ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/379423562

Mobile Application Diffusion: An Exploration of Trust and Privacy Amongst Rural Enterprises in South Africa

Chapter · March 2024

DOI: 10.1007/978-3-031-56481-9_4

CITATIONS
0

READS
23

2 authors:

Wellington Chakuzira
University of South Africa
6 PUBLICATIONS **6** CITATIONS
SEE PROFILE

Marcia Mkansi
University of South Africa
37 PUBLICATIONS **361** CITATIONS
SEE PROFILE

All content following this page was uploaded by Wellington Chakuzira on 21 September 2024.

The user has requested enhancement of the downloaded file.

Digital Services and Social Media

Mobile Application Diffusion: An Exploration of Trust and Privacy Amongst Rural Enterprises in South Africa

Wellington Chakuzira(✉) and Marcia Mkansi

University of South Africa, Pretoria, South Africa
{chakuw,mkansm}@unisa.ac.za

Abstract. This review paper presents academic literature exploring why there is a slow adoption of mobile technologies amongst rural enterprises in South Africa. The researchers conducted a thorough literature review of studies related to trust and privacy on mobile applications published in journals between January 2020 and April 2023. The study reviewed two main external variables: trust and privacy of technology adoption. The systematic review shows that common trust concerns for rural enterprises include untrusted service providers, weak security, and security attacks. Additionally, the review revealed common privacy issues and concerns, including integrity, user awareness, unobservability, and deniability as obstacles to the fast uptake of mobile applications in rural marketplaces in South Africa. Considering these factors, the paper concludes by offering practical and theoretical suggestions that can assist rural entrepreneurs in enhancing the diffusion of mobile technology.

Keywords: mobile applications · technology diffusion · trust issues · privacy concerns

1 Introduction

Marketers in many developing countries are still trying to gain a better understanding of the motivations and methods of consumer engagement with modern technologies such as mobile applications or "apps". It is interesting to note that the study of the nature of mobile applications and, consequently, the reasons for and ways in which users utilize them, has dominated the literature on this developing technology [1–3]. Understandably, the proliferation of mobile applications, akin to various digital entrepreneurial pursuits and the ubiquity of internet infrastructure, has ushered in fresh prospects and entrepreneurial models in both rural and urban marketplaces [4, 5], although the introduction of novel technological applications often encounters more skepticism within rural areas compared to urban markets [6, 7, 9]. Alavion and Taghdisi [8] contend that the distinctive characteristics and capabilities of and demand for advanced technical proficiencies make mobile application diffusion challenging in rural areas. Evidently, substantial infrastructural developments focusing on connectivity upgrades are imperative for mobile applications to thrive in rural regions [10].

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2024
M. Papadaki et al. (Eds.): EMCIS 2023, LNBIP 502, pp. 47–64, 2024.
https://doi.org/10.1007/978-3-031-56481-9_4

Undoubtedly, mobile-application use is on the rise in rural areas, serving a multitude of purposes. These include providing access to information about government initiatives, agricultural techniques, market prices, and weather forecasts, as well as facilitating money transfers and banking [3, 11, 12]. Despite the apparent opportunities generated by mobile applications, the complexities associated with technology trust and the security issues associated with mobile-application implementation have resulted in a relatively slow adoption rate among rural South African entrepreneurs [13]. While technology significantly impacts product utility [14], Rogers [15] cautions that making people use new technology for the first time can be challenging. Therefore, Sisi and Souri [13] contend that mobile applications must gain recognition among retailers and customers in these digitally challenged markets to remain competitive in rural markets. The critical question is, what are the trust and privacy peculiarities underlying rural entrepreneurs' mobile applications adoption? In subsequent sections, we review mobile applications in rural areas through different dimensions of trust and privacy concerns, for mobile applications in rural markets. Then we present methodology, followed by findings and future research implications for entrepreneurs and theory to advance diffusion on rural markets. Finally, the paper ends with concluding remarks.

2 Literature Review

Previous studies indicate that rural marketers face the most pronounced impact of the digital divide [16]. This situation often stems from factors such as limited data connectivity, power interruptions, and socio-economic disparities [17, 18]. Unless effective measures are enacted to narrow this gap, the uptake of technology in rural regions will continue to be slow. Vasileiadou, Huijben, and Raven [19] highlight the high cost of technology in rural markets as contributing to widespread technology poverty and exacerbating the digital divide. This divide is notably conspicuous among many rural residents in South Africa who lack the means to afford information and communication technologies (ICTs), perpetuating technological impoverishment across the majority of rural areas in the country. It is important to recognize that such technological poverty has the potential to increase South African communities' overall resistance to technology, which will also hinder adoption [20].

Recognizing that the adoption of technology is a multifaceted and socially intricate process, this study focuses on the need to address logical, sensitive, and contextual apprehensions [21]. This paper borrows from technology theories to address the trust and privacy concerns prevalent in rural markets. The paper acknowledges the conceptual underpinnings, practical applications, and evolutionary nature of technology adoption models and theories. These include the unified theory of acceptance and use of technology (UTAUT) [22, 23], the diffusion of innovation theory (DIT) [15], the theory of reasoned action (TRA) [24], the theory of planned behavior (TPB) [25, 26], and the technology acceptance model (TAM) [27].

These theories illuminate potential applications for the adoption of technology and provide a conceptual framework that can aid future researchers in comprehending the underlying technology models and theories shaping past, present, and future technology adoption trends. However, this paper studies the trust and privacy dimensions as potential

extension variables to any technology adoption theory mentioned earlier. As postulated by Nguyen et al., [28] there is continued uptake of technology in conducting business and in most cases the electronic data is exposed to theft, falsification, or unauthorized access. A situation which leaves customers lacking user's confidence and judgement that a specific service is free from privacy and security threat [29]. Notably trust and privacy concerns may pause a threat in all forms of technology adoptions making them important variables in technology adoption theories. Considering the foregoing postulations, the current paper reviews different dimensions of trust and privacy concerns. Now, the paper presents the relevant and recent literature for each stream.

2.1 Trust Concerns Among Rural Enterprises

Lankton, McKnight, and Tripp [30] define trust in technology as the user's confidence and judgement that a specific service is free from privacy and security threats. This public confidence plays an important role in the populace's selection of mobile applications. The collective disposition towards trust significantly influences the utilization of mobile applications in rural markets. Entrepreneurs recognize the potential of mobile applications in enhancing rural business operations [29]. However, their willingness to embrace these applications is often impeded by concerns that transmitting enterprise data over the internet might result in data tampering and privacy breaches. Al-Azawei and Alowayr [31] affirm that trust in mobile internet and data quality (essentially trust in technology) impact users' inclination to use mobile applications. This assertion is reinforced by Mkansi and Nsakanda [3], who emphasize that security and privacy concerns and distrust in mobile application services pose substantial challenges for rural South African enterprises.

In addition, trust in technology stands as a notable catalyst in decreasing the perceived risks associated with technology utilization, particularly when novel technologies and transactions with uncertain statuses are involved [31]. Given that the adoption of mobile applications in rural markets of South Africa is still in its early stages, users harbor uncertainties concerning the technical abilities of their service providers and the security and privacy aspects of the services offered [3]. Consequently, this lack of assurance frequently fosters reluctance among rural entrepreneurs to embrace and use mobile applications due to the inherent risks involved [32]. As a result, this study acknowledges the main challenges associated with untrusted cloud service providers and uses them as the basis of the analysis in the current review paper.

2.2 Privacy Concerns Among Rural Enterprises

Recognizing the transformative impact of the internet on our lives [29, 33], people now view the internet as a dependable source of information on products and services. However, the use of the internet for mobile applications in rural areas in developing countries, including South Africa, has not been growing as fast as the internet's other uses [34, 35]. One possible rationale for this uneven growth could be the hesitancy of entrepreneurs to divulge personal business information on crowd-based mobile application platforms. For example, Khan, Mihovska, Prasad and Velez, [36] indicates that the most important

reason why entrepreneurs do not use mobile applications is their concern about sending out their private business information. The survey findings demonstrate that merely 24.9% of entrepreneurs felt comfortable using mobile applications [36]. However, the media's focus on online fraud, hacking, and identity theft has likely made entrepreneurs more conscious of the dangers of using mobile applications.

While many entrepreneurs perceive mobile applications as either a menace or a nuisance, these applications hold substantial value as tools for both online and offline businesses [37]. The rapid advances in information technology and the surge in internet usage empower companies to gather, retain, and exchange consumer data, which can be harnessed for crafting more accurately targeted marketing strategies [3]. It is noteworthy that a typical entrepreneurial approach revolves around cultivating long-term relationships and a series of business transactions. This approach is facilitated through the accumulation of data pertaining to entrepreneurs' purchasing behaviors, preferences, and personal information on the internet.

Importantly, information databases necessitate entrepreneurs to share their personal information, whether by choice or circumstance. In most cases, the nature of mobile applications mandates entrepreneurs to reveal a certain amount of personal business details (for example, name, address, telephone number) and payment particulars (such as credit card numbers) [38, 39]. The problem lies in entrepreneurs' escalating concerns about privacy owing to the surge in questionable and unlawful activities associated with application usage, including a notable increase in failed deliveries, identity theft, and fraud [29]. As a result, researchers in various fields have been paying more attention to privacy and security issues in mobile applications. For instance, entrepreneurs' growing concern over their privacy is becoming a significant issue for the potential use of mobile applications [40]. The critical question is then, what motivates entrepreneurs to voluntarily share their personal business information on mobile application platforms? To address this query, this paper examines diverse facets of privacy and their impact on the usage of mobile applications within rural markets. Privacy is a broad concept that covers, amongst other things, freedom of thought, control over personal information, freedom from surveillance, protection of reputation, and immunity from searches and interrogations [6, 16, 38, 40]. The privacy dimensions previously proposed for evaluating the efficacy of overarching guidelines aimed at augmenting privacy include privacy categories, privacy principles, privacy concerns, and privacy enhancements. Figure 1 highlights elements of privacy dimensions and provides the conceptualized flow of the current study.

Figure 1 clearly displays the four privacy dimensions (privacy concern, privacy principles, privacy enhancement, and privacy categories). Embedded in each dimension are the key elements that rural marketers should understand when implementing mobile applications. Closely linked to the privacy dimensions are security challenges (untrusted customer service providers, weak security models, and security attacks), as shown in Fig. 1. Mitigating security challenges by rural marketers might increase trust among users and ensure the successful implementation of mobile applications. Considering the trust and privacy matters in mobile application usage, this study used a systematic review method to understand trust and security matters and suggest the best form of technology

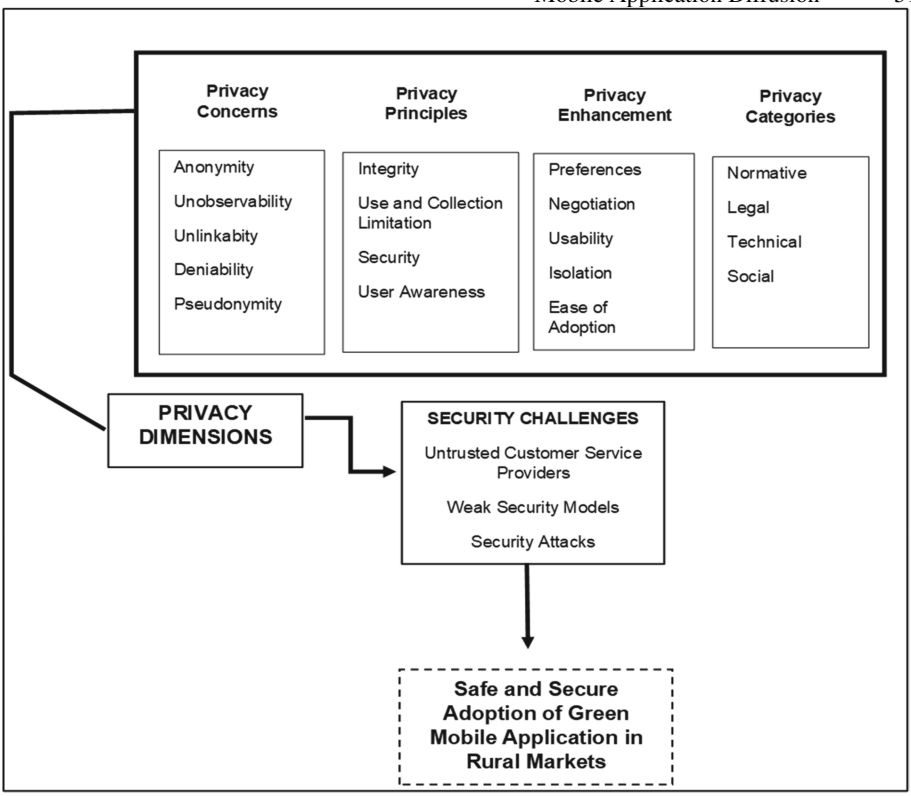

Fig. 1. Trust and privacy issues in mobile application usages

changes that is suitable for emerging rural markets. The study's methodology is detailed in the following section.

3 Methodology

This paper endeavors to provide a comprehensive and impartial synthesis of many relevant studies pertaining to trust and privacy challenges within mobile applications for rural enterprises. In line with the recommendations by Papaioannou, Sutton, and Booth [41], systematic techniques for literature review were implemented. In particular, systematic reviews are a type of literature review that involve thorough, methodical searching and are specified by predetermined eligibility criteria in accordance with guidelines [42–44]. In this study, the systematic review aims to unearth all pertinent insights relating to trust and privacy concerns surrounding mobile applications, with particular emphasis on contributions shedding light on the improvement of theory [45]. The key stages of the review process are as follows: (1) selection, (2) specification, and (3) summarizing, as shown in Fig. 2.

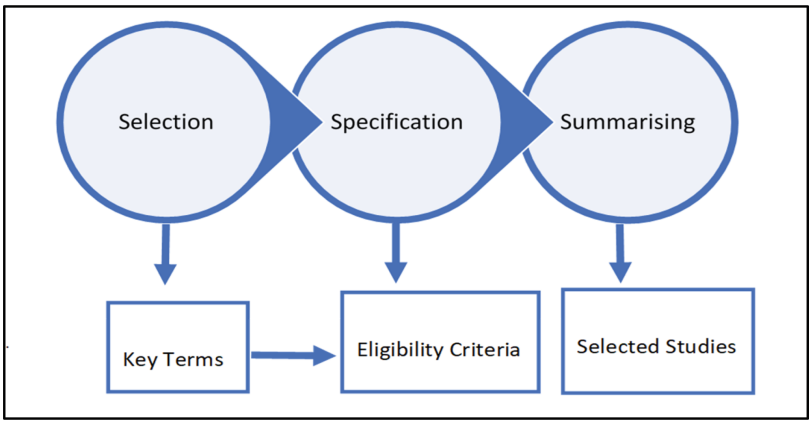

Fig. 2. Systematic review process

3.1 Selection

As recommended by Delgado-Rodríguez and Sillero-Arenas [46], the study selection criteria of a systematic review should flow directly from the review questions and be specified prior to selection. In this process, the paper considers two significant aspects throughout the selection. Firstly, the study chooses specific key terms associated with the research scope, including: "privacy concern among rural entrepreneurs;" "mobile technology in rural areas;" "trust issues among rural entrepreneurs;" "mobile applications for rural enterprises;" "user awareness;" "security attacks;" "privacy concerns;" "trust;" "anonymity;" and "integrity". Secondly, the paper employed multiple well-known digital library databases to collect resources from: Web of Science, Directory of Open Access Journals, Google Scholar, ProQuest, Research Gate, Science Direct, and Wiley.

3.2 Specification

Two straightforward standards of validation were adopted by the paper; (1) the date of publication and (2) the applicability of the study was used to govern the search results retrieved from database sources. Literature published from 2020 which addressed external variables (trust and privacy) of technology were considered. The study only used academic papers that were available online published from 2020 which included mobile application adoptions in different markets. This allowed for a thorough understanding of contemporary trust and privacy issues that marketers face regarding new technology adoptions. The search was also limited to articles released between January 2020 and April 2023. The rationale of selecting papers from 2020 was to attempt to provide critical contemporary knowledge on mobile applications, which allows for better conclusions in the modern, fast-paced technological market environments. Additionally, the selected papers contained enough information and did not stray outside the purview of crowd mobile applications among rural enterprises. Table 1 shows an analysis of the specifications of the current paper.

Table 1. Specification criteria

Source(s)	Discusses trust as an external variable	Discusses privacy as an external variable	Mobile application adoption focus area
Hajian et al. [38]		The research suggests a solution for mobile crowd-sensing-based spectrum monitoring comprised of a privacy-preserving protocol with secure rewarding capability and a trust mechanism against malicious players	
Asti, Handayani, and Azzahro [47]	This study discusses the influence of trust, perceived value, and attitude on customers repurchase intention for e-grocery		
Stocchi et al. [1]			The research presents an integrated overview of the available mobile marketing research, elaborating and clarifying what is known about how applications affect consumer experiences and value across iterative customer journeys
Gunawardana andFernando [48]	The research discusses the role of customer trust on e-service quality		
Kurniasari and Riyadi [49]	The research discusses trust issues of Indonesian e-grocery shoppers after the Covid-19 pandemic	The study discusses privacy issues of Indonesian e-grocery shoppers after the Covid-19 pandemic	

(*continued*)

Table 1. (*continued*)

Source(s)	Discusses trust as an external variable	Discusses privacy as an external variable	Mobile application adoption focus area
Singh, Gupta, Kumar, Sikdar, and Sinha [50]			The research identifies antecedents of customer satisfaction and patronage intentions in the context of e-grocery retailing through mobile applications
Mkansi, de Leeuw, and Amosun [4]			The research presents a mobile application supported by township and urban e-grocery distribution models that uses a software application
Nguyen, Hoang, and Vu Mai [28]			The study explores technology transfer through the perceptions of both business managers and technology specialists
Yang, Liu, Zhang and Yin [51]	The study empirically investigates the effects of social trust on technology innovation		
Sharma et al. [39]	The paper discusses the challenges and open issues related to security, privacy, and trust in mobile applications	The paper discusses the challenges and open issues related to security, privacy, and trust in mobile applications	

3.3 Summarizing

After screening the studied papers, the researchers finalized a full review of the findings, listed each paper's reference in summary tables, and discussed future research directions. Notably, the search results on the online database delivered a total of 123 original research papers. The researchers retained those that specifically discussed trust and privacy concerns among rural entrepreneurs adopting mobile applications, roughly 12% (15) of the total. The next section discusses the findings of this study. The articles selected mainly hailed from the fields of information management (40%), business

management (33%, or five articles), marketing (14%), and entrepreneurship (13%) (see Fig. 3).

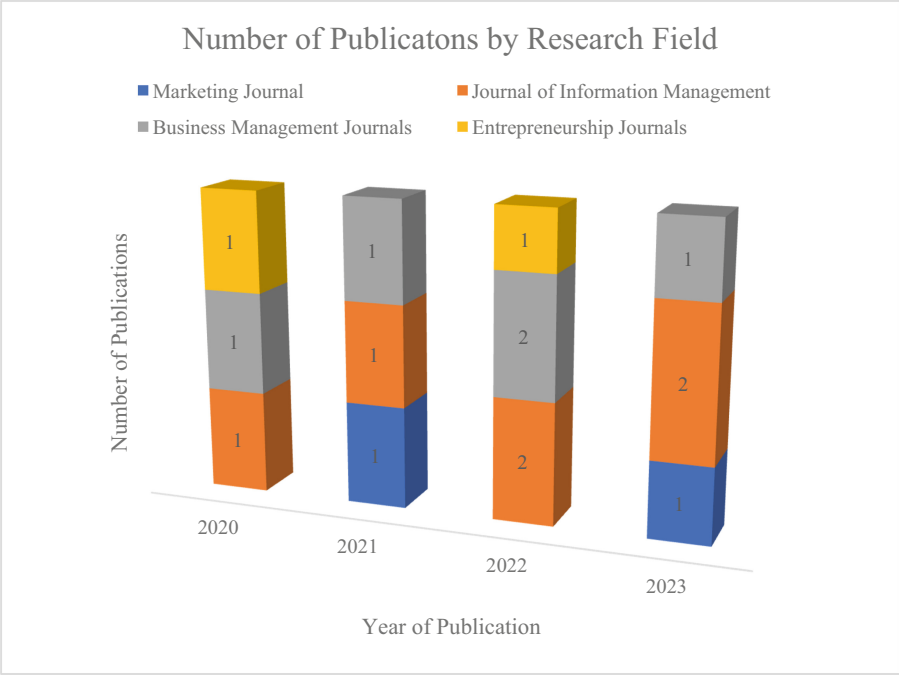

Fig. 3. Number of publications by research field from 2020 to April 2023

A pattern in publication was not evident; the number of publications were not spread evenly across the years. There were four publications in 2023, five publications in 2022 (the most in a year), and three publications in both 2021 and 2020. Most articles were published in information management and business management journals, indicating that academics have a particular interest in the interface between information management and small-business development. Figure 4 also shows that studies in these two fields were generally published every year during the period January 2020–April 2023. The next section will discuss the main findings of the research.

4 Findings

As mentioned, the findings of this paper are discussed in relation to trust challenges and privacy dimensions (see Fig. 1). Past literature on technology implementations discussed trust and privacy issues in line with innovation theories such as the TAM, UTAUT, uses and gratifications theory (UGT) [49, 50]. Indeed, these theories form a strong basis for understanding technology adoption variables, including trust and privacy issues on mobile technology implementations. However, this paper will discuss its findings under the two external variables of technology, namely security and privacy concerns.

Table 2. Mobile application-based trust and privacy analysis for entrepreneurs from 2020 to 2023

Categorization	Year	Author	Research focus	Trust and privacy dimensions													
				Untrusted service providers	Weak security	Security attacks	Integrity	User awareness	Use and collection limitation	Anonymity	Unobservability	Deniability	Preferences	Negotiation	Usability	Ease of adoption	Social and legal mitigations
Trust concerns	2023	Mkansi and Nsakanda [3]	Mobile apps, e-grocery challenges and strategies Trust and privacy-specific focus: trust and privacy challenges and strategies	√			√	√		√					√	√	
		Asti et al. [47]	Influence of trust, perceived value, and attitude on customers repurchase intention for e-grocery	√	√			√			√				√	√	
		Akinola and Asaolu [52]	A trust, privacy, and security model for e-commerce in Nigeria		√	√				√	√	√					
	2022	Stocchi et al. [1]	Mobile apps, clarifying and expanding what is known around how apps shape customer experiences and value across iterative customer journeys Trust and privacy-specific focus	√	√									√	√		
		Khaw et al. [53]	Importance of specific determinants of trust in mobile commerce contributes to providing deep insight into the factors of customer trust in mobile commerce	√	√				√	√					√	√	√
	2021	Gunawardana and Fernando [48]	The impact of e-service quality dimensions and customer satisfaction with e-groceries with the role of customer trust as a mediating variable during the epidemic			√	√	√			√	√	√			√	

(*continued*)

Table 2. (*continued*)

Categorization	Year	Author	Research focus	Trust and privacy dimensions													
				Untrusted service providers	Weak security	Security attacks	Integrity	User awareness	Use and collection limitation	Anonymity	Unobservability	Deniability	Preferences	Negotiation	Usability	Ease of adoption	Social and legal mitigations
		Yang, Liu, Zhang and Yin [51]	Social trust and green technology innovation: evidence from listed firms in China											√	√	√	√
	2020	Sharma et al. [39]	Challenges and open issues related to security, privacy, and trust in mobile applications	√	√	√			√	√			√			√	
		Kurniasari and Riyadi [49]	Trust issues of Indonesian e-grocery shoppers after the Covid-19 pandemic	√	√										√	√	
Privacy concerns	2023	Hajian et al. [38]	Method proposed that includes a privacy-preserving protocol with secure rewarding capability as well as a trust mechanism against malicious participants for mobile crowd-sensing based spectrum monitoring				√	√		√				√	√	√	
	2022	Shaw et al. [54]	A simplified model proposed for investigating mobile wallet adoption, with extensions for security, privacy, and ubiquity Tested for Canada, Germany, and the United States, and provides country-specific guidance for practitioners	√			√	√			√	√		√		√	√
		Su et al. [55]	The rrole of technology acceptance models, mobile service quality factors, and personalization and privacy in promoting customers' trust and their loyalty towards mobile food delivery apps				√		√		√				√	√	√

(*continued*)

Table 2. (*continued*)

Categorization	Year	Author	Research focus	Trust and privacy dimensions													
				Untrusted service providers	Weak security	Security attacks	Integrity	User awareness	Use and collection limitation	Anonymity	Unobservability	Deniability	Preferences	Negotiation	Usability	Ease of adoption	Social and legal mitigations
	2021	Libaque-Sáenz et al. [56]	The effect of intervention strategies, fair information practices, and the data-collection method on privacy-related decisions							√		√		√		√	
		Tay et al. [57]	How users' risk perception can be shifted towards more privacy-aware decisions through generation fluency and framing manipulations	√	√			√	√				√			√	√
	2020	Balapour et al. [58]	The relationship between users' perceived privacy concerns and their perceptions of mobile app security		√	√			√	√		√			√	√	

The study discovered three possible trust challenges for mobile application adoptions among rural South African enterprises, especially in rural markets with untrusted service providers, weak security models, and security attacks. Certainly, literature from the selected journals identifies untrusted service providers and security attacks as the main two challenges for mobile application implementations (see Table 2). The study also identifies four privacy issues that are pertinent for mobile technology usage in rural markets, namely integrity, security, user awareness and use, and collection limitation (see Table 2).

As shown in Table 2, there are two privacy concerns pertinent to rural markets that the study discovered, among others: unobservability and deniability. Other privacy dimensions, such as privacy enhancement, had limited reports in the selected papers. However, it is also important for marketers to understand enhancement issues such as preferences, negotiation, and isolation, as well as privacy categories such as legal, normative, technical, and social privacy before implementing mobile applications. Privacy is a broad notion that covers, among other things, one's right to freedom of thinking, control over one's body, privacy in one's home, control over one's personal information, freedom from surveillance, preservation of one's reputation, and immunity from searches and interrogations. Therefore, it becomes imperative to understand all privacy concerns before implementing mobile applications.

4.1 Implications for Rural Entrepreneurs

A key finding of this review paper is that, while the existing literature has indeed confirmed the significance of consumer-centric concerns in propelling the uptake of mobile application transactions within rural markets, these concerns are further amplified when entrepreneurs are assured of safeguarding their business information privacy. In addition, rural entrepreneurs should remain aware of the critical role of implementing robust security mechanisms as an integral facet of successful mobile application adoption. Lastly, when the business and financial information of rural entrepreneurs is effectively harnessed, it not only enriches their interaction with mobile applications but also cultivates a sense of trust.

Rural entrepreneurs should view data privacy and security more broadly, not only as risk-management issues but also as potential sources of competitive advantage that could greatly aid in brand building and the creation of a solid company reputation. Neglecting security issues, such as unreliable customer service providers, inadequate security models, and security breaches, can often lead to harm to brand image, business losses, and valuable time consumed by ongoing legal actions. In addition, rural entrepreneurs can ensure the security of their personal business and financial information by collaborating with mobile application service providers in conducting regular data privacy audits. While this may entail costs for rural enterprises, it is worth noting that these businesses often accumulate more data than they realize, so it is crucial to discern the necessary data, how it is stored, and the level of security protecting it.

It is also crucial for rural businesses to recognize that neglecting the importance of data collection can often ignite significant crises. For instance, overlooking privacy concerns, principles, enhancement, and categories can potentially trigger data privacy scandals. Rural entrepreneurs and mobile application service providers must make sure

that they develop and enforce clear and transparent guarantees of privacy in order for rural areas to successfully utilize mobile applications. These measures should serve as signals to businesses, assuring them of the security of their confidential information. To accomplish this, rural entrepreneurs should embrace modern marketing strategies that prioritize establishing a brand and fostering robust data privacy and security practices.

Compelling findings from the analyzed articles indicate that the adoption of mobile applications for conducting business by rural consumers is still not widespread. To tackle this issue, rural entrepreneurs must understand the nuances of mobile application functionality. Moreover, the business information presented on these mobile applications should be relevant and tailored to align with the preferences and attributes of the specific consumer segments they aim to reach. It is also imperative that these mobile applications remain consistently operational and connected, providing consumers with a sense of ubiquitous accessibility.

4.2 Implications for Theory

The findings reveal that, for rural entrepreneurs, both perceived information security and privacy play significant roles as predictive factors for consumer choice behavior and the adoption patterns of mobile application innovations. This study thus contributes to the growing body of evidence, consistent with previous works such as Balapour et al. [58] and Akinola and Asaolu [52], highlighting the influential role of privacy and information security as precursory elements impacting the acceptance of mobile applications in rural markets. Moreover, the study provides evidence suggesting the applicability of the dimensions of trust and privacy in shaping entrepreneurs' decisions regarding the adoption of mobile applications. This aligns with previous research by Shaw et al. [54] and Su et al. [55]. Consequently, the present study addresses recent calls for the exploration of alternative theories, models, and insights pertaining to the innovation adoption behaviors of contemporary entrepreneurs, particularly within rural markets.

A number of notable adoption models have been identified in the literature [52, 53]. However, these models only appear to partially account for the phenomenon of choosing to adopt new marketing strategies. What appears to be lacking is the incorporation of external variables, such as trust and privacy, which could amplify the models' explanatory capacity, mitigate misinterpretations, and offer a more comprehensive understanding of the intricate aspects typically associated with research on the diffusion of mobile applications across diverse markets. In light of this, the study recommends the integration of a set of external variables into the innovation adoption models to enrich its explanatory capabilities. Particularly noteworthy is the association of trust and privacy with the success or failure of mobile application adoption, a point emphasized by researchers and practitioners alike [52–53, 55, 57]. This underscores the potential widespread applicability of trust and privacy concerns as external variables in various studies concerning the adoption of mobile applications.

5 Conclusion

This paper offers a systematic review of studies on rural enterprises' adoption strategies for mobile applications between January 2020 and April 2023. Understandably, many contributions have empirically explored trust and privacy issues on mobile application implementations in line with technology theories. This paper systematically reviewed trust and privacy issues, bringing out the trust issues as a discussion of external variables determining adoption for rural entrepreneurs. The paper also reviewed the privacy dimension (privacy concern, privacy principles, privacy enhancement, and privacy categories), which several scholars overlook in this discourse. Notably, the study still highlights a distance in the reviewed studies between their theoretical bases and analyses of trust and privacy issues on mobile application implementations in rural markets.

There are undoubtedly some shortcomings in this literature review. First, it does not cover the full spectrum of academic publications in the management, marketing, and entrepreneurship sectors because it is based on a selection of journals chosen based on specified criteria. Second, the timeline is restricted to the years 2020–2023. This constraint was addressed by the paper's attempt to correlate findings from contemporary literature with pertinent contributions that had been published prior to 2020. This paper calls for further research on related grounds. Firstly, focused research should empirically investigate the entrepreneurial trust and privacy issues on mobile application implementations in rural markets. Secondly, focused research which explains the difference between structured and unstructured crowds is also necessary.

References

1. Stocchi, L., Pourazad, N., Michaelidou, N., Tanusondjaja, A., Harrigan, P.: Marketing research on Mobile apps: past, present and future. J. Acad. Mark. Sci. **50**(2), 195–225 (2021)
2. Deepa, N., et al.: A survey on blockchain for big data: approaches, opportunities, and future directions. Future Gener. Comput. Syst. **131**, 209–226 (2022)
3. Mkansi, M., Nsakanda, A.L.: Mobile application e-grocery retail adoption challenges and coping strategies: a South African small and medium enterprises' perspective. Electron. Commer. Res. (2023). https://doi.org/10.1007/s10660-023-09698-1
4. Mkansi, M., de Leeuw, S., Amosun, O.: Mobile application supported urban-township e-grocery distribution. Int. J. Phys. Distrib. Logist. Manag. **50**, 26–53 (2020)
5. Abubakre, M., Faik, I., Mkansi, M.: Digital entrepreneurship and indigenous value systems: an Ubuntu perspective. Inf. Syst. J. **31**, 838–862 (2021)
6. Marnewick, C.: Information and communications technology adoption amongst township micro and small business: the case of Soweto. South Afr. J. Inf. Manag. **16**, 1–12 (2014)
7. Alavion, S.J., Taghdisi, A.: Analysis of rural e-marketing based on geographic model of planned behavior. Geogr. Space **20**, 57–84 (2021)
8. Alavion, S.J., Taghdisi, A.: Rural E-marketing in Iran; Modeling villagers' intention and clustering rural regions. Inf. Process. Agric. **8**, 105–133 (2021). https://doi.org/10.1016/j.inpa.2020.02.008
9. Bruwer, L.A., Madinga, N.W., Bundwini, N.: Smart shopping: the adoption of grocery shopping apps. Br. Food J. **124**, 1383–1399 (2022)
10. Saskia, S., Mareï, N., Blanquart, C.: Innovations in e-grocery and Logistics Solutions for Cities. Transp. Res. Procedia **12**, 825–835 (2016)

11. Kumar, V.: Mobile application in agriculture development in india: policy, practices and the way forward. In: Das, K., Mishra, B.S.P., Das, M. (eds.) The Digitalization Conundrum in India. ISBE, pp. 233–247. Springer, Singapore (2020). https://doi.org/10.1007/978-981-15-6907-4_13
12. Febrianda, R.: Mobile app technology adoption in indonesia's agricultural sector. an analysis of empirical view from public R&D agency. J. STI Policy Manag. **6**, 31–40 (2021)
13. Sisi, Z., Souri, A.: Blockchain technology for energy-aware mobile crowd sensing approaches in Internet of Things. Trans. Emerg. Telecommun. Technol. e4217 (2021). https://doi.org/10.1002/ett.4217
14. Shambare, R.: The adoption of WhatsApp: breaking the vicious cycle of technological poverty in South Africa. J. Econ. Behav. Stud. **6**, 542–550 (2014)
15. Rogers, E.M.: Diffusion of Innovations: modifications of a model for telecommunications. In: Stoetzer, M.W., Mahler, A. (eds.) Die Diffusion von Innovationen in der Telekommunikation, pp. 25–38. Springer Berlin Heidelberg, Berlin, Heidelberg (1995). https://doi.org/10.1007/978-3-642-79868-9_2
16. Goncalves, G., Oliveira, T., Cruz-Jesus, F.: Understanding individual-level digital divide: evidence of an African country. Comput. Hum. Behav. **87**, 276–291 (2018)
17. Meagher, P., Upadhyaya, K., Wilkinson, B.: Combating Rural Public Works Corruption: Food-for-Work Programs in Nepal. SSRN (2001). https://ssrn.com/abstract=260044. https://doi.org/10.2139/ssrn.260044
18. Faulkner, K.T., et al.: South africa's pathways of introduction and dispersal and how they have changed over time. In: van Wilgen, B., Measey, J., Richardson, D., Wilson, J., Zengeya, T. (eds.), Biological Invasions in South Africa. Invading Nature – Springer Series in Invasion Ecology, vol 14. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-32394-3_12
19. Vasileiadou, E., Huijben, J.C.C.M., Raven, R.P.J.M.: Three is a crowd? Exploring the potential of crowdfunding for renewable energy in the Netherlands. J. Cleaner Production **128**, 142–155 (2016). https://doi.org/10.1016/j.jclepro.2015.06.028
20. Kumar, A., Sikdar, P., Gupta, M., Singh, P., Sinha, N.: Drivers of satisfaction and usage continuance in e-grocery retailing: a collaborative design supported perspective. J. Res. Interact. Market. **17**, 176–194 (2023)
21. Vahdat, A., Alizadeh, A., Quach, S., Hamelin, N.: Would you like to shop via mobile app technology? The technology acceptance model, social factors and purchase intention. Australasian Market. J. **29**(2), 187–197 (2021)
22. Venkatesh, V., Ramesh, V., Massey, A.P.: Understanding usability in mobile commerce. Commun. ACM **46**, 53–56 (2003)
23. Lai, P.C.: The literature review of technology adoption models and theories for the novelty technology. JISTEM-J. Inf. Syst. Technol. Manag. **14**, 21–38 (2017)
24. Ajzen, I., Fishbein, M.: A Bayesian analysis of attribution processes. Psychol. Bull. **82**, 261 (1975)
25. Manstead, A.S., Parker, D.: Evaluating and extending the theory of planned behaviour. Eur. Rev. Soc. Psychol. **6**, 69–95 (1995)
26. Ajzen, I.: The theory of planned behavior. Organ. Behav. Hum. Decis. Process. **50**, 179–211 (1991)
27. Venkatesh, V., Davis, F.D.: A model of the antecedents of perceived ease of use: development and test. Decis. Sci. **27**, 451–481 (1996)
28. Nguyen, T.T.M., Phan, T.H., Nguyen, H.L., Dang, T.K.T., Nguyen, N.D.: Antecedents of purchase intention toward organic food in an Asian emerging market: a study of urban Vietnamese consumers. Sustainability **11**, 4773 (2019)
29. Willie, M.M.: Customer Trust and Other Factors Associated with Digital Platforms & Marketing during a Pandemic. OAJBS Publishers (2022)

30. Lankton, N.K., McKnight, D.H., Tripp, J.: Technology, humanness, and trust: rethinking trust in technology. J. Assoc. Inf. Syst. **16**, 1 (2015)
31. Al-Azawei, A., Alowayr, A.: Predicting the intention to use and hedonic motivation for mobile learning: a comparative study in two Middle Eastern countries. Technol. Soc. **62**, 101325 (2020)
32. Miranda, I.T.P., Moletta, J., Pedroso, B., Pilatti, L.A., Picinin, C.T.: A review on green technology practices at BRICS countries: Brazil, Russia, India, China, and South Africa. SAGE Open **11**, 21582440211013780 (2021)
33. Tahaei, M., Frik, A., Vaniea, K.: Deciding on personalized ads: nudging developers about user privacy. In: SOUPS@ USENIX Security Symposium. pp. 573–596 (2021)
34. Nhamo, G., Mukonza, C.: Opportunities for women in the green economy and environmental sectors. Sustain. Dev. **28**, 823–832 (2020)
35. Randall, L., Ormstrup Vestergård, L., Wøien Meijer, M.: Rural perspectives on digital innovation: Experiences from small enterprises in the Nordic countries and Latvia (2020)
36. Khan, B., Mihovska, A., Prasad, R., Velez, F.J.: Overview of network slicing: Business and standards perspective for beyond 5g networks. IEEE Conf. Stand. Commun. Network. (CSCN) **2021**, 142–147 (2021)
37. Talwar, S., Kaur, P., Ahmed, U., Bilgihan, A., Dhir, A.: The dark side of convenience: how to reduce food waste induced by food delivery apps. Br. Food J. **125**, 205–225 (2023)
38. Hajian, G., Shahgholi Ghahfarokhi, B., Asadi Vasfi, M., Tork Ladani, B.: Privacy, trust, and secure rewarding in mobile crowd-sensing based spectrum monitoring. J. Ambient. Intell. Humaniz. Comput. **14**, 655–675 (2023)
39. Sharma, V., You, I., Andersson, K., Palmieri, F., Rehmani, M.H., Lim, J.: Security, privacy and trust for smart mobile-Internet of Things (M-IoT): a survey. IEEE Access **8**, 167123–167163 (2020)
40. Xu, G., et al.: Trust2Privacy: a novel fuzzy trust-to-privacy mechanism for mobile social networks. IEEE Wirel. Commun. **27**, 72–78 (2020)
41. Papaioannou, D., Sutton, A., Booth, A.: Systematic approaches to a successful literature review. Syst. Approaches Success. Lit. Rev. 1–336 (2016)
42. Howie, C.: Conducting your first systematic review. PsyPAG Q. Goes Electron. **113**, 32–35 (2019)
43. Khan, K.S., Kunz, R., Kleijnen, J., Antes, G.: Five steps to conducting a systematic review. J. R. Soc. Med. **96**, 118–121 (2003)
44. Page, M.J., et al.: The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. Int. J. Surg. **88**, 105906 (2021)
45. Munn, Z., Peters, M.D., Stern, C., Tufanaru, C., McArthur, A., Aromataris, E.: Systematic review or scoping review? Guidance for authors when choosing between a systematic or scoping review approach. BMC Med. Res. Methodol. **18**, 1–7 (2018)
46. Delgado-Rodríguez, M., Sillero-Arenas, M.: Systematic review and meta-analysis. Medicina Intensiva (English Edition) **42**, 444–453 (2018)
47. Asti, W.P., Handayani, P.W., Azzahro, F.: Influence of trust, perceived value, and attitude on customers' repurchase intention for e-grocery. J. Food Prod. Mark. **27**, 157–171 (2021)
48. Gunawardana, P.K.A.T.D.R., Fernando, Imali: Does customer trust mediate the impact of e-service quality dimensions? Lessons during COVID-19 Pandemic. SSRN Electron. J. (2021). https://doi.org/10.2139/ssrn.3907878
49. Kurniasari, F., Ryadi, W.T.: Determinants of indonesian e-grocery shopping behavior after covid-19 pandemic using the technology acceptance model approach. United Int. J. Res. Technol. (UIJRT) **3**(01), 12–18 (2021)
50. Singh, P., Gupta, M., Kumar, A., Sikdar, P., Sinha, N.: E-Grocery retailing mobile application: discerning determinants of repatronage intentions in an emerging economy. Int. J. Hum.-Comput. Interact. **37**, 1783–1798 (2021)

51. Yang, Y., Liu, D., Zhang, L., Yin, Y.: Social trust and green technology innovation: evidence from listed firms in China. Sustainability **13**, 4828 (2021)
52. Akinola, O., Asaolu, O.: A trust, privacy and security model for e-commerce in Nigeria. Niger. J. Technol. **42**, 152–159 (2023)
53. Khaw, K.W., et al.: Modelling and evaluating trust in mobile commerce: a hybrid three stage Fuzzy Delphi, structural equation modeling, and neural network approach. Int. J. Human-Comput. Interact. **38**, 1529–1545 (2022)
54. Shaw, N., Eschenbrenner, B., Brand, B.M.: Towards a mobile app diffusion of innovations model: a multinational study of mobile wallet adoption. J. Retail. Consum. Serv. **64**, 102768 (2022)
55. Su, D.N., Nguyen, N.A.N., Nguyen, L.N.T., Luu, T.T., Nguyen-Phuoc, D.Q.: Modeling consumers' trust in mobile food delivery apps: perspectives of technology acceptance model, mobile service quality and personalization-privacy theory. J. Hosp. Mark. Manag. **31**, 535–569 (2022)
56. Libaque-Sáenz, C.F., Wong, S.F., Chang, Y., Bravo, E.R.: The effect of Fair information practices and data collection methods on privacy-related behaviors: a study of Mobile apps. Inf. Manage. **58**, 103284 (2021)
57. Tay, S.W., Teh, P.S., Payne, S.J.: Reasoning about privacy in mobile application install decisions: risk perception and framing. Int. J. Hum.-Comput. Stud. **145**, 102517 (2021)
58. Balapour, A., Nikkhah, H.R., Sabherwal, R.: Mobile application security: role of perceived privacy as the predictor of security perceptions. Int. J. Inf. Manag. **52**, 102063 (2020)

View publication stats