*(4), 323–334. https://doi.org/10.1080/0144929X.2011.553740

Tam, C., & Oliveira, T. (2016). Understanding the impact of m-banking on individual performance: DeLone & McLean and TTF perspective. *Computers in Human Behavior*, *61*, 233–244. https://doi.org/10.1016/j.chb.2016.03.016

Tuten, T., & Bosnjak, M. (2001). Understanding differences in web usage: The role of need for cognition and the five factor model of personality. *Social Behaviour and Personality*, *29*(4), 391–398. https://doi.org/10.2224/sbp.2001.29.4.391

Urbach, N., & Ahlemann, F. (2010). Structural Equation Modeling in Information Systems Research Using Partial Least Squares. *JITTA: Journal of Information Technology Theory and Application*, *11*(2), 5.

Vedadi, A., & Warkentin, M. (2016). Continuance intention on using mobile banking applications – A replication study of information systems continuance model. *AIS Transactions on Replication Research*, *2*, 1–11. https://doi.org/10.17705/1atrr.00014

Veeramootoo, N., Nunkoo, R., & Dwivedi, Y. K. (2018). What determines success of an e-government service? Validation of an integrative model of e-filing continuance usage. *Government Information Quarterly*, *35*(2), 161–174. https://doi.org/10.1016/j.giq.2018.03.004

Were, M., Odongo, M., & Israel, C. (2021). Gender disparities in financial inclusion in Tanzania. World Institute for Development Economic Research (UNU-WIDER).

Yang, H. C. (2013). Bon appétit for apps: Young American consumers' acceptance of mobile applications. *Journal of Computer Information Systems*, *53*(3), 85–96. https://doi.org/10.1080/08874417.2013.11645635

Zwass, V. (2003). Electronic commerce and organizational innovation: Aspects and opportunities. *International Journal of Electronic Commerce*, *7*(3), 7–37. https://doi.org/10.1080/10864415.2003.11044273

Appendix: Statements used in the survey questionnaire

Code	Statement	Source
System quality		
SYQ1	The mobile banking app is easy to navigate.	
SYQ2	The mobile banking app allows me to easily find the information I am looking for.	
SYQ3	The mobile banking app is easily structured.	
SYQ4	The mobile banking app offers appropriate functionality.	
SYQ5	Mobile banking is easy to use.	
Service quality		
SEQ1	The responsible personnel are always willing to help whenever I need support with a mobile banking app.	
SEQ2	The responsible personnel provide services related to the mobile banking app at the promised time.	
SEQ3	The responsible personnel have adequate knowledge to answer my questions concerning the mobile banking app.	
SEQ4	The responsible personnel provide personal attention whenever I experience problems with the mobile banking app.	
Information quality		
INFQ1	The information provided by the mobile banking app is useful.	
INFQ2	The information provided by the mobile banking app is understandable.	
INFQ3	The information provided by the mobile banking app is interesting.	
INFQ4	The information provided by the mobile banking app is reliable.	
INFQ5	The information provided by the mobile banking app is complete.	
INFQ6	The information provided by the mobile banking app is up to date.	
Use		
USE 1	I use a mobile banking app.	
USE 2	I use the mobile banking app to manage my accounts.	
USE 3	I use the mobile banking app to make transfers.	
USE 4	I use the mobile banking app to make in-app purchases.	
User satisfaction		
SAT1	I am satisfied that the mobile banking app meets my information processing needs.	
SAT2	I am satisfied with the mobile banking app efficiency.	
SAT3	I am satisfied with the mobile banking app effectiveness.	
SAT4	Overall, I am satisfied with the mobile banking app.	

Urbach et al. (2010)

Bhattacherjee (2001)

Individual performance		Goodhue and Thompson (1995)
PERF1	The mobile banking app helps me to accomplish banking-related tasks more quickly.	
PERF2	The mobile banking app makes it easier to accomplish tasks.	
PERF3	The mobile banking app is useful for me.	
Openness		Donnellan et al. (2006); Goldberg (1999)
OPN1	I enjoy imagining new and different ideas.	
OPN2	I experience difficulty in comprehending abstract ideas	
OPN3	I am not keen to engage myself in intellectual discussions.	
OPN4	I do not enjoy daydreaming.	
Conscientiousness		
CONS1	I get chores done the right way.	
CONS2	I like to keep things in order.	
CONS3	I often forget to put things back in their proper place.	
CONS4	Many a time, I mess up things.	
Extraversion		
EXT 1	I enjoy partying frequently.	
EXT 2	I enjoy talking to new people, who are different from me.	
EXT 3	I do enjoy socializing.	
EXT 4	I enjoy going out to help people in need.	
Agreeableness		
AGR1	I sympathise with others frequently.	
AGR2	I feel for others.	
AGR3	I don't care what others are really doing.	
AGR4	I go with the majority.	
Neuroticism		
NEU1	I experience frequent mood swings.	
NEU2	I get upset easily.	
NEU3	I am relaxed most of the time.	
NEU4	I seldom feel blue.	

The Cyber Threat Landscape in South Africa: A 10-Year Review

Heloise Pieterse
Senior Researcher and Cybersecurity Specialist, Information and Cybersecurity Centre, Council for Scientific and Industrial Research (CSIR), Pretoria
https://orcid.org/0000-0002-2908-4012

Abstract
The world is witnessing a rise in cyber-related incidents. As information technology improves and the reliance on technology increases, the frequency and severity of cyber incidents escalate. The impact is felt globally, and South Africa is not immune to the effects. The country's fast-paced technological evolution continues to increase the attack surface within the cyber domain. The increased attack surface is confirmed by recent cyberattacks affecting well-known and established South African organisations. This article reviews findings from an evaluation of South Africa's cyber threat landscape that analysed 74 cyber incidents identified as occurring between 2010 and 2020. The 74 incidents are categorised according to *incident type*, *affected sector*, *perpetrator type*, and *motivation*. It is found that the most common incident type is *data exposure*, the most-affected sector is the *public* sector, the most prevalent perpetrators are *hackers*, and the most common motivation is *criminal.* The article makes recommendations about how South Africa can reduce the risk factors in its cyber threat landscape.

Keywords
cybersecurity, cyber threats, cyberattacks, cyber incidents, attack surface, compromised websites, cybercrime, data exposure, system intrusion, denial of service

DOI: https://doi.org/10.23962/10539/32213

Recommended citation
Pieterse, H. (2021). The cyber threat landscape in South Africa: A 10-year review. *The African Journal of Information and Communication (AJIC), 28*, 1-21. https://doi.org/10.23962/10539/32213

1. Introduction

The prevalence of cyber incidents globally contributes to the ever-increasing cybersecurity concerns. Well-known and established organisations, such as Solar Winds (Willett, 2021) and Microsoft (Wyatt, 2021), have fallen victim to sophisticated cyberattacks. South Africa is not immune, and has witnessed a steady increase in cyberattacks in recent years. 2019 proved pivotal as South Africa experienced a cross-industry spike in cyber incidents (Mcanyana et al., 2020), a trend that continued in 2020 and was further driven by the COVID-19 pandemic.

The City of Johannesburg (CoJ), a metropolitan municipality responsible for local governance, suffered two noteworthy cyber incidents during 2019 (Moyo, 2019a). First, in July, a ransomware attack affected City Power, CoJ's electricity utility. Second, in October, a network breach was detected after a ransom note was received from a group called the Shadow Kill hackers. Both cyber incidents caused downtime to several customer-facing systems. Following the breach at CoJ, the South African Bank Risk Information Centre (SABRIC) confirmed that the banking sector had been targeted by a wave of distributed denial of service (DDoS) attacks (Moyo, 2019b).

In 2020 the COVID-19 pandemic caused a surge in cyber incidents as the pandemic created new opportunities for attackers to exploit. During May, an accidental data leak caused by changes to the Unemployment Insurance Fund (UIF) website—changes made to accommodate the Temporary Employee/Employer Relief Scheme (TERS)—exposed employers' confidential information. The issue causing the data leak was reported by a security researcher and subsequently resolved by the UIF (Vermeulen, 2020a). In June 2020, the second-largest private hospital operator in South Africa, Life Healthcare Group, fell victim to a cyberattack. Although the full extent of the attack remains unclear, Life Healthcare Group confirmed that the attack affected admissions systems, business processing systems, and e-mail servers (Mungadze, 2020). Two months later, South Africa suffered a massive data breach when Experian, a credit bureau agency, exposed personal information to a suspected fraudster. The exposed personal information affected approximately 24 million South Africans, as well as 800,000 business entities (Moyo, 2020a). The remainder of 2020 continued to witness various cyber incidents affecting South Africa's financial, public, construction, and telecommunication sectors.

In 2021, the attractiveness of South Africa as a cyber target was further demonstrated by the large-scale cyberattack that affected Transnet, the South African state-owned rail, port, and pipeline company (Moyo, 2021). According to Noëlle van der Waag-Cowling, a cyber programme lead at the Security Institute for Governance and Leadership in Africa, the incident has been described as an act of "cyber warfare" and serves as a warning to South Africa (Goldstuck, 2021; Slabbert & Peyper, 2021).

Shortly thereafter, the Department of Justice and Constitutional Development confirmed a security breach that affected its information technology system. The breach was the result of ransomware, causing all the department's systems to be encrypted and unavailable to both internal employees and members of the public (Ngqakamba, 2021).

Globally, cyber incidents are well-documented in peer-reviewed scholarly articles and research reports. In South Africa, however, despite the steady increase in cyber incidents, the formal reporting of such incidents is not common. Neither the South African Police Service (SAPS) nor the National Prosecuting Authority (NPA) offers resources or statistics pertaining specifically to local cyber incidents. The Cybersecurity Hub—South Africa's national Computer Security Incident Response Team (CSIRT)—provides a service for stakeholders to report cyber incidents, but it does not report such incidents to the general public. Furthermore, few peer-reviewed articles exist that have evaluated South African cyber incidents. One notable exception is the Van Heerden et al. (2016) review of 12 South African cyber incidents that occurred between 1994 and 2015. Van Heerden et al. (2016) presented a new visual classification scheme for cyber incidents, which facilitates the representation of the cyber incidents according to eight distinct classes: attacker, goal, mechanism, effect, motivation, target, vulnerability, and scenario (Van Heerden et al., 2016). Another noteworthy exception is Van Niekerk's (2017) presentation of a comprehensive high-level analysis of 54 cyber incidents that affected South Africa between 1994 and 2016. Van Niekerk (2017) classifies the incidents according to impact, perpetrator, and victim types, finding the leading perpetrators to be criminals and hacktivists, and the leading impacts of the cyber incidents to be data exposure and financial theft (Van Niekerk, 2017).

Although the two above-mentioned studies do offer insight into South Africa's cyber threat landscape, they only address incidents up to the end of 2015 and 2016 respectively. This article considers a full decade of cyber incidents, from 2010 to 2020, providing an analysis of 74 newsworthy cyber incidents that affected South Africa during that period. The cyber incidents considered are categorised according to *incident type*, *sector affected*, *perpetrator type*, and *motivation*. This categorisation permits a detailed trend analysis and a picture of South Africa's current cyber threat landscape.

2. Methodology

Data collection

Since information was not readily available from official sources (e.g., SAPS, the NPA, the national CSIRT), the cyber incidents analysed were identified by reviewing published peer-reviewed articles and media reports (e.g., reports published by *ITWeb*, *MyBroadband* and *BusinessTech*), as well as by conducting targeted online searches. The selection of cyber incidents was based on the following: the incident affected a South African organisation(s) or citizens; and the impact of the incident

caused a breach (either network or data), affected services, or led to financial loss. A total of 74 cyber incidents occurring in the decade from January 2010 to December 2020 were identified.

Data analysis

Insight and guidance were taken from the approaches used by Van Heerden et al. (2016) and Van Niekerk (2017) in deciding how to categorise the 74 cyber incidents. A classification scheme was developed that consisted of four classifications, namely *incident type*, *sector affected*, *perpetrator type*, and *motivation*.

Incident type

The first classification, *incident type*, classifies the cyber incident according to one of the following types:

- *Compromised website:* intentional or unintentional activity affecting the confidentiality, integrity, or availability of the website (Kumar et al., 2019);
- *Cybercrime*: criminal activity involving a computer, network device, or network causing financial impact (Brush, n.d.);
- *Data exposure*: disclosure or leakage of data or information within the public domain (Sabillon et al., 2016; Van Niekerk, 2017);
- *System intrusion*: unauthorised or illegitimate access to a system or network (Kakareka, 2014; Van Niekerk, 2017); or
- *Denial of service*: preventing authorised or legitimate users from accessing network resources or affecting operations (Sabillon et al., 2016; Van Niekerk, 2017).

Sector affected

The second classification, *sector affected*, classifies the incident in terms of the area of the economy in which it occurred, with the following potential classifications: *construction*, *financial*, *healthcare*, *information technology (IT)*, *leisure and hospitality*, *manufacturing*, *media*, *public*, *retail*, *telecommunications*, *transportation*, or *other.*

Perpetrator type

The third classification, *perpetrator type*, classifies the individual or group responsible for the cyber incident as being of one of the following types:

- *Hacktivist*: an individual or group of individuals affiliated with activists' groups promoting political agendas or social change (Sabillon et al., 2016; Van Niekerk, 2017);
- *Insider:* an individual with a trusted relationship, institutional knowledge, and legitimate access, but acting maliciously for personal gain (Van Heerden et al., 2012; 2016; Van Niekerk, 2017);
- *Hacker:* a well-versed or unskilled individual using tools developed by elite computer users to break security and infiltrate networks or information systems (Van Heerden et al., 2016; Van Niekerk, 2017);

- *Cybercriminal*: an individual or group of individuals affiliated to criminal groups motivated by financial gain (Van Niekerk, 2017);
- *Nation state*: state-sponsored sophisticated hackers who target the information systems or networks of other countries (Sabillon et al., 2016; Van Niekerk, 2017); or
- *Non-malicious individual*: a person causing internal or external disclosure of a security flaw or a vulnerability affecting an information system.

Motivation

The fourth classification, *motivation*, classifies the rationale behind the cyber incident according to one of the following motives:

- *Political*: driven by a political aspect, such as political reasoning, spreading propaganda, or attacking political enemies (Gandhi et al., 2011; Van Heerden et al., 2012);
- *Economic*: illegal actions driven by financial gain, e.g., deploying ransomware with the purpose of acquiring paid ransom (Gandhi et al., 2011; Van Heerden et al., 2012; 2016);
- *Fun/Personal*: driven by a desire to prove skills, to solve challenging problems, or to expose security flaws, i.e., driven by non-malicious intentions (Van Heerden et al., 2012; 2016);
- *Accidental*: unintentional or unexpected discovery of a security flaw or vulnerability; or
- *Criminal*: conscious decision to intentionally conduct wrongdoing or criminal intent (but lacking financial incentive), e.g., performing a system intrusion to access personally identifiable information (PII) (Van Heerden et al., 2012; 2016).

3. Findings

High-profile cyber incidents identified

Examples of high-profile cyber incidents identified include:

2012

A hacker called H4ksniper claimed responsibility for disrupting three South African government websites (*MyBroadband*, 2012). Subsequently, various other South African websites fell victim to either hacktivists or hackers.

2014

Unpatched security vulnerabilities resulted in the mass hacking of South African websites that were using outdated versions of web content management systems such as Joomla and WordPress (*MyBroadband*, 2014). The hacks involved the insertion of hidden links to international websites to improve the page rank of the websites on the Google and Bing search engines.

2013–2014
These two years saw several accidental exposures of confidential data. Security researchers found on multiple occasions the exposure of PII by South African mobile operator, Vodacom (Muller, 2013; *BusinessTech*, 2014). Such exposure of PII can have grave consequences for organisations, especially with the coming into force of South Africa's 2013 Protection of Personal Information Act (POPIA) on 1 July 2021 (RSA, 2013).

2016-2020
Compromised websites remained frequent in the second half of the decade (McKane, 2020a; Moyo, 2017; *MyBroadband*, 2018; Mzekandaba, 2019; Vermeulen, 2016). Also significant in this period was an increase in cyber incidents exposing data. While accidental exposure of data persisted (*MyBroadband*, 2016), data exposure was increasingly politically or criminally motivated (*BusinessTech*, 2016; Moyo, 2019c).

A global trend during the latter half of the decade was the frequent occurrence of ransomware attacks. During 2017, such attacks (WannaCry and NotPetya) were driven by EternalBlue, a Windows zero-day exploit targeting a vulnerability in the server message block (SMB) protocol (Trautman & Ormerod, 2019). Originally developed by the US National Security Agency (NSA), EternalBlue was leaked by the Shadow Brokers hacker group, causing a global cyberattack. Several South African organisations were also affected by large-scale ransomware attacks, including telecommunications provider, Telkom, the Office of the Chief Justice, and a stolen vehicle recovery company, Tracker (Moyo, 2020b; *MyBroadband*, 2017; Rawlins, 2017; Vermeulen, 2020b; 2020c).

Annual frequency of cyber incidents
As seen in Figure 1, the data revealed annual increases in cyber incidents for most (but not all) of the years studied, with a particularly sharp annual increase from 2019 (11 incidents) to 2020 (19 incidents).

Figure 1: Annual cyber incident totals, 2010–2020

Incident type
Figures 2 to 4 present the classification of the 74 cyber incidents according to incident type, in three periods: 2010–2015, 2016–2018, and 2019–2020. All the cyber incidents are represented by the actual title used in media reports.

Figure 2: Classification of cyber incidents by type, 2010–2015 (21 incidents)

	Compromised Website	Cybercrime	Data Exposure	System Intrusion	Denial of Service
		Absa Land Bank Fraud.			
2010 2011	ANCYL site hacked again. ANC Youth League website hacked again.				
2012	Postbank hacked for R42m. South African websites hacked.				
2013	Aarto Web site latest hacking victim.		SAPS hack spells negligence. Joburg billing leak not a hack: whistle blower. My Vodacom security flaw exposes subscriber details.	Mass security breach of fast food payment systems in SA.	IOL hit by DoS attack. Cyber-attack behind Afrihost, MTN Internet problems.
2014	PIC website hacked. Mass hacking of South African websites.	SA scammer caught in action.	Vodacom and Cell C report security flaws. Vodacom exposing subscriber details.		E-toll site weathers denial of service attack.
2015	ANC website hacked?		175,000 SA cheaters exposed in Ashley Madison data leak.		MTN weathers DDOS attack.

Figure 3: Classification of cyber incidents by type, 2016–2018 (23 incidents)

	Compromised Website	Cybercrime	Data Exposure	System Intrusion	Denial of Service
2016	Massive number of South African websites hacked by Anonymous.	Standard Bank was hacked in R300 million fraud hit: report.	Anonymous hacks SA government database. Hackers leak SA government's sensitive financial data. MTN exposing subscribers' personal details online. Anonymous hacks Armscor website. Govt chat tool debuts; data breach on KZN site. SA Olympian's medical info hacked.		Africa Anonymous targets the SABC.
2017	DBE Web site hacked, pro-Islamic State messages posted. City of Joburg site offline.	Hackers again prove their global power.	Massive flaw in old Ster-Kinekor website leaked clients' private data. Massive South African database leak reveals private data of 30 million people. Hetzner South Africa hacked – Sensitive information exposed.	Telkom systems crippled by WannaCry ransomware. Old Mutual hacked; no losses incurred.	
2018	South African presidency website hacked.	Beware new-look Absa scam.	Huge data breach discovered with South African websites listed – Report. Data leak exposes names, ID numbers, and plain-text passwords of 934,000 South Africans. Hetzner admits to "security incident".	No financial loss in email hack: Liberty	

Figure 4: Classification of cyber incidents by type, 2019–2020 (30 incidents)

	Compromised Website	Cybercrime	Data Exposure	System Intrusion	Denial of Service
2019	SASSA Web site remains down after hack. Telkom webserver hacked, used to host phishing page.	City Power hit by ransomware attack. Suspects arrested for hacking City of Tshwane, R53m pillaged.	Garmin SA hacked, exposing users' credit card details. Adapt IT unit Conor hit by massive data breach.	SA aviation authority still to pinpoint attack source. City of Joburg hit by cyber attack.	Bad day for SA's cyber security as banks suffer DDoS attacks. Liquid Telecom, Webafrica hit by DDoS attacks. Massive DDoS attacks – South African Internet providers crippled.
2020	South African online stores targeted by hackers. ANC Youth League website hacked. SABC confirms that its website was hacked.	Tracker hack hints at more ransomware attacks in SA. NCape municipality battles devastating ransomware attack.	Momentum Metropolitan hacked. Experian hacked, 24m personal details of South Africans exposed. Lombard Insurance engages SA authorities after data breach. The main people behind Mirror Trading International. Ransomware group claims hack on Office of the Chief Justice. South Africa's communications minister WhatsApp account 'hacked'. Absa hit by data breach. Ransomware group releases data after attack on Office of the Chief Justice. Data leak on UIF COVID-19 relief scheme website.	1.7m Nedbank clients exposed after service provider hack. JSE company Omnia hit by cyber attack. Life Healthcare Group hit by cyber attack amid COVID-19. Postbank to replace 12m bank cards after security breach. Stefanutti Stocks shuts down IT systems after cyber attack.	

The most prevalent incident type across the ten years studied (see Figure 5) was *data exposure* (39.19% of incidents), followed by *compromised website* (21.62%), *system intrusion* (14.86%), *cybercrime* (13.51%), and *denial of service* (10.81%). The finding on the prominence of data exposure aligns with the finding from research conducted by Van Niekerk (2017) on the period 1994 to 2016, which found data exposure to be the most prominent impact caused by cyber incidents in South Africa. Meanwhile, this study's finding that denial of service was the type of cyber incident present in 10.81% of incidents marks a decrease in percentage share compared to the research results reported by Van Niekerk (2017) for the period 1994 to 2016. This decrease in denial of service attacks can potentially be attributed to the increase in other cyber incident types, such as *cybercrime* using ransomware (Trend Micro, 2017). Finally, the findings in this study show a significant increase in system intrusion incidents (14.86%) compared to the research results presented by Van Niekerk (2017) for the period 1994 to 2016, which found system penetration to be the least common impact type. The increase merely demonstrates an increase in cyber incidents affecting organisations that release such information to the general public.

Figure 5: Cyber incidents by type, 2010–2020

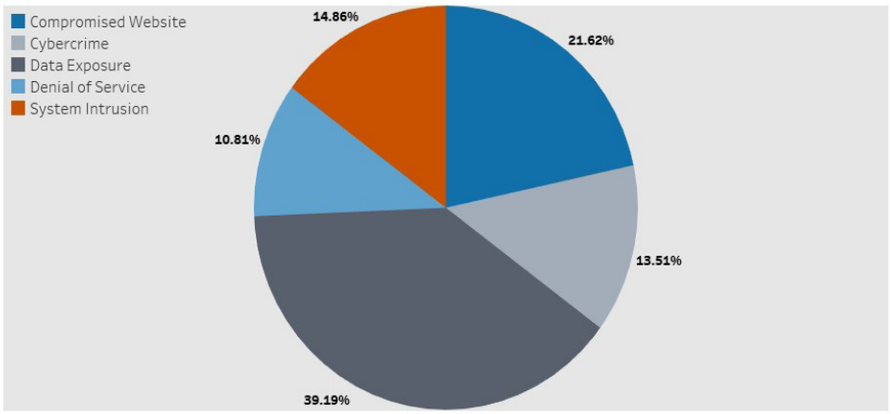
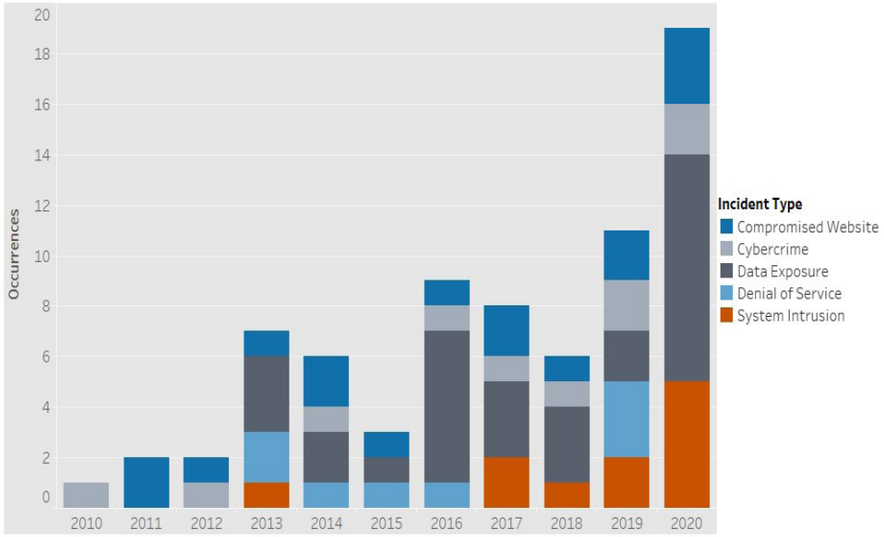


Figure 6 shows the year-by-year trends in incident type identified in this study. The most prominent incident type, *data exposure*, had notable increases in 2016 and 2020. Reporting of such incidents is expected to grow even further with the aforementioned implementation of POPIA, which requires mandatory reporting of data breaches involving personal information (Dullabh & Gabryk, 2021). Less prominent than data exposure incidents but recurring continually between 2011 and 2020 were incidents leading to *compromised websites*. Also illustrated is the small yet notable increase in the annual total of *cybercrime*-related incidents between 2018 and 2019, with 2020 maintaining the relatively high level of such attacks. These findings confirm the increasing move towards *criminally* motivated cyber incidents (see "motivation" sub-section below). Another notable trend illustrated in Figure 6 is the

recent rise of cyber incidents of the *system intrusion* type. Identified reports on such incidents confirmed illegitimate access to a system or internal network but restricted the disclosure of information describing the incident's impact (e.g., data leakage, affected services or operations, encryption of data).

Figure 6: Yearly trends in incident types, 2010–2020



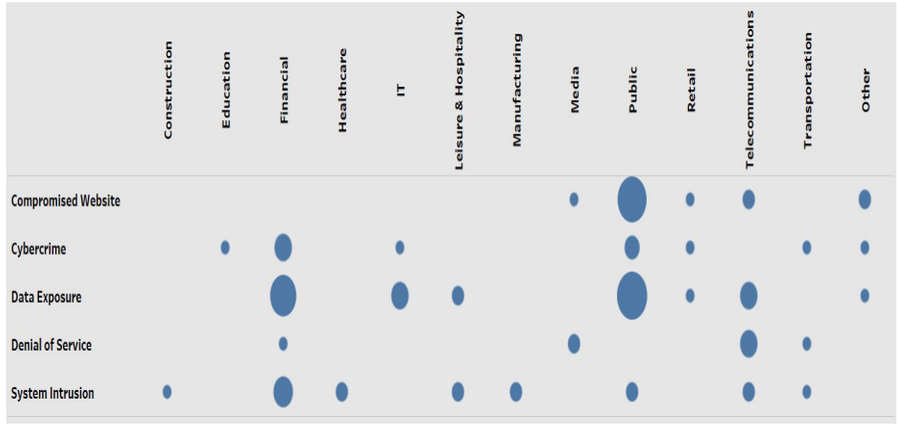
Sector affected

The findings captured in Figure 7 show that the three South African sectors most affected by the past decade's cyber incidents were the *public*, *financial*, and *telecommunications* sectors. The public sector, which consists of state-owned, publicly controlled, or publicly funded entities, often fell victim to cyber incidents causing *compromised websites* or *data exposure.* Notably, the websites of the African National Congress (ANC) and the ANC Youth League (ANCYL) were regularly targeted by hackers, negatively affecting the reputation of the organisations. Other entities in the public sector affected by cyber incidents include, but are not limited to, the Office of the Chief Justice, the Social Security Agency of South Africa (SASSA), the Administrative Adjudication of Road Traffic Offences (AARTO), the Department of Basic Education, Armscor, SAPS, and several municipalities (Nama Khoi, eThekwini, Tshwane, and Johannesburg).

In comparison to the public sector, the financial sector suffered fewer cyber incidents. However, the incidents impacted commercial banks, insurance companies, and financial institutions. While cyber incidents affecting the financial sector are expected to be primarily *economic* in motivation, the past decade witnessed an increase in incidents leaking sensitive information (see "motivation" sub-section below). Although such incidents do not have any financial implications, affected clients can still incur

financial loss due to the misuse of such exposed information. The value associated with sensitive information as a commodity on the dark web can be expected to cause a steady rise in cyber incidents targeting the financial sector.

Figure 7: Sector affected per cyber incident type, 2010–2020



Finally, the telecommunications sector of South Africa, which includes mobile operators and internet service providers (ISPs), fell victim to several cyber incidents causing *denial of service*. More specifically, the sector experienced two significant DDoS attacks during 2019. In the first attack, Liquid Telecom and Webafrica suffered a large-scale volumetric DDoS attack from international sources (Moyo, 2019d). Mitigation controls were applied, and traffic volumes returned to normal. A few weeks later, South African ISPs, RSAWEB and Cool Ideas, suffered severe DDoS attacks (Vermeulen, 2019). The co-founder of Cool Ideas confirmed that the attack exceeded 300 Gigabytes per second (Gbps). The telecommunication sector also endured several cyber incidents causing *data exposure*. On closer inspection, the exposure of the data in these cases was accidental and caused by *non-malicious individuals* (see "perpetrator type" sub-section below). Although less affected than the public and financial sectors, entities in the telecommunication sector can expect to continue being targeted by cyber incidents.

Perpetrator type

Figure 8 presents trends associated with perpetrator types. *Hackers* were found to be the most common perpetrator type, responsible for more than 50% of the cyber incidents that occurred in the past decade. While responsible for the largest subset of cyber incidents, hackers became most prevalent only in 2017. More dominant between 2012 and 2018 were *hacktivists*, who were responsible for 11 cyber incidents during the same period.

Figure 8: Trends in perpetrator type, 2010–2020

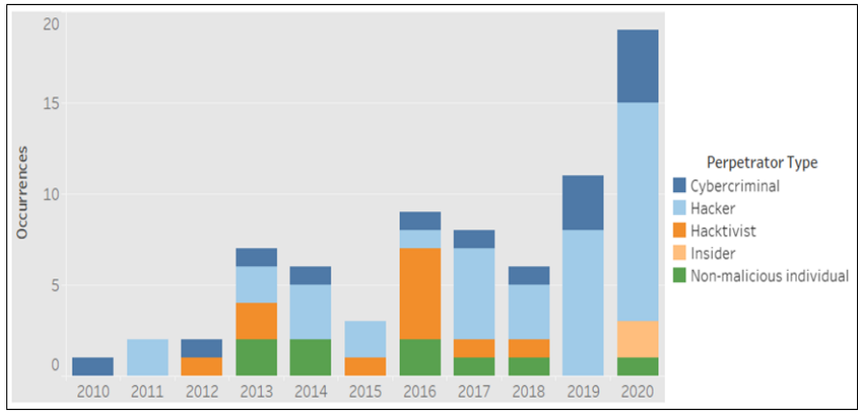
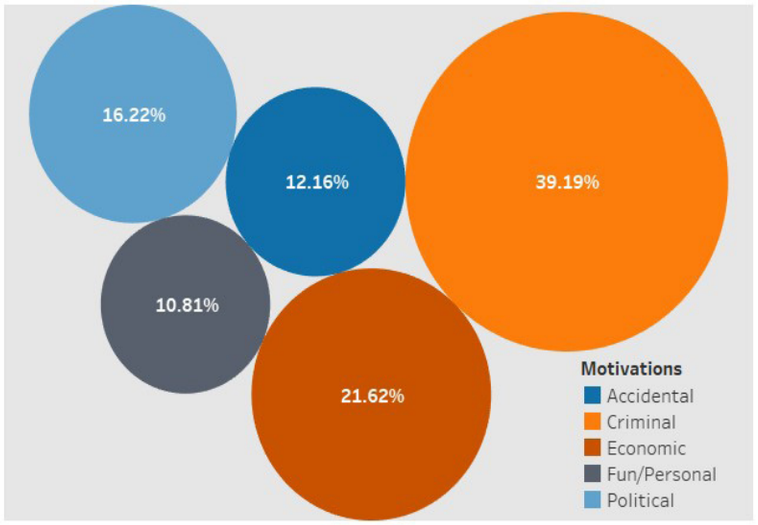


Figure 8 further illustrates the prevalence of incidents caused by *cybercriminals*. The year 2019 witnessed a sharp increase in such incidents, apparently driven partly by the rise of ransomware-related attacks. Another reality seen is the figure is the reappearance in 2020 (after being absent in 2019) of security flaws or misconfigurations generated by *non-malicious individuals*. (In total, nine such incidents were disclosed in the decade reviewed.) Also noteworthy in Figure 8 is the appearance, in 2020 and for the first time in the decade reviewed, of two cyber incidents caused by *insiders*. There were two such incidents in 2020. The first was a security breach at Postbank in which its employees stole the bank's encrypted master key (*ITWeb*, 2020). The master key provides access to Postbank's systems and enables the manipulation of captured information. The second incident was caused by internal data theft that exposed the personal information of Absa banking clients to external parties (McKane, 2020b). Absa notified affected clients and confirmed that all suspicious transactions will be reviewed in order to protect clients' interests.

Motivation

Figure 9 shows that the most common motivation found for cyber incidents in South Africa in the decade reviewed was *criminal* (39.19%). Cyber incidents driven by *economic* intent constituted 21.62% of the recorded incidents, while 16.22% of the incidents were *political* in motivation. The two least common motives, *accidental* (12.6%) and *fun/personal* (10.81%), still, when taken together, represented nearly a quarter of the identified incidents.

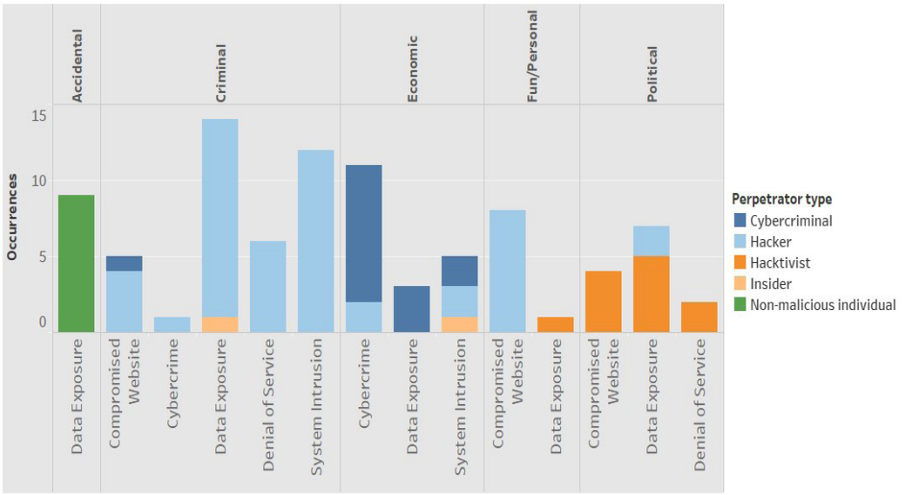
Figure 9: Motives behind cyber incidents, 2010–2020



Relationships between incident type, perpetrator type, and motivation

Figure 10 shows that a strong relationship between perpetrator type and motivation was found between *hackers* and *criminal* motivation. And, when driven by criminal intent, hackers were found to cause cyber incidents primarily leading to *data exposure* or *compromised websites* (17 incidents across these two classifications). A smaller number of hackers were motivated by *fun/personal* intentions, and these hackers were involved in seven cyber incidents causing *compromised websites*.

Figure 10: Relationships between incident type, perpetrator type, and motivation



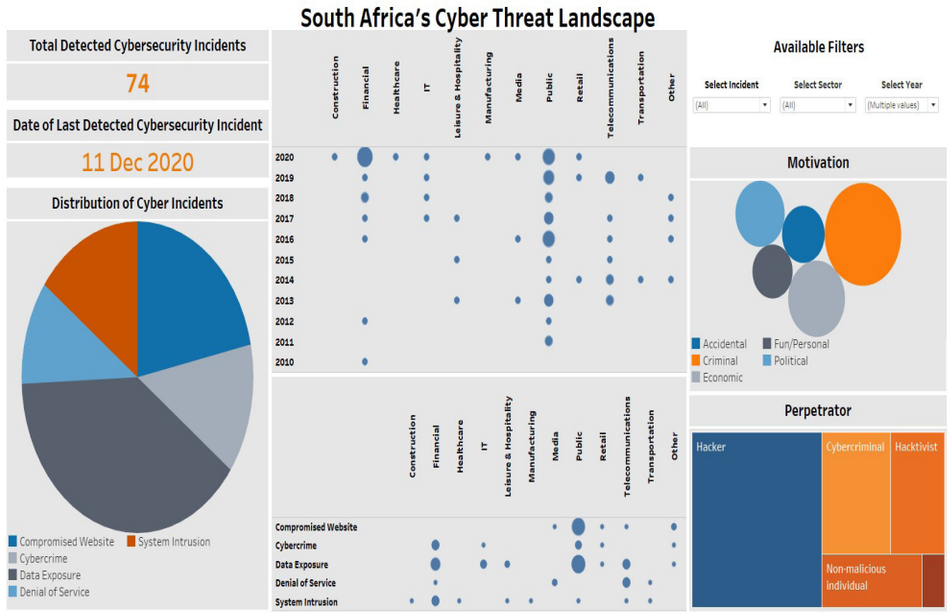
As also seen in Figure 10, *cybercriminals* were, unsurprisingly, found to be primarily driven by *economic* motives (13 incidents) and strongly associated with *cybercrime* incidents (eight incidents). The remaining five cyber incidents caused by cybercriminals, while also driven by economic incentives, resulted in *data exposures* and *system intrusions.* In these five cyber incidents, the cybercriminals either attempted fraud (using acquired or exposed credit card information) or requested ransom in the form of bitcoin (due to ransomware attacks).

Another relationship identified was between *hacktivists* and *politically* motivated cyber incidents. In total, ten cyber incidents occurred that were driven by political incentives. Half of the incidents were caused by hacktivists affiliated with Anonymous, a decentralised international activist/hacktivist movement driven by political agendas (Mikhaylova, 2014), and the remaining incidents were claimed by the hacktivist groups H4ksniper, Team Hack Argentino, World Hacker Team, Team System DZ, and Black Team. A final relationship detected in the data was between *data exposure* due to the accidental misconfiguration or disclosure by benevolent individuals (nine incidents).

A threat landscape dashboard

Figure 11 summarises the findings of this study in the form of a dashboard constructed to enable a bird's eye view of South Africa's cyber threat landscape.

Figure 11: Dashboard visualisation of South Africa's cyber threat landscape



4. Discussion

South Africa's perilous cyber threat landscape

In response to the increase in cyber incidents in South Africa, iDefense, an Accenture security intelligence company, investigated notable cyber incidents and trends during 2019. iDefense found that several factors were contributing to South Africa's increasingly perilous cyber threat landscape (Mcanyana et al., 2020). Based on the findings captured in the iDefense report and the findings from this study, it can be concluded that the following elements are negatively impacting South Africa's cybersecurity and increasing its attack surface:

Lack of investment in cybersecurity

South Africa, as a country with a developing economy, continually faces insurmountable challenges. Investment in cybersecurity practitioners is not always possible, and this influences South Africa's ability to prevent and defend itself against cyberattacks. The analysis performed confirmed that the public sector is a prime target for cyberattacks, emphasising the need for more investment in cybersecurity in this sector.

Slow development of cybercrime legislation

In general, South Africa has been slow to adopt cybercrime legislation. However, in 2021, PoPIA came into full effect and the Cybercrimes Bill was also signed into law (Act 19 of 2020) (Bhagattjee, Govuza, & Westcott, 2021). Both PoPIA and the Cybercrimes Act should influence the ability to conduct illegal operations. For example, disclosure of data breaches, as required by PoPIA, will offer more insight into the tactics deployed by such cyberattacks, which can guide the deployment of defensive measures in the future. Such insights are of great importance due to the considerable increases in cyberattacks causing data leakage in recent years.

Lack of awareness of cyber threats

As the use of technological solutions rises, more South African citizens are exposed to cyber threats—confirmed by the increase in cyber incidents witnessed in the past decade. Such an increase in cyber incidents, especially incidents causing accidental data exposure or compromised websites, shows that South Africans are inexperienced and lack technical alertness when operating in the cyber domain. Such a lack of awareness causes South Africans to be ideal targets for cyber attackers.

Increasing use of IT

Reliance on IT by South Africans increases the cyber threat landscape. Insights drawn from the analysis performed revealed that IT systems within the telecommunication sector fell victim to security flaws on several occasions. Such technologies, applications, and infrastructure pose a significant risk, especially if used inappropriately (e.g., default configurations or unpatched security weaknesses), with limited knowledge, or without the necessary approval (e.g., legacy systems).

Cyber attackers taking notice
The continual exposure of South Africa's vulnerable cyber threat landscape will undoubtedly grab the attention of other, more advanced cyber attackers. Based on the growth shown in Figure 4, cyber incidents affecting South Africa are expected to increase. While previous cyber attackers primarily targeted the public sector, attackers are widening their attack plane to other sectors such as construction, manufacturing, and healthcare. South Africa's cyber threat landscape is, therefore, expected to remain diverse and complex.

Reducing risks in the cyber threat landscape
The factors outlined above show that South Africa is currently positioned, in many respects, as an ideal target for cyberattacks. Nevertheless, some steps can be taken to reduce the number of risk factors present in South Africa's cyber threat landscape and thus reduce the attack surface:

Adopt a defence-in-depth approach
A military strategy often used in information security, defence in depth, offers a multi-layered security approach. The approach relies on the use of various security controls strategically placed throughout an IT system. The multiple security controls offer redundancy, in case a single security control fails, or a vulnerability is exploited. Redundancy is achieved by incorporating physical (e.g., locks and security guards), technical (e.g., firewalls and intrusion detection systems), and administrative (e.g., policies and procedures) controls.

Promote a security-focused cyber culture
Regular training, education, and user awareness sessions are necessary to promote a security-focused cyber culture. Not all employees are cyber-savvy and might be unaware of the potential risks associated with their online behaviour in the cyber domain. It is, therefore, important to teach employees best practices about cybersecurity, as well as the procedures to follow should an attack occur.

Utilise threat intelligence
Originally only available to well-funded organisations, threat intelligence has become more accessible due to open-source feeds. However, the providers of threat intelligence have little to no presence in South Africa. Insights derived from the threat intelligence are heavily slanted towards developed countries and might not be relevant to the South African context. The Council for Scientific and Industrial Research (CSIR) is developing a technological solution that aims to function as the primary source for cybersecurity data collection in South Africa (Burke et al., 2021). The threat intelligence derived from the collected cybersecurity data sets will have a strictly South African focus, offering a valuable source of information to better understand threats and anticipate attacks.

Focus on compliance
The first step to ensure protection against cyberattacks is to apply recommended standards and best practices (e.g., the NIST Cybersecurity Framework or ISO/IEC 27001). Furthermore, the development of an appropriate cybersecurity policy, which outlines detailed plans, rules, and practices regulating access to an organisation's system and information source, is imperative. Finally, an incident response plan must be put in place to ensure employees can respond appropriately should an incident occur.

Collaborate and report
South Africa's economic challenges can cause cybersecurity to receive less attention than required. For example, the public sector—affected by 36% of the cyber incidents identified by this study in the period 2010–2020—requires improved cyber defences but lacks financial stability. Collaboration, often described as the future of cybersecurity, offers a cost-effective means to share cyber threat information, improve preparedness, and overcome cybersecurity skill shortages. The national CSIRT is ideally situated to drive collaboration concerning cybersecurity within South Africa.

Reporting functions can include maintenance of a publicly available cyber threat dashboard of the kind provided above in section 3. This kind of visualisation of cyber incidents offers an overview of South Africa's cyber threat landscape and enables trend analysis. Such consolidated information can be used to extract intelligence to better prepare and defend against potential cyberattacks. It is recommended that a dashboard of this sort be established, published via appropriate platforms (e.g., the national CSIRT), and regularly updated, to enable all stakeholders in South Africa to have insight into the country's existing cyber threat landscape.

Be prepared for when, not if
For South African organisations, it is not a question of *if* a cyberattack will occur, but rather a question of *when*. Organisations must ensure that the required people, processes, and technologies are in place to identify, protect, detect, respond to, and recover from cyberattacks.

5. Conclusion
The purpose of this study was to investigate South Africa's current cyber threat landscape by reviewing noteworthy cyber incidents that have occurred in the past decade. In total, 74 cyber incidents were analysed. As the reliance on IT infrastructure and internet connectivity increases, South Africa's potential exposure to cyber threats will also continue to rise. As shown by this study, the most common type of cyber incident affecting South African organisations in the past decade was found to be incidents causing *data exposure*. The most frequent perpetrators were found to be a *criminally* motivated *hackers*. And the sector most often targeted was the public sector (27 known incidents between 2010 and 2020).

The prevalence of cyber incidents can be expected to continue in the coming years. South African organisations need to be cognisant of cyber threats and prepare financially viable defences. However, the inadequate reporting of cyber incidents is creating a void that limits our understanding of South Africa's cyber threat landscape. Improved collaboration with regard to the collection, analysis, and reporting of cyber incidents, guided by appropriate authorities such as the National CSIRT, is required.

The insights produced by this study, as summarised in the proposed dashboard, offer a starting point for collaborative efforts that can enable South African organisations to be better prepared and better defended against forthcoming cyberattacks.

References

Bhagattjee, P., Govuza, A., & Westcott, R. (2021, June 9). Regulating the Fourth Industrial Revolution - South Africa's Cybercrimes Bill is signed into law. Cliffe Dekker Hofmeyr.

Bing, C., & Kelly, S. (2021, May 8). Cyber attack shuts down U.S. fuel pipeline 'jugular,' Biden briefed. *Reuters*. https://www.reuters.com/technology/colonial-pipeline-halts-all-pipeline-operations-after-cybersecurity-attack-2021-05-08/

Brush, K. (n.d.). Cybercrime. TechTarget. https://searchsecurity.techtarget.com/definition/cybercrime

Burke, I., Motlhabi, M., Netshiya, R., & Pieterse, H. (2021). Lost packet warehousing service. In *Proceedings of the 16th International Conference on Cyber Warfare and Security* (pp. 501–508). ACI.

BusinessTech. (2014, October 30). Vodacom exposing subscriber details. https://businesstech.co.za/news/mobile/72054/vodacom-exposing-subscriber-details/

BusinessTech. (2016, February 16). Hackers leak SA government's sensitive financial data. https://businesstech.co.za/news/government/112817/hackers-leak-sa-governments-sensitive-financial-data/

Duffy, C. (2021, March 10). Here's what we know so far about the massive Microsoft Exchange hack. *CNN*. https://edition.cnn.com/2021/03/10/tech/microsoft-exchange-hafnium-hack-explainer/index.html

Dullabh, R., & Gabryk, N. (2021, April 13). *South Africa: Preparing for POPIA: Data breach response*. *Mondaq*. https://www.mondaq.com/southafrica/data-protection/1055314/preparing-for-popia-data-breach-response

Eaton, C., & Volz, D. (2021, May 19). Colonial Pipeline CEO tells why he paid hackers a $4.4 million ransom. *Wall Street Journal*. https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636

Gandhi, R. A., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q., & Laplante, P. A. (2011). Dimensions of cyber-attacks: Cultural, social, economic, and political. *IEEE Technology and Society Magazine*, *30*(1), 28–38. https://doi.org/10.1109/MTS.2011.940293

Goldstuck, A. (2021, August 1). Transnet cyber hack a warning of risk to SA. *BusinessLive*. https://www.businesslive.co.za/bt/business-and-economy/2021-08-01-transnet-cyber-hack-a-warning-of-risk-to-sa/

ITWeb. (2020, June 14). Postbank to replace 12m bank cards after security breach. https://www.itweb.co.za/content/nWJadvbekrmqbjO1

Kakareka, A. (2014). Detecting system intrusions. In J. R. Vacca (Ed.), *Network and system security* (2nd ed.) (pp. 1–27). Syngress. https://doi.org/10.1016/B978-0-12-416689-9.00001-0

Kumar, R., Raj, P., & Perianayagam, J. (2019). A framework to detect compromised websites using link structure anomalies. In S. Omar, S. W. Haji, & S. Phon-Amnuaisuk (Eds.), *Advances in intelligent systems and computing: Proceedings of the Computational Intelligence in Information Systems conference (CIIS 2018)* (pp. 72–84). Springer. https://doi.org/10.1007/978-3-030-03302-6_7

Mcanyana, W., Brindley, C., & Seedat, Y. (2020). *Insight into the cyberthreat landscape in South Africa.* Accenture.

McKane, J. (2020a, November 10). ANC Youth League website hacked. *MyBroadband*. https://mybroadband.co.za/news/government/374940-anc-youth-league-website-hacked.html

McKane, J. (2020b, November 30). Absa hit by data breach. *MyBroadband*. https://mybroadband.co.za/news/security/378358-absa-hit-by-data-breach.html

Mikhaylova, G. (2014). *The "Anonymous" movement: Hacktivism as an emerging form of political participation.* Texas State University, San Marcos.

Moyo, A. (2017, June 29). DBE web site hacked, pro-Islamic State messages posted. *ITWeb*. https://www.itweb.co.za/content/x4r1lyMRgpjqpmda

Moyo, A. (2019a, October 25). City of Joburg hit by cyber attack. *ITWeb.* https://www.itweb.co.za/content/dgp45qaG8gZ7X9l8

Moyo, A. (2019b, October 25). Bad day for SA's cyber security as banks suffer DDoS attacks. *ITWeb*. https://www.itweb.co.za/content/LPp6V7r4OVzqDKQz

Moyo, A. (2019c, September 13). Garmin SA hacked, exposing users' credit card details. *ITWeb*. https://www.itweb.co.za/content/O2rQGMApY5G7d1ea

Moyo, A. (2019d, October 28). Liquid Telecom, Webafrica hit by DDoS attacks. *ITWeb.* https://www.itweb.co.za/content/GxwQDM1A339MlPVo

Moyo, A. (2020a, August 19). Experian hacked, 24m personal details of South Africans exposed. *ITWeb*. https://www.itweb.co.za/content/rxP3jqBmNzpMA2ye

Moyo, A. (2020b, February 5). Tracker hack hints at more ransomware attacks in SA. *ITWeb*. https://www.itweb.co.za/content/LPp6VMr4YxNvDKQz

Moyo, A. (2021, July 22). Transnet suffers "disruption" of IT systems. *ITWeb*. https://www.itweb.co.za/content/wbrpOqgYAwY7DLZn

Muller, R. (2013, December 30). My Vodacom security flaw exposes subscriber details. *MyBroadband*. https://mybroadband.co.za/news/security/94234-my-vodacom-security-flaw-exposes-subscriber-details.html

Mungadze, S. (2020, June 9). Life Healthcare Group hit by cyber attack amid COVID-19. *ITWeb.* https://www.itweb.co.za/content/JBwErvnBK4av6Db2

MyBroadband. (2012, December 9). South African websites hacked. https://mybroadband.co.za/news/security/66474-south-african-websites-hacked.html

MyBroadband. (2014, September 21). Mass hacking of South African websites. https://mybroadband.co.za/news/security/110316-mass-hacking-of-south-african-websites.html

MyBroadband. (2016, May 30). MTN exposing subscribers' personal details online. https://mybroadband.co.za/news/cellular/166734-mtn-exposing-subscribers-personal-details-online.html

MyBroadband. (2017, May 21). Telkom systems crippled by WannaCry ransomware. https://mybroadband.co.za/news/security/211576-telkom-systems-crippled-by-wannacry-ransomware.html

MyBroadband. (2018, July 7). South African presidency website hacked. https://mybroadband.co.za/news/security/267491-south-african-presidency-website-hacked.html

Mzekandaba, S. (2019, July 23). SASSA web site remains down after hack. *ITWeb*. https://www.itweb.co.za/content/rxP3jqBpVJ27A2ye

Ngqakamba, S. (2021, September 9). Justice department's IT system brought down in ransomware attack. *News24*. https://www.news24.com/news24/southafrica/news/justice-departments-it-system-brought-down-in-ransomware-attack-20210909

Rawlins, L. K. (2017, June 28). Hackers again prove their global power. *ITWeb.* https://www.itweb.co.za/content/nLPp6VMrdbzvDKQz

Republic of South Africa (RSA). (2013). Protection of Personal Information Act (POPIA) 4 of 2013.

Sabillon, R., Cano, J., Cavaller, V., & Serra, J. (2016). Cybercrime and cybercriminals: A comprehensive study. *International Journal of Computer Networks and Communications Security*, *4*(6), 165–176.

Slabbert, A., & Peyper, L. (2021, August 1). Transnet attack is cyber warfare. *City Press.* https://www.news24.com/citypress/business/transnet-attack-is-cyber-warfare-20210801

Trautman, L. J., & Ormerod, P. (2019). Wannacry, ransomware, and the emerging threat to corporations. *Tennessee Law Review*, *86*(503), 504–556. https://doi.org/10.2139/ssrn.3238293

Trend Micro. (2017). *Ransomware: Past, present, and future*. https://documents.trendmicro.com/assets/wp/wp-ransomware-past-present-and-future.pdf

Van Heerden, R. P., Irwin, B., Burke, I. D., & Leenen, L. (2012). A computer network attack taxonomy and ontology. *International Journal of Cyber Warfare and Terrorism (IJCWT)*, *2*(3), 12–25. https://doi.org/10.4018/ijcwt.2012070102

Van Heerden, R. P., Von Soms, S., & Mooi, R. (2016). Classification of cyber attacks in South Africa. In IEEE (Ed.), *2016 IST-Africa Week Conference* (pp. 1–16). https://doi.org/10.1109/ISTAFRICA.2016.7530663

Van Niekerk, B. (2017). An analysis of cyber-incidents in South Africa. *The African Journal of Information and Communication (AJIC)*, *20*, 113–132. https://doi.org/10.23962/10539/23573

Vermeulen, J. (2016, February 12). Massive number of South African websites hacked by Anonymous. *MyBroadband*. https://mybroadband.co.za/news/security/155040-massive-number-of-south-african-websites-hacked-by-anonymous.html

Vermeulen, J. (2019, November 25). Massive DDoS attacks – South African internet providers crippled. *MyBroadband*. https://mybroadband.co.za/news/internet/329539-massive-ddos-attacks-south-african-internet-providers-crippled.html

Vermeulen, J. (2020a, May 27). Data leak on UIF COVID-19 relief scheme website. *MyBroadband.* https://mybroadband.co.za/news/cloud-hosting/353473-data-leak-on-uif-covid-19-relief-scheme-website.html

Vermeulen, J. (2020b, October 1). Ransomware group claims hack on Office of the Chief Justice. *MyBroadband*. https://mybroadband.co.za/news/security/369503-ransomware-group-claims-hack-on-office-of-the-chief-justice.html

Vermeulen, J. (2020c, November 7). Ransomware group releases data after attack on Office of the Chief Justice. *MyBroadband*. https://mybroadband.co.za/news/security/374310-ransomware-group-releases-data-after-attack-on-office-of-the-chief-justice.html

Willett, M. (2021). Lessons of the SolarWinds hack. *Survival*, *63*(2), 7–26. https://doi.org/10.1080/00396338.2021.1906001

Wyatt, M. (2021, March 16). Responding to the Microsoft Exchange Hack. Wall Street Journal Pro Cybersecurity Research.

Intermediation Capabilities of Information and Communication Technologies (ICTs) in Ghana's Agricultural Extension System

Nyamwaya Munthali
Thesis Supervisor, Postgraduate Studies Department, University of Lusaka
https://orcid.org/0000-0001-9713-3632

Rico Lie
Assistant Professor, Knowledge, Technology and Innovation Group, Wageningen University, The Netherlands
https://orcid.org/0000-0003-4228-5107

Ron van Lammeren
Associate Professor, Laboratory of Geo-Information Science and Remote Sensing, Wageningen University, The Netherlands
https://orcid.org/0000-0002-5062-882X

Annemarie van Paassen
Associate Professor, Knowledge, Technology and Innovation Group, Wageningen University, The Netherlands
https://orcid.org/0000-0001-5341-3114

Richard Asare
Country Representative, International Institute of Tropical Agriculture, Accra
https://orcid.org/0000-0002-5557-9190

Cees Leeuwis
Professor, Knowledge, Technology and Innovation Group, Wageningen University, The Netherlands
https://orcid.org/0000-0003-1146-9413

Abstract

Information and communication technologies (ICTs), specifically those that are digital and interactive, present opportunities for enhanced intermediation between actors in Ghana's agricultural extension system. To understand these opportunities, this study investigates the capabilities of ICTs in support of seven forms of intermediation in the context of agricultural extension: *disseminating (information)*, *retrieving (information)*, *harvesting (information)*, *matching (actors to services)*, *networking (among actors)*, *coordinating (actors)*, and *co-creating (among actors)*. The study identifies the types of ICTs currently functioning in Ghana's agricultural system, and applies a Delphi-inspired research design to determine the consensus and dissensus of researchers, scientists, and practitioners about the potential of these ICTs to sup-

port each of the seven intermediation capabilities. The findings reveal that experts reached consensus that interactive voice response (IVR) technologies currently have the highest potential to support *disseminating*, *retrieving*, *harvesting*, and *matching*. Meanwhile, social media messaging (SMM) technologies are currently seen as highly capable of supporting *coordinating* and, to a lesser extent, *co-creating*, but no consensus is reached on the potential of any of the technologies to support *networking*.

Keywords
information and communication technology (ICT), agricultural innovation systems (AIS), ICT for agriculture (ICT4ag), agricultural extension, intermediation, intermediation capabilities, Ghana

Acknowledgements
This research was co-funded by the Wageningen University Interdisciplinary Research and Education Fund (INREF) and the Consultative Group on International Agricultural Research's (CGIAR's) Research Program on Maize (MAIZE). The research was further supported by the CGIAR donors,[1] and by the Consortium for Improving Agriculture-based Livelihoods in Central Africa (CIALCA), which is funded by Belgian Directorate General for Development Cooperation and Humanitarian Aid (DGD).

DOI: https://doi.org/10.23962/10539/32212

Recommended citation
Munthali, N., Lie, R., Van Lammeren, R., Van Paassen, A., Asare, R., & Leeuwis, C. (2021). Intermediation capabilities of information and communication technologies (ICTs) in Ghana's agricultural extension delivery. *The African Journal of Information and Communication (AJIC), 28*, 1-37. https://doi.org/10.23962/10539/32212

1 See https://www.cgiar.org/funders/

1. Introduction

Agricultural productivity growth in Ghana, necessary to bridge the gap between potential and actual production of food and cash crops, is partly hampered by the prevailing approach to agricultural extension service delivery (Abdulai et al., 2020; Bua et al., 2020; McNamara et al., 2014; MOFA, 2007; World Bank, 2017). This approach is typified by extension largely focused on knowledge and technology transfer to farmers, rather than taking on broader roles (e.g., knowledge brokering, facilitating access to credit, and supporting market linkages) and serving a broader stakeholder base (Agyekumhene et al., 2018; Munthali et al., 2018). The narrow focus of this extension approach is problematic because farmers have multi-faceted production needs, and "improving food production […] is not just a matter of individuals [farmers] receiving messages and adopting the right technologies [from scientists/researchers], but has much more to do with altering interdependencies and coordination between various actors" (Leeuwis, 2004, p. 18).

More specifically, the prevailing extension approach fails to adequately coordinate the set of organisations[2] that support value chain actors[3] in emergent problem-solving (e.g., with respect to climate change impacts), facilitating business linkages between these actors, and facilitating the integration of scientific and other knowledges to produce appropriate knowledge and technology for value chain actors (Abdu-Raheem & Worth, 2016; Asiedu-Darko & Bekoe, 2014; McNamara et al., 2014). These drawbacks in the national extension system hamper production (Msuya & Wambura, 2016; Zwane, 2020).

Since 1996, statements of national agricultural policy objectives in Ghana have consistently posited that reorganisation and improved coordination in the sector are key to agricultural development and climate change adaptation (DAES, 2011; Sigman, 2015; Sova et al., 2014; World Bank, 2017). Based on this policy direction, proposed structural changes in the Ghanaian extension service delivery system have included accommodating private extension organisations to meet the high demand for extension services, value chain-focused interventions, and innovation platforms (Adekunle & Fatunbi, 2014; Agyekumhene et al., 2018; McNamara et al., 2014; Van Paassen et al., 2013). Thus, the extension ideology has broadened, since the 1990s, to include calls not only for top-down, one-size-fits-all approaches (i.e., training and visitation) but also for participatory and bottom-up approaches (e.g., farmer field schools) (DAES, 2011; Davis, 2008). The most recent Ghanaian extension framework is an

2 Research institutions, educational institutions, non-governmental organisations, development organisations, other government institutions, credit providers, weather service providers, transporters, and private extension service providers.
3 Farmers, input suppliers, processors, exporters, traders, retailers, wholesalers, packaging manufacturers, and other manufacturers.

integrated pluralistic extension system (Abdu-Raheem & Worth, 2016; Sigman, 2015). This approach envisages strengthened research–extension linkages, broader service delivery lines, and a larger number of service providers, with the intention of meeting the demand of farmers and other value chain actors for extension services.

Ghana's current extension ideology aligns with the agricultural innovation systems (AIS) perspective. With a view to fostering innovation in agriculture, the AIS perspective focuses on influencing relationships between multiple actors and on the conditions (e.g., policies) that affect the actors' (collective) operations (Klerkx & Leeuwis, 2008; Leeuwis, 2004; Swanson & Rajalahti, 2010). According to the AIS perspective, the focus on multiple actors' relationships is necessary because: (1) innovation occurs when interaction between diverse stakeholders is increased and open, resulting in improved knowledge exchange and access to appropriate knowledge and technology; and (2) innovation requires networking through which actors form partnerships that allow them to access business development opportunities and engage in collective action to respond to systemic challenges holistically (Koutsouris, 2012; Swanson & Rajalahti, 2010; World Bank, 2012).

Extension approaches based on the AIS perspective involve three broad intermediary roles: *demand articulation*, *matching demand and supply*, and *innovation process management*. Demand articulation involves the engagement of sector stakeholders in activities such as joint needs identification, participatory problem diagnosis and assessment, and making interdependencies explicit (Klerkx & Gildemacher, 2012). Matching demand and supply involves establishing sector contacts and developing mutually beneficial relationships—advice, credit, input, and market linkages (Howells, 2006). Lastly, innovation process management comprises the creation of discussion and negotiation space for actors to coordinate and jointly mitigate constraints, maintain relationships, and engage in knowledge-sharing and integration or co-production for continuous innovation (Leeuwis, 2010; Vitos et al., 2013).

Despite Ghana's national agricultural policy direction transitioning to an AIS-based extension approach, barriers still stand in the way of both public and private extension organisations on the path to facilitating this new direction. These factors include financial constraints (e.g., untimely and limited funding), human resource constraints (e.g., freezes in hiring staff, limited staff numbers), and skill set-related constraints (e.g., limited adaptation on the part of educational institutions to develop the facilitation capabilities of extension staff) (MOFA, 2007; Obeng et al., 2019; Sova et al., 2014).

At the same time, Ghana is a key African player in the innovative use of digital information and communication technology (ICT) (GSMA, 2019). Digital ICTs are now central to most spheres of development (Sein et al., 2019; United Nations, 2020), as represented by the ICT for development (ICT4D) discipline, which is focused on "the application of any entity that processes or communicates digital data

in order to deliver some part of the international development agenda in a developing country" (Heeks, 2017, p. 10). Among the key ICTs and ICT-enabled services harnessed for developmental purposes are interactive voice response (IVR), short message service (SMS), unstructured supplementary service data (USSD), social media (e.g., WhatsApp, Facebook), and document and data management systems (e.g., Open Data Kit). Such ICTs and ICT-enabled services present new opportunities for connectivity and information sharing to enhance communication-related service delivery (Bell, 2015; Gershon & Bell, 2013). Therefore, these technologies are being explored by scientists, researchers, and development practitioners to respond to the limitations of classical approaches to extension and interaction in Ghana's agricultural system (Cieslik et al., 2018; Fielke et al., 2020; Gakuru et al., 2009; MEST, n.d.; Qiang et al., 2012).

Currently, there is limited literature assessing the capability of different types of ICTs to drive agricultural innovation processes (Fielke et al., 2020; Van Osch & Coursaris, 2013). One such rare study presents an assessment by European experts of the capability of social media and other web-based platforms to act as drivers of agricultural innovation (Hansen et al., 2014). The study finds that a number of the platforms (particularly social media) have high capacity to support the following specific social networking functions that support innovation: discussion (Facebook, NING, ERFALAND, and Yammer); networking (Facebook, LinkedIn, and NING); crowdsourcing (ResearchGate and Crowdsourcing); cooperation (Yammer, ResearchGate, and Wikipedia); and co-production (ResearchGate and Wikipedia). However, the aforementioned European-focused study (Hansen et al., 2014) assesses forms of media that are often not easily accessible in African agricultural contexts, where farmers are typically located in rural settings with limited access to the internet and to mobile devices that support internet services (Aker, 2011; Nyamekye, 2020). Thus, the opportunities for ICTs presented in the Hansen et al. (2014) study cannot be fully leveraged in many African agricultural systems.

In this study we seek to address a research gap through the identification of opportunities for ICTs to support intermediation capabilities relevant to AIS-based extension service delivery, in an African setting—specifically Ghana. The study identifies opportunities through a consensus-building exercise that captures the perspectives of scientists and researchers in the fields of communication, innovation, and development informatics; and practitioners of ICT for agriculture (ICT4Ag).

2. Conceptual context and analytical framework

In this section we start by discussing bridging mechanisms as an overarching concept that incorporates the core concept of this study, which is intermediation capabilities. We highlight the possibility of ICTs functioning as bridging mechanisms and, in doing so, supporting extension organisations in facilitating AIS-based extension service delivery. We also outline the types of intermediation relevant to this facilitation process, and the intermediation capabilities that the ICTs may support. We conclude the section by stating the research questions.

ICTs functioning as bridging mechanisms

Farmers operate in multi-faceted production environments. Enhancing the performance of the Ghanaian agricultural sector, therefore, requires improved information (knowledge) flows among agricultural stakeholders and improved business linkages. The major stakeholders in the agricultural system are knowledge technology providers and users. Their interaction and knowledge exchange need to be enhanced, along with that of other value chain actors who currently only have loose linkages (Adolwa et al., 2017; Asiedu-Darko, 2013; McNamara et al., 2014). The other main actors in the system are bridging organisations that are involved in facilitating interaction and linkages between stakeholders (Kilelu et al., 2011; World Bank, 2012). Bridging organisations are defined by Berkes et al. (2003) as organisations that provide an arena for knowledge co-production, trust-building, sense-making, learning, vertical and horizontal collaboration, and conflict resolution.

From an innovation systems perspective, bridging organisations are regarded as intermediaries, which are "persons or organisations that, from a relatively impartial third-party position, purposefully catalyse innovation through bringing together actors and facilitating their interaction" (Klerkx & Gildemacher, 2012, p. 221). For many developing countries, it has been argued that agricultural bridging functions are best suited to, and easily assimilated by, public extension organisations, even

though other organisations (e.g., private extension organisations, non-governmental organisations (NGOs), farmer-based organisations, and research institutions) have been involved in the role (Kilelu et al., 2011). In the case of Ghana, for extension organisations to assimilate the bridging role in line with the AIS-based approach (Abdu-Raheem & Worth, 2016; Sigman, 2015), they "are required to expand their role from that of a one-to-one intermediary between research and farmers" to that which "creates many-to-many relationships to facilitate access to knowledge, skills, services, and goods from a wide range of organisations" (Kilelu et al., 2011, p. 89).

However, various other actors in agricultural systems can also take on bridging functions. These include sector-focused networks, trade associations, special government programmes, consultants, input suppliers, and, with direct relevance to this study, ICTs (Kilelu et al., 2011; Klerkx & Gildemacher, 2012). ICTs can serve as bridging mechanisms (Hansen et al., 2014; World Bank, 2012), and can be leveraged by extension organisations and other extension actors in support of functioning better as bridging organisations and engaging in AIS-based extension service delivery.

Intermediation

Hansen et al. (2014) assess the ability of social media and other ICT-enabled tools to drive agricultural innovation based on six "social network functions": *networking*, *cooperating*, *co-producing*, *crowdsourcing*, *discussing*, and *engaging*. Using this framework, Hansen et al. (2014) engaged innovation systems experts to assess the extent to which different forms of social media and other web-based platforms (e.g., YouTube, ResearchGate, LinkedIn, Facebook, Twitter) support particular networking functions that may facilitate collaboration for sharing ideas and for mobilising knowledge and resources circulating in other arenas (Granovetter, 1973; Kaushik et al., 2018).

In the African context, ICTs have been found to facilitate aspects of AIS-based extension service delivery by enabling multiple actors to network and engage in joint needs identification, knowledge-sharing, and problem-solving to meet information needs in farming systems (Ajani, 2014; Fabregas et al., 2019; Munthali et al., 2018). Mobile applications have, for example, been recognised for their ability to improve value chain linkages (Ajani, 2014; Zwane, 2020), to build timely monitoring systems (e.g., with geo-referenced data) on environmental issues and production, and to provide timely advice to enable farmers to respond to farming challenges (Gbangou et al., 2020; McCole et al., 2014).

That said, it is important to note that, in general, most studies of the role of ICTs in agricultural extension focus on the use of specific ICT tools (typically mobile apps) to provide market, technical, and weather information to farmers, rather than on ICTs' impact, or potential impact, on the provision of AIS-based extension (Aker et al., 2016; Misaki et al., 2018). Furthermore, despite ICTs falling within the typology of intermediaries that can facilitate interaction and linkages between AIS actors to foster innovation, most studies of innovation intermediaries focus on the functioning and influence of other types of intermediaries, e.g., consultants targeting individual farmers and small and medium-sized enterprises (SMEs) in the agri-food sector; consultants targeting farmer collectives and agri-food SMEs; peer network brokers; education brokers; systemic intermediaries; and research councils (Kilelu et al., 2011; Kivimaa et al., 2019; Winch et al., 2007). Therefore, existing literature does not clarify which ICTs among those available in Ghana or other African countries are most capable of supporting the specific types of intermediation required to facilitate AIS-based extension service delivery activities in these contexts. Additionally, there has been little consideration of how experts, from the academically oriented to the more location-specific and practice-oriented, look at the potential of various kinds of ICTs to augment extension service delivery.

To address these knowledge gaps, our study explored the views of communication and innovation scientists, development informatics researchers, and ICT4Ag practitioners on the current opportunities for ICTs to enhance intermediation functions within agricultural extension service delivery in Ghana.

Analytical framework: Intermediation capabilities

The framework we deployed in the study builds on the aforementioned social network functions framework of Hansen et al. (2014). Our framework modifies the Hansen et al. (2014) networking functions—*engagement*, *discussion*, *crowdsourcing*, *networking*, *co-production* and *cooperation*—by:

- merging three overlapping functions (engagement, discussion, cooperation) into two broader functions (*coordinating* and *co-creating*); and
- including additional functions (*harvesting*, *matching*, *coordinating*) relevant to facilitating AIS-based extension delivery.

Overall, we broaden the work of Hansen et al. (2014) to reflect networking as well as communication functions relevant to facilitating AIS-based extension service delivery, and we refer to these functions collectively as

intermediation capabilities. The seven intermediation capabilities in our framework—*disseminating (information)*, *retrieving (information)*, *harvesting (information)*, *matching (actors to services)*, *networking (among actors)*, *coordinating (actors)*, and *co-creating (among actors)*—are detailed below in Table 1.

Table 1: Intermediation capabilities

Intermediation capability	Description
Disseminating (information)	Enabling content to be spread widely, alerting or attracting the interest of or raising the awareness of a large group of geographically dispersed actors
Retrieving (information)	Enabling actors to retrieve information (e.g., price, weather) from a central database or to retrieve documents out of a central repository
Harvesting (information)	Enabling the gathering of feedback, ideas, and opinions through the contributions of a large group of geographically dispersed actors e.g., crowdsourcing or polling
Matching (actors to services)	Enabling supply and demand linkages – actors are able to query, consult, or search information systems and connect to advice or services
Networking (among actors)	Enabling contact between actors so that they make direct connections and are able to interact to form new (business) relationships or reinforce existing relationships
Coordinating (actors)	Facilitating virtual multi-actor engagement[4] to provide open and live communication channels that enable discussion for coordinated action e.g., acting together towards a common purpose or engaging in joint problem-solving
Co-creating (among actors)	Facilitating a common working space for multiple actors to combine and contribute contextual knowledge or information, and engage in document sharing and information storage towards a tangible output

Source: Adapted from Hansen et al. (2014), with insights from Leeuwis (2004) and Howells (2006)

Taking the intermediation capabilities listed in Table 2 as a reference, this study sought to answer the following research questions:

- How do experts assess the extent to which different ICTs support specific intermediation capabilities?
- What type of consensus or dissensus do experts reach over which ICTs can support which specific intermediation capabilities?
- What factors are contributing to consensus and dissensus among experts about which ICTs can support which specific intermediation capabilities?

4 Multi-actor engagement in this study refers to virtually connecting and placing more than one actor in a virtual "room" and around a virtual "table" where they can engage in, or take advantage of, one-to-many and many-to-many communication (i.e., have a back-and-forth exchange/interaction).

3. Methods

In this section, we report on the scoping exercise that was conducted to identify the ICTs currently being used in the Ghanaian agricultural system. The outcomes of this scoping study provided the basis for engagement with experts on their views. The section also explains the set-up of the Delphi-inspired study, which was designed to establish experts' consensus and dissensus with respect to the intermediation capabilities of the different types of ICTs that were identified through the scoping exercise.

Scoping exercise

We reviewed ICT4Ag literature on Ghana, and engaged with organisations rolling out ICT initiatives discovered in the literature, in order to identify the ICTs being used in the Ghanaian agricultural system (Aker et al., 2016; Gakuru et al., 2009; Qiang et al., 2012; World Bank, 2014). Through these scoping activities we developed an inventory of ICT4Ag platforms (see Appendix). We then examined the inventory and were able to identify nine different types of ICTs in use (see Table 2).

Table 2: Types of ICTs identified in Ghana's agricultural system

Type		Interface	Data format	Comm-unication	Mobile device needed	Minimum network needed
short message service (SMS)	SMS pull	SMS request typing	text	one-to-one	any phone	2G
	SMS push	SMS based reading	text	one-to-many	any phone	2G
interactive voice response (IVR)	IVR inbound	request-based talking and listening	audio	one-to-one	any phone	2G
	IVR outbound	request-based talking and listening	audio	one-to-many	any phone	2G
unstructured supplementary service data (USSD)		request-based typing and reading	text	one-to-one	any phone	2G
social media messaging (SMM)		request-based typing and reading	text, audio, pictorial, video	one-to-many	smart phone	4G
data management (DaM)		data gathering	text, audio, pictorial, global navigation satellite system (GNSS)	one-to-one or one-to-many	smart phone	4G
document management (DoM)		document sharing	text, audio, pictorial, video, GNSS	one-to-many	smart phone	4G
spatial (Spa)		mapping	GNSS	one-to-one or one-to-many	smart phone	4G

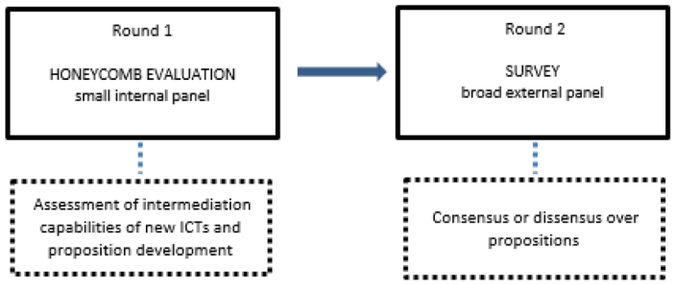
Delphi-inspired expert consensus-building study

Building on the scoping study, we developed an expert consensus-building method that was inspired by the Delphi study approach. A Delphi study is defined as "a method for systematic solicitation for judgements on a particular topic through a set of carefully designed sequential questionnaires interspersed with summarised information and feedback of opinions derived from earlier responses" (Chu & Hwang, 2008, p. 2828). It involves a "group facilitation technique, which is an iterative multistage process, designed to transform opinion into group consensus" (Hasson et al., 2000, p. 1) among experts (Benitez-Capistros et al., 2014). Benitez-Capistros et al. (2014) define an expert as a person who is competent as an authority on particular facts.

The content validity of the Delphi is enhanced by avoidance of data collection in a group setting where more dominant actors' opinions may be captured (Hasson et al., 2000). Furthermore, Delphi data collection involves more than one round of questioning, which increases concurrent validity of the method (Hasson et al., 2000), and because consensus-building is the objective of the Delphi approach, the number of these rounds is undefined and dependent on when consensus emerges or increases among participants (Benitez-Capistros et al., 2014). According to Hasson et al. (2000) and Doria et al. (2009), acceptable majorities in a Delphi-derived consensus can range from a basic majority (50–59%) to a low (60–69%), medium (70–79%) or high (≥ 80%) majority.

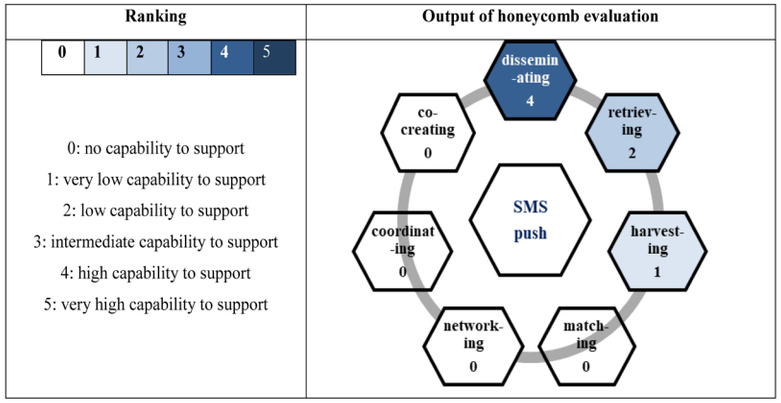
There are variations in the set-up of Delphi studies (Allen et al., 2019; Chu & Hwang, 2008). Our Delphi-inspired expert consensus-building method involved two rounds, and for each round the expert panel composition varied to fit a particular purpose (see Figure 1).

Figure 1: Summary of expert consensus-building method



First round: Honeycomb evaluation by internal panel of experts
The first round involved a small internal panel composed of the research team: four experts in the domain of communication and innovation science. The experts each individually engaged in a honeycomb evaluation to assess the intermediation capabilities of the various ICTs (see example in Figure 2) and ranked the different ICTs in relation to the seven intermediation capabilities in our framework. The ranking was based on a Likert scale ranging from "0" (no capability to support) to "5" (strong capability to support). Based on the individual honeycomb evaluations, we calculated the average rank assigned by the experts to each type of technology for each type of intermediation capability.

Figure 2: Example of honeycomb evaluation output (for "SMS push technology")



The aggregated and averaged results of the four internal experts' honeycomb evaluations were then presented to the entire internal panel to facilitate a convergence forum. The convergence forum gave the experts the opportunity to reflect on the aggregated results in relation to their individual responses, discuss areas of divergence, and ultimately reach agreement on the indicative intermediation capabilities of the different ICTs. The forum also enabled the experts to identify the significant results of the honeycomb evaluation from which 16 propositions were developed for the second round of the expert consensus-building method.

Second round: Online survey of 11 external experts
In the second round, the 16 propositions were packaged into a questionnaire format, using a five-point Likert scale that ranged from "1" (strongly disagree) to "5" (strongly agree). The questionnaire was presented to a broader expert panel made up of Ghana-focused development informatics researchers and ICT4Ag practitioners.

Potential respondents were identified from a list of invitees to a workshop convened in Accra, Ghana by the Environmental Virtual Observatories for Connective Action (EVOCA) research programme in April 2019, which targeted Ghanaian agricultural stakeholders. Additional researchers and practitioners were identified as potential respondents through a search in the SCOPUS abstract and citation database of peer-reviewed research literature. The search was composed of two steps: (1) a search using the function "(mobile technology or ICT) AND (extension or agriculture) AND (Ghana)"; and (2) screening the articles captured in the search to establish whether they were on topic and, where applicable, to identify authors who could be invited to participate in the survey.

In total, 22 potential respondents—13 researchers and nine ICT4Ag practitioners—were identified and sent an email invitation to engage in the study by completing the online questionnaire, which was administered via the web-based platform Google Forms. Of the invitees, 11 (five researchers and six practitioners—see Table 3) responded to the questionnaire during the two-week period given for responses.

Table 3: Eleven respondents

Respondent's organisation	Respondent's designation
Researchers	
Centre for Agriculture and Bioscience International, Ghana	junior researcher/project manager
University for Development Studies, Ghana	lecturer
Wageningen University, The Netherlands	PhD researcher (Ghana-focused)
Council for Scientific and Industrial Research, Ghana	junior researcher
Kumasi Institute of Technology Energy and Environment, Ghana	senior researcher
Practitioners	
Esoko, Ghana	senior manager
Grameen Foundation, Ghana	senior manager
Farm Radio International, Ghana	middle manager
Maclear Technology, Ghana	senior technical advisor
Ministry of Food and Agriculture, Ghana	district agricultural officer
Ministry of Food and Agriculture, Ghana	senior manager, extension directorate

For round two, the descriptive statistics analysed for each proposition included the mean (*qi*), the median (*Q2*), and the frequency of ranking for each point on the Likert scale. Based on these statistics, we determined whether there was positive consensus (agreement) or negative consensus (disagreement) about a proposition, or whether there was dissensus (varied ranking or polarisation) about a proposition. We considered three criteria to determine whether consensus was reached and to determine the direction of the consensus for each proposition (Table 4). These criteria were (1) the position of the mean on the Likert scale (Chu & Hwang, 2008); (2) the position of the mean in relation to the median in the data distribution (Chu & Hwang, 2008); and (3) the significance of the percentage of participants ranking a proposition on the Likert scale, ranging from low to medium to high to very high (Doria et al., 2009; Hasson et al., 2000).

Table 4: Criteria determining consensus over a proposition

Rule		Positive consensus	Dissensus	Negative consensus
1	Position of mean on Likert scale	*q*i > 3.5	2.5 > *qi* < 3.5	*qi* < 2.5
2	Position of mean in relation to median of data distribution	*qi* < Q2, indicating there is a right-skewed distribution	Q2 < *qi* < Q3, indicating there is a normal distribution	*qi* > Q2, indicating there is a left-skewed distribution
3	Position of majority ranking on Likert scale	very high consensus: ≥80% agree; high consensus: 70–79% agree; medium consensus: 60–69% agree	low consensus: 50–59% dis(agree) or <60% dis(agree)	very high consensus: ≥80% disagree; high consensus: 70–79% disagree; medium consensus: 60–69% disagree

Focus group discussion

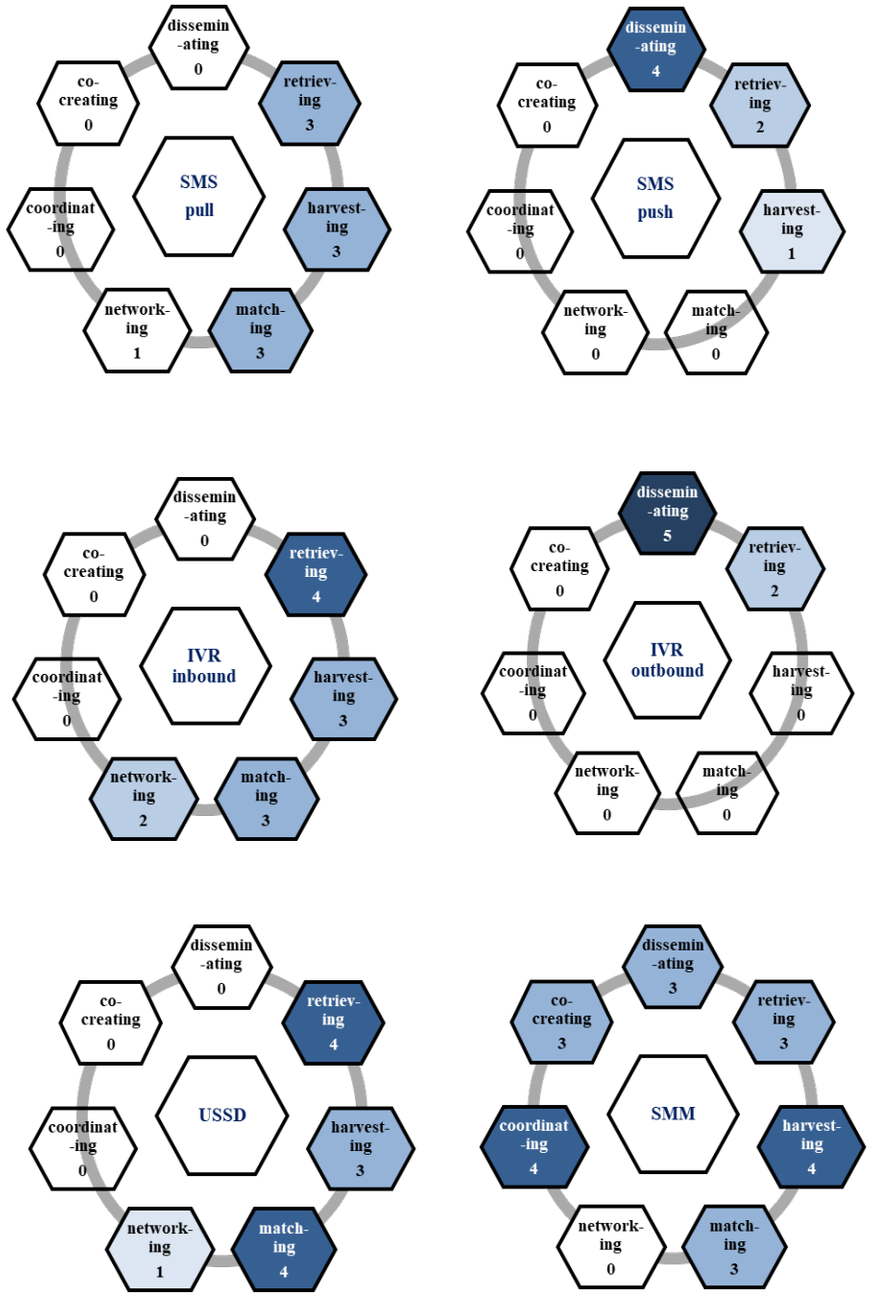
In addition to the expert consensus-building method, a focus group discussion was conducted to establish factors contributing to (positive or negative) consensus and dissensus (varying views or polarisation) over the propositions. The focus group discussion took place during the EVOCA programme's Ghana workshop. The workshop attracted 19 participants and, as part of the workshop proceedings, the participants were selectively split into four working groups that each comprised all the categories of participants present at the event (mainly various kinds of technology users). One of the working groups comprised five workshop participants who took part in the focus group: two public extension staff members, two ICT-based NGO representatives, and a small-scale farmer. We presented the aggregated questionnaire results to the focus group, and they reflected on the results and engaged in an open discussion on whether or not they agreed with them in general, and why. The discussion was recorded to facilitate thematic analysis of the plausible factors contributing to consensus and dissensus on the propositions.

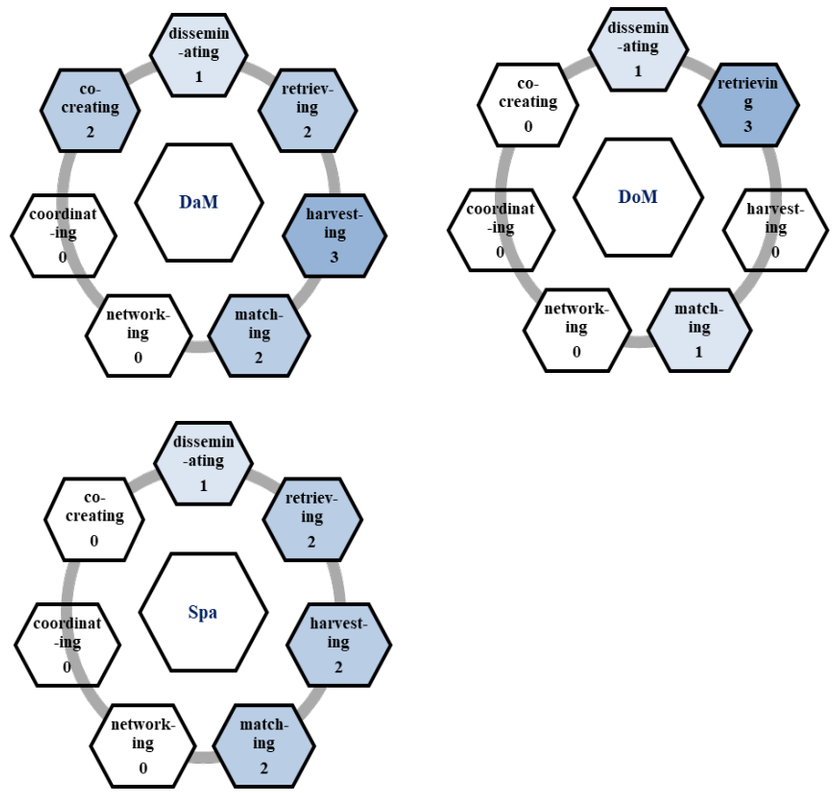
4. Findings

First round of consensus-building

The first round of the expert consensus-building, with the four-person internal panel of experts, collated views on the intermediation capability (high to low) of each ICT identified in the Ghanaian agricultural system (see Figure 3). In terms of the ICTs with a high capability to support intermediation capabilities (ranking > 3), the aggregated results of the honeycomb evaluation show that interactive voice response (IVR) outbound technologies were viewed as having very high capability to support *disseminating*, and IVR inbound technologies were viewed as having high capability to support *retrieving*. In addition, short message service (SMS) push technologies were seen as having a high capability to support *disseminating*, and unstructured supplementary service data (USSD) technologies were viewed as having a high capability to support *retrieving* and *matching*. Furthermore, the aggregated results showed that social media messaging (SMM) technologies had a high capability to support *harvesting* and *coordinating*, and an intermediate capability to support all the other intermediation capabilities, excluding *networking*.

Figure 3: First round of consensus-building: Aggregated results of honeycomb evaluation (nine honeycomb images)





With respect to technologies found to have a low capability to support specific intermediation capabilities (ranking < 3), the panel of internal experts reached consensus that spatial (Spa) technologies generally had a low capability to support all the intermediation capabilities. The panel also reached consensus that SMS pull technologies, data management (DaM) technologies, and document management (DoM) technologies also did not rank highly (ranking > 3) in terms of their capability to support any intermediation. The assessment also found that all ICTs had a low capability to support networking.

Second round of consensus-building

Based on the aggregated results of the first round of consensus-building, the four-person internal expert panel developed a number of propositions, 16 of which (see Table 5) were used to develop the online survey questionnaire for the second round.

Table 5: The 16 propositions (P1 to P16) used in second round of consensus-building

Intermediation capability	Proposition	
Disseminating (information)	P1	At present, among all the ICTs identified, IVR outbound technologies have the highest capability for disseminating information to rural farmers.
	P2	At present IVR outbound technologies have higher capability than SMS push technologies for disseminating information to rural farmers.
	P3	SMM technologies have high potential to facilitate disseminating information to rural farmers in the next 10 years.
Harvesting (information)	P4	At present, among all the ICTs identified, IVR inbound technologies have the highest capability for harvesting information from rural farmers.
	P5	At present IVR inbound technologies have higher capability than USSD technologies for harvesting information from rural farmers.
	P6	SMM technologies have higher potential than IVR inbound technologies for harvesting information from rural farmers in the next 10 years.
Retrieving (information)	P7	At present, among all the ICTs identified, IVR inbound technologies have the highest capability for allowing rural farmers to retrieve information.
	P8	At present USSD technologies have the highest capability for rural farmers to retrieve information than the other types of technologies.
	P9	SMM technologies have high potential for rural farmers to retrieve information in the next 10 years
Matching (actors to services)	P10	At present, among all the ICTs identified, USSD technologies have the highest capability to match rural farmers to services.
	P11	At present IVR inbound technologies have higher capability than USSD technologies to match rural farmers to services.
Networking (among actors)	P12	At present all the technologies identified have low capability to facilitate networking between rural farmers and other agricultural stakeholders.
	P13	SMM technologies have high potential to facilitate networking between rural farmers and other agricultural stakeholders in the next 10 years.
Coordinating (actors)	P14	At present, among all the ICTs identified, SMM technologies have the highest capability to facilitate coordination between rural farmers and other agricultural stakeholders.
Co-creating (among actors)	P15	At present SMM technologies have intermediate capability to facilitate co-creating among rural farmers and other agricultural stakeholders.
	P16	SMM technologies have high potential to facilitate co-creating among rural farmers and other agricultural stakeholders in the next 10 years.

The propositions were also developed within a specific context to aid the panel of external experts in assessing which ICTs were likely to be best suited to facilitate certain communication and networking functions in extension activities. The internal panel (more academic-oriented), therefore, required the external panel of respondents (more Ghana-specific and practice-oriented) to envision themselves as district extension staff tasked by the "Ministry of Agriculture – Headquarters" to qualify or disqualify the preliminary assessment of the current capability and future potential of specific ICTs to improve extension service delivery involving rural farmers.

Experts' consensus on propositions

The results of round two showed that seven of the 16 propositions presented to the external experts were marked by positive consensus (Table 6). Additionally, the questionnaire results showed that there was no negative consensus among the external experts about any of the propositions.

Table 6: Propositions associated with positive consensus

Type of ICT	Proposition		Criteria for positive consensus		
			Crit. 1	Crit. 2	Crit. 3
			qi > 3.5	*qi* < *Q2*	(strongly) Agree %
IVR inbound	P4	At present, [...] IVR inbound technologies have the highest capability for harvesting information from rural farmers.	3.55 > 3.5	3.55 < 4	63.64
	P7	At present, [...] IVR inbound technologies have the highest capability for rural farmers to retrieve information.	3.73 > 3.5	3.73 < 4	72.73
	P11	At present IVR inbound technologies have higher capability than USSD technologies to match rural farmers to services.	3.73 > 3.5	37.3 < 4	81.82
IVR outbound	P1	At present, [...] IVR outbound technologies have the highest capability for disseminating information to rural farmers.	3.64 > 3.5	3.64 < 4	72.73
	P2	At present IVR outbound technologies have higher capability than SMS push technologies for disseminating information to rural farmers	3.73 > 3.5	3.73 < 4	72.73
SMM	P14	At present, [...] SMM technologies have the highest capability to facilitate coordination between rural farmers and other agricultural stakeholders.	3.82 > 3.5	3.82 < 4	72.73
	P15	At present SMM technologies have intermediate capability to facilitate co-creating among rural farmers and other agricultural stakeholders.	3.82 > 3.5	3.82 < 4	90.91
Abbreviations: qi = mean; Q2 = median					

As seen in Table 6, there was positive consensus among the experts that:

- IVR inbound technologies currently have the highest capability for *harvesting* information from farmers (P4), for supporting farmers in *retrieving* information (P7), and for *matching* farmers with advice and services (P11);
- IVR outbound technologies currently have the highest capability for *disseminating* information to farmers (P1); and
- SMM technologies currently have the highest capability to support *coordinating* between agricultural stakeholders (P14) including farmers, and intermediate-level capability to facilitate *co-creating* by these stakeholders (P15).

Experts' dissensus over propositions

The experts did not reach consensus on nine of the 16 propositions (Table 7). This dissensus was determined on the basis that the propositions failed to meet all three of the consensus criteria outlined earlier.

Table 7: Propositions associated with dissensus

Type of ICT		Proposition	Criteria for dissensus					
			Crit. 1	Crit. 2		Crit. 3		
			2.5 > qi < 3.5	Q2 < qi	qi < Q3	(strongly) Disagree %	Neutral %	(strongly) Agree %
IVR inbound	P5	At present IVR inbound technologies have higher capability than USSD technologies for harvesting information from rural farmers.	2.5 > 3.36 < 3.5	4 > 3.36	3.36 < 4	18.18	27.27	54.55
USSD	P8	At present, [...] USSD technologies have the highest capability for rural farmers to retrieve information.	2.5 > 2.73 < 3.5	2 < 2.73	2.73 < 4	54.55	9.09	36.36
	P10	At present, [...] , USSD technologies have the highest capability to match rural farmers to services.	2.5 > 2.73 < 3.5	2 < 2.73	2.73 < 4	54.55	9.09	36.36
SMM	P3	SMM technologies have high potential to facilitate the dissemination of information to rural farmers in the next 10 years.	2.5 > 3 < 3.5	3 > 3.00	3.00 < 3.5	36.36	36.36	27.27
	P6	SMM technologies have higher potential than IVR inbound technologies for harvesting information from rural farmers in the next 10 years.	2.5 > 3.18 < 3.5	3 < 3.18	3.18 < 4	18.18	36.36	45.45
	P9	SMM technologies have high potential for rural farmers to retrieve information in the next 10 years.	2.5 > 3.18 < 3.5	4 > 3.18	3.18 < 4	36.36	9.09	54.55
	P13	SMM technologies have high potential to facilitate networking between rural farmers and other agricultural stakeholders in the next 10 years.	2.5 > 3.27 < 3.5	3 < 3.27	3.27 < 4	36.36	18.18	45.45
	P16	SMM technologies have high potential to facilitate co-creating among rural farmers and other agricultural stakeholders in the next 10 years.	2.5 > 3.55 > 3.5	4 > 3.55	3.55 < 4	18.18	27.27	54.55
All	P12	At present all the technologies identified have low capability to facilitate networking between rural farmers and other agricultural stakeholders.	2.5 > 2.55 < 3.5	2 < 2.73	2.55 < 4	54.55	0.00	45.45

Abbreviations: qi: mean; Q2: median; Q3: "middle" value in the second half of the rank-ordered data

Specifically, as seen in Table 7, it was found that experts had varied views on:

- whether IVR inbound technologies currently have a higher capability than USSD technologies to facilitate the *harvesting* of information from rural farmers (P5);
- the current capability of USSD technologies to facilitate *retrieving* of information by rural farmers (P8), or to facilitate *matching* of farmers with agricultural services (P10);
- the current capability of all the technologies identified to support *networking* between rural farmers and other agricultural stakeholders (P12);
- the future potential of SMM technologies to facilitate *disseminating*, *harvesting* and *retrieving* information targeted at or involving farmers (P3, P6, P9); and
- the future potential of SMM technologies to support *networking* and *co-creating* between agricultural stakeholders (P13, P16).

Focus group findings: Factors contributing to consensus and dissensus

Consensus on high capabilities of IVR technology

The focus group discussion revealed two factors contributing to the external experts' consensus on the high intermediation capabilities of IVR inbound and outbound technologies at present, as described above. One factor was that IVR technologies operate on basic and feature mobile phones (i.e., non-smart phones) that are accessible to rural Ghanaian farmers. The other factor was that IVR technologies, unlike SMS or USSD technologies, generate audio as opposed to textual content. This makes them more compatible with the generally low literacy levels of the farmers. In the words of one focus group participant:

> At the moment, IVR is known widely and used because it is programmed in a language that the end user understands. It does not involve text messages and is available on any kind of phone.

Consensus and dissensus on capabilities of SMM technology

The focus group also established the reasons behind experts' consensus on certain intermediation capabilities of SMM technologies and dissensus on other SMM capabilities. The consensus on the high capability of SMM technologies to support *coordinating* between agricultural stakeholders, at present, was found in the focus group to be a result of the view that SMM technologies facilitate, to a greater extent than other ICTs, rapid and easy interaction and feedback. Another reason for the consensus on the high capability of SMM for coordinating, at present, was the assumption that most coordination functions involve service providers (e.g., extension agents) working together with lead farmers, i.e., with lead farmers who, because they have

higher literacy levels and greater financial means than the average farmers, are likely to have access to the smartphones necessary for the use of SMM technologies. According to a focus group participant:

> Social media applications are the medium of swift information exchange and facilitation at the moment. […] because of the infiltration of cheaper smartphones [...] most lead farmers have this platform [WhatsApp], which makes them easily organise meetings, and solicit for assistance and information from each [agricultural] actor when need be.

Meanwhile, the consensus on SMM technologies' current capability to support *co-creating* was that the capability is only at an intermediate level. On this point, it was found in the focus group that the experts took into consideration that many rural farmers currently lack access to smartphones that support the use of SMM technologies, and also that the generally low levels of literacy of farmers affects their ability to engage intensively with or on SMM technologies. In relation to these challenges with farmers taking advantage of SMM technologies, some experts pointed to alternative communication mechanisms, such as face-to-face meetings, being more appropriate than SMM, at present, for facilitating co-creation involving rural Ghanaian farmers.

Moving to the factors contributing to the dissensus regarding the future intermediation capabilities of SMM in *disseminating*, *retrieving*, and *harvesting* information, the variation in views was found in the focus group to be due to different levels of optimism among the focus group participants on rural farmers' future access to smartphones and the farmers' future literacy levels. The more optimistic respondents were confident in farmers' increased access to smartphones and increased literacy over the next 10 years. Representing the optimistic view, one focus group participant argued as follows:

> [...] but it [the situation] is not static. Maybe in 10 years the youth will become more active farmers and be more inclined to use WhatsApp.

However, pessimistic views were also expressed. For example, one focus group respondent stated:

> [...] right now it has been tagged that you [farmers] need a lot of money to get a smartphone, let alone the [poor] internet connectivity within rural areas.

Another focus group participant added an additional pessimistic view:

> I am not even looking at the costs of [mobile data] bundles. Let's look at how old the active rural farmers will be and what their educational level will be. When you talk about the farmers now, most of them are within the range of 30–35 and they will be 40–50 in the next 10 years. In the next 10 years we will be dealing with the same crop of farmers. Therefore, I do not expect to see significant changes in relation to their adoption of such new technology [SMM technologies].

5. Discussion and conclusion

The starting point of this study was that ICTs have the capacity to respond to information- and interaction-related needs in Ghana's agricultural extension service delivery. Through the inputs of a total of 15 varied experts in two rounds, we assessed the capability of nine types of ICTs operating in Ghana to support specific communication and networking functions (intermediation capabilities) that are required to facilitate AIS-based extension service delivery. In this section we highlight the results, specifically instances of positive consensus and of dissensus, in experts' views on the intermediation capabilities of the ICTs identified, and discuss these instances with reference to the reasoning provided by the focus group participants and in the context of existing literature. Based on this analysis and discussion we point out opportunities for specific ICTs to support certain communication and networking functions that are required to facilitate AIS-based extension service delivery, as well as alternative scenarios. Finally, this section reflects on the validity of the Delphi-inspired research design and highlights potential areas for future research.

Positive consensus over technologies' intermediation capabilities

Below we discuss and identify opportunities for IVR and SMM technologies to support intermediation.

IVR technologies

The results show that experts reached positive consensus on the high capability of IVR technologies to support *disseminating*, *retrieving*, and *harvesting* information, at present, and to support *matching* actors to services targeted at rural farmers, also at present. These findings are congruent with previous research pointing to IVR technology having great potential to reach farmers directly (Dittoh et al., 2013; McNamara et al., 2014). It is clear that many scientists, researchers, and practitioners view IVR technologies as being appropriate for supporting these specific communication functions involving rural communities. This is largely because, as found in our focus group discussion and also as argued in the literature, these technologies are audio-based and thus fit rural farmers' literacy levels, and these technologies are supported by the low-cost basic and feature mobile phones that most rural farmers can readily access (Aker et al., 2016; Dittoh et al., 2013; Schmidt et al., 2010).

SMM technologies

We also found that there was positive consensus among experts on the high capabilities of SMM technologies to support *coordinating* between farmers and other agricultural actors at present. Therefore, in this case, it is also clear that various experts, including Fabregas et al. (2019), see opportunities for SMM technologies to support the coordination of activities involving farmers and other agricultural actors. Furthermore, according to the focus group and other studies, the consensus reported is due to SMM technologies enabling speedy information dissemination and immediate feedback (Bennett & Segerberg, 2012; Munthali et al., 2018; Stevens et al., 2016).

However, despite the full spectrum of SMM technologies' features, the study found that these technologies only have the potential to support a certain type of coordinating—not as defined in Table 2. The focus group reported that SMM technologies tended to be used by lead farmers to interact with agricultural stakeholders (other than farmers) on a one-on-one basis. Specifically, focus group participants indicated that lead farmers use SMM technologies for speedy one-to-one communication with these other agricultural stakeholders to support aspects of coordination (e.g., organising meetings)—as Martin and Hall (2011) also report—as opposed to using the technologies to facilitate many-to-many communication to support, for instance, multi-actor (stakeholder) knowledge exchange and joint problem-solving. The SMM technologies were not cited as having the potential to facilitate virtual, multi-actor open and live communication for coordinated action to solve emerging problem. Thus, there are indications that the possibilities of leveraging SMM technologies' ability to facilitate multi-actor discursive spaces are currently limited in Ghana's extension practice.

Last, various experts were of the collective view that at present SMM technologies have only intermediate capabilities to support *co-creating* involving rural farmers and other agricultural stakeholders. Thus, the experts saw SMM technology as currently having neither high nor low capability to support the co-creating function, which requires multi-actor engagement and many-to-many communication. The focus group participants provided insights into factors contributing to this survey outcome. Certain focus group discussants were optimistic about farmers' educational levels and smartphone access increasing in the near future, thus allowing farmers to engage with SMM technologies that have the technical capacity to support engagement and communication for co-creating. Other focus group participants held a pessimistic view on the matter.

Dissensus over technologies' intermediation capabilities

Experts did not reach positive or negative consensus on a number of propositions. They had a mix of positive, neutral, and negative views on these propositions. We now discuss and identify these instances of dissensus in relation to intermediation via IVR, USSD, and SMM technologies.

IVR technologies

There was dissensus among the experts in our study on whether IVR inbound technologies have a higher capability than USSD technologies to support *harvesting*, at present. At the same time, and as already mentioned, there was positive consensus among the experts that IVR inbound technologies have the highest capability, among all the technologies identified (including USSD), to support this communication function. A plausible explanation for these inconsistent findings is that experts judged IVR inbound and USSD technologies, comparatively, as possessing equal technical abilities to support harvesting, but when explicitly asked which technology had the highest potential to retrieve information directly from farmers in the Ghanaian context, they identified IVR inbound technologies. Moreover, the existing literature, the analysis in the previous section on positive consensus, and the focus group inputs all point to a finding that IVR inbound technologies are best suited to support direct harvesting of information from Ghanaian rural farmers as these technologies support audio content and operate on basic mobile phones (Aker et al., 2016).

USSD technologies

We found that there was no consensus among experts regarding USSD technologies' capability, at present, to support farmers in *retrieving* information or *matching* actors (farmers) to services over other ICTs. This dissensus was based on the competing pessimistic and optimistic views of experts on farmers' literacy levels. Meanwhile, the focus group and the literature point to IVR technologies having higher capacity to support these communication functions in comparison to other technologies. For example, Perrier et al. (2015) state that IVR technology is better-suited than USSD to reach literacy-constrained audiences.

SMM technologies

There was also dissensus among experts on the future potential of SMM technologies to support *disseminating*, *harvesting*, and *retrieving* targeted at rural farmers, or *networking* and *co-creating* involving rural farmers and other agricultural stakeholders. This outcome could be attributed to the competing and diverging views of experts, as already mentioned above, on the future dynamics of farmers' access to, and use of, the mobile smartphones that support these technologies.

For the networking function specifically, the findings above related to SMM technologies—and the dissensus found on the propostion that all the technologies identified have low capability to support networking at present—lead to the conclusion that it is unclear which ICTs are best suited to support the function.

Unlike the aforementioned findings on experts' views on the possibility of leveraging SMM technologies to support networking in the Ghanaian context, the Hansen study (Hansen et al., 2014) found that social media currently has high potential, in the European context, to support networking and co-creating. The difference between the Hansen at al. (2014) findings and those of this study point to two issues that require consideration. The first issue is that the findings of the European-focused study could largely be influenced by the context—a context in which farmers have higher literacy levels and easier access to smartphones than farmers in most African countries (ITU, 2021). The second issue is that at present, as suggested by this study's focus group participants, networking intermediation capabilities are likely to be best-supported, in contexts such as those found in Ghana, by alternative communication mechanisms such as conventional face-to-face meetings, which remain relevant in the functioning of agricultural systems where intensive interaction is required (Leeuwis et al., 2018; Materia et al., 2015). Such communication mechanisms have been cited (Molony, 2006) as trusted social networking methods that, in the African context, are the most appropriate modes of interaction given the prevailing literacy levels and types of mobile phones owned in rural agricultural settings (Dittoh et al., 2013).

Validity of the consensus-building method

It is necessary to reflect on the validity of the expert consensus-building method that we applied in this study. In line with Delphi's general principles, our consensus-building method included more than one round of individual responses by experts (Hasson et al., 2000). However, our approach deviated from a typical Delphi in that it did not require that the same experts be involved in each of the two rounds. For our method, each set of experts was engaged for the distinct purpose of one round, so that we fostered concurrent validity by aggregating the views of a small group of experts in the first round and then presenting these views, for affirmation and/or refutation, to a broader expert panel in a following round. We developed this approach so as to allow the views of the internal expert panel (communication and innovation experts) to be subjected to assessment by experts who are more engaged than the internal panel with the Ghanaian context, and so as to be able to establish consensus and dissensus among a wide range of experts. Furthermore, a Delphi study is typically considered valid based on the input of 16 to 60 experts (Hasson et al., 2000). However, lower numbers of experts have been reported in other Delphi studies (Benitez-Capistros et al., 2014). It is our view that the inputs of the 15 experts in this study provide valuable insights because the design of the consensus-building method fostered concurrence validity.

Future research

Opportunities for future research can be identified from this study. Further research could shed light on ICTs' application and role in supporting broader (AIS-based) extension service delivery. This study is an experts' assessment of the intermediation capabilities of technologies identified in Ghana and provides insights into how experts view specific ICTs' potential to support communication and networking functions relevant to AIS-based extension service delivery. Going forward, empirical research is recommended to establish how the technologies practically support extension activities involved in AIS-based extension service delivery, in a variety of contexts.

Based on the findings of this study and related literature, it is probable that certain ICTs can currently support certain AIS-based extension activities. IVR technologies may support the broadcasting of knowledge and early warning alerts to rural stakeholders as part of coordination efforts in problem-solving, and enable the stakeholders to retrieve knowledge and other information (e.g., on weather, prices) (Aker et al., 2016). IVR technologies could also match farmers with service providers and suppliers, as well as allow for the harvesting of information from farmers and other rural stakeholders (Viamo, 2020) as inputs for systemic problem diagnosis. On the other hand, the technologies identified do not seem to have the potential to support multi-stakeholder engagement for collaborative problem diagnosis and problem-solving. This is based on two considerations: (1) this study found no clarity on whether any of the ICTs identified support the *networking* function; and (2) SMM technologies currently have the potential to largely support only one-to-one communication and coordination. Furthermore, given this study's finding that SMM technologies have only an intermediate capability to support *co-creating,* it is therefore unclear whether these technologies can fully support the combining of knowledge to facilitate innovation among agricultural stakeholders in extension practice.

References

Abdu-Raheem, K. A., & Worth, S. H. (2016). Suggesting a new paradigm for agricultural extension policy: The case of West African countries. *South African Journal of Agricultural Extension (SAJAE)*, *44*(2), 216–230. https://doi.org/10.17159/2413-3221/2016/v44n2a425

Abdulai, I., Hoffmann, M. P., Jassogne, L., Asare, R., Graefe, S., Tao, H. H., Muilerman, S., Vaast, P., Van Asten, P., Läderach, P., & Rötter, R. P. (2020). Variations in yield gaps of smallholder cocoa systems and the main determining factors along a climate gradient in Ghana. *Agricultural Systems*, *181*, 102812. https://doi.org/10.1016/j.agsy.2020.102812

Adekunle, A. A., & Fatunbi, A. O. (2014). A new theory of change in African agriculture. *Middle-East Journal of Scientific Research*, *21*(7), 1083–1096. https://doi.org/10.5829/idosi.mejsr.2014.21.07.21564

Adolwa, I. S., Schwarze, S., Bellwood-Howard, I., Schareika, N., & Buerkert, A. (2017). A comparative analysis of agricultural knowledge and innovation systems in Kenya and Ghana: Sustainable agricultural intensification in the rural–urban interface. *Agriculture and Human Values*, *34*(2), 453–472. https://doi.org/10.1007/s10460-016-9725-0

Agyekumhene, C., De Vries, J. R., Van Paassen, A., Macnaghten, P., Schut, M., & Bregt, A. (2018). Digital platforms for smallholder credit access: The mediation of trust for cooperation in maize value chain financing. *NJAS – Wageningen Journal of Life Sciences*, *86–87*(July), 77–88. https://doi.org/10.1016/j.njas.2018.06.001

Ajani, E. N. (2014). Promoting the use of information and communication technologies (ICTs) for agricultural transformation in sub-Saharan Africa: Implications for policy. *Journal of Agricultural & Food Information*, *15*(1), 42–53. https://doi.org/10.1080/10496505.2013.858049

Aker, J. C. (2011). Dial "A" for agriculture: A review of information and communication technologies for agricultural extension in developing countries. *Agricultural Economics*, *42*(6), 631–647. https://doi.org/10.1111/j.1574-0862.2011.00545.x

Aker, J. C., Ghosh, I., & Burrell, J. (2016). The promise (and pitfalls) of ICT for agriculture initiatives. *Agricultural Economics*, *47*, 35–48. https://doi.org/10.1111/agec.12301

Allen, T., Prosperi, P., Cogill, B., Padilla, M., & Peri, I. (2019). A Delphi approach to develop sustainable food system metrics. *Social Indicators Research*, *141*(3), 1307–1339. https://doi.org/10.1007/s11205-018-1865-8

Asiedu-Darko, E. (2013). Agricultural extension delivery in Ghana: A case study of factors affecting it in Ashanti, Eastern and Northern regions of Ghana. *Journal of Agricultural Extension and Rural Development*, *5*(2), 37–41.

Asiedu-Darko, E., & Bekoe, S. (2014). ICTs as enablers in the dissemination of agricultural technologies: A study in the East Akim District, Eastern Ghana. *Asian Journal of Agricultural Extension, Economics & Sociology*, *3*(3), 224–232. https://doi.org/10.9734/ajaees/2014/7661

Bell, M. (2015). *Information and communication technologies for agricultural extension and advisory services: ICT – Powering behavior change for a brighter agricultural future*. MEAS Discussion Paper. https://meas.illinois.edu/wp-content/uploads/2015/04/Bell-2015-ICT-for-Brighter-Ag-Future-MEAS-Discussion-Paper.pdf

Benitez-Capistros, F., Hugé, J., & Koedam, N. (2014). Environmental impacts on the Galapagos Islands: Identification of interactions, perceptions and steps ahead. *Ecological Indicators*, *38*(2014), 113–123. https://doi.org/10.1016/j.ecolind.2013.10.019

Bennett, W. L., & Segerberg, A. (2012). The logic of connective action: Digital media and the personalization of contentious politics. *Information, Communication & Society*, *15*(5), 739–768. https://doi.org/10.1080/1369118X.2012.670661

Berkes, F., Colding, J., & Folke, C. (2003). *Navigating social-ecological systems: Building resilience for complexity and change*. Cambridge University Press.

Bua, S., El Mejahed, K., MacCarthy, D., Adogoba, D. S., Kissiedu, I. N., Atakora, W. K., Fosu, M., & Bindraban, P. S. (2020). Yield responses of maize to fertilizers in Ghana. In *IFDC FERARI Research Report*. https://www.ifdc.org/projects/

Chu, H. C., & Hwang, G. J. (2008). A Delphi-based approach to developing expert systems with the cooperation of multiple experts. *Expert Systems with Applications*, *34*(4), 2826–2840. https://doi.org/10.1016/j.eswa.2007.05.034

Cieslik, K. J., Leeuwis, C., Dewulf, A. R. P. J., Lie, R., Werners, S. E., Van Wessel, M., Feindt, P., & Struik, P. C. (2018). Addressing socio-ecological development challenges in the digital age: Exploring the potential of Environmental Virtual Observatories for Connective Action (EVOCA). *NJAS – Wageningen Journal of Life Sciences*, *86–87*(2018), 2–11. https://doi.org/10.1016/j.njas.2018.07.006

Davis, K. E. (2008). Extension in Sub-Saharan Africa: Overview and assessment of past and current models, and future prospects. *Journal of International Agricultural and Extension Education*, *15*(3), 15–28.

Directorate of Agricultural Extension Services of Ghana (DAES). (2011). *Agricultural extension approaches being implemented in Ghana*. https://www.g-fras.org/en/reviews-assesments/item/949-agricultural-extension-approaches-being-implemented-in-ghana.html

Dittoh, F., Van Aart, C., & De Boer, V. (2013). Voice-based marketing for agricultural products: A case study in rural Northern Ghana. In *ICTD '13: Proceedings of the Sixth International Conference on Information and Communications Technologies and Development: Notes* (Vol. 2) (pp. 21–24). https://doi.org/10.1145/2517899.2517924

Doria, M. de F., Boyd, E., Tompkins, E. L., & Adger, W. N. (2009). Using expert elicitation to define successful adaptation to climate change. *Environmental Science and Policy*, *12*(7), 810–819. https://doi.org/10.1016/j.envsci.2009.04.001

Fabregas, R., Kremer, M., & Schilbach, F. (2019). Realizing the potential of digital development: The case of agricultural advice. *Science*, *366*(6471), 1–9. https://doi.org/10.1126/science.aay3038

Fielke, S., Taylor, B., & Jakku, E. (2020). Digitalisation of agricultural knowledge and advice networks: A state-of-the-art review. *Agricultural Systems*, *180*(2020), 1–11. https://doi.org/10.1016/j.agsy.2019.102763

Gakuru, M., Winters, K., & Stepman, F. (2009). *Innovative farmer advisory services using ICT*. https://www.w3.org/2008/10/MW4D_WS/papers/fara.pdf

Gbangou, T., Ludwig, F., Van Slobbe, E., Greuell, W., & Kranjac-Berisavljevic, G. (2020). Rainfall and dry spell occurrence in Ghana: Trends and seasonal predictions with a dynamical and a statistical model. *Theoretical and Applied Climatology*, *141*, 371–387. https://doi.org/10.1007/s00704-020-03212-5

Gershon, I., & Bell, J. A. (2013). Introduction: The newness of new media. *Culture, Theory and Critique*, *54*(3), 259–264. https://doi.org/10.1080/14735784.2013.852732

Granovetter, M. S. (1973). The strength of weak ties. *American Journal of Sociology*, *78*, 1360–1380. https://doi.org/10.1086/225469

GSMA. (2019). *618 active tech hubs: The backbone of Africa's tech ecosystem*. Mobile Innovation. https://www.gsma.com/mobilefordevelopment/blog/618-active-tech-hubs-the-backbone-of-africas-tech-ecosystem/

Hansen, J. P., Jespersen, L. M., Brunori, G., Jensen, A. L., Holst, K., Mathiesen, C., Halberg, N., & Ankjær Rasmussen, I. (2014). ICT and social media as drivers of multi-actor innovation in agriculture. In *World Congress on Computers in Agriculture and Natural Resources* (pp. 1–8). https://doi.org/10.13140/2.1.3549.8242

Hasson, F., Keeney, S., & McKenna, H. (2000). Research guidelines for the Delphi survey technique. *Journal of Advanced Nursing*, *32*(4), 1008–1015. https://doi.org/10.1046/j.1365-2648.2000.t01-1-01567.x

Heeks, R. (2017). *Information and communication technology for development (ICT4D)*. Routledge. https://doi.org/10.4324/9781315652603

Howells, J. (2006). Intermediation and the role of intermediaries in innovation. *Research Policy*, *35*(2006), 715–728. https://doi.org/10.1016/j.respol.2006.03.005

International Telecommunication Union (ITU). (2021). *Connectivity in the least developed countries: Status report*.

Kaushik, P., Chowdhuy, A., Odame, H. H., & Van Passen, A. (2018). Social media for enhancing stakeholders' innovation networks in Ontario, Canada. *Journal of Agricultural & Food Information*, *19*(1), 1–23. https://doi.org/10.1080/10496505.2018.1430579

Kilelu, C. W., Klerkx, L., Leeuwis, C., & Hall, A. (2011). Beyond knowledge brokering: An exploratory study on innovation intermediaries in an evolving smallholder agricultural system in Kenya. *Knowledge Management for Development Journal*, *7*(1), 84–108. https://doi.org/10.1080/19474199.2011.593859

Kivimaa, P., Boon, W., Hyysalo, S., & Klerkx, L. (2019). Towards a typology of intermediaries in sustainability transitions: A systematic review and a research agenda. *Research Policy*, *48*(4), 1062–1075. https://doi.org/10.1016/j.respol.2018.10.006

Klerkx, L., & Gildemacher, P. (2012). The role of innovation brokers in agricultural innovation systems. In *Agricultural innovation systems: An investment sourcebook* (pp. 221–230). https://doi.org/10.1787/9789264167445-19-en

Klerkx, L., & Leeuwis, C. (2008). Institutionalizing end-user demand steering in agricultural R&D: Farmer levy funding of R&D in the Netherlands. *Research Ethics*, *37*(3), 460–472. https://doi.org/10.1016/j.respol.2007.11.007

Koutsouris, A. (2012). Facilitating agricultural innovation systems: A critical realist approach. *Studies in Agricultural Economics*, *114*, 64–70. https://doi.org/10.7896/j.1210

Leeuwis, C. (2004). *Communication for rural innovation: Rethinking agricultural extension*. Blackwell Science. http://www.modares.ac.ir/uploads/Agr.Oth.Lib.8.pdf#page=20&zoom=auto,-161,323

Leeuwis, C. (2010). Changing views of agricultural innovation: Implications for communicative intervention and science. In F. G. Palis, G. R. Singleton, M. C. Casimero, & B. Hardy (Eds.), *Research to impact: Case studies for natural resource management for irrigated rice in Asia* (pp. 15–32). International Rice Research Institute.

Leeuwis, C., Cieslik, K. J., Aarts, M. N. C., Dewulf, A. R. P. J., Ludwig, F., Werners, S. E., & Struik, P. C. (2018). Reflections on the potential of virtual citizen science platforms to address collective action challenges: Lessons and implications for future research. *NJAS – Wageningen Journal of Life Sciences*, *86–87*, 146–157. https://doi.org/10.1016/j.njas.2018.07.008

Martin, B. L., & Hall, H. (2011). Mobile phones and rural livelihoods: Diffusion, uses, and perceived impacts among farmers in rural Uganda. *Information Technologies & International Development*, *7*(4), 17–34.

Materia, V. C., Giarè, F., & Klerkx, L. (2015). Increasing knowledge flows between the agricultural research and advisory system in Italy: Combining virtual and non-virtual interaction in communities of practice. *The Journal of Agricultural Education and Extension*, *21*(3), 203–218. https://doi.org/10.1080/1389224X.2014.928226

McCole, D., Culbertson, M. J., & McNamara, P. E. (2014). Addressing the challenges of extension and advisory services in Uganda: The Grameen Foundation's Community Knowledge Worker Program. *Journal of International Agricultural and Extension Education*, *21*(1), 6–18. https://doi.org/10.5191/jiaee.2014.20101

McNamara, P. E., Dale, J., Keane, J., & Ferguson, O. (2014). *Strengthening pluralistic agricultural extension in Ghana*. USAID and MEAS.

MEST. (n.d.). https://meltwater.org/

Ministry of Food and Agriculture (MOFA). (2007). Food and Agriculture Sector Development Policy. Government of Ghana.

Misaki, E., Gaiani, S., & Tedre, M. (2018). Challenges facing sub-Saharan small-scale farmers in accessing farming information through mobile phones: A systematic literature review. *Electronic Journal of Information Systems in Developing Countries*, *84*(4), 1–12. https://doi.org/10.1002/isd2.12034

Molony, T. (2006). "I don't trust the phone; It always lies": Trust and information and communication technologies in Tanzanian micro- and small enterprises. *Information Technologies and International Development*, *3*(4), 67–83.

Msuya, C. P., & Wambura, R. M. (2016). Factors influencing extension service delivery in maize production by using agricultural innovation system in Morogoro and Dodoma Regions, Tanzania. *South African Journal of Agricultural Extension (SAJAE)*, *44*(2), 248–255. https://doi.org/10.17159/2413-3221/2016/v44n2a431

Munthali, N., Leeuwis, C., Van Paassen, A., Lie, R., Asare, R., Van Lammeren, R., & Schut, M. (2018). Innovation intermediation in a digital age: Comparing public and private new-ICT platforms for agricultural extension in Ghana. *NJAS – Wageningen Journal of Life Sciences*, *86–87*, 64–76. https://doi.org/10.1016/j.njas.2018.05.001

Nyamekye, A. B. (2020). *Towards a new generation of climate information systems: Information systems and actionable knowledge creation for adapative decision-making in rice farming systems in Ghana*. Wageningen University and Research Centre.

Obeng, F. K., Gumah, S., & Mintah, S. (2019). Farmers' perceptions of information and communication technology (ICT) use in extension service delivery in Northern Region, Ghana. *Ghana Journal of Science, Technology and Development*, *6*(1), 21–29. https://doi.org/10.47881/126.967x

Perrier, T., Derenzi, B., & Anderson, R. (2015). USSD: The third universal app. *Association for Computing Machinery Conference December 1-2*, 13–21. https://doi.org/10.1145/2830629.2830645

Qiang, C. Z., Kuek, S. C., Dymond, A., & Esselaar, S. (2012). *Mobile applications for agriculture and rural development*. World Bank.

Schmidt, C., Gorman, T. J., Gary, M. S., & Bayor, A. A. (2010). Impact of low-cost, on-demand, information access in a remote Ghanaian village. *ACM International Conference Proceeding Series*, *8*(2), 85–100. https://doi.org/10.1145/2369220.2369261

Sein, M. K., Thapa, D., Hatakka, M., & Sæbø, Ø. (2019). A holistic perspective on the theoretical foundations for ICT4D research. *Information Technology for Development*, *21*(1), 7–25. https://doi.org/10.1080/02681102.2018.1503589

Sigman, V. (2015). *Agricultural extension policy forum: Ghana*. Report on the Policy Forum sponsored by Ghana Directorate of Agricultural Extension Services, Ministry of Food and Agriculture; Modernizing Extension and Advisory Services; and Agriculture Policy Support Project.

Sova, C., Chaudhury, A., Nelson, W., & Nutsukpo, D. K. (2014). *Climate change adaptation policy in Ghana: Priorities for the agriculture sector*. Working Paper No. 68. CGIAR Research Program on Climate Change, Agriculture and Food Security (CCAFS).

Stevens, T. M., Aarts, N., Termeer, C. J. A. M., & Dewulf, A. (2016). Social media as a new playing field for the governance of agro-food sustainability. *Current Opinion in Environmental Sustainability*, *18*, 99–106. https://doi.org/10.1016/j.cosust.2015.11.010

Swanson, B. E., & Rajalahti, R. (2010). *Strengthening agricultural extension and advisory systems: Procedures for assessing, transforming, and evaluating extension systems*. Agriculture and Rural Development Discussion Paper No. 45. World Bank. https://hdl.handle.net/10986/23993

United Nations. (2020). Sustainable Development Goal 9: Investing in ICT Access and Quality Education to Promote Lasting Peace. https://sdgs.un.org/

Van Osch, W., & Coursaris, C. (2013). Organizational social media: A comprehensive framework and research agenda. In *46th Hawaii International Conference on Systems Sciences* (pp. 700–707). https://doi.org/10.1109/HICSS.2013.439

Van Paassen, A., Klerkx, L., Adu-Acheampong, R., Dembele, F., & Traore, M. (2013). Choice-making in facilitation of agricultural innovation platforms in different contexts in West Africa: Experiences from Benin, Ghana and Mali. *Knowledge Management for Development Journal*, *9*(3), 79–94.

Viamo. (2020). *Mobile surveys*. https://viamo.io/services/mobile-surveys/

Vitos, M., Lewis, J., Stevens, M., & Haklay, M. (2013). Making local knowledge matter: Supporting non-literate people to monitor poaching in Congo. Paper presented to 3rd ACM Symposium on Computing for Development, January 11-12, Bangalore. https://doi.org/10.1145/2442882.2442884

Winch, G. M., & Courtney, R. (2007). The organization of innovation brokers: An international review. *Technology Analysis & Strategic Management*, *19*(6), 747–763. https://doi.org/10.1080/09537320701711223

World Bank. (2012). *Agricultural innovation systems: An investment sourcebook*. https://doi.org/10.1596/978-0-8213-8684-2

World Bank. (2014). *Mobile at the base of the pyramid: Ghana, Mozambique, Nigeria, Zambia*.

World Bank. (2017). *Ghana agriculture sector policy note: Transforming agriculture for economic growth, job creation and food security*.

Zwane, E. (2020). The role of agricultural innovation system in sustainable food security. *South African Journal of Agricultural Extension*, *48*(1), 122–134.

Appendix: Inventory of ICT4Ag platforms identified

Platform, services	Constituent ICTs
E-agriculture https://www.e-agriculture.gov.gh/ Direct to farmers: o E-farm – farmer audio agricultural information library o Call centre – access to subject matter specialists o Farmer engagement platform Extension provision: o Web portal – repository of value chain actors, service providers, and stakeholders; and dissemination of new technologies and agricultural current affairs o E-extension – to collect farmers' geo, bio, and crop data; and digitise field and pest and disease monitoring reports o E-subsidy – electronic registration of farmers with GPS integration and unique ID generator to facilitate efficient fertiliser subsidy distribution	IVR inbound DaM SMM Spa
AgroTech SmartEx Trader and outgrower schemes: o Farmer discovery and enrolment with GPS integration – farmer registration, and records of farm practices and credit activities o Farmer management – protocol of agent routine tied to key crop growth stages of farm operations to deliver timely support o Value chain and service linkages – access to agribusiness service providers and value chain actors o Information and knowledge repository – collection of technical information on crop production, processing, and marketing o Monitoring, evaluation, and learning – analyse farmer data to learn their needs and requirements, and track their performance. Additonally, tracking of agents' activities through a dashboard	DaM DoM Spa
Esoko https://www.esoko.com/ Direct to farmers: o Market prices and weather o Agronomic tips o Buy and sell marketplace – reach agent through call centre, sorted by location, commodity, quantity and grade, and place offer that is SMS to buyer(s) o Farmer Helpline call centre – access to agri-extension experts, market prices, and weather forecasts Extension provision: o Knowledge plus – knowledge respository templates o Insyts – digitised reporting templates and real-time analytics o Real-time message alerts Business-to-business services – for government institutions, NGOs, social projects: o Buy-and-sell marketplace – reach agent through call centre and place offer that is sent to farmers via SMS o Targeted marketing messages, announcements, and alerts o Polling and feedback o Knowledge repository templates o Digitised reporting templates	SMS push IVR inbound IVR outboud SMS pull DoM DaM Spa

mFarms https://www.mfarms.org/solutions/ Direct to farmers: o Commodity and agri-input prices o Precision agriculture o M-Xtension – provides good agricultural practices o Farmer to market – facilitates linkage between farmers, and input and ouput markets through human agents To extension providers, agro-dealers, seed producers, off takers: o Field agent management – agent database development and service provision/ activity tracking o Farm-level monitoring – farmer database development with farm mapping and farming activity Business-to-business services – for NGOs, FBOs, agro-dealers, logistics or warehousing companies, aggregators, processing companies: o Targeted advertising and messaging with instant delivery reports and dashboards o Targeted short surveys and polling for organisations (NGOs, input suppliers, etc.) to track their performance o Warehousing, and stock and sales tracking systems o Loan management systems o Fleet management systems	SMS pull SMS push DaM IVR outbound Spa
Plantwise https://www.plantwise.org/KnowledgeBank For plant health and protection institutions and extension providers: o Plantwise factsheet – repository of crop-based pest and disease management advice o Plantwise data collector – digitised "prescription form" to record farmers' biodata, plant health problem diagnosis and prescriptions o Plantwise plant doctors' platform – pest and disease alert and knowledge-sharing platform	DoM DaM SMM Spa
Scientific Animations Without Borders (SAWBO) https://sawbo-animations.org/home/ For extension providers: o Video library – extension information accessible as 2D, 2.5D, and 3D animations with voice overlay	DoM
Complete Farmer https://www.completefarmer.com/ For farmers: o Builds and manages farms for individuals and provides real-time monitoring sensor and drone feed data through an online dashboard	DaM Spa
QualiTrace https://www.facebook.com/QualiTrace/ For input buyers: o Anti-counterfeiting solution – enabling input buyers to confirm the authenticity of farm inputs by dialling the barcode of the purchased product through a USSD application prompt	USSD
Akokotakra https://akokotakra.com/app For farmers: o Mobile and web-based management system that enables poultry farmers to record, monitor, and track their operations	DaM Spa

Ghalani https://www.facebook.com/ghalaniapp/ For farmers and agri-businesses: o Electronic management of farm records	DaM Spa
TROTRO Tractor https://www.trotrotractor.com/ For farmers: o land preparation, planting, spraying, threshing, shelling, and transportation services	USSD IVR inbound
Ignitia Iska https://www.ignitia.se/ Direct to farmer: o Location-specific weather updates – daily, monthly, and seasonal rain forecasts	SMS push
Farmerline https://farmerline.co/ Direct to farmers: o Weather forecasts o Agronomy tips – customised to location (GPS) and production stage o Market prices o Market place – access to farm inputs, water, solar energy, and financial services – aggregated demand for inputs (type and location) for Farmerline to supply goods Business-to-business – off takers, input dealers, global food companies, government institutions, research organisations, NGOs, financial institutions: o Polling and short surveys o Engagement platform – send customised bulk messages o Data collection, management, and analytics – including farm-level monitoring, field monitoring, farmer profiling, and farm mapping through delivery o Building credit history to access advanced financial services through a mobile money payment platform o Mobile payments and savings platform o Plant health and vegetation change monitoring using satellites	SMS push USSD IVR inbound IVR outbound DaM Spa
Moringa https://moringaconnect.com/ Extension provision: o In-house electronic data collection form and analytics, paired with GIS mapping system to monitor plant growth and trace moringa trees from planting to processing	DaM Spa
MTN MoMo (e-wallet) https://mtn.com.gh/momo/ Direct to farmers: Mobile banking – payments, loans and savings, micro insurance Business-to-business: o Mobile banking – payments, loans and savings, micro insurance	USSD
VOTO Mobile (Viamo) https://viamo.io/services/information-sharing/ Direct to farmers: o Mass-messaging on good agricultural practices o Mass-messaging on price information and weather forecasts Business-to-business: o Mobile data collection – track field activities, monitor disaster response, report on stock levels, measure attendance, follow-up on referrals o Polling priorities, needs, and feedback from farmers or stakeholders o Mass-messaging to advertise and inform farmers or stakeholders	SMS push USSD IVR outbound DaM Spa

Farm Radio International https://farmradio.org/ghana/ Direct to farmers: o Access to messages, alerts, radio programme segments, and ability to leave audio message o Commodity-based farm tips For radio stations and businesses: o Conduct surveys using audio messages o Farmer feedback on radio broadcasts o Uliza polling – voting by beeping/flashing to two phone numbers desginated for a "yes" or "no" response – listeners use basic phone to vote on IVR system, view results and recording. Number announced on radio station – call number and answer with number or record, flash call back o Automated callback or SMS with market information	IVR outbound IVR inbound SMS pull SMS push
Manobi Africa https://www.manobi.com Direct to farmers: o Listing and precise georeferencing of farming plots o Marketplace (offers and demands) between large and small producers, and traders, buyers, and importers o Real-time monitoring of prices of agricultural products in wholesale and retail markets o Epidemic alerts, weather forecasts, calculation yields Extension provision: o Data collection – digitised monitoring data on agricultural operations during crop production Business-to-business: o Collaborative platforms – facilitate multi-actor engagement for cooperatives, associations, etc. o Data collection – surveys and advanced monitoring and evaluation o Inventory management system	DaM SMS push Spa
CocoaLink https://www.hersheytrading.ch/en_us/good-business/creating-goodness/cocoa-sustainability/cocoa-link.html Direct to farmers: o Farmers can send in (photo) inquiries directly to experts and other farmers o Farmers receive weekly messages (farming practices, farm safety, child labour, crop disease prevention, post-harvest production, and marketing) from COCOBOD o Digital access to educational content – planting tips, correct input usage, and descriptions of best practices Extension provision: o Electronic farmer data collection	SMS push DaM DoM Spa IVR outbound
Farmforce https://farmforce.com/ Out-grower schemes and NGO (groups or cooperatives or exporters) – agent o Crop growth stage, pest scouting and monitoring results, bio-data, input usage, and recording or estimating harvests / yields o Manage micro-loans and perform audits o Historical information of where crop came from at supermarket level o Tracking specific produce through the value chain o Bulk messaging to field staff and farmers o Electronic (field audit) survey	SMS push DaM Spa

Freedom Fone https://archive.flossmanuals.net/freedom-fone/what-does-freedom-fone-do Direct to farmers: o Sharing audio information with an audience – educational dramas, market information, recorded radio programmes, or short news items For businesses: o Polling – enable audience to vote on an issue using their phone o Collect SMS feedback from audience – updates about specific news events, alerts, or time-critical information o Get your audience to leave audio messages to share their opinion on a particular topic or make reports in their own language (IVR inbound)	SMS pull IVR outbound IVR inbound
SavaNet https://savanet-gh.org/?q=content/what-we-do Direct to farmers: o Farmer group linkage to extension agents, ICT professionals, and researchers etc. (conference using mobile phone and portable external speakers) o Farm area mapping and analysis o Soil testing and analysis o Record keeping o Market access and weather forecasts	Spa DaM
SyeComp https://syecomp.com Business-to-business and service to NGOs: o Farmland surveying o Farm mapping o Certification support and traceability	Spa
GeoTraceability Extension service provision: o Tailored business plans – processing field data and agronomic practices to generate appropriate recommendations for business plans Business-to-business or project services: o Survey design tools and electronic data collection o Mapping production areas and relevant infrastructure o Traceability tools o Tailored messages to targeted groups of producers o Interoperating data from multiple platforms and data sources onto one database o Cloud-based data management structure to securely store and recall unlimited amounts of data	SMS push DaM Spa
Anitrack and Animat https://gh.linkedin.com/company/anitrack Direct to farmers: o Anitrack: a web application that enables animal identification, and health tracking of livestock using sensors (wearable tracking devices around the neck of the animal) to monitor vitals such as temperature and report when necessary sensors go off – sending a message to a registered veterinarian o Animat: a website for livestock producers to place their stock online for buyers to see	SMS push DaM Spa

Applying Blockchain Technology to Security-Related Aspects of Electronic Healthcare Record Infrastructure

Ryno Adlam
Master of Technology student, School of Information Technology, Nelson Mandela University, Port Elizabeth, South Africa
https://orcid.org/0000-0002-6514-3673

Bertram Haskins
Associate Professor, School of Information Technology, Nelson Mandela University, Port Elizabeth, South Africa
https://orcid.org/0000-0002-9762-7381

Abstract
The centralised architecture employed by electronic health records (EHRs) may constitute a single point of failure. From the perspective of availability, an alternative cloud-based EHR infrastructure is effective and efficient. However, this increased availability has created challenges related to the security and privacy of patients' medical records. The sensitive nature of EHRs attracts the attention of cyber-criminals. There has been a rise in the number of data breaches related to EHRs. The infrastructure used by EHRs does not assure the privacy and security of patients' medical records. Features of blockchain platforms, such as decentralisation, immutability, auditability, and transparency, may provide a viable means of augmenting or improving services related to the security of EHRs. This study presents a series of experimental data flow configurations to test the application of blockchain technology to aspects of EHRs. The insights gained from these experiments are founded on a theoretical base to provide recommendations for applying blockchain technology to services related to the security of EHR infrastructure. These recommendations may be employed by developers when redesigning existing EHR systems or deploying new EHR systems.

Keywords
healthcare, electronic health records (EHRs), blockchain, information security

DOI: https://doi.org/10.23962/10539/32211

Recommended citation
Adlam, R., & Haskins, B. (2021). Applying blockchain technology to key aspects of electronic healthcare record infrastructure. *The African Journal of Information and Communication (AJIC), 28*, 1-28. https://doi.org/10.23962/10539/32211

1. Introduction

An electronic health record (EHR) is the electronic equivalent of the medical history of a specific patient. It presents potential benefits, such as a reduction of errors, an increase in the availability of medical records, and, as a knock-on effect, an improvement in the quality of patient care (Thakkar & Davis, 2006). However, EHR systems may encounter several challenges in the form of data breaches, privacy compromises, interoperability, auditability, and fraud. EHR systems currently utilise a centralised architecture that requires a centralised authority of trust and leaves medical records vulnerable due to a single point of failure (Liang et al., 2017). Highly sensitive patient-related information is associated with an EHR, including information such as patient demographic details, medical history, and data points related to patient vital signs (Menachemi & Collum, 2011). This wealth of information makes EHRs lucrative targets for cybercriminals and, as a result, the number and severity of successful cyberattacks on EHRs are increasing (Ronquillo et al., 2018). The conventional model employed by EHR systems can no longer ensure the security and privacy of patient health records (Kshetri & Carolina, 2018). The privacy and security of EHRs may be improved by the desirable features of blockchain technology such as decentralisation, immutability, auditability, and transparency (Emmadi et al., 2019).

To improve or augment the services related to the security of electronic healthcare infrastructure, developers may turn to blockchain technologies, but may be unfamiliar with how or where to apply them to the EHR infrastructure. Therefore, the objective of this study is to present recommendations for applying blockchain technology to services related to the security of the electronic healthcare record infrastructure. The remainder of this article is structured as follows: section 2 presents an overview of key background concepts; section 3 discusses how aspects of blockchain technology may be applied to EHRs; and section 4 provides an overview of the workflows generated from experimenting with blockchain technologies. Insights gained from the experiments and theory are presented as a set of recommendations in section 5, and the study is concluded in section 6.

2. Background

EHRs are widely used to maintain patient data in an online format. Blockchain technology is a means of storing information in a distributed fashion. To understand how these concepts could intersect, this section provides an overview of the respective technologies, their component aspects, and examples of their use.

Electronic health records (EHRs)

The healthcare industry is continually evolving. The evolution towards EHRs from a paper-based system has been fuelled by new advancements in the realm of information technology (Seol et al, 2018). The EHR is the electronic equivalent of a patient's full medical record, promising benefits such as the improved sharing of information, saving time for medical professionals, a cost reduction, reducing the number of

errors, and a general improvement in the quality of patient care (Dekker & Etalle, 2007; Thakkar & Davis, 2006). EHR systems are subject to privacy regulations as they deal with patient information such as a patient's medical history, vital signs, and demographic information, all of which are considered sensitive. As a result of this highly sensitive information contained in EHRs, they face constant cyberattacks, and the number of these attacks are on the rise (Kshetri & Carolina, 2018). In 2015, more than 112 million records were exposed through data breaches (Kshetri & Carolina, 2018; Ronquillo et al., 2018).

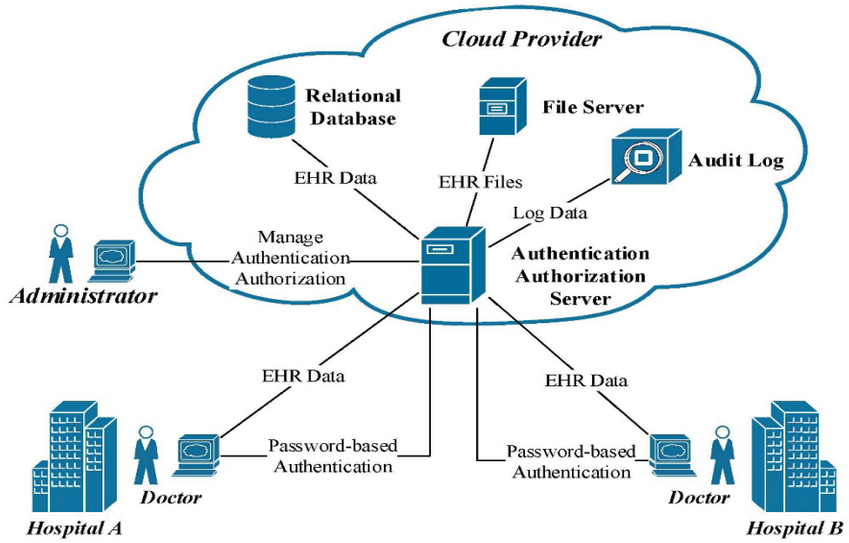
EHRs are soft targets for those with nefarious purposes because they may not be as well protected, but contain a wealth of personal information. The stolen data is either sold on the black market or the hackers hold the EHRs for ransom. The WannaCry ransomware cyberattack in 2017 affected countless healthcare providers who were forced to either pay the ransom or close their doors to further patient care (Ronquillo et al., 2018). Therefore, it stands to reason that the privacy and overall security of a patient's EHR cannot be adequately ensured by the traditional centralised information storage and transport architecture (Kshetri & Carolina, 2018).

Relational databases, which are an example of a centralised client-server, multi-user architecture, are frequently used to store patient EHRs (Griggs et al., 2018). Although a client-server-based model ensures that all clients have access to a centralised store of information, this model does run the risk of clients losing access to the information if the server is unavailable, resulting in a single point of failure (Liang et al., 2017). A modern version of the client-server model is that of cloud services or cloud computing. This model allows client devices to access a remote virtualised server via an internet connection. A virtual server provides benefits such as improved scalability and flexibility, greater availability, and a reduction in overall operational costs (Ziglari & Negini, 2017). Such an always-on and accessible solution greatly improves the efficiency and availability of an EHR solution, but does raise further concerns with regard to privacy and security. The improvement of accessibility of the EHRs not only holds true for those who may legally access them, but also for those with harmful intent.

An overview of the current EHR model is illustrated in Figure 1. The model provides an overview of the various types of activities undertaken and the actors involved in the traditional model, as well as how the data flows between these activities and actors. By studying these details, it is possible to identify a few high-level processes used to support the current client-server EHR system implementation. These processes are the transport of data, authentication, authorisation, and auditing. The transport of data is very dependent on the underlying hardware, the communication protocols in use on the hardware, and the connections established by the various operating systems and related software, such as relational databases and client-based software. Adding security may be done on the level of the lower-level transport stream or be built into the database and client connection, but is largely left to the EHR

developer/infrastructure creator's discretion. The sub-sections that follow delve deeper into the concepts of authentication, authorisation, and auditing.

Figure 1: EHR system overview diagram (Adlam & Haskins, 2019



Authentication

Authentication refers to the process of identifying which user is requesting access to the system, so as restrict access to that system's functions. Users' identities are also required for audit purposes (Cilliers, 2017). As with many centralised systems, EHR systems make use of password-based authentication (Kshetri & Carolina, 2018). Although automated password generation, effective organisational password policies, and the application of multi-factor authentication can largely mitigate the risks of password-based authentication, these measures are not universally in place. In most instances, the passwords are manually created by humans and are considered to be weak and easily cracked by utilising techniques such as social engineering, password guessing, and brute-forcing (Kshetri, 2017). Passwords are commonly stored in a centralised relational database, which may represent a single point of failure if the passwords are not hashed to avoid an attacker retrieving them. When an authentication database is compromised, this often leads to secondary attacks as passwords are frequently reused. Password-based authentication is therefore considered vulnerable to cyberattacks (Mosakheil, 2018).

Authorisation

System functions should be available only to those with the appropriate rights. These rights are determined by the process of authorisation and applied through a variety of authorisation mechanisms (Cilliers, 2017). When applied correctly, authorisation

serves to mitigate the risk of disclosing information to unauthorised persons. Ferraiolo et al. (2003) define role-based access control (RBAC) as a system by which users gain access to computer system objects based upon their role in the organisation. The RBAC model is frequently used by EHR systems to authorise user activities (Seol et al., 2018). In this model, the application code, hosted on a central server, contains the encoded RBAC rules. These rules provide users with specific roles, which govern their access to resources. As the rules are stored in a central server, this presents yet another possible failure point for the system. A compromised system could allow an attacker to modify user privileges (either their own or those of other users) or allow them to hijack another user account, which could grant them privileged access to restricted areas of a system. The RBAC model does not deal well with complex attributes such as subject attributes, object attributes, action attributes, and contextual attributes. Subject attributes describe a user, object attributes describe the resource that the subject is attempting to access, action attributes describe the actions that the subject is attempting on the object, e.g. to read or write, and contextual attributes describe the environment, e.g. specific times when actions are allowed.

Since an EHR may contain complex attributes, it requires a mechanism that provides dynamic access control and may be set at a very fine-grained level (Seol et al., 2018). With RBAC restricting access only according to a user's role, it may need to consist of a multitude of custom role applications if fine-grained, dynamic access control is required. This approach may be difficult to maintain and track. An example is the *doctor* role. A *doctor* should not be able to access the records of all the patients in the system; only the records of their own patients should be accessible. An RBAC-based system would require each person with the *doctor* role to have individualised access rights assigned to access their respective patients (Franqueira & Wieringa, 2012).

Auditing

Audit logs are a recording of all the actions a user has performed on a system (Dekker & Etalle, 2007). They are useful in identifying how, when, where, why and by whom data was accessed, modified, and/or leaked. This yields a form of system auditing. Tamper-proof, immutable audit logs provide a means of ensuring data integrity by providing a consistent audit trail to aid in the discovery of data breaches and the identification of compromised user accounts (Kshetri, 2017). Unfortunately, EHR systems have no standardised means of generating audit logs.

2. Blockchain technology

A ledger is a structure that maintains details regarding transactions. Distributed ledger technology distributes the ledger among participants, which may be spread across various organisations and sites (Bashir, 2017, p. 27). Blockchain technology enhances this approach by chaining together unrelated blocks in a linked-list manner. This linked structure may be perceived as a chain of connected blocks, leading to the name "blockchain".

Overview

Simply put, a blockchain may be perceived as a form of distributed database which is under the control of a group of individuals. The blockchain network consists of a series of interconnected devices referred to as nodes. To add a record to this database requires that a user (on a specific node) proposes a transaction. The transaction is then broadcast to all its peer nodes, which in turn validate the transaction using known algorithms. A verified transaction is combined into a block along with other transactions. The technique for adding the block to the blockchain results in a transaction that is practically immutable (Bashir, 2017, p. 27). Fundamentally, this does not constitute new technology, but existing technology applied differently. A term frequently associated with blockchain technology is "cryptocurrency", although this is not entirely accurate. Cryptocurrency is an application of blockchain technology and thus it may be considered a subset of blockchain technology, but not an equivalent term (Bashir, 2017, p. 23).

All the peers in a blockchain network need to agree as to the validity of the history of transactions in the chain. This agreement is referred to as consensus (Bergquist, 2017). Consensus may be calculated using two approaches, namely a proof-based or a Byzantine fault tolerance-based approach. Proof-based consensus works on the principle that a leader is elected based on a form of proof that provides a specific node with the authority to propose a new value. In Byzantine fault tolerance-based consensus, new values are proposed during rounds of voting (Bashir, 2017, p. 28).

Depending on who has access to or maintains the blockchain infrastructure, blockchain networks may be classified as public, permissioned (enterprise), or private. Public blockchain networks are open to the public and anyone can partake in the consensus process (Bashir, 2017, p. 26). As public blockchain networks utilise identities based on pseudonyms, it is challenging to establish and control the identities of participants. Enterprise blockchain networks, also known as permissioned blockchains, are being developed to cater to enterprise use cases (Emmadi et al., 2019). Permissioned blockchain systems are controlled by a quorum of organisations and, as a result, are classified as semi-decentralised. The membership of a permissioned blockchain system is strictly controlled and transactions are generally confidential between participants. Privacy, confidentiality, authorisation, user identity, and auditability are key features omitted in public blockchain networks, but permissioned blockchain networks are integrating them to support enterprise-based use cases.

Table 1: Comparison of blockchain types

Criteria	Public	Permissioned	Private
Architecture	Decentralised	Semi-decentralised	Centralised
Immutability	Virtually tamper-proof	Tamper-evident	Tamper-evident
Transparency	Full transparency	Semi-transparent	Semi-transparent, No transparency
Transaction speed	Slow	Fast	Fast

Consortium networks may consist of various enterprise entities which require the private and secure sharing of information. This focus on privacy is one of the challenges to the adoption of enterprise-grade blockchain technology (Bashir, 2017, p. 461). A measure of privacy can be ensured by applying varying levels of isolation so that only authorised parties are granted access to confidential information. However, the use of a shared ledger in blockchain technology serves to promote transparency, which may be seen as a polar opposite to privacy. A goal of permissioned blockchain technology is, therefore, to attempt a balance between privacy and transparency (Emmadi et al., 2019). Private blockchain systems are classified as centralised since they are largely owned and operated by a single organisation. Various types of blockchain networks have been mentioned so far. Table 1 provides a summarised comparison of these different types of networks.

The widespread adoption of blockchain has led to the development of various independent implementations of the technology. Each of these technologies has its strengths and suitability for various applications. Table 2 compares popular blockchain platforms in terms of network type, consensus algorithm, data privacy, smart contract languages, and application (what it is used for).

Table 2: Comparison of popular blockchain platforms

Feature	Platform		
	Bitcoin	Ethereum	Hyperledger Fabric
Application	Cryptocurrency	Multi-purpose	Multi-purpose
Consensus	Proof-of-work	Proof-of-work, proof-of-stake	Solo, Kafka
Data privacy	-	ZKP	TLS, ZKP, Channels
Smart contract language	Go, C++	Solidity, Serpent, LLL	Go, Java
Type	Public	Public, private, permissioned	Private, permissioned

Blockchain platforms

Bitcoin was introduced in a white paper in the autumn of 2008. The Bitcoin open-source software was released in 2009, and the founder of Bitcoin remains anonymously known as Satoshi Nakamoto (Laurence, 2017, p. 32). Bitcoin is a popular cryptocurrency, the success of which sparked the blockchain revolution. Bitcoin makes use of an extensive consensus algorithm known as proof-of-work to validate transactions. Proof-of-work is known by the Bitcoin community as *mining*. Bitcoin miners use highly specialised equipment that is not only expensive, but also consumes large amounts of electricity to operate. Mining is necessary to keep the Bitcoin network safe, stable, and secure (Laurence, 2017, p. 34).

The developers of Ethereum were interested in turning Bitcoin into a blockchain platform that could support business and government use. Bitcoin was already well-established and would have needed a substantial code overhaul to support the number of transactions required for a business use case. The upgrade was considered too severe by the Bitcoin community and Ethereum was therefore released as a stand-alone platform in July 2015. It is currently the most developed and innovative blockchain in use (Laurence, 2017, p. 42).

Ethereum smart contracts are used to digitally verify or enforce that all contractual terms are met before a transaction takes place (Bergquist, 2017). The need for third-party involvement is eliminated by the use of these irreversible and intractable smart contracts, which demonstrates why they should be submitted for thorough testing before being deployed on a production network (Bashir, 2017, p. 198).

In 2015, the Linux Foundation initiated the Hyperledger project (Laurence, 2017, p. 81). Fabric was the first production-ready framework created in 2017 under the greater Hyperledger project. The project has since grown to encompass four other frameworks, namely Burrow, Indy, Iroha, and Sawtooth Lake (Hyperledger Architecture Working Group, 2017). Hyperledger Fabric was created to address issues such as confidentiality, privacy, and scalability (Bashir, 2017, p. 362) and also to facilitate the delivery of blockchain networks suitable for use in a business environment. Many of its modules are swappable, making it possible for developers to select a suitable consensus algorithm, such as Kafka ordering, before creating a custom blockchain network (Saraf & Sabadra, 2018). The role of the Kafka ordering service is to maintain the order of the blocks in the blockchain (Saraf & Sabadra, 2018). Swappable modules, such as the Kafka service, provide a Hyperledger Fabric implementation with a large measure of flexibility and scalability that is not available in some other types of blockchain networks, such as Bitcoin. Another feature of Fabric is its use of transport layer security (TLS), which provides a form of encrypted tunnel between two nodes and is used to preserve privacy.

Peer-to-peer technology is used to facilitate the creation of channels in Hyperledger Fabric, enabling participants to share confidential information and allowing the information to be viewable only by participants on a particular channel (Bashir, 2017, p. 362). Participants are allowed to belong to multiple channels on the same network. Many programming languages are supported in Hyperledger Fabric, via the use of container technologies, enabling developers to create chain-code (smart contracts) in languages such as Java, Node.js, and Go (Bashir, 2017, p. 362). Although a Fabric transaction is anonymous, confidential, and private, it may be traced and linked to participants by authorised auditors. This is facilitated by the membership service, with which all participants need to register to access the network (Saraf & Sabadra, 2018).

Users interacting with the Fabric network are identified by the use of digital certificates. These certificates are issued (or revoked) by the Fabric Certificate Authority (Fabric CA) (Hyperledger, 2021, p. 51). The digital certificate contains encoded authorisation attributes, as part of an attribute-based access control (ABAC) system. This allows the digital certificate to be used as a means of identifying participants and restricting their access to specific aspects of the blockchain network.

This section by no means presents all the various blockchain platforms, as providing further in-depth discussions of, among others, Kadena, Dfinity, Corda, and the various Hyperledger platforms would require a separate publication. However, this overview of the three technologies discussed does provide some insight into the wide variety of technologies available. With these technologies in mind, the following section discusses how aspects of them may be applied to security-related aspects of EHRs.

3. Applying blockchain technology to EHRs

Blockchain technology is not a one-off, drop-in replacement for all security-related aspects of EHRs. Individual features of blockchain technology may, however, present opportunities to address aspects of EHR security dimensions related to authentication, authorisation, audit logs, data storage, and transactions. The following sub-sections discuss how each of these EHR security-related services may be augmented, replaced, or enhanced using blockchain technology.

Authentication

Authentication is used to identify a user requesting access to the system. Systems need to be able to identify users to restrict access to system functions. Users' identities are also required for audit purposes (Cilliers, 2017).

Enterprise systems traditionally utilise password-based authentication, which often relies on a centralised architecture such as a relational database (Kshetri & Carolina, 2018). Blockchain technology can leverage smart contracts and public key

infrastructure (PKI) to replace password-based authentication with certificate-based authentication.

Permissioned blockchain technology can utilise smart contracts and certificate-based authentication to replace the traditional password-based authentication mechanism. Certificate-based authentication removes the human factor from the authentication process. Certificates are often created with a 2048-bit key size, which is much larger than an average password size. It is considered to be impractical to brute-force a certificate, as a standard desktop computer would take years to crack it. Certificates come with an expiration date, which can reduce the risk of prolonged data exposure. Blockchain technology can leverage smart contracts to validate user certificates and effectively mitigate the risk of a single point of failure.

Authorisation

Appropriate authorisation mechanisms should be employed to restrict user access to specific system functions. The actions that an authorised user may perform on a system are determined by the process of authorisation (Cilliers, 2017). The application of authorisation mitigates the risk of disclosing information to users who should not have access to it (Seol et al., 2018).

Enterprise systems predominantly utilise centralised authorisation architecture. Blockchain technology can replace the prominent centralised authorisation architecture with a distributed architecture. Enterprise systems commonly rely on a role-based access control (RBAC) model to restrict access to information. Blockchain technology can leverage PKI and smart contracts to create a distributed attribute-based access control (ABAC) model.

A user's certificate may be encoded with attributes to restrict their access to specific resources. Permissioned blockchain technology makes use of this attribute-based access control to enable a fine-grained access control model. This access-restriction may be based on action attributes, contextual attributes, object attributes, and subject attributes. The actions that a user is allowed to take on a system, such as reading and writing, are determined by action attributes. The types of actions a user is allowed to take may also depend on their operating system and the platform they are using to access the system, or the time of day; these attributes are referred to as contextual attributes. Object attributes are used to enforce which system object types may be accessed by the user, e.g. a medical record or information related to a specific department. Lastly, subject attributes are descriptive attributes related to the specific user requesting system access, such as departmental or job title. When used in conjunction, these different types of attributes may be encoded into smart contracts and distributed across the blockchain network. This type of distributed, authorisation architecture helps to establish a network without a single point of failure.

Audit logs

An audit log is a recording of all the actions that a user has performed on a system. Audit logs are useful in identifying how, when, where, why, and by whom data was accessed, modified, and/or leaked. Tampering with audit logs frequently occurs to cover a criminal's tracks (Dekker & Etalle, 2007). Enterprise systems predominantly utilise a centralised audit log architecture. Audit logs are commonly stored locally in a file or remotely on a relational database, but these methods of storage are not considered to be immutable. Blockchain technology could provide a distributed and practically immutable audit log. Permissioned blockchain networks make use of a membership service to identify users interacting in the blockchain network (Bashir, 2017, p. 362). The user's identity can be used to record all the actions performed by the user on the blockchain network. Permissioned blockchain technology can be used to generate a semi-decentralised, tamper-evident, and standardised audit log for EHR systems.

Data storage

Data storage is the act of recording information electronically. Data can be stored by utilising a variety of structures and architectures, all of which have advantages and disadvantages.

Enterprise systems predominantly use a centralised client-server model to store data. Centralised data storage such as a relational database used by enterprise systems provides a high degree of transaction throughput, but could be vulnerable due to a single point of failure (Liang et al., 2017). Blockchain technology can replace the common centralised client-server model with an append-only storage approach for EHR systems (Bashir, 2017, p. 438). This storage model can ensure data integrity from data creation to data retrieval. A single point of failure can also be averted with the use of blockchain technology (Kshetri & Carolina, 2018). Permissioned blockchain technology can be used to enhance the privacy of data being stored on a blockchain network. Cryptographic techniques such as zero-knowledge proofs can be used to store data privately and to ensure that data integrity can be maintained without revealing private information (Bünz et al., 2017).

Transactions

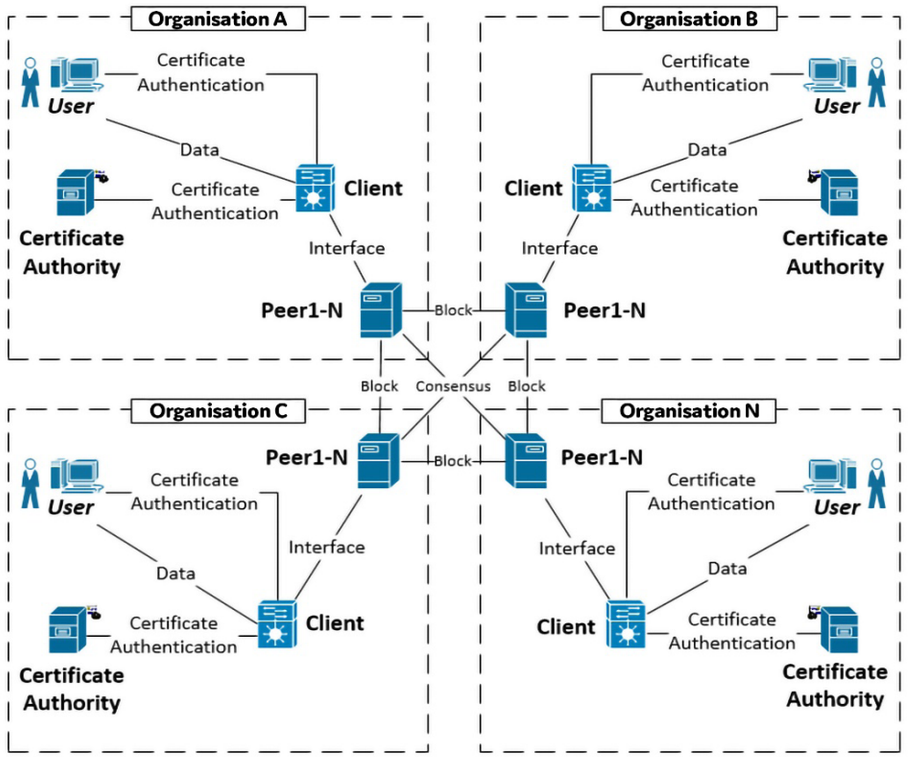
Transactions are used to add, update, or retrieve data from databases. Data transactions in this context also apply to the sharing of information between authorised parties. Information travelling on the network is a prime target for interception by those with nefarious purposes. Therefore, the common transaction process, used by enterprise systems and which still relies on a centralised client-server model, is a prime candidate for replacement by a peer-to-peer, permissioned blockchain replacement.

4. Implementation

Although the theoretical grounding seems to support the idea that certain aspects of the EHR infrastructure could be replaced with selected blockchain technologies, it is necessary to determine whether this is practically feasible. To that end, we created a series of test setups to determine whether the theoretical assumptions are accurate. Although the functionality explained in this section could be ported to any permissioned blockchain network that supports smart contracts and certificate-based authentication, Hyperledger Fabric was selected because of the features it provides, its level of customisability, and the authors' familiarity with the platform.

Figure 2 illustrates a generic version of a permissioned blockchain network, consisting of certificate authorities (CAs), clients, and peers. The role of the CAs is to issue, revoke, and/or validate digital certificates. Clients are the point of interaction with the blockchain network, and peers store the linked-list of blocks, which form part of the blockchain. The peers may be synchronised in a permissioned blockchain platform via a variety of different consensus algorithms.

Figure 2: Proposed network topology



Organisations are linked together using their respective peers. Each organisation requires at least one of each network component, as illustrated in Figure 2. The organisations are advised to include multiple peers for internal redundancy purposes. The following section uses this diagram as a baseline setup to present recommendations for applying blockchain technology to security-related services in an electronic healthcare record infrastructure.

5. Recommendations

Using the generic blockchain network described in section 4, test setups were created to address issues related to authentication, authorisation, audit logs, data storage, and transactions, as they relate to EHRs. During the creation of these test setups, various lessons were learned, which may be used to inform and/or guide anyone who wishes to implement blockchain technology to replace or augment EHR processes.

The remainder of this section, therefore, presents recommendations for applying blockchain technology to security-related services in an electronic healthcare record infrastructure. The recommendations may be used to augment individual aspects of an existing EHR system or used as a combined solution. The combination of these recommendations presents a unique EHR domain-specific overview for any systems administrator or architectural designer planning to integrate blockchain technology into an EHR system. The recommendations are grounded in theory and reinforced by insights gained from experimentation.

Use digital certificates as a means of EHR user authentication

Problems addressed

Human error or a lack of strong password selection may result in a compromised EHR system. In addition, a central database, serving as an authentication server in an EHR system, may be compromised, resulting in a disruption of service or data theft.

Motivation

Password-based authentication is not secure enough for sensitive information. The human factor in password-based authentication is the main weak point and, as passwords are often created by humans, they are usually short and weak. This is because it is difficult for humans to remember long and complex passwords. Wherever possible, make use of certificate-based authentication as it limits the human factor in password selection.

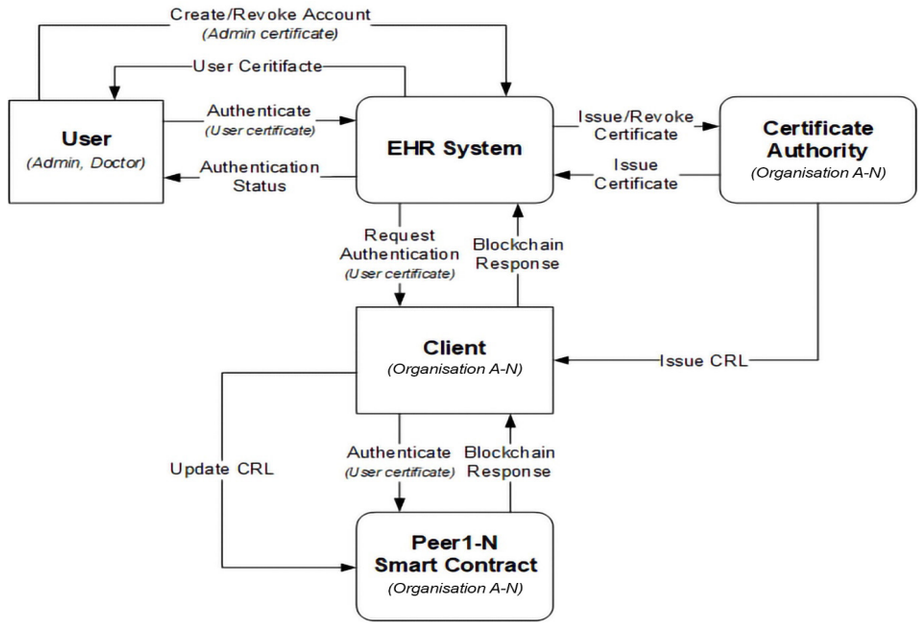
Passwords are commonly stored in a centralised database. When an authentication database is compromised, passwords can be stolen and this can result in breaches. These breaches may allow an attacker to gather sensitive information, which may, in turn, result in even more widespread breaches. Digital certificates are published with two keys, known as a private key and a public key. The public key is derived from the private key and both these keys are required for authentication. The private keys of

certificates are commonly stored on the user's machine and users are encouraged to safeguard their private keys by storing them in a hardware security module (HSM) or trusted platform module (TPM). Not all certificates are stored in a centralised architecture. The certificate revocation list (CRL) is also distributed across all the peers in the blockchain network. It is thus increasingly difficult to tamper with the authentication mechanism, as the majority of the peers in the blockchain network need to be compromised.

The blockchain approach

The information flow of the blockchain-based authentication model is illustrated in Figure 3. Administrators of the EHR system can create and revoke digital certificates and the certificates are issued and revoked by the certificate authority. When a user's digital certificate has been revoked, a CRL is generated.

Figure 3: Blockchain authentication data flow diagram



The peers in the blockchain network receive a CRL update command to update the CRL stored on the peers. Users can authenticate with the EHR system by providing the system with their certificate. The certificate is then passed to the client, which is then sent to a peer in the network. The peer authenticates the user by running the authentication smart contract, which validates the certificate and returns a response. This response determines the authentication status of a user. The pseudocode outlined in Figure 4 presents an example of an authentication function.

Figure 4: Authentication pseudocode

```
Do sanitisation check on the function inputs;
  Get the users certificate;
  Validate users certificate;
  if the user certificate has been signed by an trusted CA then

    if user certificate is not present on CRL then
      Grant user access;
    else
      Deny user access;
    end if

  else
    Deny user access;
  end if
```

Employ an attribute-based access control (ABAC) model based on EHR attributes

Problems addressed

Role-based access control (RBAC) systems require role definitions for restricting various actions and access to resources. This results in a role explosion in an EHR system, with many user and resource types requiring access control, as each customised user role, such as doctor or administrator, would require a new system role to restrict specific actions and rights on the various system attributes. In addition, RBAC rules are hosted on centralised, relational databases. A compromised relational database could provide an attacker with the ability to add, modify, or remove user privileges or even allow a specific privileged user account to be compromised to give an unauthorised user access to the system.

Motivation

RBAC-based control rules are frequently hosted on a centralised server and embedded into application code. User access requests are compared to the role description stored in a centralised relational database, presenting a possible single point of failure. The RBAC model does not deal well with complex attributes such as subject attributes, object attributes, action attributes, and contextual attributes. An EHR system contains many sensitive attributes, such as patient diagnosis, medication, or even health insurance information, and could contain multiple user-types, such as doctor, healthcare worker, and administrator, which would each need to have their own access rules defined for the various attributes in the system. For instance, a hospital administrator may need to access a patient's health insurance information, but not their medication. The large number of rules which may be required, as well as the centralised storage requirements of an RBAC-based model, make an attribute-based access control (ABAC) model a more suitable solution in the EHR domain.

ABAC presents a means to provide a more fine-grained access control model as access may be restricted based upon a combination of various actions, and contextual, object, and subject attributes. This combined approach yields a system of complex rules which may be encoded into the broader network structure. ABAC makes it a bit more impractical for an attacker to gain unauthorised access as it is based on a series of attributes and access control rules. The digital certificates in an ABAC system contain the encoded ABAC attributes and the access control rules are encoded into smart contracts which are distributed across the network. An attacker would therefore need to steal an administrator's digital certificate or compromise the majority of peers in the specific blockchain network for any illicit action to go undetected.

The blockchain approach

The information flow of the blockchain-based authorisation model is illustrated in Figure 5. The data flow diagram is based on Figure 3, but omits details regarding authorisation to focus on the authorisation process. Users should first be authenticated before the authorisation process is performed. This structure assumes a user has a valid certificate when attempting to execute an operation on the EHR system. The EHR system contacts the blockchain client to invoke the authorisation smart contract stored on the peers in the network. The smart contract validates the user attributes stored in the certificate against the authorisation rules embedded in the smart contract. The smart contract then returns an authorisation response. The pseudocode outlined in Figure 6 presents an example of an authorisation function.

Figure 5: Blockchain authorisation data flow diagram

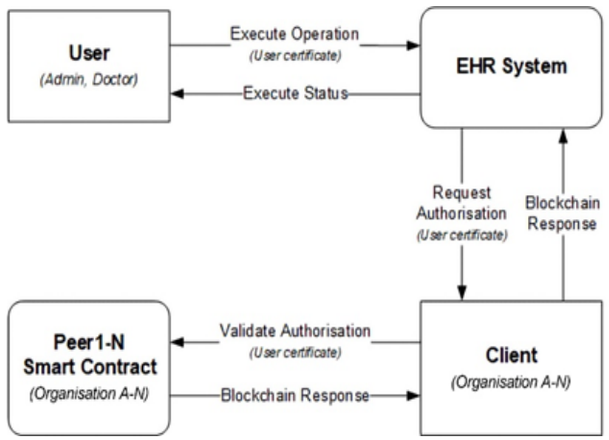


Figure 6: Authorisation pseudocode

```
Do sanitisation check on the function inputs;
   Get the users certificate;
   Validate users certificate;
   Get user's identity from certificate;
   Get user's attributes from certificate;

   if the user attributes match the authorisation rules
      Grant access to the user;

      if userID is present on a stored list
         Grant further access;
      else
         Deny further access;
      end if;

   else
      Deny access to the user;
   end if;
```

Preserve EHR data integrity using a blockchain-based audit log model

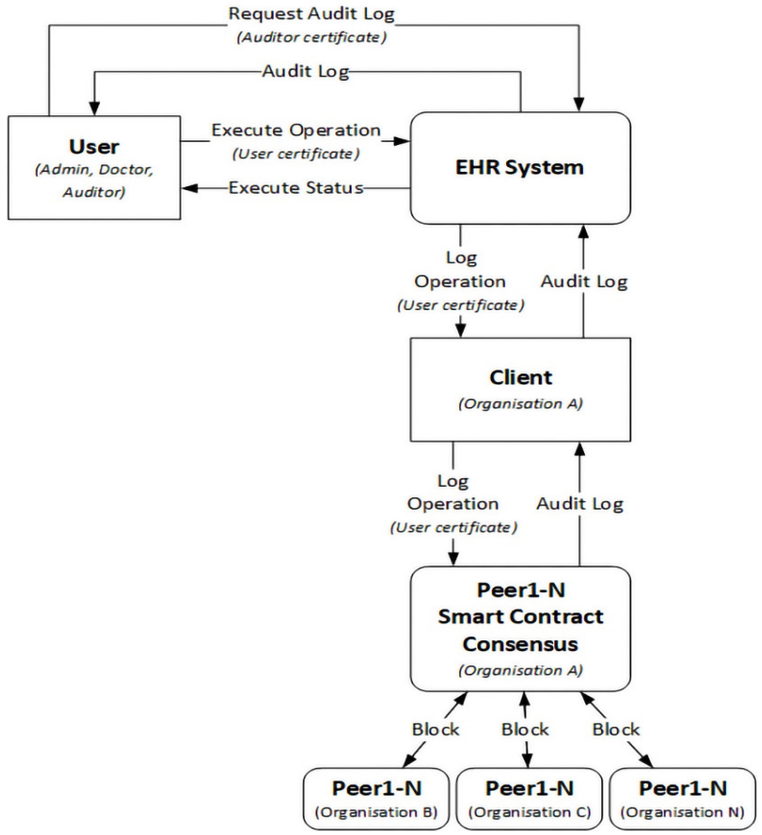
Problem addressed

Traditional EHR audit log systems are built around a centralised architecture. Audit logs are often stored in a relational database or on a file server. While these methods of storage work practically, they represent a single point of failure. Compromising one of these storage methods would enable cybercriminals to erase their tracks, thus allowing their actions to remain undetected. As a result, the integrity of the data stored in the relational database cannot be guaranteed. When dealing with the health information of patients, compromised data could have deadly consequences.

Motivation

Blockchain-based audit logs are permanent and tamper-evident. Blockchain is an append-only data structure that is distributed across several peers and cybercriminals would have to attack the majority of the peers in the network simultaneously to corrupt the audit log. This attack would not go unnoticed. Even if cyber-criminals did hijack a user's account, the changes made by the account would not go undetected. The changes made to the audit log would be appended, leaving the previous records intact. This could then be used to flag suspicious accounts and track the cybercriminals responsible. Data integrity can therefore be preserved through the use of blockchain technology.

Figure 7: Blockchain audit log data flow diagram



The blockchain approach

The information flow of the blockchain-based audit log model is illustrated in Figure 7. The data flow diagram is based on Figures 3 and 5. The audit log data flow diagram omits the authentication and authorisation process to simplify the diagram. The process assumes that a user has been authenticated. When a user attempts to execute an operation on the EHR system, an event is triggered, which sends metadata to the client. Metadata could include details such as the actions performed by a user on an object and the result of the performed actions. The metadata is sent from the client to the peers in the blockchain network. At a later stage, authorised auditors can request the audit log from the EHR system. The audit log could also be used by doctors to validate the integrity of EHR data in their possession. Figure 8 outlines pseudocode to retrieve an audit log by range. Figure 9 provides pseudocode to append an audit log entry to a blockchain network.

Figure 8: GetAuditLog() pseudocode

```
Function AuditLog GetAuditLog(Date startDate, Date endDate) {

  Do sanitisation check on the function inputs;
  Get the user certificate;
  Validate user certificate;
  Get user's attributes from certificate;

  if the user attributes match the authorisation rules
     return AuditLogByRange(startDate, endDate);
  else
     Deny access to the user;
     CreateUnauthorisedLogEntry(log);
  end if; }
```

Figure 9: AppendAuditLog() pseudocode

```
Function AppendAuditLog(AuditLog log) {

  Do sanitisation check on the function inputs;
  Get the device certificate;
  if device certificate is not valid then
     Deny access to the device;
  end if

  Get device attributes from certificate;
  if the device attributes match the authorisation rules
     Get user certificate;
     if user certificate is valid then
        CreateLogEntry(log);
     else
        CreateUnauthorisedLogEntry(log);
     end if
  else
     CreateUnauthorisedLogEntry(log);
     Deny access to the device;
  end if;  }
```

Ensure EHR data immutability by adopting a blockchain-based storage model

Problem addressed

Traditional storage models are mostly built around a centralised architecture such as a relational database. Relational databases do not store data in an immutable manner. This practice may not align with all the policies and regulations regarding the storage of EHRs.

Motivation

The nature of blockchain technology is to store records immutably in an append-only format. Storing EHRs in a blockchain network is mostly in line with the policies surrounding EHRs. Laws and policies differ from country to country or region to region, but the Health Professions Council of South Africa (HPCSA) stipulates that when health records are stored in an electronic format, they should be stored in an append-only format (HPCSA, 2016). Copies of the records should be made and stored in different physical locations. The copies are used to detect tampering with EHRs. Health records should also be kept for at least five years. The South African Protection of Personal Information (POPI) Act, however, states that users should be able to request that their personally identifiable information be purged from a service (RSA, 2013, sect. 24).

Relational databases satisfy the personally identifiable information requirements by supporting the purging of records as stipulated in legislation such as the POPI Act. Blockchain technology is aligned with these policies, as the data stored in a blockchain network is distributed across peer nodes situated in different physical locations. As blockchain technology stores data immutably, it cannot satisfy this requirement. Blockchain technology can, however, support the traditional centralised infrastructure by storing a hash of data that is contained in a relational database. This method of storing EHRs would enable stakeholders to run integrity checks on data stored in the traditional architecture. The hash of the data stored in the traditional storage model can be compared with the hash stored in the blockchain storage model. The two hashes should be identical to pass an integrity check. Blockchain technology can thus support the integrity of EHRs stored in traditional architecture.

The blockchain approach

The information flow of the blockchain-based storage model is illustrated in Figure 10. The data flow diagram is based on Figures 3 and 5. The storage data flow diagram omits the authentication and authorisation process to simplify the diagram. The process assumes that a user has been authenticated; when that user wants to view, add to, or edit a patient's record, they can do so by contacting the EHR system. The EHR system would then request or send the information to the blockchain client. The blockchain client then forwards the request to one of the peers in the network and the relevant smart contract code is then executed on the peer. The smart contract then proposes a transaction to the blockchain network. This transaction is bundled together into a block and appended to the blockchain. The consensus algorithm ensures that all the peers are synchronised.

Figure 10: Blockchain storage data flow diagram

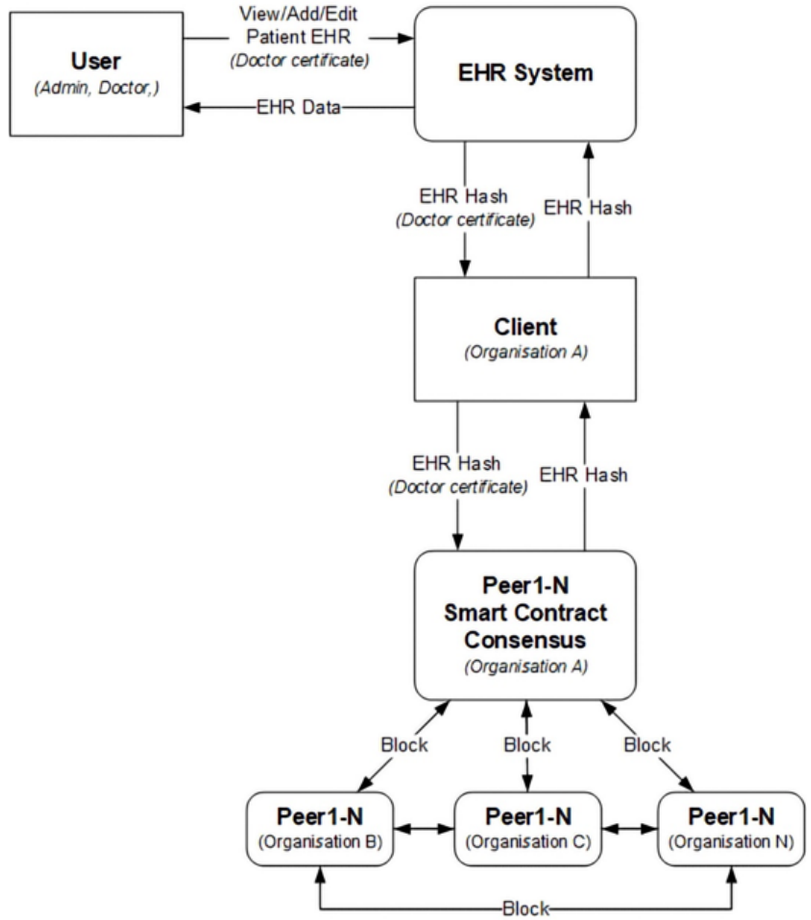


Figure 11 outlines pseudocode for adding or updating a record in the blockchain network. Retrieving records from the blockchain could be achieved with the pseudocode written in Figure 12.

Figure 11: AppendData() pseudocode

```
Function AppendData(Data data) {

   Do sanitisation check on the function inputs;
   Get the user certificate;
   Validate user certificate;
   Get user's attributes from certificate;
   if the user attributes match the authorisation rules
      CreateDataEntry(data);
   else
      Deny access to the user;
   end if;  }
```

Figure 12: GetData() pseudocode

```
response Function GetData(Key key) {

   Do sanitisation check on the function inputs;
   Get the user certificate;
   Validate user certificate;

   Get user's attributes from certificate;
   if the user attributes match the authorisation rules
      if user is present on authorisation list
         return GetData(key);
      else
         Deny access to the user;
      end if
   else
      Deny access to the user;
   end if;  }
```

Transact private EHR data using a blockchain-based transaction model

Problem addressed

The traditional transaction model relies on a third party to handle private information. The information would be sent from the sending client to a centralised third-party server back to the receiving client. This approach can increase the risk of a man in the middle attack.

Motivation

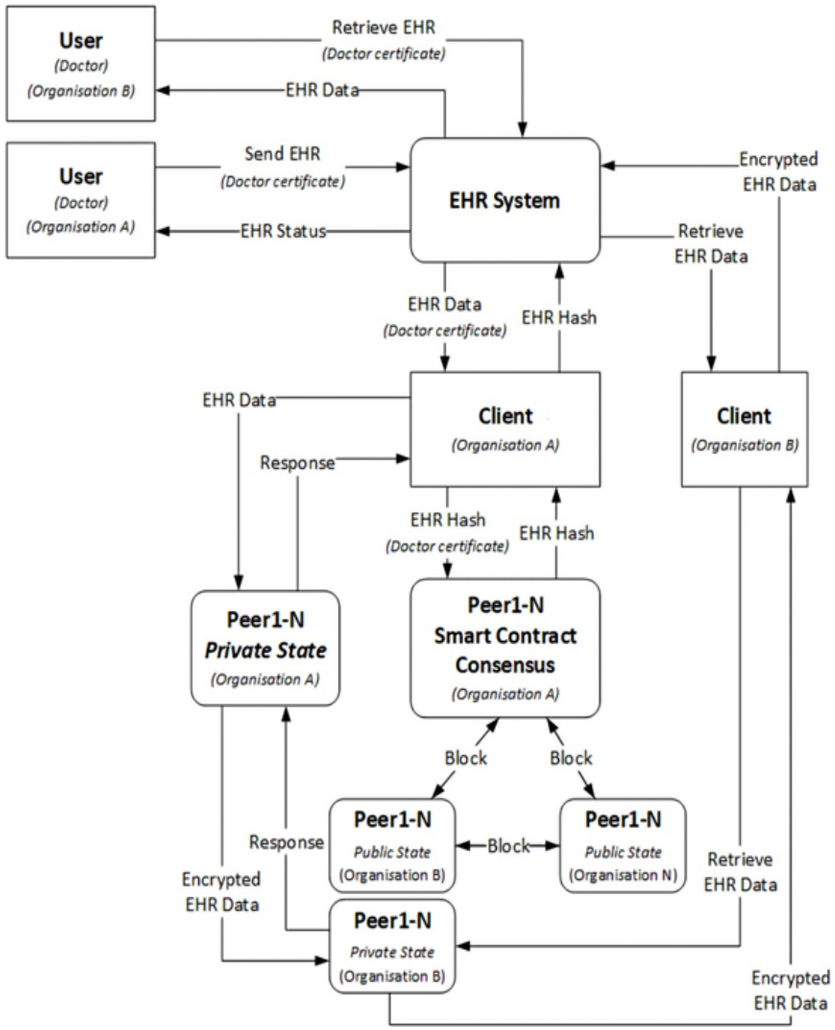
Blockchain technology enables a sending client to send private information directly to the receiving client without relying on a third party to relay the information, thus enabling healthcare providers to transact a patient's health records without relying on a third party.

Blockchain technology could be used as a synchronisation service to transact information between organisational data stores. Coupling the blockchain-based transaction model with the authentication, authorisation, and audit log model would establish a robust sync service with full audibility across multiple organisations, which could include hospitals, private practices, pathology laboratories, medical insurance companies, pharmacies, auditors, or medical boards. This would, in turn, enable patients to visit any healthcare provider that is a part of the blockchain network. The patient could then provide authorisation to the healthcare provider to sync their information with its data stores, essentially providing the healthcare provider with their EHR. The authentication, authorisation, and audit log model would be distributed across all the organisations, logically forming a single unified system. Blockchain technology could thus provide a robust semi-decentralised transaction model.

The blockchain approach

The information flow of the blockchain-based transaction model is illustrated in Figure 13. The data flow diagram is based on Figures 3 and 5. The transaction data flow diagram omits the authentication and authorisation process to simplify the diagram. The process assumes that a user has been authenticated. Users from one organisation can send a patient's EHR to another organisation, and the EHR system encrypts the record and sends it to the blockchain client. The blockchain client forwards the encrypted EHR data to all the organisational peers involved in the transaction. The respective peers store this transaction in their private state. This means that only the organisations involved in this transaction would have the EHR data stored in their peer's private state. The blockchain client then creates a hash of the transacted EHR data and broadcasts that to all the peer's public states. These peers also include peers from other organisations that are not a part of the transaction. This is to ensure a level of transparency and auditability across organisational bounds. The organisations' part of the transaction can then retrieve the EHR record from their peer's private state. The sending organisation could specify an expiration date for the transaction, meaning that the data would be available to an organisation only for a specific period. After the period has expired, the data is automatically purged from the blockchain and only the hash of the transaction remains.

Figure 13: Blockchain transaction data flow diagram



The *TransactData* method in Figure 14 outlines pseudocode to transact data between organisations that are part of the blockchain network. Retrieving transacted data could be achieved with the pseudocode function presented in Figure 15.

Figure 14: TransactData() pseudocode

```
Function TransactData(Transient data, Recipients recipients, Time TimeToLive) {

  Do sanitisation check on the function inputs;
  Get the users certificate;
  Validate users certificate;
  Get user's identity from certificate;
  Get user's attributes from certificate;

  if the user attributes match the authorisation rules
    if userID is present on authorisation list
        for each recipient
          Set data expiration date;
          Encrypt data with recipient public key;
          Encrypt data with recipient peer public key;
          Send data to receipt's peer private state;
        next
        StorePublic(senderSignature, recipients, dataHash) for all peers;
    else
        Deny further access;
    end if;

  else
     Deny access to the user;
  end if;   }
```

Figure 15: GetTransactedData() pseudocode

```
response Function GetTransactedData(Key key) {

  Do sanitisation check on the function inputs;
  Get the users certificate;
  Validate users certificate;
  Get user's identity from certificate;
  Get user's attributes from certificate;

  if the user attributes match the authorisation rules
    if userID is present on authorisation list
        Return GetPeerPrivateSate(key);
    else
        Deny further access;
    end if;

  else
     Deny access to the user;
  end if;  }
```

6. Conclusions and future work

To aid in the application of blockchain technology to existing or new EHR infrastructure, this study set out to present recommendations for applying blockchain technology to security-related services in an electronic healthcare record infrastructure. To this end, experimental setups were created to address specific requirements of EHRs, using blockchain technology. The insights gained from these experiments were condensed into a series of recommendations for the application of blockchain technology to security-related services in EHRs.

Although it is most certainly a viable alternative, blockchain technology is not necessarily the best solution in all cases. Its immutability is a strength when it comes to preserving details, but also a weakness in a world governed by privacy laws, regulations, and Acts, such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States, the European General Data Protection Regulation (GDPR), and South Africa's POPI Act. Implementation of the various technologies may also require expertise that may not be found among the administrators of existing EHR systems. The costs associated with the change in infrastructure may also be prohibitive. Therefore, the application of blockchain technologies may be a better choice for implementing new EHR systems and not for the conversion of existing systems.

The work presented in this study is experimental in nature and has been implemented only in a virtual environment. A future study will focus further on the shortcomings and strengths of EHRs, by surveying the stakeholders of existing EHR systems. These insights may then be used, along with further experimentation, to derive a model for the application of blockchain technology to security-related services in EHR systems. Future studies may also delve into how the concept of self-sovereign identity (SSI), which allows a person to have sole control over who may access their personal information (Ferdous et al., 2019), may be integrated into a blockchain-based EHR system.

References

Adlam, R., & Haskins, B. (2019). A permissioned blockchain approach to the authorization process in electronic health records. In IEEE (Ed.), *2019 International Multidisciplinary Information Technology and Engineering Conference (IMITEC)* (pp. 1–8). https://doi.org/10.1109/IMITEC45504.2019.9015927

Bashir, I. (2017). *Mastering blockchain.* Packt Publishing.

Bergquist, J. H. (2017). *Blockchain technology and smart contracts privacy-preserving tools.* Master's thesis, Uppsala University, Sweden. http://uu.diva-portal.org/smash/get/diva2:1107612/FULLTEXT01.pdf

Bünz, B., Bootle, J., Boneh, D., Poelstra, A., Wuille, P., & Maxwell, G. (2017). Bulletproofs: Short proofs for confidential transactions and more. In IEEE (Ed.), *2018 IEEE Symposium on Security and Privacy* (pp. 315–334). https://doi.org/10.1109/SP.2018.00020

Cilliers, L. (2017). Exploring information assurance to support electronic health record systems. In IEEE (Ed.), *2017 IST-Africa Week Conference (IST-Africa)* (pp. 1–8). https://doi.org/10.23919/ISTAFRICA.2017.8102363

Dagher, G. G., Mohler, J., Milojkovic, M., & Marella, P. B. (2018). Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustainable Cities and Society*, *39*, 283–297. https://doi.org/10.1016/j.scs.2018.02.014

Dekker, M. A. C., & Etalle, S. (2007). Audit-based access control for electronic health records. *Electronic Notes in Theoretical Computer Science*, *168*(1), 221–236. https://doi.org/10.1016/j.entcs.2006.08.028

Emmadi, N., Vigneswaran, R., Kanchanapalli, S., Maddali, L., & Narumanchi, H. (2019). Practical deployability of permissioned blockchains. In W. Abramowicz, & A. Paschke (Eds.), *Business information systems workshops* (pp. 229–243). Springer International. https://doi.org/10.1007/978-3-030-04849-5_21

Ferdous, M. S., Chowdhury, F., & Alassafi, M. O. (2019). In search of self-sovereign identity leveraging blockchain technology. *IEEE Access*, *7*, 103059–103079. https://doi.org/10.1109/ACCESS.2019.2931173

Ferraiolo, D., Kuhn, D. R., & Chandramouli, R. (2003). Role-based access control. Artech House.

Franqueira, V. N. L., & Wieringa, R. J. (2012). Role-based access control in retrospect. *IEEE Computer*, *45*(6), 81–88. https://doi.org/10.1109/MC.2012.38

Griggs, K. N., Ossipova, O., Kohlios, C. P., Baccarini, A. N., Howson, E. A., & Hayajneh, T. (2018). Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. *Journal of Medical Systems*, *42*(7), 130. https://doi.org/10.1007/s10916-018-0982-x

Guo, R., Shi, H., Zhao, Q., & Zheng, D. (2018). Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems. *IEEE Access*, *6*, 11676–11686. https://doi.org/10.1109/ACCESS.2018.2801266

Health Professions Council of South Africa (HPCSA). (2016). *Booklet 9: Guidelines on the keeping of patient records.*

Hyperledger. (2021). Hyperledger-fabricdocs documentation: Release master. Hyperledger. https://buildmedia.readthedocs.org/media/pdf/hyperledger-fabric/release-1.4/hyperledger-fabric.pdf

Hyperledger Architecture Working Group. (2017). Hyperledger architecture, volume 1. https://www.hyperledger.org/wp-content/uploads/2017/08/Hyperledger_Arch_WG_Paper_1_Consensus.pdf

Kshetri, N. (2017). Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommunications Policy*, *41*(10), 1027–1038. https://doi.org/10.1016/j.telpol.2017.09.003

Kshetri, N., & Carolina, N. (2018). Blockchain and electronic healthcare records. *IEEE Computer Society*, *51*(12), 59–63. https://doi.org/10.1109/MC.2018.2880021

Laurence, T. (2017). *Blockchain for dummies*. Wiley.

Liang, X., Zhao, J., Shetty, S., Liu, J., & Li, D. (2017). Integrating blockchain for data sharing and collaboration in mobile healthcare applications. In IEEE (Ed.), *2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)* (pp. 1-5). https://doi.org/10.1109/PIMRC.2017.8292361

Menachemi, N., & Collum, T. H. (2011). Benefits and drawbacks of electronic health record systems. *Risk Management and Healthcare Policy*, *4*, 47–55. https://doi.org/10.2147/RMHP.S12985

Mosakheil, J. H. (2018). Security threats classification in blockchains. *Culminating Projects in Information* Assurance, 48. https://repository.stcloudstate.edu/msia_etds/48/

Republic of South Africa (RSA). (2013). Protection of Personal Information Act 4 of 2013. *Government Gazette*, Vol. 581, No. 37067.

Ronquillo, J. G., Winterholler, J. E., Cwikla, K., & Szymanski, R. (2018). Health IT, hacking, and cybersecurity: National trends in data breaches of protected health information. *Journal of the American Medical Informatics Association*, *1*, 15–19. https://doi.org/10.1093/jamiaopen/ooy019

Saraf, C., & Sabadra, S. (2018). Blockchain platforms: A compendium. In IEEE (Ed.), *2018 IEEE International Conference on Innovative Research and Development (ICIRD)* (pp. 1–6). https://doi.org/10.1109/ICIRD.2018.8376323

Seol, K., Kim, Y.-G., Lee, E., Seo, Y.-D., & Baik, D.-K. (2018). Privacy-preserving attribute-based access control model for XML-based electronic health record system. *IEEE Access*, *6*, 9114–9128. https://doi.org/10.1109/ACCESS.2018.2800288

Thakkar, M., & Davis, D. C. (2006). Risks, barriers, and benefits of EHR systems: A comparative study based on size of hospital. *Perspectives in Health Information Management*, *3*(5), 1–19.

Ziglari, H., & Negini, A. (2017). Evaluating cloud deployment models based on security in EHR system. In IEEE (Ed.), *2017 International Conference on Engineering and Technology (ICET)* (pp. 1–6). https://doi.org/10.1109/ICEngTechnol.2017.8308142

E-Government Information Systems (IS) Project Failure in Developing Countries: Lessons from the Literature

Joseph B. Nyansiro
Doctoral student, Department of Computer Science and Engineering, University of Dar es Salaam
https://orcid.org/0000-0003-1523-7601

Joel S. Mtebe
Associate Professor, Department of Computer Science and Engineering, University of Dar es Salaam
https://orcid.org/0000-0003-2760-7673

Mussa M. Kissaka
Senior Lecturer, Department of Electronics and Telecommunication Engineering, University of Dar es Salaam
https://orcid.org/0000-0002-8607-7556

Abstract
E-government information systems (IS) projects experience numerous challenges that can lead to total or partial failure. The project failure factors have been identified and studied by numerous researchers, but the root causes of such failures are not well-articulated. In this study, literature on e-government IS project failures in developing-world contexts is reviewed through the application of qualitative meta-synthesis, design–reality gap analysis, and root cause analysis. In the process, 18 causal factors and 181 root causes are identified as responsible for e-government IS project failures. The most prevalent of the 18 causal factors are found to be *inadequate system requirements engineering* (with 22 root causes), *inadequate project management* (19 root causes), and *missing or incomplete features* (16 root causes). These findings can be of use to future researchers, policymakers, and practitioners seeking to identify methods of avoiding e-government IS failures, particularly in developing-world contexts.

Keywords
e-government, information systems (IS), project failure, literature review, qualitative meta-synthesis, design–reality gap analysis, ITPOSMO, root cause analysis

Acknowledgement
Google partially supported this work through the Google Africa PhD Fellowship Program.

DOI: https://doi.org/10.23962/10539/32210

Recommended citation
Nyansiro, J. B., Mtebe, J. S., & Kissaka, M. M. (2021). E-government information systems (IS) project failure in developing countries: Lessons from the literature. *The African Journal of Information and Communication (AJIC), 28*, 1-29.
https://doi.org/10.23962/10539/32210

1. Introduction

E-government information systems (IS) are increasingly becoming essential tools for the delivery of government services and the improvement of government administration in developing-world countries. Such systems enable citizens to access government services at a relatively low cost compared to traditional face-to-face services, making government services more convenient and accessible (Gilbert et al., 2004). These systems also transform the relationships between governments and their citizens by reducing citizens' personal interactions with government staff, thus increasing transparency and reducing corruption (Sun et al., 2015).

In Tanzania, notable e-government systems include the electronic payment gateway (GePG), which facilitates the collection of government revenues electronically from various sources, while simplifying the way citizens pay government bills (i.e., making payments through mobile phones and banks). Similarly, the traffic management system (TMS) facilitates the payment of drivers' fines by electronic means. The Ministry of Lands Information System (MOLIS) enables citizens to perform self-assessments of land rent and accrued penalties due to delayed payment, to generate bills, and to pay through the GePG. The system has helped to avoid multiple allocations of plots and minimise citizens' complaints about plot allocations. Other notable information systems include the national payment system (NPS), the electronic clearing house (ECH), the integrated financial management system (IFMS), the integrated human resource and payroll system, and the retail payment system (RPS) (Ministry of Works, Transport and Communication, 2016; Sæbø, 2012).

However, many e-government projects in Tanzania, as in other developing countries, have experienced challenges leading to total or partial failure (Gunawong & Gao, 2017). For example, Tanzania's Mwananchi portal—launched in 2009, revamped in 2014, and designed to act as the main information gateway between citizens and the government—was abandoned. And an e-claims system, acquired by the National Health Insurance Fund (NHIF) of Tanzania to facilitate the processing of insurance claims by health service providers, was delivered and accepted with critical features missing. As a result, some of the essential claim processing steps, including data exchange between subsystems, were performed manually. The system was prone to errors, labour-intensive, and took a long time to process claims (National Audit Office of Tanzania, 2019). Another project had to be initiated to fix the identified problems.

In Lesotho, an evaluation of four e-government websites revealed that they were missing critical features and functionalities in terms of accessibility, usability, transparency, and interactivity (Thakur & Singh, 2012). In South Africa, the eThekwini Municipality's Revenue Management System (RMS) project, initiated in 2003, was only completed in 2016 and had a budget overrun of 666% (Comins, 2020; Thakur & Singh, 2012).

In an effort to better understand the main causes of e-government IS project failures in developing-world contexts, we conducted a literature review that applied qualitative meta-synthesis, design–reality gap analysis, and root cause analysis.

2. Research design

Analytical frameworks

Qualitative meta-synthesis

Qualitative meta-synthesis is a research method that involves the collection, interpretation, translation, and synthesis of findings across multiple qualitative studies (Sandelowski et al., 1997). The authors selected this method because most studies on e-government project failure are qualitative. This method is suitable for studies that require the integration of results from multiple qualitative studies as it combines both literature review and critical interpretation.

Design–reality gap analysis

In influential working papers on e-government for development, Heeks (2003; 2001) posits that most e-government project failures are the result of "design–reality gaps". Heeks (2003; 2001) proposes seven dimensions that must be analysed in order to understand these gaps, using the acronym "ITPOSMO" to represent the seven dimensions, as follows:

- information;
- technology;
- processes;
- objectives and values;
- staffing and skills;
- management systems and structures; and
- other resources: time and money (Heeks, 2003, p. 3).

Root cause analysis

Root cause analysis seeks to understand what happened and why it happened (Livingston et al., 2001). Al-Ahmad et al. (2009) use root cause analysis to review the literature on information technology (IT) project failures, finding that root causes fall under six factors: project management, top management, technology, organisational, complexity, and processes. Dalal and Chhillar (2013) conducted an empirical study to determine the root causes of software failures. According to Dalal and Chhillar (2013), the primary cause of software failure was inadequate testing due to insufficient testing tools, insufficient test cases, and lack of negative testing. Other root causes were inadequate project planning, requirement engineering, and design.

Methodology

Data collection

We performed multiple rounds of searches through different libraries, including Google Scholar, ACM Digital Library, Research Gate, IEEE Xplore, Springer, and Science Direct. The following keywords were used: e-government project failure; a case study of e-government project failure; causes of e-government project failure; factors leading to e-government project failure; the success of e-government projects; barriers of e-government systems; challenges of e-government projects; and issues of e-government projects. A total of 86 studies were found, and 64 articles were selected to be used in this study. The chosen studies were academic research articles and industrials research reports with a primary focus on the failure or success of e-government IS projects.

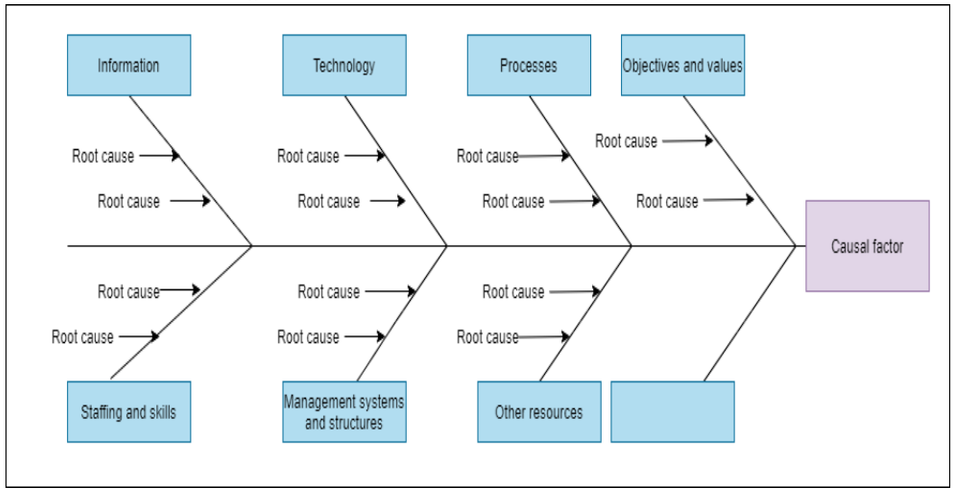
Causal factor charting

We used qualitative meta-synthesis to identify, across the 64 pieces of literature, the main causal factors that have been found to be responsible for IS project failure. Eighteen causal factors were identified. Additional literature searching was conducted to locate articles focusing on the identified causal factors and their root cause. A number of additional articles were identified, covering the following themes: user involvement (2 articles), e-government project management (6), e-government architecture (2), technology complexity (4), software testing (2), e-government infrastructure (3), information (2), requirement engineering (5), business processes management in governments (5), change management (2), management structure (2), e-government skills (2), top management involvement (1), and e-government systems integration (1).

Root cause identification

Fishbone diagrams were used to visualise the identified root causes linked to each of the 18 causal factors. The seven ITPOSMO design–reality gap dimensions served as root cause categories for each causal factor, drawn as branches connected to the backbone (the causal factor). The root causes identified in the literature were then mapped onto each of the seven root cause categories, as illustrated in Figure 1.

Figure 1: Fishbone diagram with seven root cause categories (ITPOSMO dimensions)



3. Findings

A total of 18 causal factors were identified in the literature via qualitative meta-synthesis, as shown in Table 1.

Table 1: Causal factors identified in existing literature

	Causal factor	Literature
1	Inadequate system requirements engineering	Baguma & Lubega (2013), Goedeke et al. (2017), Hussain, Mkpojiogu, & Abdullah, (2016), Sweis (2015), Hofmann & Lehner (2001), Bubenko (1995), Michael & Boniface (2014), Zakaria et al. (2011)
2	Inadequate project management	Afyonluoğlu et al. (2014), Aikins (2012), Baguma & Lubega (2013), Goedeke et al. (2017), Gunawong & Gao (2017), Hossan et al. (2006), Imran et al. (2017), Rajapakse et al. (2012), Rajala & Aaltonen (2020), Sweis (2015), S. R. A. Shah et al. (2011), Twizeyimana et al. (2018)
3	Missing or incomplete features	Baguma & Lubega (2013), Damoah & Akwei (2017), Goedeke et al. (2017), Gunawong & Gao (2017)
4	Inadequate project planning	Aikins (2012), Baguma & Lubega (2013), Bakunzibake et al. (2018), Ghapanchi & Albadvi (2008), Goedeke et al. (2017), Hossan et al. (2006), Rajala & Aaltonen (2020), Rajapakse et al. (2012), Twizeyimana et al. (2018)
5	Inappropriate choice of technology	Goedeke et al. (2017), Ghapanchi & Albadvi (2008), Lau (2003)
6	Insufficient top management support	Aikins (2012), Baguma & Lubega (2013), Bakunzibake et al. (2018), Goedeke et al. (2017), Ojha & Pandey (2017), Sweis (2015)

	Causal factor	Literature
7	Integration failure	Al-Khanjari et al. (2014), Ghapanchi & Albadvi (2008), Goedeke et al. (2017), Lam (2005)
8	Procurement and contract shortcomings	Goedeke et al. (2017), Ojha & Pandey (2017), Rajapakse et al. (2012)
9	Inadequate business process management (BPM)	Afyonluoğlu et al. (2014), Baguma & Lubega (2013), Bakunzibake et al. (2018), Dada (2006), Goedeke et al. (2017), Gartlan & Shanks (2007), Martin & Montagna (2006), Reffat (2003), Swartz (2018), Trkman (2010)
10	Insufficient IS testing	Goedeke et al. (2017), Mansor & Ndudi (2015), Rajala & Aaltonen (2020), Rajapakse et al. (2012)
11	Insufficient change management	Afyonluoğlu et al. (2014), Aikins (2012), Bakunzibake et al. (2018), Ghapanchi & Albadvi (2008), Dada (2006), Hossan et al. (2006), Nograsek (2011)
12	Staffing and skills shortfalls	Abbas et al. (2017), Baguma & Lubega (2013), Dada (2006), Goedeke et al. (2017), Hossan et al. (2006), Rajala & Aaltonen (2020), Rajapakse et al. (2012), Ojha & Pandey (2017), Twizeyimana et al. (2018), Zakaria et al. (2011)
13	Technical over-complexity	Goedeke et al. (2017), Abbas et al. (2017), Botchkarev & Finnigan (2015), Sweis (2015), Lau (2003), Mukherjee (2008)
14	Obsolete technology	Baguma & Lubega (2013), Goedeke et al. (2017)
15	Information gaps	Heeks (2001), Rajapakse et al. (2012), Vyas et al. (2014)
16	Inadequate infrastructure	Baguma & Lubega (2013), Dahiya & Mathew (2018), Bakunzibake et al. (2018), Goedeke et al. (2017), Hossan et al. (2006), Rahman et al. (2014), Twizeyimana et al. (2018)
17	Political interference	Abbas et al. (2017), Baguma & Lubega (2013), Hossan et al. (2006), Rajala & Aaltonen (2020), Toots (2019)
18	Inappropriate organisational management structure	Abbas et al. (2017), Goedeke et al. (2017), Rajala & Aaltonen (2020), S. R. A. Shah et al. (2011)

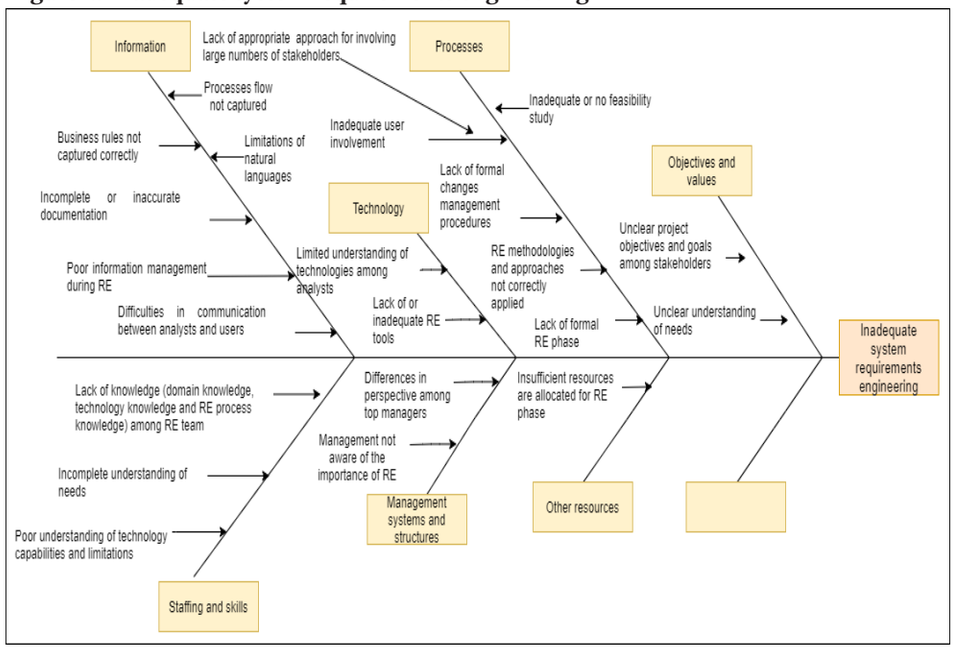
For each of the 18 causal factors tabulated above, root causes were identified in the literature, and mapped onto fishbone diagrams. The 18 sub-sections that follow explain each of the causal factors and provide a fishbone diagram for each causal factor's root causes.

Inadequate system requirements engineering

Requirements engineering is the process of discovering, documenting, and analysing services to be offered by a given system and the constraints under which those services should be provided (Feldgen & Clua, 2014). It involves systematic investigation and studying existing systems, processes, materials, operating environments, users' needs, and other artefacts to establish the new system's needs (Ullah et al., 2011). Bail (2010) estimated that inadequate system requirements specifications caused 50% of

IS project failures. For instance, the student information system implemented by the Uganda Management Institute (UMI) failed because it missed vital features in the finance module. The analyst failed to include these features' requirements in the initial requirements specification document (Baguma & Lubega, 2013). Requirements engineering problems include missing requirements, incomplete requirements, ambiguous requirements, poor requirement traceability, elicitation of irrelevant requirements, and poor requirements management (Shah & Patel, 2014). The root causes of inadequate information system requirements engineering are presented in Figure 2.

Figure 2: Inadequate system requirements engineering

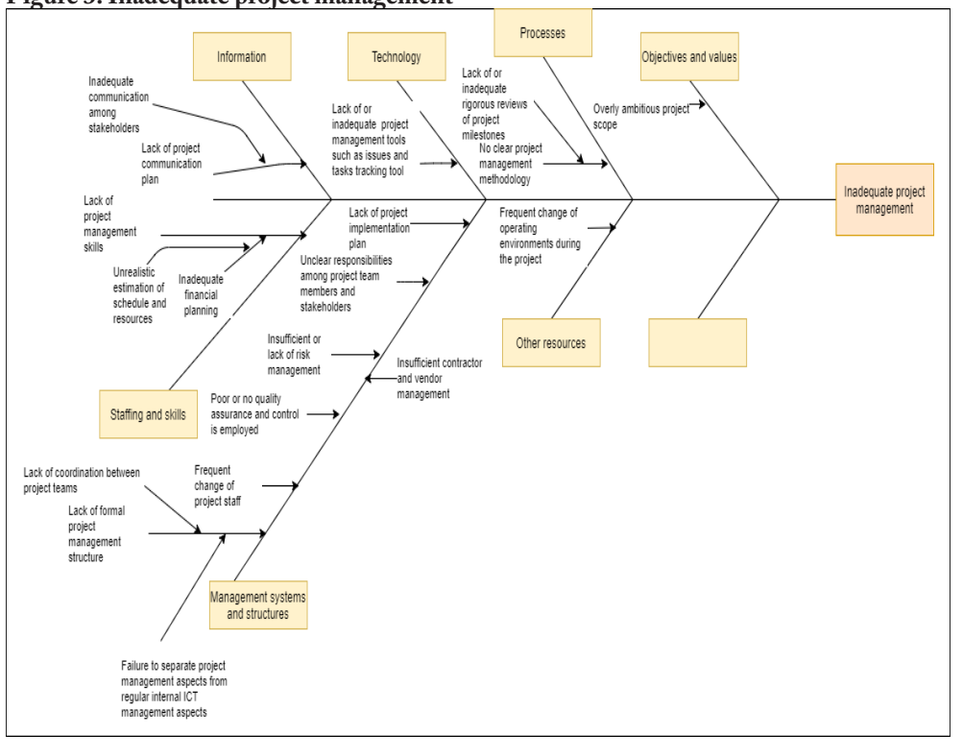


Inadequate project management

Project management is the application of knowledge, skills, tools, and techniques to guide the project activities in accordance with project objectives and goals (Imran et al., 2017). Many e-government IS projects fail due to inadequate project management. The electronic National Traffic Information System (e-NaTIS) in

South Africa failed mainly due to poor project management (Rajapakse et al., 2012). E-government projects should adopt proven project management methodologies, align their goals with organisational strategic goals, and hire competent people to manage them (Aikins, 2012). The root causes of inadequate project management are shown in Figure 3.

Figure 3: Inadequate project management

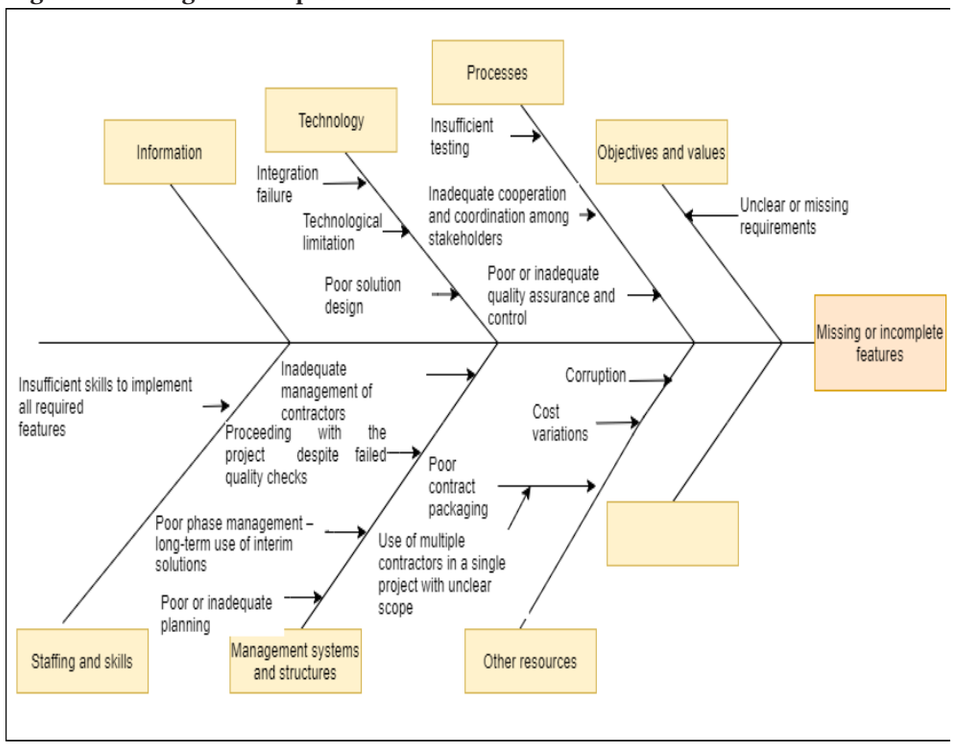


Missing or incomplete features

An IS project is said to be successful if it is delivered within time, budget, and with desired quality, features, and usability that reflects the real needs of the customers or users (Hussain, Mkpojiogu, & Abdullah, 2016). In some cases, e-government IS

projects are delivered and accepted with missing or incomplete vital features, thus failing to function and provide the anticipated results (Baguma & Lubega, 2013; Damoah & Akwei, 2017). This practice leads to a total or partial failure of the e-government IS project. For example, the Friend a Gorilla project in Uganda, implemented to raise awareness and funds for promoting Gorilla conservation, was delivered without crucial features for the online selling of promotional materials and SMS-based Gorilla friending (Baguma & Lubega, 2013). Several root causes can lead to the delivery of incomplete projects, including government officials' compromises due to corruption, and the failure to follow the correct procedures (Damoah & Akwei, 2017). Other root causes are as indicated in Figure 4.

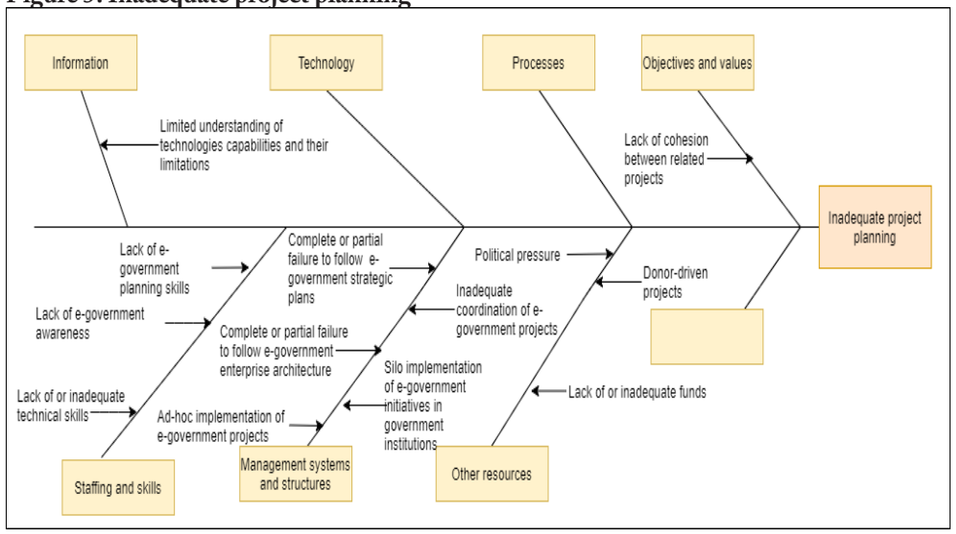
Figure 4: Missing or incomplete features



Inadequate project planning

The project plan outlines activities, timelines, resources, risks, constraints, expected output, and baseline information against which the project can be conducted, monitored, and evaluated (Imran et al., 2017). Many of the challenges facing e-government projects can be avoided or minimised if projects are thoroughly planned (Ghapanchi & Albadvi, 2008). The e-Revenue License project in Sri-Lanka is considered a successful e-government initiative because it was adequately planned (Rajapakse et al., 2012). The root causes of inadequate project planning are shown in Figure 5.

Figure 5: Inadequate project planning

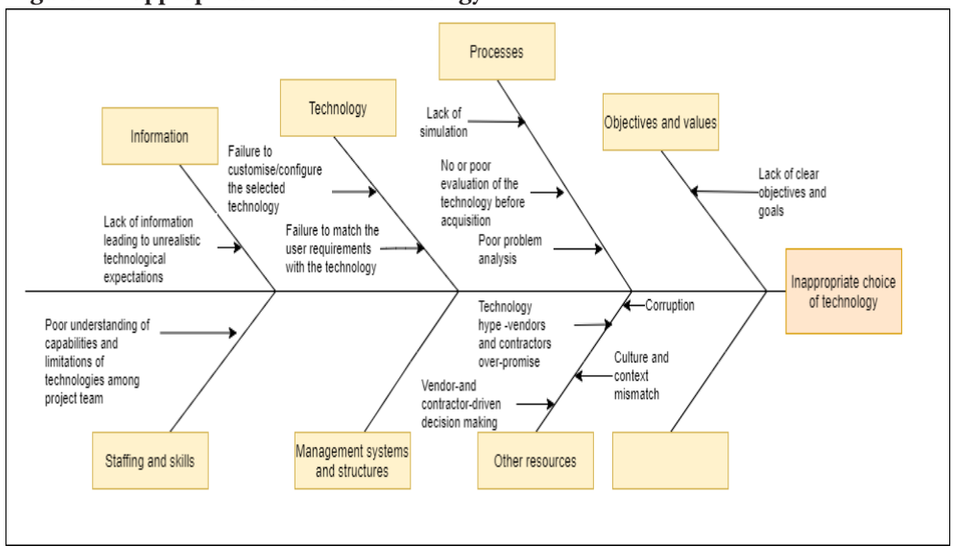


Inappropriate choice of technology

When selecting technology for a particular project, several factors must be considered, including easy to learn and use, fit for the purpose, easy to integrate with existing systems, availability of documentation and support, availability of skills, overall implementation costs, overall perceived quality, and usefulness (Hussein et al., 2007). Factors such as vendor hype and corruption may influence the choice of technology, leading to what is commonly known as vendor-driven projects (Damoah & Akwei, 2017). Thailand's smart card project, as described by Gunawong and Gao (2017), is an example of the use of inappropriate technology in an e-government initiative.

This project, which was launched in 2003 and abandoned in 2006, produced smart cards that could not be used electronically. Governments are advised to thoroughly evaluate the technologies before contracting suppliers (Lau, 2003). The root causes of inappropriate choice of technology are shown in Figure 6.

Figure 6: Inappropriate choice of technology

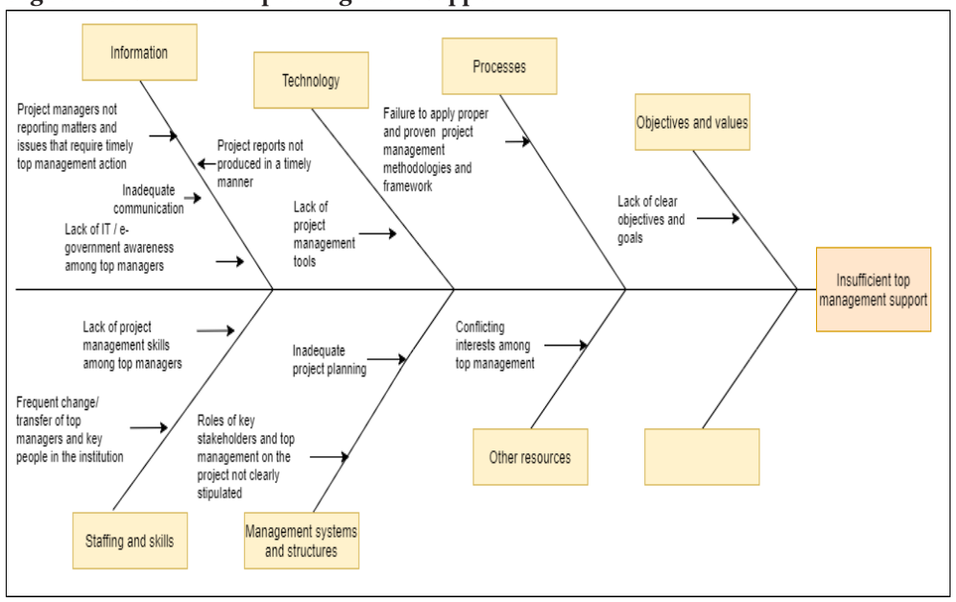


Insufficient top management support

As owners and sponsors of the e-government IS project, top managers are expected to closely follow up on critical aspects of the project, including ensuring that the project goals, objectives, vision, and values reflect those of the organisation. Top managers have to ensure that the project is managed according to the organisation's standards and that resources are made available in a timely fashion. They also have to ensure that project risks are identified and adequately mitigated. A systematic review of the project will ensure that milestones are accomplished in a timely fashion and

that project resources are appropriately used. Finally, top managers must promote the project to internal and external stakeholders (Ojha & Pandey, 2017; Zwikael, 2014). The root causes of insufficient top management support are shown in Figure 7.

Figure 7: Insufficient top management support

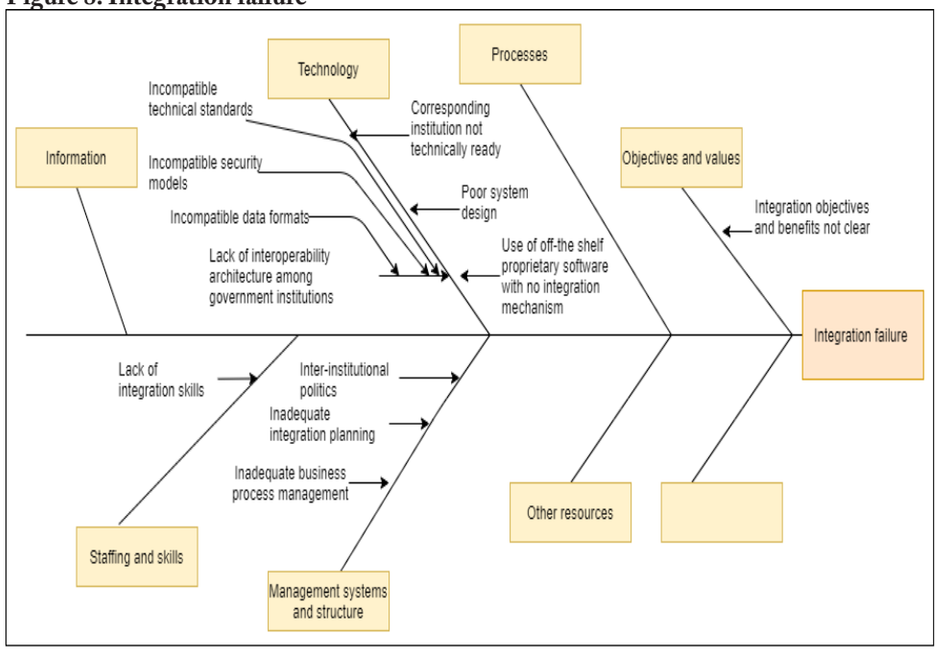


Integration failure

Delivering seamless services requires e-government systems to be integrated vertically and horizontally (Layne & Lee, 2001). However, this has been difficult to achieve (Sun et al., 2015). According to Lam, W. (2005), e-government systems integration challenges are categorised into four main categories: strategy, technology, policy, and organisation. Most government institutions and agencies develop their e-government systems independent from one another without paying much attention to how other government institutions and agencies might interact with them (Al-Khanjari et al., 2014). For example, integration between the citizen help requests (CHR) system designed by Bangladesh Police to facilitate online incident reporting and an identification system to authenticate the requesters failed due to technology and

organisational issues. Therefore, the police kept receiving requests with fake names, addresses, and contact information (Hasan, 2015). The root causes of integration failure are shown in Figure 8.

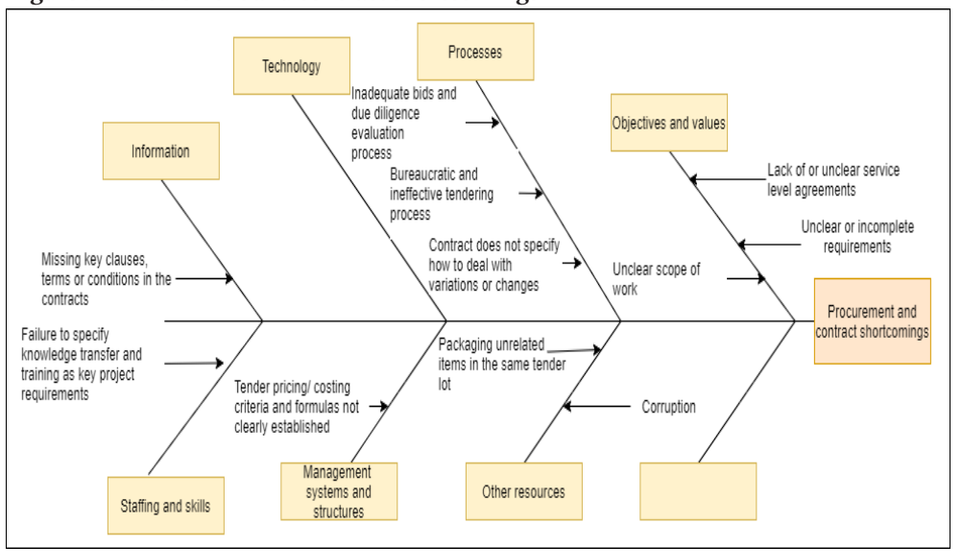
Figure 8: Integration failure



Procurement and contract shortcomings

Government institutions outsource most e-government IS projects to external vendors, contractors, and suppliers through legally binding contracts. Different forms of public-private partnerships are used in some cases (Ojha & Pandey, 2017). In either situation, it is essential to have a contract that specifies the parties involved, their obligations, the consequences for failure to meet the obligations, and settlement procedures for disagreement (Afyonluoğlu et al., 2014). Failure to have a fair contract may lead to legal issues, which may eventually lead to project failure. Figure 9 presents the root causes of procurement and contract shortcomings.

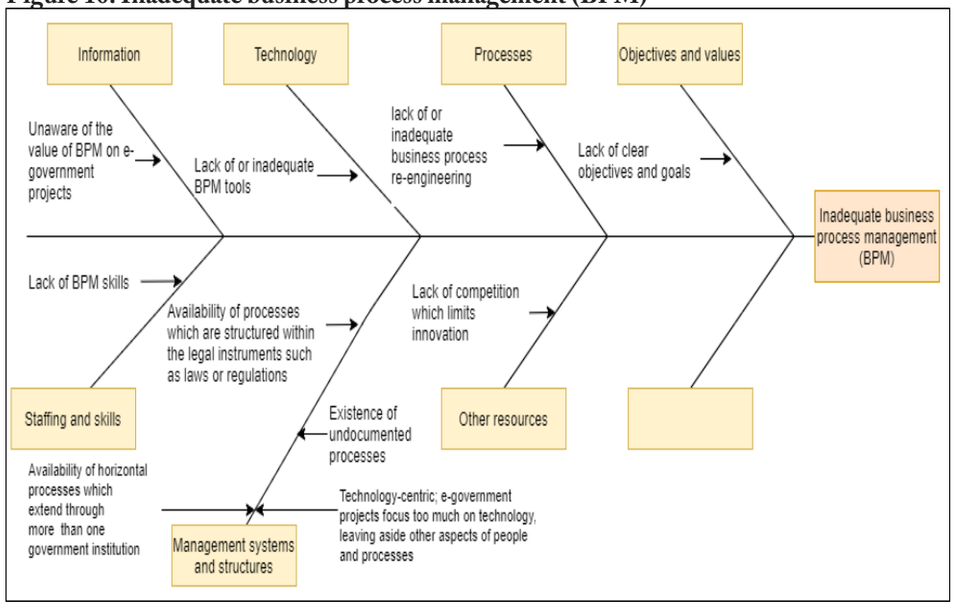
Figure 9: Procurement and contract shortcomings



Inadequate business process management (BPM)

Business process management (BPM) is an organisational strategy to identify, model, analyse, measure, automate, optimise, and continually improve fundamental activities in an organisation (Trkman, 2010). The overall objective of e-government initiatives is to improve public service delivery and enhance administration processes through e-services. In this case, BPM and e-government are two initiatives that have to go together as they complement each other. Unfortunately, most e-government IS projects are designed without BPM as a significant component (Martin & Montagna, 2006). Implementing an e-government information system without undertaking process re-engineering may lead to undesirable results and eventually project failure. The root causes of inadequate BPM are shown in Figure 10.

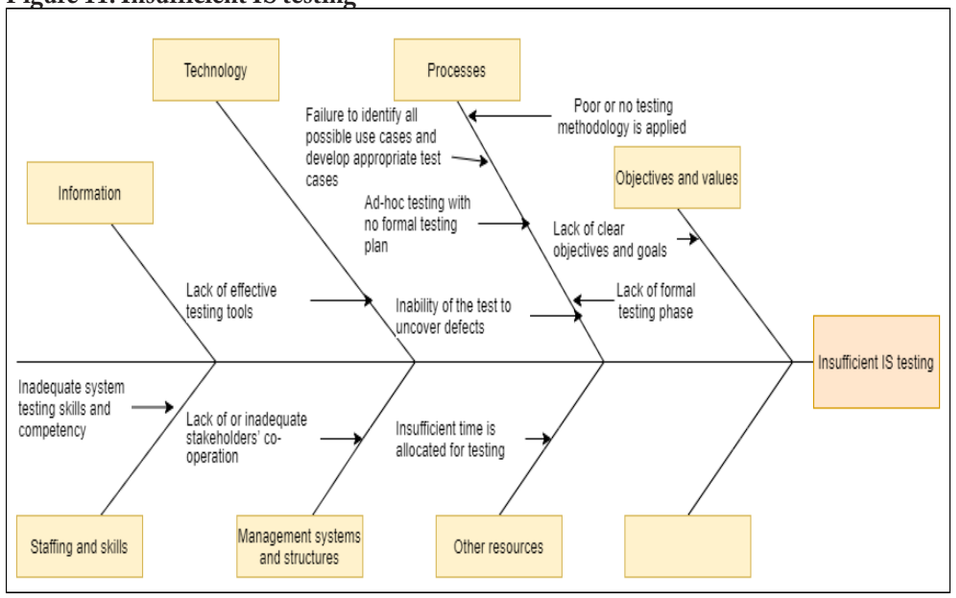
Figure 10: Inadequate business process management (BPM)



Insufficient IS testing

IS testing is one of the critical phases in the system development life cycle, aiming to verify, validate, detect, and fix errors in the system (Chaudhary, 2017). During the verification process, the developed system is checked to assess its conformity against the specified requirements. Insufficient system testing leads to the system's inability to meet stakeholders' expectations and needs, leading to abandonment (Mansor & Ndudi, 2015). The root causes of insufficient IS testing are shown in Figure 11.

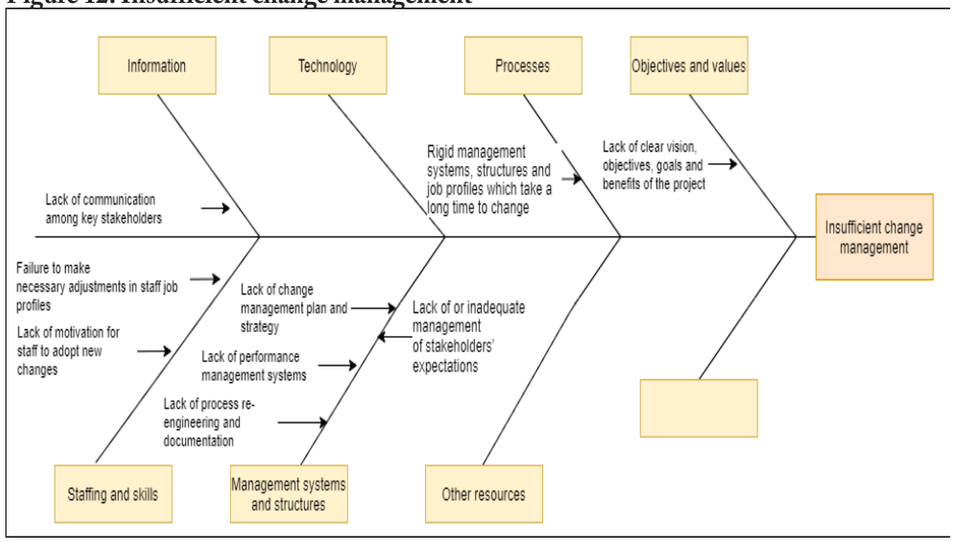
Figure 11: Insufficient IS testing



Insufficient change management

E-government projects are transformational as they tend to change the business process, service delivery mechanisms, and organisational structure (Afyonluoğlu et al., 2014). Successful transformation requires an appropriate change management process. Some e-government systems projects fail due to the institution's inability to make the necessary institutional rearrangements to shift from the old processes to the new processes offered by the developed e-government IS. A practical change management framework to support the successful implementation of the e-government system project must consider all the organisation's aspects, including technology, administration, operation, legislation, people, and organisation (Afyonluoğlu et al., 2014; Nograsek, 2011). The root causes of insufficient management are shown in Figure 12.

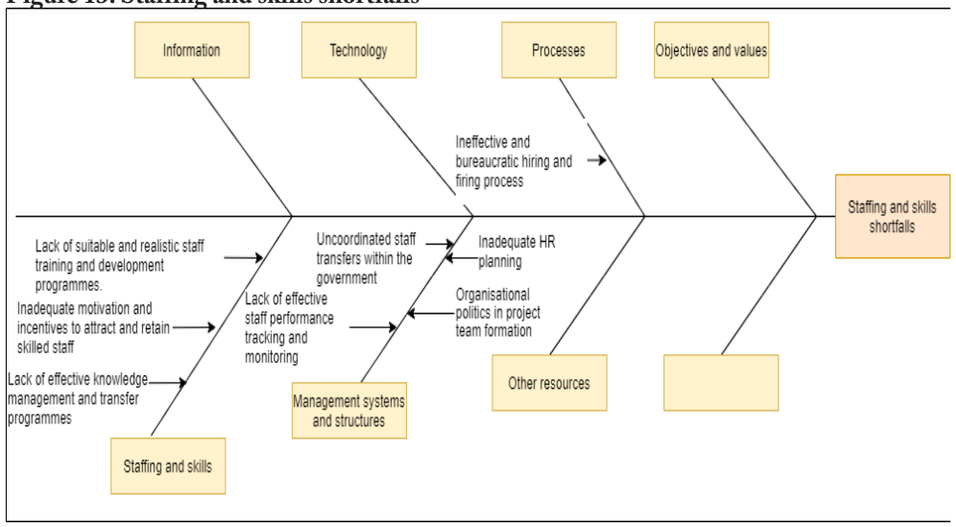
Figure 12: Insufficient change management



Staffing and skills shortfalls

An effective e-government project implementation team must possess essential skills, including: strategic information technology skills, information society skills, information management skills, technical skills, project management skills, and communication and presentation skills (Lau, 2003; Al Salmi et al., 2017). Most governments in developing countries suffer from a severe shortage of skilled staff (Rahman et al., 2014). The lack of relevant technical skills within the e-government project team negatively impacts the information systems quality (Ghapanchi & Albadvi, 2008). Khan and Islamabad (2009) estimated that Pakistan's government is getting barely 40% of results from its investment in e-government initiatives due to the lack of a skilled workforce. The root causes of staffing and skills shortfalls are shown in Figure 13.

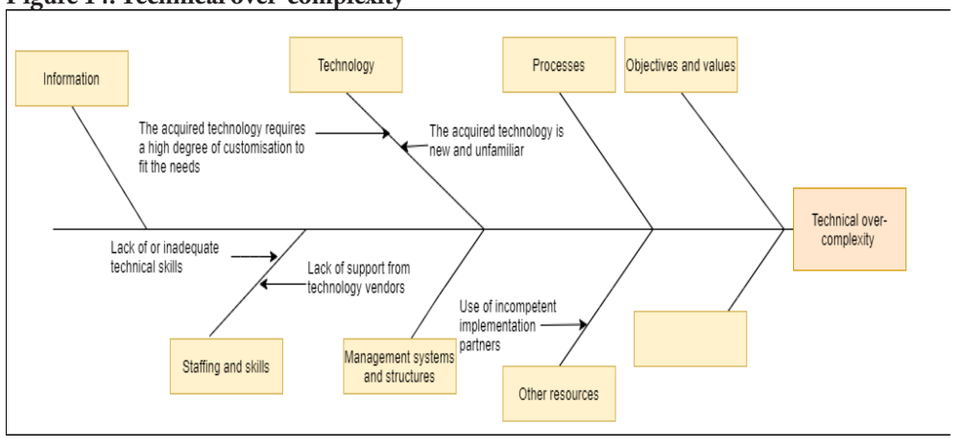
Figure 13: Staffing and skills shortfalls



Technical over-complexity

In this context, technical complexity refers to the difficulty of solving a given problem using the technology in question. It includes the inability to precisely determine information and processing requirements, data communication, and the overall system design, setup, and configurations (Xia & Lee, 2005). Lack of intensive technology evaluation is a leading cause of technical complexities and problems in e-government IS projects. Learning from previous project mistakes is crucial in mitigating risks and failures in new projects (Mukherjee, 2008). Figure 14 presents the root causes of technical over-complexity.

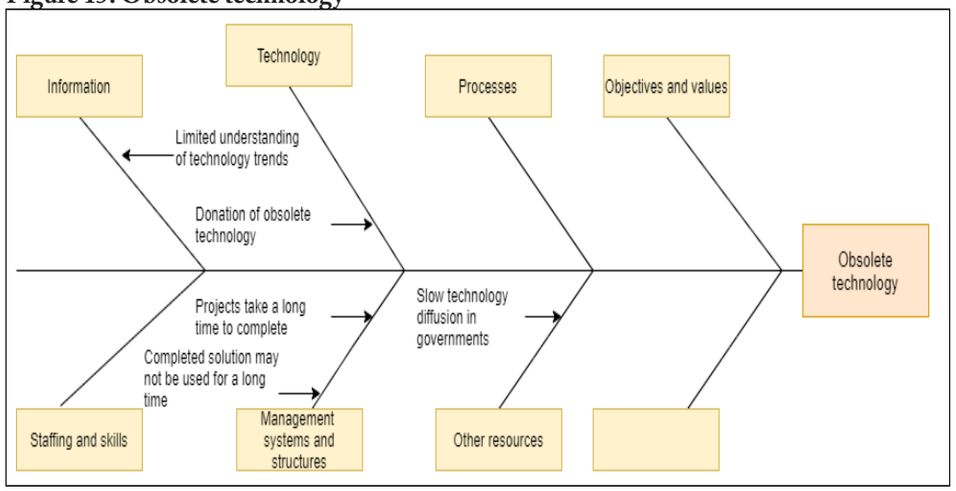
Figure 14: Technical over-complexity



Obsolete technology

The planning and implementation of e-government systems projects take a relatively long period of time. Consequently, some e-government projects are delivered while their associated technologies are or are about to become obsolete. Developing countries also suffer from adopting outdated technology when technological equipment and systems are donated by developed countries. The root causes of obsolete technology are shown in Figure 15.

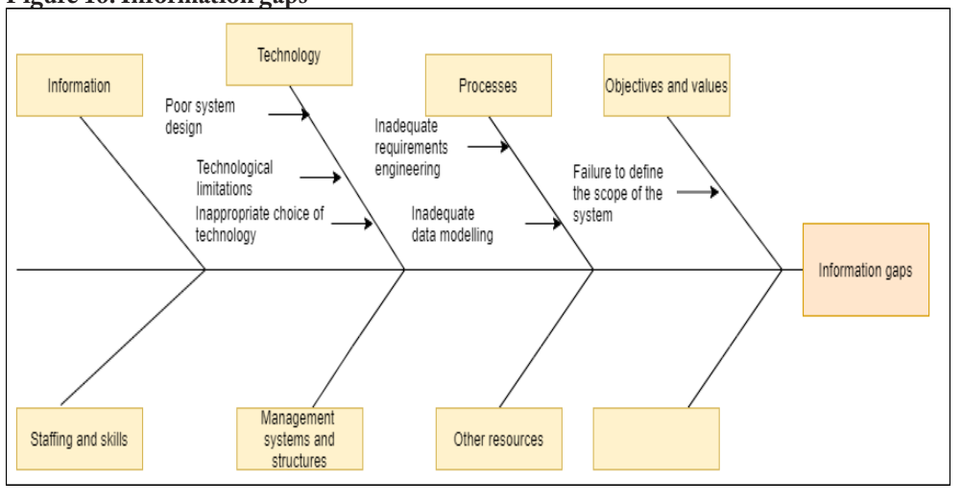
Figure 15: Obsolete technology



Information gaps

Mismatch of data between what is captured or produced by the system and what is required by users of the system can lead to e-government IS failure (Heeks, 2001). In e-government IS, the information gaps exist in three situations: capturing unnecessary information not required for processing or reporting; the failure to capture essential information necessary for processing or reporting; and asking for particular information that may not be available or relevant to some users or scenarios. For instance, the citizen help requests (CHR) system designed by Bangladesh Police required a request to have a valid signature of the requestor to start the investigation (Hasan, 2015). Citizens' inability to provide digital signatures online made the system unusable (Hasan, 2015). The root causes of information gaps are shown in Figure 16.

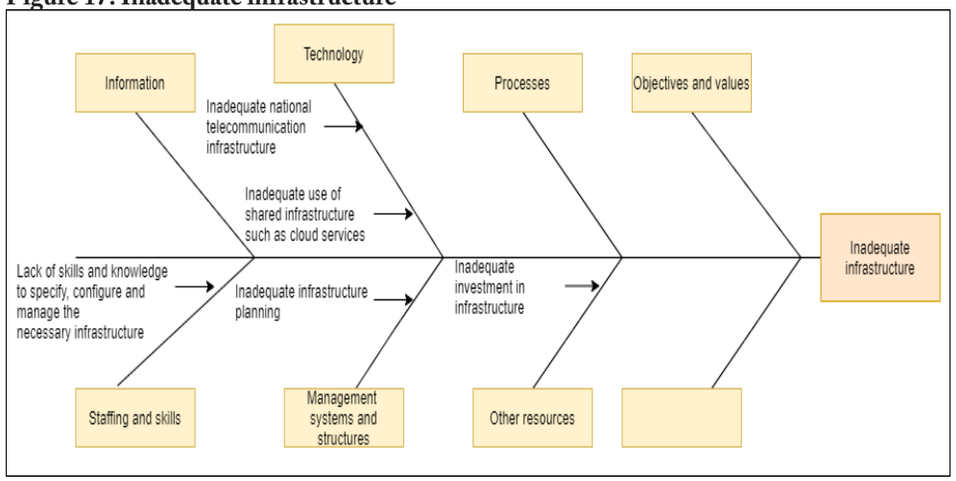
Figure 16: Information gaps



Inadequate infrastructure

E-government infrastructure encompasses hardware platforms, software platforms, middleware, data communications equipment, networks, backup hardware, disaster recovery hardware, and security technologies (Dahiya & Mathew, 2018). These devices and equipment make it possible to offer e-government services that are accessible to users. In IT, the performance and effectiveness of infrastructure are measured with reference to: reliability – its ability to ensure continuous uptime; scalability – its ability to accommodate increased load; and flexibility – its ability to accommodate changes that may be required (Dahiya & Mathew, 2018). The root causes of inadequate infrastructure are presented in Figure 17.

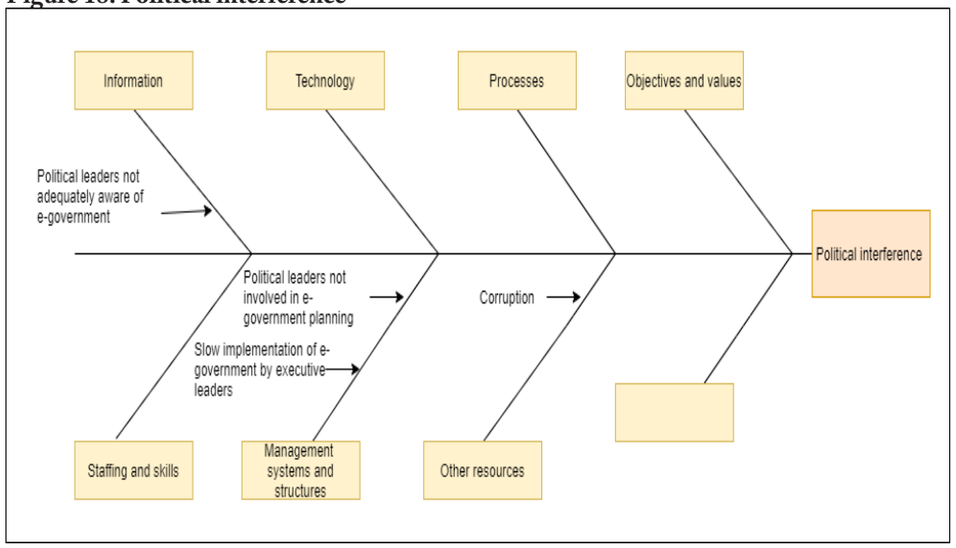
Figure 17: Inadequate infrastructure



Political interference

Governments are run by politicians who influence many aspects of decision making, leadership, and development initiatives. Politicians influence many government projects in positive or negative ways through several means, such as appointing personnel responsible for projects, manipulating project scopes and deliverables to suit their political interests, and making various decisions (Baguma & Lubega, 2013; Rajala & Aaltonen, 2020). E-government IS projects may also similarly suffer or benefit from political interference. The root causes of political interference are shown in Figure 18.

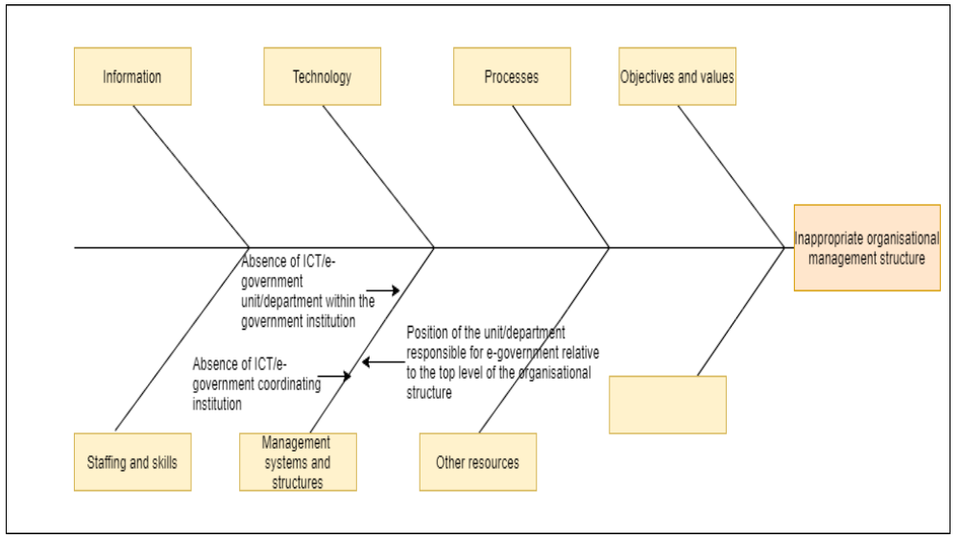
Figure 18: Political interference



Inappropriate organisational management structure

Government institutions are structured to support their core mandates. They employ a hierarchical structure with bureaucratic leadership, tight relationships, and rigid rules and procedures (Matte, 2017). Organisational structure is a critical element of e-government governance. Organisations implementing e-government initiatives must undertake the necessary reforms to accommodate and manage the e-government system's changes. The root causes of inappropriate organisational management structure are shown in Figure 19.

Figure 19: Inappropriate organisational management structure

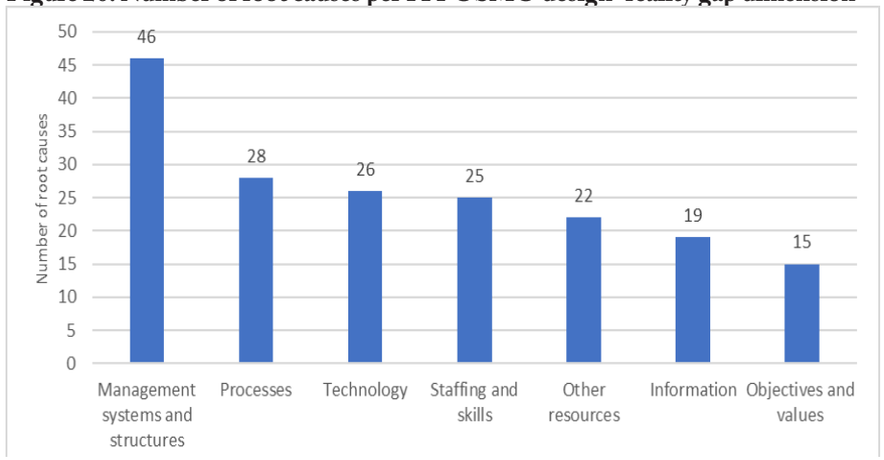


4. Analysis and conclusions

Design–reality gaps

The findings show that developing-world e-government IS projects fail due to root causes linked to all seven ITPOSMO design–reality gap dimensions suggested by Heeks (2003). The ITPOSMO *management systems and structures* dimension had the highest number of root causes, totalling 46. In this dimension, most of the root causes were found to fall under seven of the 18 identified casual factors: *inadequate project planning*, *inadequate project management*, *inadequate top management support*, *procurement and contractual issues*, *inadequate BPM*, *insufficient change management*, and *inappropriate organisational management structure*. The *processes* and *technology* dimensions were the second and third most prominent problematic ITPOSMO dimensions, with 28 and 26 root causes respectively. Figure 20 shows the number of root causes found to be linked to each of the seven ITPOSMO design–reality gap dimensions.

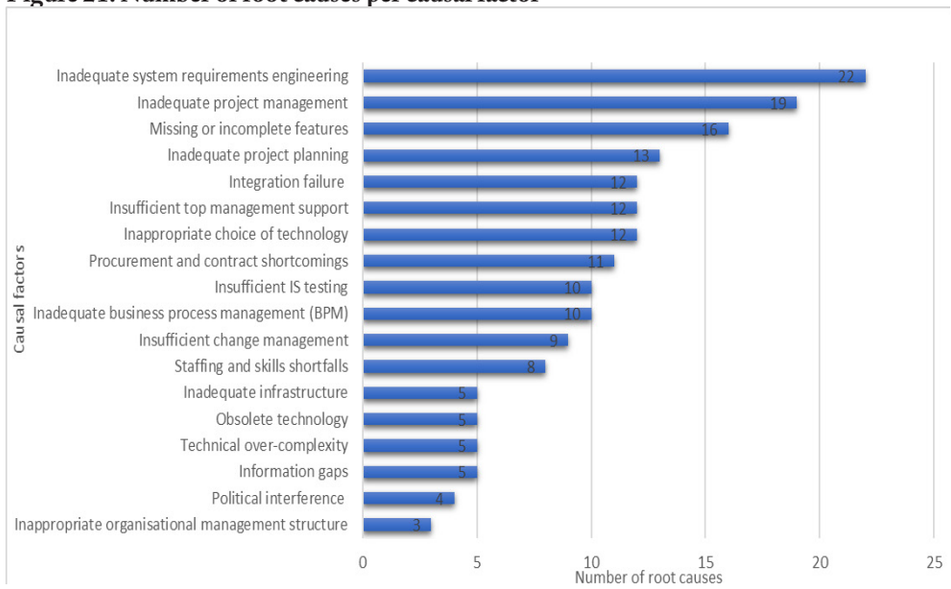
Figure 20: Number of root causes per ITPOSMO design–reality gap dimension



Causal factors

Among the 18 identified causal factors, *inadequate systems requirement engineering* was found to have the highest number of root causes, totalling 22. *Inadequate project management* and *missing or incomplete features* were the second and third most prominent causal factors, with 19 and 16 root causes respectively. Figure 21 shows the number of root causes per causal factor. The causal factors having a large number of root causes are likely to be the ones that require the most attention in order to mitigate their potential to lead to e-government project failure.

Figure 21: Number of root causes per causal factor



E-government information systems are complex, as they tend to have numerous components serving multiple stakeholders with different needs, views, preferences, and operating environments. This study reveals that e-government IS projects do not fail due to a single reason but rather due to a combination of several factors associated with design–reality gaps. Therefore, the successful implementation of an e-government IS project requires broad multi-dimensional strategies that address all seven potential design–reality gap dimensions.

This study provides both theoretical and practical contributions in the e-government IS domain. From a theoretical perspective, the study extends design–reality gap theory by identifying the root causes of such gaps for each identified cause of e-government IS project failure. From a practical perspective, the study findings may be useful to researchers, policymakers, and practitioners seeking to understand the necessary components of appropriate e-government IS interventions in developing-world settings. Understanding the root causes of problems is essential to developing practical solutions. Future studies can focus on establishing theoretical and methodological frameworks and tools to address the challenges identified in this study.

References

Abbas, A., Faiz, A., Fatima, A., & Avdic, A. (2017). Reasons for the failure of government IT projects in Pakistan: A contemporary study. In IEEE (Ed.), *2017 International Conference on Service Systems and Service Management (ICSSSM 2017)*. https://doi.org/10.1109/ICSSSM.2017.7996223

Afyonluoğlu, M., Aydin, A., Sevil, S. G., Yüksel, E., & Güngör, M. K. (2014). An e-government project management approach with e-transformation perspective. *International Journal of eBusiness and eGovernment Studies*, *6*(1), 21–33.

Aikins, S. K. (2012). Improving e-government project management: Best practices and critical success factors. In S. K. Aikins (Ed.), *Managing e-government projects: Concepts, issues, and best practices* (pp. 42–60). IGI Global. https://doi.org/10.4018/978-1-4666-0086-7.ch003

Al-Ahmad, W., Al-Fagih, K., Khanfar, K., Alsamara, K., Abuleil, S., & Abu-Salem, H. (2009). A taxonomy of an IT project failure: Root causes. *International Management Review, 5*(1), 93–104.

Al-Khanjari, Z. A., Al-Hosni, N., & Kraiem, N. (2014). Developing a service oriented e-government architecture towards achieving e-government interoperability. *International Journal of Software Engineering and its Applications*, *8*(5), 29–42. https://doi.org/10.14257/ijseia.2014.8.5.04

Al Salmi, M., Mohtar, S., & Hasnan, N. (2017). Skills and factors of e-government: Case study of Sultanate of Oman. *International Journal of Innovation, Management and Technology*, *8*(4), 313–319. https://doi.org/10.18178/ijimt.2017.8.4.747

Al-Zwainy, F. M. S., Mohammed, I. A., & Varouqa, I. F. (2018). Diagnosing the causes of failure in the construction sector using root cause analysis technique. *Journal of Engineering*, 1804053, 1–12. https://doi.org/10.1155/2018/1804053

Baguma, R., & Lubega, J. (2013). Factors for success and failure of e-government projects. In *ICEGOV'13: Proceedings of the 7th International Conference on Theory and Practice of Electronic Governance* (pp. 194–197). https://doi.org/10.1145/2591888.2591921

Bail, W. (2010). Effective requirements engineering. In *SIGAda '10:Proceedings of the ACM SIGAda Annual International Conference on SIGAda*. https://doi.org/10.1145/1879063.1879065

Bakunzibake, P., Grönlund, Å., & Klein, G. O. (2018). E-government implementation in developing countries: Enterprise content management in Rwanda. In H. J. Scholl, O. Glassey, & M. Janssen (Eds.), *Electronic government and electronic participation*. IOS Press. https://doi.org/10.3233/978-1-61499-670-5-251

Boota, M. W., Ahmad, N., & Masoom, A. H. (2014). Requirement engineering issues and their solutions. *International Journal of Engineering and Technical Research (IJETR 2014)*, *2*(11), 50–56.

Botchkarev, A., & Finnigan, P. (2015). Complexity in the context of information systems project management. *Organisational Project Management*, *2*(1), 15–34. https://doi.org/10.5130/opm.v2i1.4272

Bubenko, J. A. (1995). Challenges in requirements engineering. In IEEE (Ed.), *Proceedings of IEEE International Symposium on Requirements Engineering (RE'95)* (pp. 160–162). https://doi.org/10.1109/isre.1995.512557

National Audit Office of Tanzania. (2019). *Performance audit report on the management of provision of national health insurance services*. Ministry of Finance. http://www.nao.go.tz/?wpfb_dl=303

Chaudhary, S. (2017). Latest software testing tools and techniques: A review. *International Journal of Advanced Research in Computer Science and Software Engineering*, *7*(5), 538–540. https://doi.org/10.23956/ijarcsse/SV7I5/0138

Comins, L. (2020, March 12). eThekwini's billing system shock: Residents slapped with inflated bills. *The Mercury*. https://www.iol.co.za/mercury/news/ethekwinis-billing-system-shock-residents-slapped-with-inflated-bills-44685080

Dada, D. (2006). The failure of e-government in developing countries: A literature review. *The Electronic Journal of Information Systems in Developing Countries*, *26*(1), 1–10. https://doi.org/10.1002/j.1681-4835.2006.tb00176.x

Dahiya, D., & Mathew, S. K. (2018). IT infrastructure capability and e-government system performance: An empirical study. *Transforming Government: People, Process and Policy*, *12*(1), 16–38. https://doi.org/10.1108/TG-07-2017-0038

Dalal, S., & Chhillar, R. S. (2013). Empirical study of root cause analysis of software failure. *ACM SIGSOFT Software Engineering Notes*, *38*(4), 1–7. https://doi.org/10.1145/2492248.2492263

Damoah, I. S., & Akwei, C. (2017). Government project failure in Ghana: A multidimensional approach. *International Journal of Managing Projects in Business*, *10*(1), 32–59. https://doi.org/10.1108/IJMPB-02-2016-0017

Dwivedi, Y. K., Wastell, D., Laumer, S., Henriksen, H. Z., Myers, M. D., Bunker, D., Elbanna, A., Ravishankar, M. N., & Srivastava, S. C. (2014). Research on information systems failures and successes: Status update and future directions. *Information Systems Frontiers*, *17*(1), 143–157. https://doi.org/10.1007/s10796-014-9500-y

Feldgen, M., & Clua, O. (2014). Teaching effective requirements engineering for large-scale software development with scaffolding. In IEEE (Ed.), *2014 IEEE Frontiers in Education Conference (FIE) proceedings*. https://doi.org/10.1109/FIE.2014.7044176

Gartlan, J., & Shanks, G. (2007). The alignment of business and information technology strategy in Australia. *Australasian Journal of Information Systems*, *14*(2), 113–139. https://doi.org/10.3127/ajis.v14i2.184

Ghapanchi, A., & Albadvi, A. (2008). A framework for e-government planning and implementation. *Electronic Government: An International Journal, 5*(1), 71–90. https://doi.org/10.1504/EG.2008.016129

Gilbert, D., Balestrini, P., & Littleboy, D. (2004). Barriers and benefits in the adoption of e-government. *International Journal of Public Sector Management*, *17*(4), 286–301. https://doi.org/10.1108/09513550410539794

Goedeke, J., Mueller, M., & Pankratz, O. (2017). Uncovering the causes of information system project failure. In *AMCIS 2017 proceedings* (pp. 1–10).

Gunawong, P., & Gao, P. (2017). Understanding e-government failure in the developing country context: A process-oriented study. *Information Technology for Development*, *23*(1), 153–178. https://doi.org/10.1080/02681102.2016.1269713

Hangal, S., & Lam, M. S. (2002). Tracking down software bugs using automatic anomaly detection. In *ICSE '02: Proceedings of the 24th International Conference on Software Engineering* (pp. 291–301). https://doi.org/10.1145/581376.581377

Hasan, M. M. (2015). E-government success and failure: A case study of Bangladesh police. *Daffodil International University Journal of Science and Technology*, *10*(1), 61–67.

Heeks, R. (Ed.). (1999). *Reinventing government in the information age: International practice in IT-enabled public sector reform* (1st ed.). Routledge. https://doi.org/10.4324/9780203204962

Heeks, R. (2001). *Understanding e-governance for development*. iGovernment Working Paper 11. https://doi.org/10.2139/ssrn.3540058

Heeks, R. (2003). *Most eGovernment-for-development projects fail: How can risks be reduced?* iGovernment Working Paper 14. https://doi.org/10.2139/ssrn.3540052

Hofmann, H. F., & Lehner, F. (2001). Requirements engineering as a success factor in software projects. *IEEE Software*, *18*(4), 58–66. https://doi.org/10.1109/MS.2001.936219

Hossan, C. G., & Kushchu, I. (2006). Success and failure factors for e-government projects implementation in developing countries: A study on the perception of government officials of Bangladesh. https://www.semanticscholar.org/paper/Success-and-Failure-Factors-for-e-Government-in-%3A-A-Hossan-Habib/2f519f1afb33ed4acc870aa2459681fce84a2399

Hussain, A., Mkpojiogu, E. O. C., & Abdullah, I. (2016). Requirements engineering practices in UUMIT centre: An assessment based on the perceptions of in-house software developers. *Journal of Telecommunication, Electronic and Computer Engineering*, *8*(8), 27–32.

Hussain, A., Mkpojiogu, E. O. C., & Kamal, F. M. (2016). The role of requirements in the success or failure of software projects. *International Review of Management and Marketing*, *6*(S7), 306–311.

Hussein, R., Shahriza, N., & Karim, A. (2007). The impact of technological factors on information systems success in the electronic-government context. *Business Process Management Journal*, *13*(5), 613–627. https://doi.org/10.1108/14637150710823110

Imran, A., Gregor, S., & Turner, T. (2017). *eGovernment management for developing countries* (2nd ed.). ACPI.

Khan, N., & Islamabad, D. E. (2009). Public sector innovation: Case study of e-government projects in Pakistan. *The Pakistan Development Review*, *48*(4), 439–457. https://doi.org/10.30541/v48i4IIpp.439-457

Lachal, J., Revah-Levy, A., Orri, M., & Moro, M. R. (2017). Metasynthesis: An original method to synthesize qualitative literature in psychiatry. *Frontiers in Psychiatry*, *8*, 269. https://doi.org/10.3389/fpsyt.2017.00269

Lam, W. (2005). Barriers to e-government integration. *Journal of Enterprise Information Management*, *18*(5), 511–530. https://doi.org/10.1108/17410390510623981

Lau, E. (2003). *5th Global Forum on Reinventing Government, Mexico City, 5 November 2003: Challenges for e-government development*. OECD E-government Project.

Layne, K., & Lee, J. (2001). Developing fully functional e-government: A four stage model. *Government Information Quarterly*, *18*(2), 122–136. https://doi.org/10.1016/S0740-624X(01)00066-1

Livingston, A. D., Jackson, G., & Priestley, K. (2001). *Root causes analysis: Literature review*. HSE Books.

Mansor, Z., & Ndudi, E. E. (2015). Issues, challenges and best practices of software testing activity. In *Recent Advances in Computer Engineering* (pp. 42–47), proceedings of ACE 2015, Seoul. https://www.wseas.us/e-library/conferences/2015/Seoul/ACE/ACE-06.pdf

Martin, R. L., & Montagna, J. M. (2006). Business process reengineering role in electronic government. In D. E. Avison, S. Elliot, J. Krogstie, & J. Pries-Heje (Eds.) *The past and future of information systems: 1976–2006 and beyond: IFIP 19th World Computer Congress, TC-8, Information System Stream, August 21–23, 2006, Santiago, Chile* (pp. 77–88). Springer. https://doi.org/10.1007/978-0-387-34732-5

Matte, R. (2017). Bureaucratic structures and organizational performance: A comparative study of Kampala Capital City Authority and National Planning Authority. *Journal of Public Administration and Policy Research*, *9*(1), 1–16. https://doi.org/10.5897/JPAPR2016.0377

Michael, K. A., & Boniface, K. A. (2014). Inadequate requirements engineering process: A key factor for poor software development in developing nations: A case study. *International Journal of Computer, Electrical, Automation, Control and Information Engineering*, *8*(9), 1572–1575.

Mukherjee, I. (2008). Understanding information system failures from the complexity perspective. *Journal of Social Sciences*, *4*(4), 308–319. https://doi.org/10.3844/jssp.2008.308.319

Ministry of Works, Transport and Communication (2016). National Information and Communication Technology (ICT) Policy. Government of Tanzania.

Nograsek, J. (2011). Change management as a critical success factor in e-government implementation. *Business Systems Research*, *2*(2), 1–56. https://doi.org/10.2478/v10305-012-0016-y

Ojha, S., & Pandey, I. M. (2017). Management and financing of e-government projects in India: Does financing strategy add value? *IIMB Management Review*, *20*, 1–19. https://doi.org/10.1016/j.iimb.2017.04.002

Paradies, M., & Busch, D. (1988). Root cause analysis at Savannah River Plant nuclear power station. In *Conference record for 1988 IEEE Fourth Conference on Human Factors and Power Plants*. https://doi.org/10.1109/HFPP.1988.27547

Patanakul, P. (2014). Managing large-scale IS/IT projects in the public sector: Problems and causes leading to poor performance. *Journal of High Technology Management Research*, *25*(1), 21–35. https://doi.org/10.1016/j.hitech.2013.12.004

Pohl, K. (2010). *Requirements engineering: Fundamentals, principles, and techniques* (1st ed). Springer.

Rahman, S., Rashid, N., Yadlapalli, A., & Yiqun, L. (2014). Determining factors of e-government implementation: A multi-criteria decision-making approach. In *Proceedings - Pacific Asia Conference on Information Systems (PACIS 2014)*.

Rajala, T., & Aaltonen, H. (2020). Reasons for the failure of information technology projects in the public sector. In H. Sullivan, H. Dickinson, & H. Henderson (Eds.), *The Palgrave handbook of the public servant* (pp. 1–21). Palgrave MacMillan. https://doi.org/10.1007/978-3-030-03008-7_78-1

Rajapakse, J., Van der Vyver, A., & Hommes, E. (2012). E-government implementations in developing countries: Success and failure, two case studies. In IEEE (Ed.), *2012 IEEE 6th International Conference on Information and Automation for Sustainability* (pp. 95–100). https://doi.org/10.1109/ICIAFS.2012.6419888

Palanisamy, R. (2004). Issues and challenges in electronic governance planning. *Electronic Government, an International Journal*, *1*(3), 253-272. https://doi.org/10.1504/EG.2004.005551

Reffat, R. M. (2003). Developing a successful e-government. In *The proceedings of the Symposium on E-Government: Opportunities and Challenge, Muscat Municipality* (pp 1–13).

Sæbø, Ø. (2012). E-government in Tanzania: Current status and future challenges. In H. J. Scholl, M. Janssen, M. A. Wimmer, C. E. Moe, & L. S. Flak (Eds.), *Electronic government: 11th IFIP WG 8.5 International Conference, EGOV 2012, Kristiansand, Norway, September 3-6, 2012*. (pp. 198–209). https://doi.org/10.1007/978-3-642-33489-4_17

Sandelowski, M., Docherty, S., & Emden, C. (1997). Qualitative metasynthesis: Issues and techniques. *Research in Nursing & Health*, *20*(4), 365–371. https://doi.org/10.1002/(SICI)1098-240X(199708)20:4<365::AID-NUR9>3.0.CO;2-E

Shah, S. R. A., Khan, A. Z., & Khalil, D. M. S. (2011). Project management practices in e-government projects: A case study of electronic government directorate (EGD) in Pakistan. *International Journal of Business and Social Science*, *2*(7), 235–243.

Shah, T., & Patel, S. V. (2014). A review of requirement engineering issues and challenges in various software development methods. *International Journal of Computer Applications*, *99*(15), 36–45. https://doi.org/10.5120/17451-8370

Sun, P. L., Ku, C. Y., & Shih, D. H. (2015). An implementation framework for e-government 2.0. *Telematics and Informatics*, *32*(3), 504–520. https://doi.org/10.1016/j.tele.2014.12.003

Swartz, E. M. J. (2018). Challenges to the implementation of business process re-engineering of the recruitment process in the Ministry of Fisheries and Marine Resources, Namibia. MPA thesis, Faculty of Economic and Management Sciences, University of Stellenbosch. https://scholar.sun.ac.za/handle/10019.1/103566

Sweis, R. J. (2015). An investigation of failure in information systems projects: The case of Jordan. *Journal of Management Research*, *7*(1), 173–185. https://doi.org/10.5296/jmr.v7i1.7002

Thakur, S., & Singh, S. (2012). A study of some e-government activities in South Africa. *2012 E-Leadership Conference on Sustainable e-Government and e-Business Innovations (E-LEADERSHIP)* (pp. 1–11). https://doi.org/10.1109/e-Leadership.2012.6524704

Tomić, B., & Brkić, V. S. (2011). Effective root cause analysis and corrective action process. *Journal of Engineering Management and Competitiveness (JEMC)*, *1*(1/2), 16–20. http://www.tfzr.uns.ac.rs/jemc

Toots, M. (2019). Why e-participation systems fail: The case of Estonia's Osale.ee. *Government Information Quarterly*, *36*(3), 546–559. https://doi.org/10.1016/j.giq.2019.02.002

Trkman, P. (2010). The critical success factors of business process management. *International Journal of Information Management*, *30*(2), 125–134. https://doi.org/10.1016/j.ijinfomgt.2009.07.003

Twizeyimana, J. D., Larsson, H., & Grönlund, Å. (2018). Egovernment in Rwanda: Implementation, challenges and reflections. *The Electronic Journal of E-Government*, *16*(1), 19–31.

Ullah, S., Iqbal, M., & Khan, A. M. (2011). A survey on issues in non-functional requirements elicitation. In *Proceedings of International Conference on Computer Networks and Information Technology* (pp. 333–340). https://doi.org/10.1109/ICCNIT.2011.6020890

Urquhart, C. (2010). Systematic reviewing, meta-analysis and meta-synthesis for evidence-based library and information science. *Information Research*, *15*(3). http://informationr.net/ir/15-3/colis7/colis708.html

Verner, J., Sampson, J., & Cerpa, N. (2008). What factors lead to software project failure? In *2008 Second International Conference on Research Challenges in Information Science* (pp. 71–80). https://doi.org/10.1109/RCIS.2008.4632095

Vyas, V., Vyas, S., & Kundan, A. (2014). Management information system: Information needs of organisation. *International Journal of Information & Computation Technology*, *4*(17), 1903–1908.

Williams, P. M. (2001). Techniques for root cause analysis. *Baylor University Medical Center Proceedings*, *14*(2), 154–157. https://doi.org/10.1080/08998280.2001.11927753

Xia, W., & Lee, G. (2005). Complexity of information systems development projects: Conceptualization and measurement development. *Journal of Management Information Systems*, *22*(1), 45–83. https://doi.org/10.1080/07421222.2003.11045831

Zakaria, N. H., Haron, A., Sahibuddin, S., & Harun, M. (2011). Requirement engineering critical issues in public sector software project success factor. *International Journal of Information and Electronics Engineering*, *1*(3), 200–209. https://doi.org/10.7763/IJIEE.2011.V1.32

Zwikael, O. (2014). Top management involvement in project management: Exclusive support practices for different project scenarios. *International Journal of Managing Projects in Business*, *1*(3), 387–403. https://doi.org/10.1108/17538370810883837

A Sociocultural Framework to Analyse M-Learning Options for Early Childhood Development (ECD) Practitioner Training

Susanna Oosthuizen
Chief Operating Officer, Penreach; and Master's student, Department of Childhood Education, University of Johannesburg
https://orcid.org/0000-0002-7691-3362

Nicky Roberts
Associate Professor, Department of Childhood Education, University of Johannesburg
https://orcid.org/0000-0002-1910-0162

Abstract
This article, a contribution to m-learning (mobile learning) research, centres on the motivation for, and development of, a suitable framework to analyse m-learning options for early childhood development (ECD) practitioners. Grounded in a sociocultural learning perspective, the framework was developed as part of a larger study into the feasibility of m-learning for ECD practitioners in the Penreach professional development programme in Mpumalanga Province, South Africa. Analysis of existing frameworks enabled the development of a new, modified framework to suit the Penreach context. Here we unpack the framework and explain its development. The new, modified framework aims to assist researchers, developers, and implementers by prompting consideration of five sociocultural learning features associated with m-learning in ECD, namely: *device access*, *data affordability*, *authenticity*, *collaboration*, and *personalisation*.

Keywords
m-learning, mobile learning, early childhood development (ECD), professional development, training, sociocultural learning

DOI: https://doi.org/10.23962/10539/32209

Recommended citation
Oosthuizen, S., & Roberts, N. (2021). A sociocultural framework to analyse m-learning options for early childhood development (ECD) practitioner training. *The African Journal of Information and Communication (AJIC), 28*, 1-20.
https://doi.org/10.23962/10539/32209

1. Introduction

Early childhood development (ECD)

In the past decade, international and African-based research studies and policy frameworks have highlighted the significance of early childhood development (ECD). The World Bank's 2018 *World development report* found that foundational skills in early childhood are essential for future learning, and that effective ECD interventions are necessary to significantly improve (especially poor) children's ability to learn (World Bank, 2018, p. 114). The potential that quality ECD has for the improvement of the learning outcomes of poor children is of critical importance in South Africa, where the majority of children under six live in poverty (Ashley-Cooper et al., 2012; Hall, 2010). Prominent authors in the field of ECD in South Africa concur that more trained ECD practitioners are required in order to achieve a universal and quality ECD for all children (Ashley-Cooper et al., 2012; Biersteker et al., 2008).

South Africa's National Development Plan 2030 (NPC, 2012) and National Integrated Early Childhood Development Policy (RSA, 2015) mention the need to improve access to quality ECD for poor children. The latter encapsulates the vision for ECD in South Africa as follows: "[a]ll infants, young children and their families in South Africa [should] live in environments conducive to their optimal development" (RSA, 2015, p. 48).

The recent National Income Dynamics Study – Coronavirus Rapid Mobile Survey (NIDS-CRAM) survey found that, in 2021, about 36% of South African families with children under the age of six reported a child attending an ECD centre (other than Grade R) (Wills & Kika-Mistry, 2021). This reflects a recovery in ECD attendance to almost the pre-pandemic levels of 39%, following significant disruptions due to COVID-19 in 2020 (Wills & Kika-Mistry, 2021). May et al. (2020) report that poverty, unemployment, and hunger rose dramatically under the COVID-19-related "hard lockdown", with 47% of South African households running out of money to buy food in May/June 2020, while child and adult hunger increased to 15% and 22% respectively.

Less than half of South African children under the age of six access any form of early learning (Stats SA, 2016, p. 64). The most recent data indicates that of the 7 million children aged 0 to 5 years old, only 3.3 million are accessing some kind of early learning programme. Within this cohort, 69% of 3- to 5-year-olds attend a learning programme or Grade R, while only 30% of 0- to 2-year-olds attend such programmes, i.e., 70% of 0- to 2-year-olds are cared for exclusively at home (Thorogood et al., 2020).

A study by the Department of Basic Education (DBE), the Department of Social Development (DSD), and UNICEF identified a shortage of qualified practitioners

to meet the demands of ECD provision in South Africa (DBE, DSD & UNICEF, 2011, p. 87) and recommended the preparation of more skilled practitioners to deliver in poor communities. This skills gap in ECD was also highlighted in a 2014 audit of the ECD sector by the Department of Social Development (DSD, 2014), which reported both a shortage of qualified practitioners to meet the demands of ECD (2014, p. 134) as well as a skills gap among current working practitioners (2014, p. 94).

M-learning

At the same time, the potential offered by mobile learning (m-learning) is receiving increasing attention in South Africa and internationally. Prompted by the rapid uptake of mobile technology in Africa and the Middle East, UNESCO undertook a study in 2012 on the potential of m-learning to improve teaching practice in these regions (Isaacs, 2012). That study found that the use of such technology can influence the supply of qualified teachers in remote areas (Isaacs, 2012, p. 11). Subsequently, South African and international researchers collaborated to develop a definitive m-learning curriculum framework applicable to South Africa (Botha et al., 2012). The framework's authors found that "teacher development is one of the most manageable and cost-effective ways of using mobile technologies to break into the cycle and the system of Education" (Botha et al., 2012, p. 2). A literature review by Alawani and Singh (2017), aimed at establishing a conceptual framework for mobile learning in teacher professional development in the United Arab Emirates, points to the potential of m-learning as a complementary method to enhance teacher professional development, especially due to its ability to reach remote areas and provide ubiquitous access to content, expertise, and peer-based support (2017, p. 150). Both the Botha et al. (2012) and Alawani and Singh (2017) studies recognise the potential value of m-learning to support and possibly scale educator training.

Insofar as educator training is concerned, pre-grade R ECD practitioners have traditionally been considered a poor audience for digital learning. Benner and Pence (2013) suggest that this is due to negative perceptions of their education levels, their ability to access technology, and their willingness to take up non-traditional forms of learning. The South African Department of Basic Education (DBE) (2018) has developed and invested in a Professional Development Framework for Digital Learning. The framework, however, focuses intensively on curriculum and school-based systems to support integration of digital skills, and omits attention to pre-grade R (the pre-school reception year) ECD.

Lack of research on m-learning in pre-grade R context in South Africa

Despite the increased interest in m-learning and ECD respectively, there is a marked lack of research on m-learning in ECD, especially in the African and South African context (Roberts & Spencer-Smith, 2019). Botha et al. (2012) found that there existed only limited local examples of m-learning to draw from for South African

implementation. In addition to this general dearth of local studies on m-learning, few studies to date have focused on pre-grade R practitioner development and m-learning.

A search of the LearnTechLib database (previously EdITLib) shows a telling decline in search results when drilling down from "m-learning" (47,424 articles), to "m-learning and ECD" (43 articles) to "ECD and m-learning and Africa" (6) and "ECD and m-learning and South Africa" (5). None of the African studies focused on pre-grade R practitioner development. A search of the *South African Journal of Childhood Education (SAJCE)*[1] database yielded eight results related to "m-learning and ECD" and none of these pertained to pre-grade R practitioner skill training. Roberts and Spencer-Smith (2019) point to a 2016 special edition of the *SAJCE*, in which m-learning was notably absent from the interventions listed as useful in improving the instructional practice of ECD educators in the African context.

Chee et al. (2017) identify a dearth of research about m-learning in ECD in a global meta-analysis of 144 peer-reviewed articles on m-learning from six eminent journals spanning five years (2017, p. 118). No sample in any of the studies was from a pre-primary educational setting and no studies pertained to ECD practitioner skills training. Trucano (2013), reporting for UNESCO, hails South Africa as a leader in Africa with regard to "cutting-edge" m-learning initiatives and research. Yet, Trucano (2013) only refers to two interventions to support this claim: the Yoza Project[2] and Dr Maths,[3] both aimed at children above five years of age. Botha and Vosloo (2008) present four examples of medium- to large-scale m-learning interventions in South Africa, none of which is ECD-focused: Dr Math, M4Girls, Imfundo yami/yethu, and Angles on MXit. More recent and local studies that focus on technology use in teacher development exclude pre-Grade R ECD practitioners. For example, Herselman and Botha (2014), working on mobile tablet interventions, report on their learnings from interventions in rural schools (grades R to 12) in the South Africa's Eastern Cape Province. This study does not include the pre-Grade R level. Isaacs, Roberts, Spencer-Smith and Brink (2019) report on a professional development intervention for Grade R practitioners which included minimal use of mobile phones (via WhatsApp). While this study includes consideration for ECD centres, this is only at the Grade R level and not at the pre-Grade R level.

On the basis of the above, there is a clear need for empirical research on the integration of m-learning into pre-Grade R training and development in the South African context. There is also a paucity of literature that attempts to provide a theoretical

1 *SAJCE* is the only South African journal with an ECD focus.
2 See https://m4lit.wordpress.com
3 See https://drmaths.com

framework to examine m-learning in different contexts (Kearney et al., 2012). According to these authors, educational research has up to now not clearly defined which pedagogies are most suitable for m-learning.

The gap in research on the application of m-learning for skills training in pre-Grade R ECD, especially in South Africa, is marked and provided one motivation for this research. The other motivation was more localised and practical: the need to make ECD practitioners at the pre-Grade R level part of the dialogue about if and how m-learning can contribute to their skills training. This required a suitable framework to analyse m-learning options within the specific sociocultural environment of Penreach pre-Grade R ECD practitioner training in Mpumalanga Province, South Africa.

2. Conceptual framing

In this section, we set out our conceptual framework, making explicit our adoption of a sociocultural perspective on learning, and explaining what this means. We then argue (1) that a sociocultural perspective is relevant to educator professional development; and (2) that a sociocultural perspective is relevant to assessments of m-learning options.

Sociocultural perspective on learning

The approach to learning adopted in the broader study, and hence in this article, is a sociocultural perspective, which acknowledges the reciprocal effect that learning and learning tools have on each other and which we argue is appropriate for assessing m-learning options for Penreach pre-Grade R ECD practitioner training.

A sociocultural perspective recognises the influence that circumstances and culture have on an individual's behaviour, specifically related to their learning. The sociocultural perspective also proposes that knowledge is co-constructed through interaction (Conole, 2004; Eun, 2008; Kelly, 2007; Vygotsky, 1978). Sociocultural theory emanates from the work of Vygotsky (1978), who proposed that learning is a socially mediated process where learners (adults and children) are jointly responsible for learning, and that learning is optimised when in the Zone of Proximal Development (ZPD). In Vygotskian thinking, the origin of knowledge construction lies in social interaction and not in an individual mind. Knowledge is co-constructed, and this process is mediated by tools and artefacts from a specific environment and cultural context (Shabani, 2016).

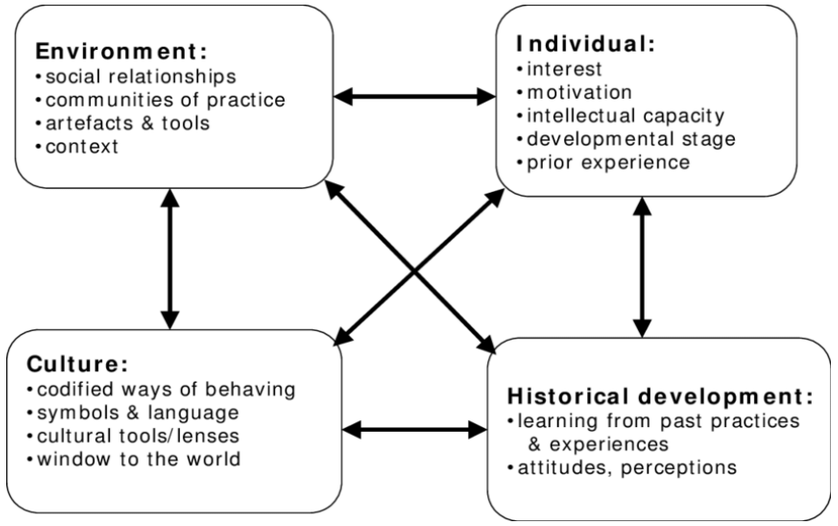
Eun (2008) argues that a sociocultural perspective is relevant to educator professional development and applies a sociocultural perspective as a unified theory to explain the most effective mechanism for educators to acquire knowledge and skills (2008, p. 135). Eun (2008) defines four key theoretical concepts from Vygotsky's work, namely *social interaction*, *internalisation*, *mediation*, and *psychological systems*.

According to Eun (2008), *social interaction* is a key concept for professional development, and manifests through workshops, study groups, seminars, and mentoring, where knowledge is developed through interacting with others. Shabani (2016) supports this assertion, and describes study groups as collaborative opportunities to discuss common challenges and co-construct knowledge as solutions. *Internalisation* in Eun's conception takes the form of self-study and individual activities. With regard to *mediation* Eun (2008) describes indirect or mediated activity as necessary for any development to occur after the initial professional development experiences. Mediated activity uses three mediators, namely tools (materials, resources), signs (newsletters and journals), and other human beings. Last, the *psychological systems* described by Eun focus on changing the attitude and instructional practice of educators (2008, p. 144).

The work of Eun (2008), Shabani (2016) and Alawani and Singh (2017) grounds educator professional development in sociocultural theory, and regards professional development as largely *intramental* (occurring within the mind) and social (occurring among people). It also describes the most effective social interaction for professional development as that which takes place within the ZPD, where it is easiest to collaborate and build knowledge. This implies that the "when" and "how" of ECD professional development are important, including the when and how of using m-learning. Eun (2008), like Shabani (2016), suggests that, from a sociocultural standpoint, educator professional development is most effective when it is grounded in practice. In addition, Eun (2008) asserts that professional development is also most effective in constructs such as "professional learning communities" where educator–learners have shared goals and can collaborate to co-construct knowledge that is relevant to their shared context (Eun, 2008, p. 146).

Kelly (2007) proposes that the theoretical work on the factors that contribute to the learner's sociocultural environment points to four mutually interacting core elements (see Figure 1): *environment*, *individual*, *culture*, and *historical development*.

Figure 1: Four core elements of sociocultural theory (Kelly, 2007)



Source: Kelly (2007, p. 56)

Relevance of sociocultural perspective on m-learning

Adopting a sociocultural perspective on m-learning is appropriate within the South African context because it aligns with the Department of Basic Education's (2018) aforementioned Professional Development Framework for Digital Learning, which notes that:

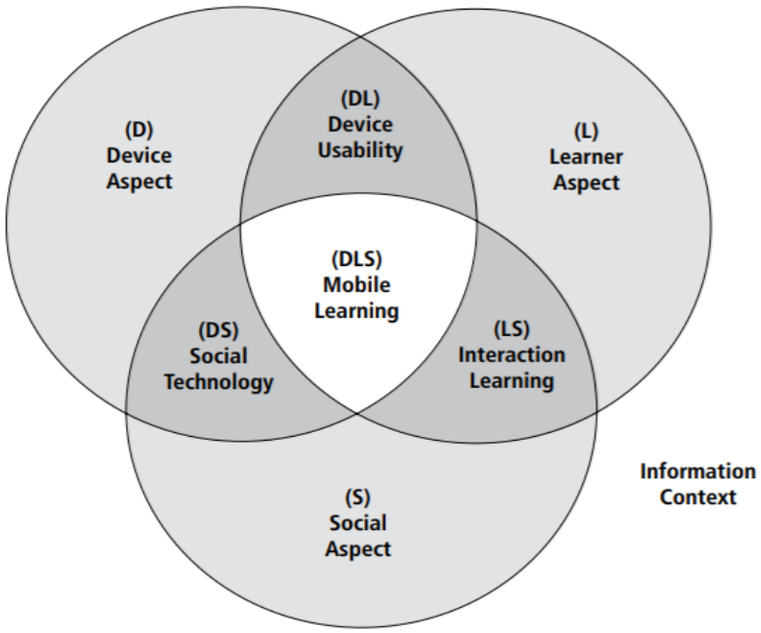
> It is necessary for teacher professional development to specifically address how digital tools and resources can support teaching and enhance learning in different subjects in a wide range of socio-economic contexts that teachers encounter in South Africa. (DBE, 2018, p. 10).

Traxler (2007) proposes that research on m-learning should develop concepts emanating from the learner perspective and not the perspective that forefronts technology as the driving force of the learning experience. Traxler (2007) points to the preponderance of frameworks for m-learning that focus more on technology than on pedagogy, and states:

> So mobile learning is not about 'mobile' as previously understood, or about 'learning' as previously understood, but part of a new mobile conception of society. (This may contrast with technology enhanced learning or technology supported, both of which give the impression that technology does something to learning.) (Traxler, 2007, p. 5).

Koole (2009) proposes a framework for rational analysis of mobile education (FRAME) (see Figure 2), in which m-learning is in terms of three interacting aspects: *device*, *learner*, and *social context* (Koole, 2009, p. 27).

Figure 2: FRAME model for m-learning (Koole, 2009)



Source: Koole (2009, p. 27)

Koole's (2009) FRAME model resonates with Traxler's view through its inclusion of the social context as one of the three key interacting spheres to understand how m-learning manifests. And by describing the interaction between spheres, it aligns with Traxler's view that technology does not influence learning in a one-directional way. Making use of the ideas of Vygotsky (1978), Koole (2009) posits that the ideal m-learning environment manifests where *mediation* exists, through which "the nature of the interaction itself changes as learners interact with each other, their environments, tools, and information" (Koole, 2009, p. 39). This is clearly a sociocultural perspective on m-learning, in that it views learning as a process of interactions that take place within a learner's social and cultural context. The work of Traxler (2007) and Koole (2009) firmly establishes the sociocultural context as critical in understanding m-learning.

3. Research design

The larger Penreach study, of which the research outlined in this article was part, assessed the feasibility of three different m-learning applications before choosing one for use to support pre-Grade R ECD practitioners. In order to achieve this aim, a suitable framework for analysing m-learning options for professional development was required, and thus the conceptual exploration covered by this article was conducted.

Research setting

The general research setting is the ECD practitioner training landscape in South Africa, which has been studied by the likes of Biersteker et al. (2008), Ashley-Cooper et al. (2012), Feza (2013), and the Department of Social Development (DSD, 2014). Evident from these studies is the need for ECD skills training to move away from a distance-based and theoretically oriented training, to training that is practical, contains practical demonstrations, is embedded in the real work of the practitioner, provides sufficient support during and after training, and assists practitioners to provide quality services where they operate.

The specific setting for the Penreach study (hereafter "the Penreach context") is a rural context where pre-Grade R ECD practitioners are supported in their ongoing professional development. These pre-Grade R practitioners are working in severely under-resourced environments in Mpumalanga Province, often earning less than minimum wage. These educators' socio-economic context influences their ability to use m-learning. Therefore, as is seen later in this article, the cost of owning a smart device and the cost of mobile network access for m-learning were considered to be directly related to feasibility.

Research purpose

This article describes the process undertaken to develop a new, modified sociocultural framework to assess m-learning tools and select the one most suitable for use by ECD practitioners in the Penreach project in rural Mpumalanga.

Research questions

The two research questions guiding the research outlined in this article were:

- What are the available frameworks to assess m-learning options for professional development of educators that may be relevant to the Penreach context?
- Which framework, or combination/adaptation of frameworks, is suitable for the task of assessing the feasibility of three m-learning applications for Penreach?

Methods

A scan of the literature was conducted and several conceptual and analytical frameworks were consulted. Studies and articles were identified that present seminal findings on, or well-received theories about, m-learning. The research problem spanned knowledge areas of "education", "early childhood development", "practitioner training", "skills training", "practitioner professional development", "technology", "learning technology", and "mobile learning". With this in mind, Boolean searches were conducted using the LearnTechLib database, the *Journal of Research in Learning Technology*, the *South African Journal of Childhood Education (SAJCE)*, and the UNESCO database for papers presented at its annual Mobile Learning Week.

The research questions simultaneously demanded knowledge of the South African ECD practitioner training context in general, and of the Penreach context in particular. Without this, the relevance or suitability of any framework on m-learning and educator development could not be judged. For the general context, literature on South African research in the ECD and m-learning fields was consulted. For determining the Penreach context, this study had the benefit of the detailed contextual knowledge of this article's lead author Oosthuizen, who holds a senior position in Penreach's professional development programme. Further contextual knowledge was obtained through an empirical study conducted by Oosthuizen, which included surveys completed by all the ECD practitioners, and structured interviews with four practitioners during a follow-up site visit. The findings from the empirical study are not the subject of this article. Suffice to note that the planning and preparation for that study deepened the ability of this article's lead author to judge the suitability and relevance of theoretical frameworks to the Penreach context.

4. Findings

In discussing the findings we reflect on each of the two research questions in turn.

Research question 1: Available frameworks

- *What are the available frameworks to assess m-learning options for professional development of educators that may be relevant to the Penreach context?*

As we consulted the literature it became clear that m-learning frameworks were neither plentiful nor standardised, and that m-learning tools tended to omit a focus on pedagogy. Danaher et al. (2009) argue that there seems to be a high demand for tools and technology in m-learning, but less support for research that relates these tools and techniques to an underlying pedagogy. Given the continuous advancement of mobile technology, Danaher et al. (2009) suggest that researchers should push the pedagogy agenda, and learn from one another so that m-learning is understood according to its value for learning (Danaher et al., 2009, p. 3). This view echoes the Laurillard (2002) view that "technology is looking for a problem to solve in education", and that a technology focus promotes the misleading notion that the technology precedes or leads education. Laurillard (2002) argues that the better approach is to start by identifying the problem in education and then selecting and applying an m-learning approach that fits the pedagogical needs.

Roberts and Spencer-Smith (2019) lament the lack of comparable or standard frameworks in studies on m-learning, noting that the paucity of standardised frameworks makes it difficult to draw meaningful comparisons between findings (Roberts & Spencer-Smith, 2019, p. 3). Roberts and Spencer-Smith (2019) propose adaptation or improvement of their own modified analytical framework for studies in the m-learning field, in order to establish "commonly agreed metrics and approaches, to measure and reflect on efficacy" (Roberts & Spencer-Smith, 2019, p. 10). Isaacs, Roberts and Spencer-Smith (2019) apply the Roberts and Spencer-Smith (2019) framework to their analysis of four m-learning pilots in Africa.

Our scan of the literature identified four frameworks pertaining to m-learning which we found had potential relevance to the Penreach context:

- the Alawani and Singh (2017) "smart mobile learning conceptual framework for professional development", which emphasises contextualisation, social aspect, and personalisation;
- the Laurillard (2002) "conversational framework", which offers a distinct focus on pedagogy;
- the Kearney et al. (2012) "pedagogical framework for m-learning", which draws on and adapts the Laurillard (2002) framework; and
- the Roberts and Spencer-Smith (2019) "analytical framework for describing m-learning interventions".

We now briefly describe each framework in turn.

Alawani and Singh (2017) "smart mobile learning" framework

The Alawani and Singh (2017) framework reverberates with elements of Eun (2008) and Shabani (2016). Alawani and Singh (2017) conducted a study about the experience of m-learning by teachers in a professional development context in the United Arab Emirates. The research found that effective m-learning in professional development is dependent on its contextualisation. Equally important and included in their framework are the social aspects of professional learning and the fact that learning at this level needs to be personalised (2017, p. 156).

Laurillard (2002) "conversational" framework

Laurillard's (2002) framework has a distinct focus on pedagogy, in that it defines the pedagogy required for optimal learning. More specifically, it consists of a flow of questions that interact in an iterative way. The framework was designed to be used in learning design. The pedagogical soundness of the learning design can be measured by how many of the questions in the framework can be answered. Laurillard

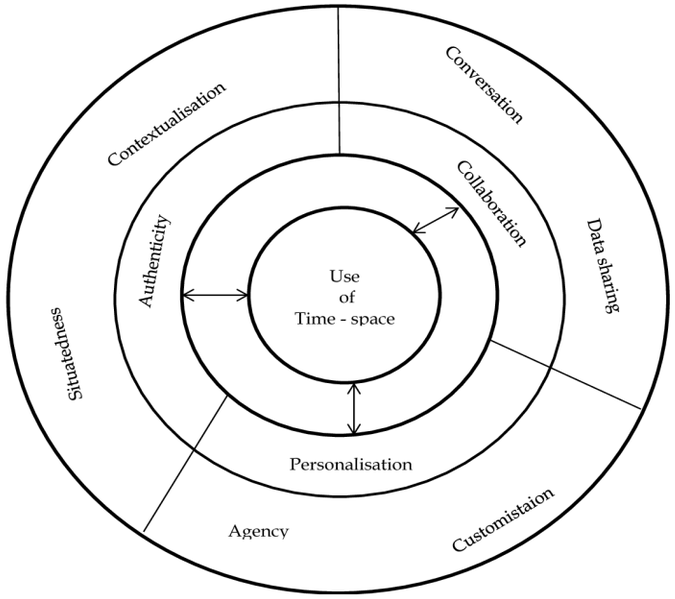
(2002) describes the application of the framework as relevant to m-learning design. A pedagogically sound m-learning design would, according to the conversational framework, include aspects of collaboration, communication, and sharing (Laurillard, 2002). Laurillard's (2002) conversation framework suggests that from a pedagogical perspective, the learner's practice is improved if knowledge outputs can be shared with peers. In addition, through peer discussion, reflection can occur, which enhances the learner's own conceptual understanding of the topic. Laurillard (2002) found that in m-learning, the affective motivation for learning increases with the opportunity to communicate with others. Finally, an optimal learning experience is created where information and artefacts can be shared (Laurillard, 2002, p. 18).

Kearney et al. (2012) "pedagogical framework"

In the development of their pedagogical framework, Kearney et al. (2012) draw on insights from Traxler (2007), Koole (2009), and Laurillard (2002). Kearney et al. (2012) attempt to include the most important social characteristics and relationships that affected m-learning. During their research process, Kearney et al. (2021) identified "time-space" as integral to m-learning, contributing a new dimension to the study of m-learning. They position "time-space" as central in their framework, with m-learning positioned as transcending the traditional limitations of formal learning by making it possible to learn anywhere and anytime. By overcoming the spatial and temporal features of classroom-based learning, "learning time" in m-learning becomes socially negotiated. Participants in the learning experience can agree where and when interaction takes place, without negatively affecting the learning itself (Koole, 2009). According to Kearney et al. (2012), one must accept that the pedagogy of m-learning takes place within this "malleable space-time context", and this should be central to understanding m-learning (2012, p. 4).

Kearney et al. (2012) test what they see as eight key features of m-learning: *portability*, *social interaction*, *contextual sensitivity*, *connectivity*, *individuality*, *usability*, *learning*, and *integration into practice*. These features emerged from the work of Koole (2009) and Klopfer et al. (2002). The eight features are arranged in different relationships to one another to form a conceptual framework. Three versions of this framework were tested over the course of 18 months with eight academics in an Australian university and eight trainee teachers in the UK who used m-learning as part of their professional training. The final framework that emerges from their research contains three main features: *collaboration*, *authenticity*, and *personalisation*. The authors posit that these three features, along with six sub-scales, would be effective in analysing the pedagogy behind m-learning (see Figure 3).

Figure 3: Kearney et al. (2012) framework



Source: Kearney et al. (2012, p. 8)

Collaboration describes learning through interaction with others and mediated by tools (Conole, 2004; Laurillard, 2002; Shabani, 2016). It is therefore included as one of the key features in the Kearney et al. (2012) framework. *Authenticity* refers to how learning practices are similar to what a learner needs to do in the "real world" (Kearney et al., 2012, p. 9). Authentic learning is considered one of the most effective ways to ensure so-called "deep learning" and is pedagogically relevant (Herrington & Oliver, 2001). In a study on innovative learning in the 21st century, the OECD (2017) highlights authentic and collaborative learning as critical to optimal digitally enabled learning environments. The *personalisation* feature is developed by Kearney et al. (2012) from the body of research about mobile tools and learner agency, most notably that of Klopfer et al. (2002) and Pachler et al. (2010). It describes the ability of the learner to form their own learning experience based on their social context and own needs.

Roberts and Spencer-Smith (2019) framework

Working from an initial model by Pouezevara and Strigel (2012) that puts forward three m-learning spectra, the Roberts and Spencer-Smith (2019) framework adds three additional spectra for a total of six. The three spectra set out by Pouezevara and

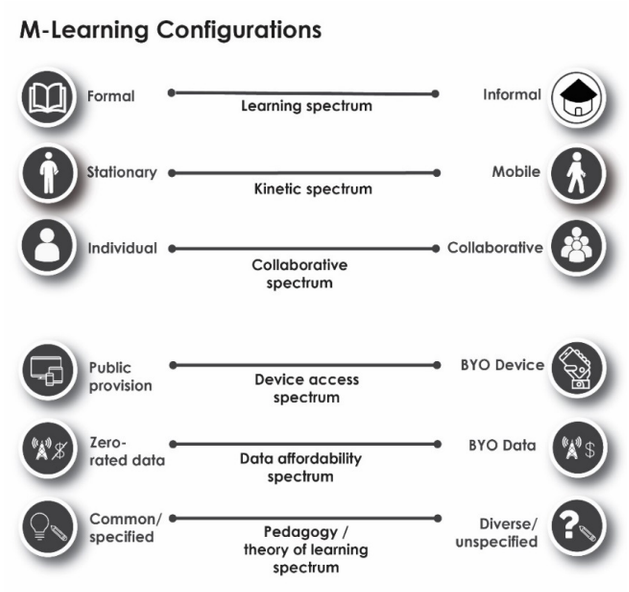
Strigel (2012) are:

- *learning* spectrum (between formal or informal);
- *kinetic* spectrum (between static and mobile); and
- *collaboration* spectrum (between individual and group).

Each of the three Pouezevara and Strigel (2012) spectra is non-binary, meaning that m-learning occurs along the spectrum between the two possibilities.

To take account of the resource-constrained environments prevalent in South Africa, Roberts and Spencer-Smith (2019) add *device access* and *data affordability* spectra (see Figure 4). International and local studies have confirmed the importance of access and affordability elements in m-learning delivery (Benner & Pence, 2013; Ebner & Grimus, 2013; Nedungadi & Raman, 2012). The *device access* spectrum ranges from m-learning that is designed or used with free devices provided to learners to a situation where learners need to bring their own device (i.e., bring your own device, or BYOD). Within this range, different permutations of learning design can manifest. For instance, learners can be required to bring their own devices but may also receive a subsidy towards monthly device costs. The *data affordability* spectrum can range from scenarios where mobile data is provided or subsidised to situations where learners need to pay all of their own data costs.

Figure 4: Roberts and Spencer-Smith (2019) framework



Source: Adapted from Roberts and Spencer-Smith (2019, p. 4)

Finally, Roberts and Spencer-Smith (2019) add *pedagogy/theory of learning* as a spectrum, with "a well-defined and articulated theory of learning" at one end of the spectrum, and "no articulation of learning theory" at the other end. In adding this spectrum to their framework, Roberts and Spencer-Smith (2019) seek to take account of the concerns raised by Danaher et al. (2009) and Laurillard (2002) regarding under-emphasis on pedagogy in some approaches to m-learning.

Research question 2: Framework suitable for Penreach

- *Which framework, or combination/adaptation of frameworks, is suitable for the task of assessing the feasibility of three m-learning applications for Penreach?*

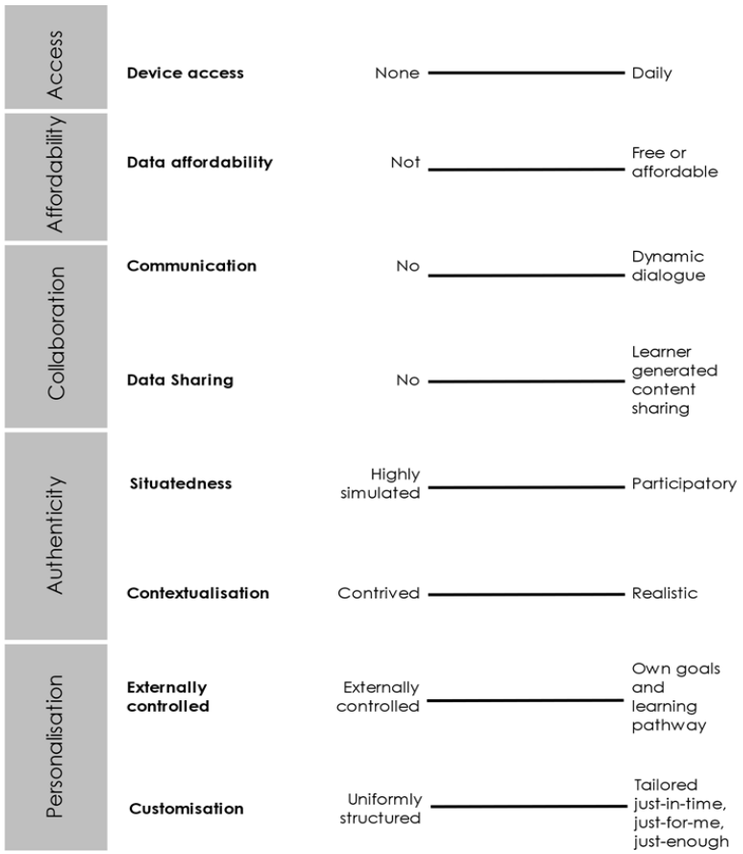
The framework we found to be suitable for assessing Penreach m-learning applications incorporates key features from both the Kearney et al. (2012) and the Roberts and Spencer-Smith (2019) frameworks. It is firmly located within a sociocultural learning perspective.

All three components of the Kearney et al. (2012) framework—*collaboration*, *authenticity*, and *personalisation*—are included in the framework. With respect to the Roberts and Spencer-Smith (2019) framework, its *collaborative* spectrum was already represented in the Kearney et al. (2012) framework, and it was determined that the *learning* spectrum could be left out as it was not foregrounded in this study. (ECD skills training in the Penreach programme, and other similar programmes, is voluntary, non-accredited, and not part of a formal training curriculum. Learning takes place through workshops, with the application of newly acquired skills in the workplace. The m-learning setting was therefore already defined. The m-learning could be done at home, at work, or during the Penreach workshop, and none of these configurations was considered to have had an impact on the feasibility.)

The *kinetic* spectrum, adopted by the Roberts and Spencer-Smith (2019) framework from Pouezevara and Strigel (2012), was also not included, because the degree to which Penreach practitioners were required to sit or perform activities while using m-learning was not considered important in terms of feasibility. And the Roberts and Spencer-Smith (2019) *pedagogy/theory of learning* spectrum was included because it was felt that Penreach had already explicitly adopted a sociocultural perspective.

It was determined that the Roberts and Spencer-Smith (2019) *device access* and *data affordability* spectra were highly relevant given Penreach's focus on a resource-constrained environment. The resulting framework (see Figure 6) comprises: *collaboration*, *authenticity*, and *personalisation*.

Figure 6: Framework for assessment of Penreach m-learning applications



5. Conclusion

The need for a framework to assess m-learning applications in ECD was identified as part of a larger study into the feasibility of this form of learning in the South African ECD training context. First, the dearth of research about m-learning in pre-Grade R practitioner training was recognised. Existing research did, however, allow for the development of a conceptual frame for analysing the feasibility of m-learning in the ECD training context. We adopted a sociocultural perspective for the training of ECD practitioners, recognising the reciprocal influence between the practitioner and the environment as part of the learning process. Particularly useful was the initial research into m-learning as a field by Traxler (2007), Koole (2009), and Laurillard (2002), which locates m-learning in the realm of sociocultural learning.

Further exploration allowed us to consider different existing sociocultural frameworks for m-learning. Based on this analysis, we determined the need for a new, modified framework. Elements of recent frameworks developed by Kearney et al. (2012) and Roberts and Spencer-Smith (2019) were combined to develop a sociocultural learning framework that conceives of feasible m-learning in ECD as featuring *device access*, *data affordability*, *authenticity*, *collaboration*, and *personalisation*.

In the South African ECD context, practitioners operate in environments where no or little subsidy exists for accessing m-learning devices and data. In addition to these issues of access and affordability, the highly practical and situated work of educating young children requires a learning environment for practitioners that enables collaborative, authentic, and personalised learning. The modified analytical framework that incorporates these sociocultural dimensions is intended for use by researchers and implementers when considering the use of m-learning in ECD training—including m-learning in the pre-Grade R training context—in under-resourced contexts.

References

Alawani, A. S., & Singh, A. D. (2017). A smart mobile learning conceptual framework for professional development of UAE in-service teachers. *International Journal of Management and Applied Research*, *4*(3), 146–165. https://doi.org/10.18646/2056.43.17-012

Ashley-Cooper, M., Atmore, E., & Van Niekerk, L. (2012). Challenges facing the early childhood development sector in South Africa. *South African Journal of Childhood Education*, *2*(1), 120–139. https://doi.org/10.4102/sajce.v2i1.25

Pachler, N. Cook, & Bachmair, B., (2010). Appropriation of mobile cultural resources for learning. *International Journal of Mobile and Blended Learning*, *2*(1), 1–211. https://doi.org/10.4018/jmbl.2010010101

Benner, A., & Pence, A. (2013). From e- to m-learning: Feasibility for an African-delivered tertiary program. *E-Learning and Digital Media*, *10*(1), 13–21. https://doi.org/10.2304/elea.2013.10.1.13

Biersteker, L., Dawes, A., & Irvine, M. (2008). *Scaling up early childhood development (ECD) (0–4 years) in South Africa. What makes a difference to child outcomes in the period 0–4? Inputs for quality ECD interventions*. Human Sciences Research Council. https://www.gtac.gov.za/Researchdocs/What%20makes%20a%20difference%20to%20childoutcomes%20in%20the%20period%200-4.pdf

Botha, A., Batchelor, J., Traxler, J., De Waard, I., & Herselman, M. (2012). Towards a mobile learning curriculum framework. In P. Cunningham, & M. Cunningham (Eds.), *IST-Africa 2012 conference proceedings.* IIMC. https://itg.academia.edu/IgnatiaIngedeWaard/Papers/1645325/Towards_a_Mobile_Curriculum_Framework

Botha, A., & Vosloo, S. (2009). Mobile learning: South African examples. Paper presented to Mobile Learning Institute Summit, Lusaka. https://www.slideshare.net/stevevosloo/mobile-learning-south-african-examples

Chee, K. N., Yahaya, N., Ibrahim, N. H., & Noor Hassan, M. (2017). Review of mobile learning trends 2010-2015: A meta-analysis. *Educational Technology & Society*, *20*(2), 113–126. https://www.researchgate.net/publication/315696935_Review_of_Mobile_Learning_Trends_2010-2015_A_Meta-Analysis

Conole, G. (2004). E-learning: The hype and the reality. *Journal of Interactive Media in Education*, *12*, 1–18. https://doi.org/10.5334/2004-12

Danaher, P., Gururajan, R., & Hafeez-Baig, A. (2009). Transforming the practice of mobile learning: Promoting pedagogical innovation through education principles and strategies that work. In D. Parson, & H. Rvu (Eds.), *Innovative and mobile learning: Techniques and technologies* (pp. 21–46). IGI Global. https://doi.org/10.4018/978-1-60566-062-2.ch002

Department of Basic Education (DBE). (2018). *Professional development framework for digital learning*.Government of South Africa. https://www.education.gov.za/Portals/0/Documents/Publications/Digital%20Learning%20Framework.pdf?ver=2018-07-09-101748-95

DBE, Department of Social Development (DSD), & UNICEF. (2011). *Tracking public expenditure and assessing service quality in early childhood development in South Africa*. https://www.unicef.org/southafrica/media/1736/file/ZAF-tracking-public-expenditure-and-assessing-service-quality-in-early-childhood-development-2011.pdf

Department of Social Development (DSD). (2006). *Guidelines for early childhood development services*. Government of South Africa. https://www.gov.za/sites/default/files/gcis_document/201409/childhooddev0.pdf

Department of Social Development (DSD). (2014). *Audit of early childhood development (ECD) centres: National report*. Government of South Africa. https://ilifalabantwana.co.za/wp-content/uploads/2015/08/ECDAuditNationalReport20140731ReviewedFINALVersionES11.pdf

Ebner, M., & Grimus M. (2013). M-learning in Sub Saharan Africa context. What is it about? Paper presented at the World Conference on Educational Media and Technology, 24–28 June, Victoria, BC, Canada. https://www.researchgate.net/publication/283727687_M-Learning_in_Sub_Saharan_Africa_Context-_What_is_it_about

Eun, B. (2008). Making connections: Grounding professional development in the developmental theories of Vygotsky. *The Teacher Educator*, *43*(2), 134–155. https://doi.org/10.1080/08878730701838934

Feza, N. (2014). Inequities and lack of professionalisation of early childhood development practice hinder opportunities for mathematics stimulation and realisation of South African policy on quality education for all. *International Journal of Inclusive Education*, *18*(9), 888–902. https://doi.org/10.1080/13603116.2013.855266

Hall, K. (2019). Income poverty, unemployment and social grants. In M. Shung-King, L. Lake, D. Sanders, & M. Hendricks (Eds.), *South African child gauge 2019* (pp. 222–227). Children's Institute, University of Cape Town. http://childrencount.uct.ac.za/uploads/publications/ChildGauge%202019_final.pdf

Herrington, J., & Oliver, R. (2001). *A beginner's guide to e-learning and e-teaching in higher education*. Centre for Research in Information Technology and Communications, Edith Cowan University, Western Australia. http://researchrepository.murdoch.edu.au/1903/

Herselman, M., & Botha, A. (Eds.). (2014). *Designing and implementing an information communication technology for rural education development (ICT4RED) initiative in a resource constrain[ed] environment: Nciba school district, Eastern Cape, South Africa*. CSIR Meraka. http://hdl.handle.net/10204/8094

Isaacs, S. (2012). *Mobile learning for teachers in Africa and the Middle East*. UNESCO Working Paper Series on Mobile Learning. http://www.schoolnet.org.za/sharing/mobile_learning_AME.pdf

Isaacs, S., Roberts, N., & Spencer-Smith, G. (2019). Learning with mobile devices: A comparison of four mobile learning pilots in Africa. *South African Journal of Education*, *39*(3), 1–13. https://doi.org/10.15700/saje.v39n3a1656

Isaacs, S., Roberts, N., Spencer-Smith, G., & Brink, S. (2019). Learning through play in Grade R classrooms: Measuring practitioners' confidence, knowledge and practice. *South African Journal of Childhood Education*, *9*(1), 1–11. https://doi.org/10.4102/sajce.v9i1.704

Kearney, M., Schuck, S., Burden, K., & Aubusson, P. (2012). Viewing mobile learning from a pedagogical perspective. *Research in Learning Technology*, *20*(1), 1–17. https://doi.org/10.3402/rlt.v20i0.14406

Kelly, L. J. (2007). *The interrelationships between adult museum visitors' learning identities and their museum experiences*. PhD thesis, University of Technology, Sydney.

Klopfer, E., Squire, K., & Jenkins, H. (2002). Environmental detectives: PDAs as a window into a virtual simulated world. In IEEE (Ed.), *Proceedings of IEEE International Workshop on Wireless and Mobile Technologies in Education (WMTE'02)* (pp. 95–98). https://doi.org/10.1109/WMTE.2002.1039227

Koole, M. (2009). A model for framing mobile learning. In M. Ally (Ed.), *Mobile learning: Transforming the delivery of education and training* (pp. 26–50). Athabasca University Press.

Laurillard, D. (2002). *Rethinking university teaching: A conversational framework for the effective use of learning technologies* (2nd ed.). Routledge Falmer. https://doi.org/10.4324/9780203304846

May, J., Witten, C., Lake, L., & Skelton, A. (2020). The slow violence of malnutrition. In J. May, C. Witten, & L. Lake (Eds.), *South African child gauge 2020* (pp. 24–45). Children's Institute, University of Cape Town.

National Planning Commission (NPC). (2012). *National development plan 2030: Our future – make it work*. Government of South Africa. https://www.gov.za/sites/default/files/gcis_document/201409/ndp-2030-our-future-make-it-workr.pdf

Nedungadi, P., & Raman, R. (2012). A new approach to personalization: Integrating e-learning and m-learning. *Educational Technology Research and Development*, *60*(4), 659–678. https://doi.org/10.1007/s11423-012-9250-9

Organisation for Economic Co-operation and Development (OECD). (2017). *The OECD handbook for innovative learning environments, educational research and innovation*. OECD Publishing.

Pouezevara, S., & Strigel, C. (2012). *Mobile learning and numeracy: Filling gaps and expanding opportunities for early grade learning.* RTI International. https://www.rti.org/pubs/mobilelearningnumeracy_rti_final_17dec12_edit.pdf

Republic of South Africa (RSA). (2015). National Integrated Early Childhood Development Policy. https://www.gov.za/sites/default/files/gcis_document/201610/national-integrated-ecd-policy-web-version-final-01-08-2016a.pdf

Roberts, N., & Spencer-Smith, G. (2019). A modified analytical framework for describing m-learning (as applied to early grade Mathematics). *South African Journal of Childhood Education*, *9*(1), 1–11. https://doi.org/10.4102/sajce.v9i1.532

Shabani, K. (2016). Applications of Vygotsky's socio-cultural approach for teachers' professional development. *Cogent Education*, *3*(1), 1–10. https://doi.org/10.1080/2331186X.2016.1252177

Statistics South Africa (Stats SA). (2016). *Education Series IV: Early Childhood Development in South Africa 2016.* Government of South Africa. http://www.statssa.gov.za/publications/92-01-04/92-01-042016.pdf

Thorogood, C., Goeiman, H., Berry, L., & Lake, L. (2020). Food and nutrition security for the preschool child: Enhancing early childhood development. In J. May, C. Witten, & L. Lake (Eds.), *South African child gauge 2020* (pp. 96–110). Children's Institute, University of Cape Town.

Traxler, J. (2007). Defining, discussing and evaluating mobile learning: The moving finger writes and having writ …. *The International Review of Research in Open and Distributed Learning*, *8*(2), 1–12. https://doi.org/10.19173/irrodl.v8i2.346

Trucano, M. (2016). *SABER-ICT Framework Paper for Policy Analysis: Documenting national educational technology policies around the world and their evolution over time.* World Bank. https://doi.org/10.1596/26107

Vygotsky, L. S. (1978). *Mind in society: The development of higher psychological processes.* Harvard University Press.

Wills, G., & Kika-Mistry, J. (2021). *Early childhood development in South Africa during the COVID-19 pandemic: Evidence from National Income Dynamics Study – Coronavirus Rapid Mobile Survey (NIDS-CRAM): Waves 2–5.* https://cramsurvey.org/wp-content/uploads/2021/07/14.-Wills-G-_-Kika-Mistry-J.-2021-Early-Childhood-Development-in-South-Africa-during-the-n-COVID-19-pandemic-Evidence-from-NIDS-CRAM-Waves-2-5.pdf

World Bank. (2018). *World development report: Learning to realize education's promise.* https://doi.org/10.1596/978-1-4648-1096-1

Cybersecurity Policymaking in the BRICS Countries: From Addressing National Priorities to Seeking International Cooperation

Luca Belli
Professor of Internet Governance and Regulation, Head of Center for Technology and Society (CTS), and Head of CyberBRICS project, Fundação Getulio Vargas (FGV) Law School, Rio de Janeiro
https://orcid.org/0000-0002-9997-2998

Abstract
In the concluding statement of the 2021 BRICS Summit, the bloc's five members—Brazil, Russia, India, China, and South Africa—pledged to pursue enhanced cooperation on cybersecurity issues, including by "establishing legal frameworks of cooperation among BRICS" and a BRICS intergovernmental agreement on cybersecurity. This piece briefly outlines the mounting relevance of cybersecurity for the BRICS countries, recent national policymaking in this area in the bloc, and the dynamics at play as the BRICS countries seek to further intensify and structure their cooperation on cybersecurity matters.

Keywords
cybersecurity, data protection, personal information, content moderation, cybercrime, policy, policymaking, BRICS, Brazil, Russia, India, China, South Africa

Acknowledgement
This piece draws on the contents of a blog post (Belli, 2021c) for the Directions blog of the European Union Institute for Security Studies (EUISS) Cyber Diplomacy Initiative (EU Cyber Direct). The author thanks Dr. Patryk Pawlak for feedback on the content of that blog.

DOI: https://doi.org/10.23962/10539/32208

Recommended citation
Belli, L. (2021). Cybersecurity policymaking in the BRICS countries: From addressing national priorities to seeking international cooperation. *The African Journal of Information and Communication (AJIC), 28*, 1-14.
https://doi.org/10.23962/10539/32208

1. Introduction

The 13th BRICS Summit, hosted by India on 9 September 2021, gave prominent attention to cybersecurity as one of the priorities identified in the Summit's concluding New Delhi Declaration (BRICS, 2021). Engagement and initiatives regarding cybersecurity by the BRICS countries—Brazil, Russia, India, China, and South Africa—have gained remarkable relevance in recent years. BRICS governments have adopted numerous laws that either explicitly frame cybersecurity or regulate some closely related aspects, and some of these legislative and regulatory initiatives may have a significant impact at the international level (see Belli, 2021a, 2021b). Importantly, the five countries' national approaches present several points of overlap and tend towards convergence, but at the same time we can identify significant points of divergence.

Despite growing alignment in several aspects of their priorities and policies, it is useful to recall that the BRICS bloc is a particularly young and unusual initiative, encompassing enormously different countries. After being created as a mere acronym, signifying countries with remarkable economic growth forecast,[1] in 2001, the BRICs organised their first informal meeting, in 2006, on the margins of that year's UN General Assembly. The first BRICs heads of state meeting was held in 2009 and, in 2011, the full integration of South Africa transformed the acronym into a larger and stronger BRICS. In 2014, the bloc established the BRICS-led New Development Bank,[2] its most prominent achievement, and, over subsequent years, more than 100 high-level events, partnerships, and initiatives have been promoted by the bloc every year.[3] This year, 2021, marks its 15th anniversary.

The BRICS' desire to cooperate on cybersecurity policy can be traced back to its 2013 eThekwini Declaration and Action Plan at the closing of the BRICS Summit in Durban, South Africa, which, for the first time, stated the need "to contribute to and participate in a peaceful, secure, and open cyberspace" and called for the elaboration of "universally accepted norms, standards and practices" (BRICS, 2013).

We should note that it was not a coincidence that BRICS countries' interest in digital policy issues related to cybersecurity—such as data protection, critical infrastructure security, cybercrime, and cyber defence—started to gain an increasingly essential and strategic role for the group in 2013 (see Belli, 2021b). It was indeed in that year that former US National Security Agency (NSA) contractor Edward Snowden (currently still in exile in Russia) revealed the unprecedented scale and pervasiveness of the

1 The acronym was first coined, in 2001, by a Goldman Sachs economist (O'Neill, 2001).
2 See https://www.ndb.int
3 For overviews of the evolution of BRICS, see Stuenkel (2016, 2020).

American-led global surveillance schemes which included, inter alia, the wiretapping of the personal phone of Brazilian President Dilma Rousseff (MacAskill & Dance, 2013).

BRICS cooperation in this area has intensified ever since. Notably, in the 2015 Ufa Declaration, at the conclusion of the 7th BRICS Summit, hosted by Russia, leaders established a "Working Group of Experts of the BRICS States on security in the use of ICTs" with a mandate to, inter alia, "develop practical cooperation with each other in order to address common security challenges in the use of ICTs" (BRICS, 2015). Also in that year, the BRICS ICT ministers signed a Memorandum of Understanding on Cooperation in Science, Technology, and Innovation (see Zhao et al., 2018), with the aim of promoting cooperation in these fields. Several concrete outputs followed these developments (see Belli, 2021b), including the BRICS Digital Partnership, the BRICS Partnership on New Industrial Revolution (PartNIR), the Innovation BRICS Network (iBRICS Network), and the BRICS Institute of Future Networks—all of which contributed to the construction of an enhanced cooperation process (see Belli, 2020b), combining policy, technology, and research initiatives.

The initiatives mentioned in this introductory section illustrate that the BRICS countries have adopted a remarkably interesting and sophisticated approach to cooperation and regulation. While agreeing on shared principles and high-level objectives through the annual declarations, they have crafted a blend of normative and developmental approaches to shape the ways in which their cooperation and regulation should unfold. Such an approach is not immediately intelligible for an observer used to considering only the normative side of regulation. Indeed, cooperation and regulation, be they on cybersecurity or on any other matters, cannot be achieved merely through norm-making. From a developmental perspective, it is much more effective to invest in research and development, rather than simply relying on norms in order to regulate economy, society, and technology.

The consideration proposed above, of the need to distinguish between normative and developmental dimensions of regulation, is essential to understanding the complexity of BRICS, before beginning the analysis of the latest normative policy steps taken by the group members. The primary aim of this article is, indeed, to focus on the increasing rapprochement of normative cybersecurity policy priorities and regulatory strategies across the grouping, rather than focusing on the developmental aspects of the bloc's approach to regulation. In this spirit, the following section provides an overview of some of the key policy developments, allowing the reader to understand how cybersecurity-related policies may be converging or diverging in specific areas.

2. Brazil

In 2020, Brazil adopted a new Cybersecurity Strategy,[4] enacted a new Data Protection Law[5] (best-known as "LGPD", in its Portuguese acronym), and tabled a regulation for social media content in the form of the Internet Freedom, Responsibility, and Transparency Bill (frequently referred to as the "Fake News Bill").[6] In mid-2021, Brazil created a new Federal Cyber Incident Management Network for federal public administrations[7] and rapidly adopted—and abandoned—the Executive Order 1068/2021,[8] altering the intermediary liability framework established by the Brazilian Internet Rights Framework (Marco Civil da Internet).[9]

The implications of these policy steps are mixed. The new Federal Cyber Incident Management Network is widely seen as welcome, but the Cybersecurity Strategy has been criticised for lacking the definition of objectives, budget, responsibilities, and deadlines—all of which are indeed the central elements of any strategy. The LGPD, strongly inspired by the EU's General Data Protection Regulation (GDPR), entered into force in September 2020, and represents a major step forward by introducing obligations to integrate privacy and data security measures into products and services—so-called "data protection by design". However, considerable work still needs to be done in terms of implementation. For example, despite the LGPD's creation of a new Data Protection Agency, Brazil witnesses major data leakages with remarkable frequency. In January 2021, personal data from the entire Brazilian population was leaked (see Belli, 2020a), and, while considerable advancements have occurred, the country is still far from having a data protection culture—one where all stakeholders are aware of data-related challenges, understand the social value of data protection, and cooperate to protect personal information (Belli & Doneda, 2021).

The proposed social media regulation (the Fake News Bill) has been criticised for introducing traceability requirements that would weaken encryption and raise the thorny issue of user-identification requirements (Iunes & Macedo, 2021). Notably, the Bill has raised such a level of criticism that the Special Rapporteur on Freedom of Expression of the Organisation of American States sent an official communication to Brazil stating that the provisions proposed in the original version of the Bill were "highly problematic in light of the principles of the right to freedom of expression consonant with Brazil's obligations under the International Covenant on Civil and Political Rights (ICCPR) and the American Convention on Human Rights (ACHR)."[10]

Meanwhile, the Executive Order altering intermediary liability had a very short life. As soon as it was adopted, it was unanimously criticised for the fact that it was likely to unduly affect freedom of expression and business operations. The Order aimed to prohibit social networks from removing misinformation when the content is of a "political, ideological, scientific, artistic or religious nature", even if contrary to a platform's terms of service. The Brazilian Supreme Court duly suspended the Order in September 2021,[11] less than two weeks after its adoption by the Federal Government, on the grounds that it was unconstitutional.

3. Russia

Russia enacted its Internet Sovereignty Law in 2019 (see Shcherbovitch et al., 2019), and, in 2021, amended its Data Protection Law and its Law on Information, IT and Protection of Information (see Zanfir-Fortuna & Iminova, 2021). The Internet Sovereignty Law purportedly aims to protect the country from cyberattacks. Under certain circumstances, it allows the Federal Government to mandate the disconnection of the Russian segment of the internet, the "Runet", from the global internet. While the extent to which Russia can implement an "infrastructure-embedded control" (Daucé & Musiani, 2021) of this sort remains unclear, the aim is overtly to be able to cut off its internet from the rest of the world (Musiani et al., 2019).

The Russian sovereign internet provisions aim at reproducing China's course of action in the early 2000s with its "Great Firewall of China", which created a large

4 See Decree nº 10.222/2020: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Decreto/D10222.htm

5 See unofficial English version of the Brazilian General Data Protection Law: https://cyberbrics.info/brazilian-general-data-protection-law-lgpd-unofficial-english-version/

6 See Bill nº 2.630/2020: https://www25.senado.leg.br/web/atividade/materias/-/materia/141944

7 See Secretaria Geral da Presidência da República (2021, July 19). Presidente Bolsonaro cria a Rede Federal de Gestão de Incidentes Cibernéticos: https://www.gov.br/secretariageral/pt-br/noticias/2021/julho/presidente-bolsonaro-cria-a-rede-federal-de-gestao-de-incidentes-ciberneticos

8 See https://www.in.gov.br/en/web/dou/-/medida-provisoria-n-1.068-de-6-de-setembro-de-2021-343277275?s=08

9 Law 12.965/2014, known as the Brazilian Civil Rights Framework for the Internet, or Marco Civil da Internet (MCI) in Portuguese, is the federal law that establishes the principles and rules that govern the use of the internet in Brazil. Despite being categorised as an ordinary law, the MCI has been considered as the "Internet Constitution" of Brazil, because it defines the foundational elements of internet governance and regulation in the country, building into the law a marked intention to protect fundamental rights and freedoms online. The MCI is considered a symbol of participatory democracy due to the online consultation process that led to its creation. The process leading to the elaboration of the draft MCI bill was initiated and orchestrated by the Center for Technology and Society at Fundação Getulio Vargas (CTS-FGV), in partnership with the Brazilian Ministry of Justice and the Brazilian Internet Steering Committee (see CGI.br, 2014). While the elaboration of the MCI was initiated under President Luiz Inácio Lula da Silva, the processes culminated with the sanction of President Dilma Rousseff who, in response to intelligence revelations by NSA contractor Edward Snowden, called for the implementation of strong guarantees of human rights on the internet.

10 See Relatoria Especial para a Liberdade de Expressão da CIDH. CIDH/RELE/Art. 41/7-2020/65 (3 July 2020): http://www.oas.org/es/cidh/expresion/documentos_basicos/PORTCARTAONUCIDH-BRASILINTERNET2020.pdf

11 See Supremo Tribunal Federal. Medida Cautelar na Ação Direta de Inconstitucionalidade 6.991 (14 September 2021): https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=757262152&prcID=6253449

national intranet that was connected through only limited channels to the rest of the internet outside the country. However, when China decided to implement its plan, at the dawn of the 21st century, the internet was much less pervasive than it is today. The Chinese citizens of the early 2000s were not reliant on the open internet for their everyday lives. The Russians of the 2020s, in contrast, have grown accustomed to a relatively open internet, making the necessary financial resources, personnel, technology, and disruption caused by the disconnection of the Runet significantly more complicated and intensive, compared to the situation in early 2000s China (Daucé & Musiani, 2021).

Amendments to two other Russian laws—the Data Protection Law and the Information Law—entered into force in March 2021. The amendments to the former create new requirements for personal data sharing and new oversight attributions for Roskomnadzor, the Federal Media and Information Regulator. The Information Law amendments require social networks to monitor content and "restrict access immediately" for users sharing information about sensitive matters such as state secrets, terrorism, pornography, promoting violence or riots, or using obscene language. These latter requirements have drawn objections from the European Court of Human Rights—to which Russia is subject, as a member of the Council of Europe[12]—that, in June 2020, criticised the law for allowing the government to take down or block online content without requiring a court order (see Grover & Thomas, 2021).

4. India

The Indian government made headlines in 2021 with its new Information Technology Intermediary Guidelines and Digital Media Ethics Code Rules, 2021 ("IT Rules"),[13] and the tabling of the latest version of its Personal Data Protection (PDP) Bill is expected very soon.

The IT Rules establish a wide range of requirements, the most controversial of which are its social media content takedown framework and content traceability mandate (Rule 4(2)). The content takedown provisions are seen as excessively broad, as they allow the government to issue orders to intermediaries, requesting them to take down information hosted by them, thus considerably increasing the government's capability to restrict freedom of expression online. In respect of the Rule 4(2) content-tracing provision, major social media networks (i.e., those with more than 5 million users) now have an obligation to enable the tracing of the originators of content on their platforms, i.e., the social media platforms are required to keep a metadata trail

12 See https://www.coe.int/en/web/about-us/our-member-states

13 See Press Information Bureau of the Government of India (2021, February 25). Government notifies Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021. https://www.pib.gov.in/PressReleseDetail.aspx?PRID=1700749

of their users' communications in order to be able to respond to government requests to trace specific messages.

This latter provision—as with the similar traceability provisions in the aforementioned Brazilian Fake News Bill—has been criticised for its potential to jeopardise the use of end-to-end encryption to maintain anonymity (SFLC.IN, 2021). Both WhatsApp and its parent company, Facebook—now also known as Meta—have filed petitions in the High Court of Delhi challenging Rule 4(2), emphasising that the provision undermines user privacy. WhatsApp contends that such a system requires it to *de facto* store metadata of each message sent though its platform, enabling "a new form of mass surveillance" (SFLC.IN, 2021).

The PDP Bill, when enacted, will help provide legal certainty on a variety of issues that intersect with those discussed above. Importantly, India is the only BRICS country that has not yet adopted a data protection law, and its PDP Bill is very similar in many respects to the other BRICS countries' frameworks.[14] The Bill aims to establish a comprehensive framework for regulating personal data processing, and is structured in 14 chapters that, inter alia, provide definitions; establish detailed obligations of the "data fiduciaries", including data security obligations; clarify the grounds for processing personal data; define the rights of "data principal"; and create a new regulator, the Data Protection Authority of India.

The first version of the PDP Bill was proposed by the government in 2018 in the aftermath of the Puttaswamy case (see CIS, 2020), a landmark decision by the Supreme Court of India that created a new fundamental right to privacy in the country. The Bill has been altered (and broadened) substantially in the intervening years, including the addition of a contentious section 35, which ascribes to the government an ample right to exempt governmental agencies from the application of the PDP Bill. Such evolutions led one of its original drafters, retired Supreme Court judge Justice B. N. Srikrishna, to characterise one of the Bill's most recent versions as "a blank cheque to the state" (Sircar, 2020).

5. China

China has been extremely busy in 2021 in respect of data-related policies, with special attention being paid to the cybersecurity dimension of data processing. China seems to be one of the few places in the world where policymaking outpaces technology developments and where regulation is strictly enforced (*The Economist*, 2021). The Chinese policy emphasis on data matters reflects Beijing's clear understanding of the key strategic advantage brought by having sound data protection and data security

14 For a detailed comparative analysis of the personal data frameworks of the BRICS countries, see https://cyberbrics.info/data-protection-across-brics-countries

frameworks (Belli, 2019), and its consideration of (personal) data—of which China is the largest producer globally—as an increasingly essential and valuable asset.

China enacted its new Civil Code[15] in January 2021, creating new legal rights to privacy and the protection of personal information. In August 2021, the Chinese National People's Congress adopted the new Personal Information Protection Law[16] (PIPL), and the Cyberspace Administration of China has since released a draft Regulation on Automobile Data Security for comment.[17] The PIPL, which may be seen as a GDPR with Chinese characteristics, defines China's comprehensive data protection system, setting general rules that are then to be specified according to the needs of particular sectors. To start complementing the PIPL, in October 2021 China adopted its Ethical Specifications of Next-Generation Artificial Intelligence,[18] and opened a consultation on Draft Guidance on Security Assessments for Cross-Border Data Transfers.[19]

In June 2021, Beijing adopted its new Data Security Law (DSL),[20] which defines more stringent requirements for processing "important data", "core state data", and "sensitive data", and extends (to all automated data-processing) the requirement to comply with the Multi-Level Protection Scheme (MLPS)[21] mandated by the 2017 Cybersecurity Law.[22] The DSL extends data localisation obligations, which mandate the storage of data in servers located in the national territory, to the aforementioned "important data". Article 21 of the DSL prescribes that "[e]ach region and department, shall stipulate a regional, departmental, as well as relevant industrial and sectoral important data specified catalogue, according to the data categorization." Important data listed in such catalogues may encompass an enormous spectrum of data linked to economic development, national security, the public interest, individuals' rights, and corporates' interests. Such important data are subject to special security requirements as well as international transfer restrictions.[23] While the latest Chinese policies have strengthened data localisation obligations, it is important to note that such requirements were already present in the country, via the 2017 Cybersecurity Law, and were probably inspired by Russia's data localisation provisions introduced in 2015 (Shcherbovich, 2021).

In 2020, China adopted the Provisions on the Governance of the Online Information Content Ecosystem,[24] which play a major role in regulating online content. The Provisions define which categories of content are considered illegal, what content producers are encouraged to develop and publish, and an obligation to prevent the production of "undesirable" types of content. Illegal content includes any message instigating criminal activities or violence or defaming others. Encouraged content includes that which fosters "core socialist values", the doctrine of the Communist Party, and "positive and wholesome" messages. Undesirable content includes sensationalist headlines, coarse and vulgar language, gossip, and content that fosters improper habits that might be emulated by minors. Also in 2020, China announced its willingness to launch a Global Data Security Initiative, but so far this initiative has not gained meaningful traction.

6. South Africa

South Africa has also undertaken significant policy updates in 2021 that are relevant to cybersecurity (see Mabunda, 2021). As in the rest of the world, the COVID-19 pandemic has obliged the South African population to increasingly rely on electronic communications, connected devices, and digital services. While this has boosted the much-acclaimed "Fourth Industrial Revolution",[25] it has also offered an ideal ground for the proliferation of cybercrimes, including data breaches, online fraud, and identity theft. In June 2021, President Cyril Ramaphosa signed the new Cybercrimes Act of South Africa into law,[26] thus bringing the country up to date with international best practices. The Act creates new crimes in respect of certain types of access and interception of data, certain uses of software and hardware tools, and certain acts of interference with data or computer programs.

15 See http://www.npc.gov.cn/englishnpc/c23934/202012/f627aa3a4651475db936899d69419d1e/files/47c16489e186437eab3244495cb47d66.pdf

16 See https://digichina.stanford.edu/news/translation-personal-information-protection-law-peoples-republic-china-effective-nov-1-2021

17 See https://www.gov.cn/xinwen/2021-05/12/content_5606075.htm

18 See https://www.most.gov.cn/kjbgz/202109/t20210926_177063.html

19 See https://digichina.stanford.edu/work/translation-outbound-data-transfer-security-assessment-measures-draft-for-comment-oct-2021/

20 See the unofficial English version of China's Data Security Law: http://www.cov.com/-/media/files/corporate/publications/file_repository/data-security-law-bilingual.pdf

21 The MLPS is a cybersecurity compliance scheme that applies to virtually all organisations in China. It was first introduced in 1994 and subsequently updated in 2019, in accordance with Article 21 of the Cybersecurity Law. The MLPS classifies systems based on the damage that a hypothetical vulnerability of the system may pose to China's cybersecurity. The scheme requires all network operators to ensure that their networks are protected against interference, damage, or unauthorised access. Under MLPS, all network operators are required to classify their infrastructure and application systems on a 1 to 5 scale, and fulfil protection obligations accordingly. Systems ranked at 3 or higher are considered higher-stake, and are subject to notably stricter obligations, including on data security. See https://www.protiviti.com/HK-en/insights/pov-multiple-level-protection-scheme

22 See http://lawinfochina.com/display.aspx?id=22826&lib=law

23 Appendix A of the Draft Guidelines for Cross-Border Data Transfer Security Assessments provides a detailed list of "important data" in different sectors. For instance, in the military sector, "important data" encompass information on the name, quantity, source and agent of purchased components, software, materials, industrial control equipment test instruments, geographical location, construction plans, security planning, secrecy level, plant drawings, storage volume, reserves of military research, and production institutions. See https://www.cac.gov.cn/2021-10/29/c_1637102874600858.htm

24 See the unofficial English translation of the Provisions on the Governance of the Online Ecosystem: https://www.chinalawtranslate.com/en/internetgovernance/

25 See Presidency of the Republic of South Africa (2020). *Report of the Presidential Commission on the Fourth Industrial Revolution*: https://cyberbrics.info/report-of-the-presidential-commission-on-the-fourth-industrial-revolution

26 See https://cyberbrics.info/cybercrime-act-south-africa/

In July 2021, the one-year grace period for the country's Protection of Personal Information Act (POPIA)[27] ended, thus making the law fully enforceable after an eight-year gestation period. The law was formally approved in 2013, but its implementation was subsequently put on hold while a new Information Regulator was established and South Africans were prepared for compliance. The Information Regulator is the data protection authority established by POPIA. Although it held its first meeting at the end of 2016, only in 2021 did it become able to duly monitor the implementation of POPIA, at the end of the grace period. POPIA draws significant inspiration from the European data protection regimes, establishing data protection principles, data subject rights, and an ample range of obligations, including security measures that must be implemented when processing personal data (according to sections 20 and 21 of POPIA). There are several points of intersection between POPIA and the Cybercrimes Act, due the latter's criminalisation of conduct that "interferes with a computer data storage medium or a computer system."[28]

It is interesting to note that South Africa is a signatory to the Council of Europe's Budapest Convention on Cybercrime,[29] despite not being a member of the Council. Meanwhile Russia, which is a Council member, has never signed the Convention and has been actively promoting international efforts to create a cybercrime treaty within the UN.

7. Enhanced cooperation at the international level?

As seen above, some parallels can be seen at national level in BRICS countries with respect to certain approaches to cybersecurity matters. At the same time, the countries' calls for enhanced cooperation, within the bloc, on such issues are becoming increasingly explicit (Belli, 2019). Indeed, in the aforementioned 2021 New Delhi Declaration, BRICS leaders expressed the intention to

> […] advance practical intra-BRICS cooperation in this domain, including through the implementation of the BRICS Roadmap of Practical Cooperation on ensuring Security in the Use of ICTs and the activities of the BRICS Working Group on Security in the use of ICTs, and underscore[d] also the importance of establishing legal frameworks of cooperation among BRICS States on this matter and acknowledge[d] the work towards consideration and elaboration of proposals, including on a BRICS intergovernmental agreement on cooperation on ensuring security in the use of ICTs and on bilateral agreements among BRICS countries. (BRICS, 2021)

The ease with which enhanced BRICS cooperation on cybersecurity matters can occur remains unclear. Cybercrime is a highly sensitive issue, and national

27 See https://popia.co.za/
28 For an analysis of the intersections, see Snail (2021).
29 See https://www.coe.int/en/web/impact-convention-human-rights/convention-on-cybercrime

policymakers' decisions regarding which acts constitute cybercrimes are highly subject to their domestic legal, political, cultural, and economic particularities.

While South Africa has signed the Budapest Convention and Brazil has declared its intention to do so,[30] China, India, and Russia have not—and these three have a clear preference to coordinate their cybercrime initiatives within the UN and, to some extent, within the Shanghai Cooperation Organisation (SCO).[31] Since 2011, the SCO has elaborated upon an International Code of Conduct for Information Security, which was updated in 2015, reaffirming that "policy authority for Internet-related public policy issues is the sovereign right of States" and including the pledge "[n]ot to use information and communications technologies and information and communications networks to carry out activities which run counter to the task of maintaining international peace and security".[32]

When speaking as a bloc, the BRICS countries have consistently emphasised that the UN is the most appropriate venue for international policy development on cybersecurity and cybercrime. Willingness to enhance cooperation on such topics within the UN was recently reiterated by BRICS National Security Advisors,[33] and some members of this grouping have explicitly expressed interest in working on a "pentalateral" agreement to create a comprehensive system for countering cyber-threats. The BRICS 2021 New Delhi Declaration saluted the consensus found in the July 2021 report of the UN Group of Governmental Experts (GGE) on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security.[34] Conspicuously, the GGE was composed of experts from a grouping of 25 countries that included all of the BRICS nations and was chaired by Brazilian diplomat Guilherme Patriota, who is Brazil's Consul-General in Mumbai.[35]

30 See Ministério das Relações Exteriores (2019, December 11). Processo de adesão à Convenção de Budapeste - Nota Conjunta do Ministério das Relações Exteriores e do Ministério da Justiça e Segurança Pública: https://www.gov.br/mre/pt-br/canais_atendimento/imprensa/notas-a-imprensa/2019/processo-de-adesao-a-convencao-de-budapeste-nota-conjunta-do-ministerio-das-relacoes-exteriores--e-do-ministerio-da-justica-e-seguranca-publica
31 The Shanghai Cooperation Organisation (SCO), http://eng.sectsco.org, is an intergovernmental organisation aimed at political, economic, and security cooperation. It covers three-fifths of the Eurasian continent, 40% of the world population, and more than 20% of global GDP. The SCO is the successor of the "Shanghai Five" group, established in 1996 with the Treaty on Deepening Military Trust in Border Regions, in Shanghai, by the heads of states of China, Russia, Kazakhstan, Kyrgyzstan, and Tajikistan.
32 See https://www.fmprc.gov.cn/mfa_eng/wjdt_665385/2649_665393/t858323.shtml
33 See BRICS National Security Advisors (2020). The 10th Meeting of BRICS National Security Advisors: https://india.mid.ru/en/counter_terrorism/10th_meeting_of_brics_national_security_advisors
34 See https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf
35 See https://www.un.org/disarmament/group-of-governmental-experts/

Russia has been calling for the development of an internationally binding treaty on cybercrime at the UN level since the early 2010s.[36] In December 2018, the UN General Assembly approved a resolution,[37] sponsored by Russia and a group of aligned countries, establishing an "open-ended ad hoc intergovernmental committee of experts" to "elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes" under the auspices of the UN. While Russian proposals for a cybersecurity treaty have failed to crystallise sufficient consensus over the past decade, the most recent developments suggest that the situation is rapidly evolving, and that this initiative needs to be monitored closely, as numerous countries may now find the idea of a cybersecurity treaty appealing. The first substantial meeting of the ad hoc intergovernmental committee is planned for January 2022.

References

Ballard, M. (2010, April 20). UN rejects international cybercrime treaty. *Computer Weekly*. https://www.computerweekly.com/news/1280092617/UN-rejects-international-cybercrime-treaty

Belli, L. (2019, November 13). From BRICS to CyberBRICS: New cybersecurity cooperation. *China Today*. http://www.chinatoday.com.cn/ctenglish/2018/tpxw/201911/t20191113_800184922.html

Belli, L. (2020a, February 3). The largest personal data leakage in Brazilian history. *Open Democracy*. https://www.opendemocracy.net/en/largest-personal-data-leakage-brazilian-history/

Belli, L. (2020b). Data protection in the BRICS countries: Enhanced cooperation and convergence towards legal interoperability. CyberBRICS. https://cyberbrics.info/data-protection-in-the-brics-countries-enhanced-cooperation-and-convergence-towards-legal-interoperability/

Belli, L. (Ed.) (2021a). *CyberBRICS: Cybersecurity regulations in the BRICS countries*. Springer.

Belli, L. (2021b). CyberBRICS: A multidimensional approach to cybersecurity for the BRICS. In L. Belli (Ed.), *CyberBRICS: Cybersecurity regulations in the BRICS countries*. Springer.

Belli, L. (2021c, September 17). Cybersecurity convergence in the BRICS countries. [Blog post.] *Directions*. European Union. https://directionsblog.eu/cybersecurity-convergence-in-the-brics-countries/

Belli, L., & Doneda, D. (2021, September 2). O que falta ao Brasil e à América Latina para uma proteção de dados efetiva? JOTA. https://www.jota.info/opiniao-e-analise/artigos/o-que-falta-ao-brasil-e-a-america-latina-para-uma-protecao-de-dados-efetiva-02092021

BRICS. (2013). eThekwini Declaration and Action Plan. http://mea.gov.in/bilateral-documents.htm?dtl/21482

36 See Ballard (2010).

37 See UN Doc. A/C.3/74/L.11/Rev.1: https://undocs.org/A/C.3/74/L.11/Rev.1

BRICS. (2015). VII BRICS Summit - Ufa Declaration. https://www.brics2021.gov.in/BRICSDocuments/2015/Ufa-Declaration-2015.pdf

BRICS. (2021). BRICS India 2021 - XIII BRICS Summit - New Delhi Declaration. https://brics2021.gov.in/brics/public/uploads/docpdf/getdocu-51.pdf

Centre for Internet and Society (CIS). (2020). The Centre for Internet and Society's comments and recommendations to the: The Personal Data Protection Bill 2019. https://cis-india.org/accessibility/blog/cis-comments-pdp-bill-2019

Comitê Gestor da Internet no Brasil (CGI.br). (2014, April 20). Um pouco sobre o Marco Civil da Internet. https://www.cgi.br/noticia/notas/um-pouco-sobre-o-marco-civil-da-internet

Daucé, F., & Musiani, F. (2021). Infrastructure-embedded control, circumvention and sovereignty in the Russian Internet: An introduction. *First Monday*, *26*(5). https://doi.org/10.5210/fm.v26i5.11685

Grover, G., & Thomas, A. (2021, February 22). Notes from a foreign field: The European Court of Human Rights on Russia's website blocking. CyberBRICS. https://cyberbrics.info/notes-from-a-foreign-field-the-european-court-of-human-rights-on-russias-website-blocking/

Iunes, J., & Macedo, N. (2021, June 1). Por onde anda o PL das Fake News? É necessário focar no aprimoramento dos deveres procedimentais, respeitando o regime de responsabilização adotado pelo Marco Civil da Internet. Portal FGV. https://portal.fgv.br/artigos/onde-anda-pl-fake-news-e-necessario-focar-aprimoramento-deveres-procedimentais-respeitando

Mabunda, S. (2021). Cybersecurity in South Africa: Towards best practices. In L. Belli (Ed.), *CyberBRICS: Cybersecurity regulations in the BRICS countries*. Springer.

MacAskill, E., & Dance, G. (2013, November 1). NSA files: Decoded. *The Guardian*. https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1

Musiani, F., Loveluck, B., Daucé, F., & Ermoshina, K. (2019, October 28). "Digital sovereignty": Can Russia cut off its internet from the rest of the world? *The Conversation*. https://theconversation.com/digital-sovereignty-can-russia-cut-off-its-internet-from-the-rest-of-the-world-125952

O'Neill, J. (2001). *Building better global economic BRICs*. Global Economics Paper No. 66. Goldman Sachs. https://www.goldmansachs.com/insights/archive/archive-pdfs/build-better-brics.pdf

Shcherbovich, A. (2021). Data protection and cybersecurity legislation of the Russian Federation in the context of the "sovereignization" of the internet in Russia. In L. Belli (Ed.), *CyberBRICS: Cybersecurity regulations in the BRICS countries*. Springer.

Shcherbovitch, S., Granberg, S., & Carvalho, A. (2019, May 8). Sovereign internet law signed by the President of Russia. CyberBRICS. https://cyberbrics.info/sovereign-internet-law-signed-by-the-president-of-russia/

Sircar, S. (2020, March 3). A blank cheque to Govt: Justice Srikrishna on Data Protection Bill. *The Quint*. https://www.thequint.com/news/india/personal-data-protection-bill-a-blank-signed-cheque-to-government-justice-srikrishna

Snail, S. (2021, June 15). Legal intersections between the Protection of Personal Information Act 4 of 2013 (POPIA) and the Cyber Crimes Act 19 of 2020. CyberBRICS. https://cyberbrics.info/legal-intersections-between-the-protection-of-personal-information-act-4-of-2013-popia-and-the-cyber-crimes-act-19-of-2020-2/

Software Freedom Law Center, India (SFLC.IN). (2021, May 28). Legal challenges to the traceability provision: What is happening in India? https://sflc.in/legal-challenges-traceability-provision-what-happening-india

Stuenkel, O. (2016). *Post-Western world: How emerging powers are remaking global order*. Polity Press.

Stuenkel, O. (2020). *The BRICS and the future of global order* (2nd ed.). Lexington Books.

The Economist. (2021, September 11). China has become a laboratory for the regulation of digital technology. https://www.economist.com/china/2021/09/11/china-has-become-a-laboratory-for-the-regulation-of-digital-technology

Zanfir-Fortuna, G., & Iminova, R. (2021, March 2). Russia: New law requires express consent for making personal data available to the public and for any subsequent dissemination. CyberBRICS. https://cyberbrics.info/russia-new-law-requires-express-consent-for-making-personal-data-available-to-the-public-and-for-any-subsequent-dissemination

Zhao, X., Li, M., Huang, M., & Sokolov, A. (Eds.). (2018). *BRICS innovative competitiveness report 2017*. https://publications.hse.ru/mirror/pubs/share/direct/252594344

THE AFRICAN JOURNAL OF INFORMATION AND COMMUNICATION (AJIC)

Published by the LINK Centre
University of the Witwatersrand (Wits)
Johannesburg, South Africa
https://www.wits.ac.za/linkcentre

ISSN 2077-7213 (online version)
ISSN 2077-7205 (print version)