



Online Security and Sustainable SME Adoption of Digital Platforms

ONILEOWO Temitope Teniola¹ & FASUAN Emmanuel Olawale²

¹Department of Entrepreneurship Studies, Faculty of Management Sciences, Ekiti State University, Ado-Ekiti, Ekiti State, Nigeria

²Department of Peace and Security Studies, Faculty of Multidisciplinary Studies, Ekiti State University, Ado-Ekiti, Ekiti State, Nigeria

DOI: <https://doi.org/10.68050/JAMS.2026.708>

Received: 24 September 2026; Accepted: 30 September 2026; Published: 07 October 2026

ABSTRACT

Digital platforms increasingly provide small and medium-sized enterprises (SMEs) with opportunities to access markets, conduct transactions, engage customers, and improve operational efficiency. However, sustained SME engagement with digital platforms is challenged by rising cybersecurity threats, particularly in developing economies where firms often face constraints in financial resources, digital infrastructure, and technical expertise. This conceptual study explores the influence of online security on the sustainable adoption of digital platforms by integrating trust and perceived risk perspectives with the Technology Acceptance Model (TAM). An integrative conceptual review of academic literature, policy documents, and institutional reports was undertaken to identify, evaluate, and synthesise evidence on online security, technology acceptance, trust, perceived risk, and sustained digital-platform adoption. Online security is conceptualised as a fundamental platform-level and organisational requirement encompassing confidentiality, data integrity, authentication, availability, fraud prevention, and secure payment processing. It is positioned as an antecedent of trust and a negative antecedent of perceived risk, while perceived usefulness and perceived ease of use remain core TAM determinants of adoption. Trust and perceived risk are conceptualised as parallel mediating mechanisms through which online security may influence sustainable digital-platform adoption. The study further recognises that security requirements vary across e-commerce, fintech and digital-payment platforms, social commerce, cloud-based applications, and digital supply-chain platforms. The framework highlights security-enabled trust and reduced uncertainty in shaping entrepreneurs' willingness to maintain routine, reliable, and confident engagement with digital platforms. By integrating technological, psychological, and security dimensions, the study extends understanding of secure digital entrepreneurship beyond cybersecurity as a technical risk-management concern to its potential role in sustaining SME participation in digital markets. It proposes theoretically grounded relationships for future empirical testing and provides implications for SMEs, platform providers, financial institutions, and policymakers seeking to promote secure, resilient, and inclusive digital economies.

Keywords: Cybersecurity; Online security; Digital platform adoption; Small and medium-sized enterprises (SMEs); Perceived risk; Trust; Technology Acceptance Model; Digital entrepreneurship

INTRODUCTION

Small and Medium Enterprises (SMEs) are widely recognised as critical drivers of economic growth, employment generation, innovation, and poverty reduction across both developed and developing economies. Due to their strategic role in national development, SMEs contribute significantly to employment opportunities, productivity, and economic sustainability worldwide (Tu, Kubatko, Melnyk, Li, Kovalov, & Yaremenko, 2025). In recent years, however, rapid technological advancement and the growing digitalisation of business activities have fundamentally reshaped the way SMEs operate. As a result, many SMEs now rely on digital technologies to improve efficiency, strengthen competitiveness, enhance customer engagement, and



expand market reach. In particular, the adoption of technologies such as e-commerce platforms, mobile banking, fintech services, cloud computing, digital payment systems, and social media marketing has transformed SMEs' operational capacity beyond traditional business boundaries. Through these digital platforms, SMEs can market products, communicate with customers, process payments, manage inventories, and access regional and international markets with relatively low operational costs (Sujatha & Karthikeyan, 2021). Furthermore, social media and digital marketing tools have provided SMEs with affordable and direct channels for customer interaction, brand promotion, and market visibility (Onileowo, Muharam, & George, 2024; Rampaul, 2025). Similarly, cloud computing and fintech innovations have improved business flexibility by offering affordable access to accounting systems, digital financial services, data storage, and remote business management tools. Consequently, digital transformation has become an important pathway for SMEs to improve productivity, operational efficiency, and long-term competitiveness (Al-Rikabi, 2025).

Despite these benefits, concerns over the security of online transactions remain a serious challenge to the effective adoption and use of digital technologies among SMEs. As more business activities move into digital spaces, SMEs are becoming increasingly vulnerable to cyber threats such as hacking, phishing, identity theft, financial fraud, and data breaches. Online security refers to the protection of electronic transactions, digital platforms, and sensitive business information from unauthorised access and cyberattacks through the use of security technologies, policies, and protective procedures (Miracle, 2024). Unfortunately, many SMEs often lack the financial resources, technical expertise, and cybersecurity infrastructure needed to adequately protect their digital operations. As digital business activities continue to expand, cybersecurity threats have also become more frequent and sophisticated. SMEs increasingly face risks such as phishing, ransomware, malware attacks, payment fraud, hacking, and unauthorised access to business databases. These threats pose serious financial and reputational risks to businesses, especially SMEs, which often lack the technical expertise and security infrastructure needed to effectively protect digital assets and sensitive information (Tu, Kubatko, Melnyk, Li, Kovalov, & Yaremenko, 2025). In many instances, cyberattacks can disrupt operations, reduce customer confidence, and discourage businesses from fully embracing digital technologies.

Moreover, SMEs are particularly vulnerable due to limited financial resources, inadequate technological infrastructure, and low cybersecurity awareness (Onileowo, Muharam, & Ramily, 2022). Unlike large organisations that can invest in advanced security systems and dedicated information technology teams, many SMEs struggle to afford sophisticated cybersecurity measures such as encryption technologies, firewalls, intrusion detection systems, and multi-factor authentication. Consequently, cybercriminals frequently perceive SMEs as easy targets with weaker digital defences (Miracle, 2024). This growing vulnerability continues to create uncertainty and fear among SME owners regarding the safety of online transactions. As a result, trust has become a critical factor influencing SMEs' willingness to adopt and continuously use digital platforms. In digital business environments where financial transactions and customer data are involved, perceptions of security and reliability play a major role in technology acceptance. SMEs are more likely to embrace digital platforms when they believe their business information and customer data can be adequately protected. This concern aligns with the Technology Acceptance Model (TAM) developed by Fred Davis (1989), who emphasises perceived usefulness and perceived ease of use as key determinants of technology adoption.

However, in the context of online transactions, perceived security and trust have emerged as equally important factors influencing acceptance of digital technology (Sujatha & Karthikeyan, 2021). Even when digital platforms offer operational and financial benefits, SMEs may hesitate to adopt them if they perceive online systems as vulnerable to fraud, cyberattacks, or data breaches. Similarly, customers are increasingly concerned about the security of their financial information and personal data when conducting online transactions. Consequently, SMEs recognise the need to establish secure digital environments that can strengthen customer trust, protect business reputation, and encourage repeat transactions.

To improve online transaction security, businesses now adopt various cybersecurity measures, including Secure Sockets Layer (SSL) certificates, data encryption, secure payment gateways, biometric verification, and two-factor authentication. These technologies help create safer digital environments for both businesses and consumers while also enhancing confidence in online transactions. More importantly, SMEs that invest in



strong cybersecurity practices are better positioned to build customer trust and remain competitive in digital markets (Onileowo, 2024).

Nevertheless, the challenge is even more pronounced in many developing economies where weak digital infrastructure, unreliable internet connectivity, unstable power supply, limited digital literacy, and inadequate cybersecurity regulations continue to hinder secure digital transactions. In countries experiencing rising levels of cybercrime, many SME owners remain cautious about adopting digital platforms due to fear of financial loss and online fraud. Although governments, financial institutions, and technology providers continue to promote digitalisation and cashless economies, the success of these initiatives largely depends on the availability of secure and trustworthy digital transaction systems (Bassey, Oscar, Ebong, Oyekunle, & Matthew, 2025)

Given the growing dependence of SMEs on digital technologies, understanding the role of online security in sustainable digital-platform adoption has become increasingly important. Existing research has established the relevance of perceived usefulness and perceived ease of use, while studies of electronic commerce and e-services have separately demonstrated the importance of trust and perceived risk. However, the literature remains conceptually fragmented regarding the mechanism through which online security is connected to these acceptance constructs and, ultimately, to sustained SME platform use. The present study addresses this gap by developing an integrative conceptual framework in which online security is positioned as an antecedent of trust and perceived risk, while trust and perceived risk operate as parallel mediating mechanisms between security and sustainable adoption. The study therefore asks: (1) how should online security be conceptually positioned within an extended TAM framework for SMEs, (2) through what mechanisms do trust and perceived risk connect security to adoption, and (3) how do the security requirements of different digital-platform categories affect the sustainability of SME adoption? The contribution is a theoretically explicit framework and a set of propositions that can be subjected to empirical testing.

METHODOLOGY

Review Design

This study employs an integrated conceptual literature review instead of a systematic review, meta-analysis, or primary empirical design. Younas, Shahzad, & Inayat (2022) and Fundoni, Porcu, & Melis, (2023). suggest that an integrative review is essential when there is a necessity to combine various types of information to develop or enhance a conceptual framework. To integrate factors such as TAM, trust, perceived risk, cybersecurity, and the adoption of digital platforms by SMEs, the review was designed to provide a clear and replicable overview of the literature search, screening, evaluation, and synthesis processes, all while ensuring the conceptual adaptability required for this undertaking.

Information Sources and Search Strategy

Emphasis was placed on literature indexed in Scopus, which could be accessed via bibliographic searches, Google Scholar, publisher or institutional repositories, and various academic databases and search services relevant to research in technology, business, information systems, entrepreneurship, and information management. Other areas considered included cybersecurity, digital payments, data protection, the digitalization of SMEs, and the governance of digital platforms. Boolean operators were employed in the search method to connect essential concepts. The subsequent search strings served as illustrations: "online security" + SMEs + "digital platform adoption"; "trust" + cybersecurity + SMEs; "perceived risk" + "technology acceptance"; "perceived security" + e-commerce + SMEs; trust + "digital platform" + SMEs; and "digital payments" + security + SMEs. To identify foundational theoretical contributions and related studies, utilizing a method known as backward reference checking on relevant articles. To encompass a wide range of works related to digital business, entrepreneurship, finance, and information systems, the search was intentionally expansive.



Selection Criteria and Eligibility

Sources were considered eligible when they (a) addressed at least one of the core constructs of online security, trust, perceived risk, perceived usefulness, perceived ease of use, or digital-platform adoption; (b) focused on digital business, e-commerce, fintech, digital payments, cloud systems, social commerce, or closely related digital environments; (c) provided a conceptual, theoretical, empirical, policy, or institutional basis relevant to SMEs; and (d) were published in English or available as an English-language institutional source. Priority was given to peer-reviewed journal articles and established theoretical works, with recent literature used to capture developments in cybersecurity and SME digitalisation. Sources were excluded when they were unrelated to digital adoption or security, duplicated another record, lacked sufficient bibliographic information, or addressed purely technical cybersecurity issues without a link to organisational or user adoption. No claim of exhaustive systematic-review coverage is made.

Literature Evaluation and Data Extraction

The criteria employed to assess eligible sources included conceptual relevance, theoretical clarity, methodological credibility (when applicable), and a direct contribution to the study issue. Each source was meticulously gathered using a structured extraction matrix, categorized by publication details, study context, platform category, theoretical lens, security dimension, trust or risk mechanism, adoption outcome, and primary implication. The subject of SME digitalization and cybersecurity has been updated by incorporating recent studies, while still preserving foundational sources that maintain their theoretical significance. Through this approach, the study can reduce reliance on singular outcomes and gain a clearer understanding of which concepts support the definitions of constructs and which ones reinforce the proposed relationships.

Synthesis Procedure

The evidence synthesis comprised four distinct steps, characterized by its thematic and relational aspects. Online security and the sustainable utilization of digital platforms were initially articulated and examined in the review. Secondly, the findings concerning trust, perceived risk, and factors from the Technology Acceptance Model were gathered and assessed. Third, the study charted recurring relationships to determine whether security functioned as a conditional factor, antecedent, mediator, or predictor. The fourth step involved the development of a conceptual framework and propositions derived from the amalgamated evidence. The synthesis refrains from asserting pooled effect sizes and leans more toward an interpretive approach rather than a purely statistical one, aligning with the characteristics of an integrative review. As a result, the framework represents a conceptual notion that requires validation through practical application.

ONLINE SECURITY

Concept of Online Security

Online security refers to the set of measures, systems, and practices used to protect digital transactions and the sensitive information exchanged through online platforms. It focuses on safeguarding data from unauthorised access, cyberattacks, fraud, and breaches while ensuring that financial and commercial activities conducted over the internet remain safe, reliable, and trustworthy. At its core, it is built on four key principles: confidentiality, integrity, authenticity, and availability of information (Sujatha & Karthikeyan, 2021).

Moreover, with the rapid expansion of digital technologies such as e-commerce platforms, mobile banking, cloud services, and online marketplaces, the volume of online transactions has grown significantly. While these innovations have made business operations faster, more convenient, and globally accessible, they have also increased exposure to cybersecurity threats. Common risks include phishing scams, identity theft, ransomware attacks, data interception, and payment fraud. These threats not only compromise financial resources but also undermine trust in digital systems (Al-Rikabi, 2025).

For modern businesses, especially in digitally dependent environments, according to Sujatha & Karthikeyan (2021) online security goes beyond technical protection. It also serves as a foundation for maintaining



customer trust, ensuring business continuity, protecting brand reputation, and complying with regulatory standards. In essence, it has become a critical requirement for sustaining safe participation in the digital economy and enabling long-term operational resilience (Miracle, 2024).

Importance of Online Security for SMEs

Online security has become increasingly vital for Small and Medium Enterprises (SMEs) as they adopt digital tools to enhance efficiency, competitiveness, and market reach. According to Madondo, & Dhoba, (2025) the widespread use of e-commerce platforms, digital payment systems, mobile banking, cloud computing, and online marketing has opened new growth opportunities for SMEs. However, these benefits come with significant cybersecurity risks that can threaten financial stability, customer confidence, and long-term sustainability (Mohammed, Dziyauddin, & Latiff, 2023).

One of the most important roles of transaction security is the development of trust. Customers are more willing to engage with businesses when they are confident that their personal and financial information is protected. A secure digital environment encourages repeat transactions, strengthens customer loyalty, and enhances the business's overall reputation. In contrast, security breaches can quickly erode trust and lead to customer loss and reputational damage that may be difficult to recover from (Sujatha & Karthikeyan, 2021).

In addition, online security helps SMEs reduce financial and operational risks. Cyber threats such as phishing attacks, ransomware, and payment fraud can result in significant financial losses and disrupt business operations. For SMEs, which often operate with limited financial buffers, such disruptions can be particularly damaging. Strong security systems help prevent these incidents and ensure continuity in business activities.

Perceived security also plays a key role in technology adoption. Drawing from the Technology Acceptance Model (TAM), SMEs are more likely to adopt digital platforms when they believe the systems are secure, useful, and reliable. When businesses are confident that adequate safeguards are in place, they are more willing to fully embrace digital transformation (Ursavaş, 2022).

Furthermore, secure transaction systems as highlighted by Tu, Kubatko, Melnyk, Li, Kovalov, & Yaremenko, (2025) support regulatory compliance and enhance competitive advantage. However, many regulatory frameworks now require strict data protection and cybersecurity compliance. SMEs that prioritise security are better positioned to meet these obligations while also distinguishing themselves in competitive markets through credibility and professionalism.

Ultimately, online security is not just a technical requirement but a strategic necessity for SMEs. It underpins trust, operational continuity, regulatory compliance, and sustainable digital growth in an increasingly interconnected business environment (Das, S., Kundu, & Bhattacharya, 2020).

SME ADOPTION OF DIGITAL PLATFORMS

Concept of SME Digital Platform Adoption

The adoption of digital platforms by SMEs is understood as the readiness, selection, and implementation of digital technologies within business processes to improve efficiency, productivity, profitability, and competitiveness. Meanwhile, Madondo & Dhoba (2025) argue that adoption is not only about the initial use but also about continued use and full integration of digital systems into organisational processes. It is the degree to which SMEs adopt technological innovations to improve business performance and react to changing market environments (Das, Kundu, & Bhattacharya, 2020). There are several internal and external factors that affect adoption, such as organisational readiness, the cost of technology, the availability of infrastructure, managerial skills, and perceived usefulness and perceived ease of use. Crucially, SMEs adopt digital platforms when they perceive that such technologies will provide tangible business benefits and will be easy to use and secure (Davis, 1989; Donbesuur, Ampong, Owusu-Yirenkyi, & Chu, 2020).



Digital Platform Adoption by SMEs

SMEs are continuously using digital platforms in their business activities as part of digital transformation. Moreover, digital platforms are technology-enabled systems that support business activities, including marketing, communication, financial transactions, service delivery and supply chain coordination. Thus, the use of these platforms is now essential for SMEs to remain competitive in a global and increasingly digital economy (Tu, Kubatko, Melnyk, Li, Kovalov, & Yaremenko, 2025). The integration of digital platforms must be distinguished from the implementation of technology only when necessary. In the context of this research, "sustainable adoption" refers to the consistent use of digital platforms that maintains value for the organization while ensuring that security, reliability, usability, and operational continuity are upheld at satisfactory levels. Thus, sustainability encompasses not only the preservation of the environment but also ensuring the continued functionality of systems.

Digital Platform Categories and Security Requirements

The integration of digital platforms must be distinguished from the implementation of technology only when necessary. In the context of this research, "sustainable adoption" refers to the consistent use of digital platforms that maintains value for the organization while ensuring that security, reliability, usability, and operational continuity are upheld at satisfactory levels. Thus, sustainability encompasses not only the preservation of the environment but also ensuring the continued functionality of systems.

E-commerce and Digital Platforms

Ensuring the confidentiality and safety of online shoppers' accounts, orders, products, payment information, and transaction history stands as a paramount concern for e-commerce platforms. Key aspects encompass dependable payment systems, user verification, secure connections, fraud prevention measures, and safeguarding personal information. Impersonation, detrimental associations, manipulation tactics, managing client information via chat and integrated payment features, along with publicly accessible accounts, represent further threats posed by social-commerce platforms. Seller confidence and customer readiness to engage in transactions could be influenced by security indicators for small and medium enterprises.

Fintech, Online Banking and Digital-Payment Platforms

Due to their direct facilitation of fund transfers, account access, payment authorization, and the exchange of financial information, fintech, online banking, and digital payment environments expose small and medium-sized enterprises to significant financial and identity-related risks. Consequently, fundamental requirements encompass secure authentication, encryption, transaction monitoring, rapid incident response, multi-factor authentication, and fraud detection. Given the rapid financial and reputational damage that can arise from a security breach in these scenarios, the sense of trust and perceived risk is significantly shaped by individuals' feelings of security regarding the system.

Cloud-Based Business Platforms

Numerous security issues arise with cloud-based platforms, including those related to storage, accounting, and corporate applications. These issues centre on aspects such as access control, data confidentiality, availability, backup, recovery, secure APIs, and the reliability of providers. By depending on external providers rather than overseeing their own infrastructure, SMEs must place their trust in the provider's expertise, governance, continuity, and security protocols, alongside the application interface.

Digital Supply-Chain Platforms

Integrity, availability, authentication, and secure information transmission are crucial elements of digital supply-chain platforms. Small and medium-sized enterprises depend on these platforms for numerous functions, such as managing inventory, coordinating with suppliers, handling transportation, tracking shipments, and fulfilling orders. Even without a direct exchange of funds, a compromised or unreachable



system can bring operations to a standstill. Although all these groups follow the same fundamental security standards, the most critical ones vary based on factors such as the type of data managed, the severity of possible failures, the financial stakes involved, and the number of third parties involved. This concept perceives the platform category primarily as a contextual boundary condition rather than a formal moderator subject to statistical testing.

Due to this disparity, the conceptual model cannot assume that all digital environments attribute the same level of importance to the same security technique. One instance of a digital platform that small and medium-sized enterprises commonly utilize is an online retail site. Businesses now have the opportunity to display their products online, engage with a broader audience, and generate sales free from the constraints of physical storefronts due to these platforms. E-commerce platforms facilitate access for small and medium-sized enterprises (SMEs) to both domestic and global markets by lowering operational costs. In a recent article, Miracle observes that small and medium-sized enterprises (SMEs) have gained the ability to compete with significantly larger corporations in online marketplaces, a shift attributed to the rise of e-commerce.

The mobile payment solutions that have fundamentally transformed the financial transactions of small and medium-sized enterprises represent another important category. Mobile payment platforms enable businesses to gather and transfer funds through mobile devices, reducing their reliance on cash transactions. This holds significant relevance in developing countries where conventional financial infrastructures may still be absent. Utilizing mobile payments enables small and medium-sized enterprises to conserve both time and resources, while simultaneously broadening their reach to financial services.

Consequently, a significant element in the digital uptake of small and medium-sized enterprises is the role of social commerce platforms. These platforms enable the promotion of products, engagement with consumers, and the smooth execution of transactions by combining the elements of online shopping with social networking. Social commerce offers numerous advantages for small and medium-sized enterprises (SMEs), such as increased consumer engagement, reduced marketing costs, and enhanced brand visibility (Madondo & Dhoba, 2025). Consumers tend to exhibit increased loyalty toward brands following their participation in real-time dialogs with these brands on social media marketplaces and various other platforms. Additionally, an increasing number of small and medium-sized enterprises are adopting cloud accounting software for tasks such as record-keeping, payroll management, tax preparation, and business analytics. Cloud-based systems offer a cost-effective, scalable, and flexible solution for SMEs, eliminating the need for expensive on-premises infrastructure. Alongside improving operational efficiency and decision-making, these systems provide immediate access to financial data (Mohammed, Dziyauddin, & Latiff, 2023).

Furthermore, small and medium-sized enterprises utilize the internet banking system, which serves as a crucial digital platform. Through the use of advanced technologies, businesses can efficiently oversee their accounts, submit loan applications, settle bills, and execute fund transfers, all without the need to step into a bank branch. Access to financial services has expanded, transaction times have been shortened, and overall efficiency has improved through the advent of online banking. People's perceptions of the security and trustworthiness of their financial institutions significantly influence the adoption of online banking (Miracle, 2024).

The significance of digital supply chain platforms for small and medium-sized enterprises engaged in production, logistics, and distribution is increasingly recognized. These platforms enable effective inventory management, facilitate real-time product tracking, enhance supplier collaboration, and optimize logistics. Transforming supply chain processes through digitization enables small and medium-sized enterprises (SMEs) to enhance efficiency, reduce delays, and improve customer service, ultimately leading to heightened customer satisfaction (Tu, Kubatko, Melnyk, Li, Kovalov, & Yaremenko, 2025).

THEORETICAL FOUNDATION

Technology Acceptance Model (TAM) in SMEs

Several theoretical models have been developed to explain the adoption of digital technologies in SMEs and



the reasons behind it. One of the most influential models is the Technology Acceptance Model (TAM) developed by (Davis 1989; Donbesuur, Ampong, Owusu-Yirenkyi, & Chu, 2020). TAM suggests that an individual's or organisation's intention to use technology is influenced by two major factors: perceived usefulness and perceived ease of use. In SMEs, the likelihood of adopting digital platforms is influenced by business owners' perception that these platforms will improve performance and are easy to use. The Unified Theory of Acceptance and Use of Technology (UTAUT) by Ursavaş (2022) is another frequently used model. UTAUT adds other determinants to earlier models, such as social influence and facilitating conditions. The findings indicate that SMEs' adoption of digital platforms is influenced by perceived usefulness, ease of use, organisational support, availability of infrastructure, and external pressure from customers and competitors.

Das, Kundu, & Bhattacharya (2020) provided important insights into SME digital adoption. The theory explains how innovations spread through a population over time. It identifies relative advantage, compatibility, complexity, trialability, and observability as important factors influencing adoption. SMEs are more likely to adopt digital platforms when they perceive clear benefits over traditional methods and when the technology is compatible with existing business practices.

Furthermore, an overarching conclusion across major theories of technology adoption is that trust and perceived security are crucial factors in adoption decisions, especially in digital settings involving financial transactions and sensitive data. While TAM and UTAUT focus on usefulness and ease of use, recent studies increasingly acknowledge the importance of perceived security as an extension of the two models for e-commerce and online financial systems (Bassey, Oscar, Ebong, Oyekunle, & Matthew, 2025). Trust is the confidence that SMEs have in digital platforms to securely process transactions, protect data and deliver reliable services. SMEs that perceive digital platforms as secure are more likely to engage in online transactions and integrate digital systems into their operations. On the other hand, concerns about fraud, cyberattacks, and data breaches can have a significant impact on adoption rates, even when platforms are perceived as useful and easy to use (Miracle, 2024).

Perceived security also affects customer behaviour and, in turn, influences SME adoption decisions. SMEs tend to adopt digital platforms, seeing customers preferring secure and trustworthy online transaction systems. Trust and security thus become key factors in the successful adoption and continued use of digital technologies in SME operations. SME adoption of digital platforms is a multi-dimensional process influenced by technological, organisational and environmental factors. However, the increasing prevalence of cyber threats has made trust and perceived security key determinants of digital transformation among SMEs.

Integrating TAM, Trust, Perceived Risk and Online Security

The core acceptance logic of the framework is provided by TAM. As noted by Davis (1989), the concepts of perceived usefulness (PU) and perceived ease of use (PEOU) regarding a digital platform serve as indicators of a small and medium-sized enterprise decision-maker's belief in the potential enhancement of business performance and the minimal effort required to learn and utilize the platform. However, PU and PEOU fail to fully address the uncertainty inherent in digitally mediated transactions. The anticipated benefits and assurance in the dependability and security of the transaction setting stand out as the two crucial elements influencing online acceptance, as highlighted by studies that combine the technology acceptance model with concepts of trust and risk.

Within the current framework, internet security is defined as an antecedent rather than being seen as mediating or moderating. The degree of assurance that individuals possess regarding the technological and organizational strategies implemented to safeguard sensitive information serves as an indicator of the effectiveness of these strategies. Given that SMEs are likely to perceive the platform as a trustworthy means of securing data and facilitating transactions, it is anticipated that enhanced online security will bolster their confidence. At the same time, enhanced security protocols are expected to diminish the perception of risk, as these protocols reduce the likelihood and consequences of fraud, unauthorized access, data corruption, and unsuccessful transactions. This reasoning aligns with research that views risk as a detrimental utility associated with adoption and integrates perceived risk into frameworks of technological acceptance (Nazari-Shirkouhi,



Badizadeh, Dashtpeyma, & Ghodsi, 2023; Uche, Osuagwu, Nwosu, & Otika, 2021).

The study recognizes trust and perceived risk as two interconnected processes that operate together. When a small or medium-sized enterprise (SME) places trust in a digital platform, its provider, and the associated transaction partners, it signifies a strong belief in their capacity to fulfill obligations reliably and securely. The platform's perceived risk encompasses various factors, including financial, privacy, security, performance, and operational risks. The SME assesses these elements in relation to the possible adverse outcomes and uncertainties that may arise from utilizing the platform. Sustainable adoption is anticipated to increase with higher levels of trust and decrease when perceived risk is minimal.

Consequently, the realm of online security can impact adoption in two significant manners: initially, by reducing barriers associated with security; and subsequently, by enhancing trust and diminishing perceived risk. The model continues to utilize PU and PEOU as direct indicators of acceptance. It is expected that the ease of use will enhance perceived usefulness, as a more user-friendly platform can make its benefits more readily available. Furthermore, both perceived usefulness and ease of use are projected to contribute to the promotion of sustainable adoption. Although a platform may be efficient and easy to use, it can still face challenges in gaining acceptance due to apprehensions regarding security. This highlights the importance of viewing security as a fundamental component of the overall acceptance model, rather than a substitute for it. When a platform lacks practicality or user-friendliness, no matter how strong its security features are, long-term adoption will falter. Consequently, the model perceives adoption as the outcome of additional evaluations related to functionality and assurance.

Construct Definitions and Proposed Associations

Construct	Definition in this study	Role in conceptual model
Online security	Online security encompasses the extent to which individuals feel that suitable organizational and technological safeguards are established to secure their personal information, financial dealings, and the authenticity and integrity of their data.	It serves as a fundamental element; a precursor to trust and risk awareness; a direct predictor of sustained adoption.
Trust	Trust is essential for the digital platform, suppliers, and transaction partners to demonstrate capability, reliability, and security in fulfilling their commitments.	A parallel mediation mechanism serves as a positive sign for sustainable adoption.
Perceived risk	Involves uncertainty regarding the potential financial, privacy, security, performance, and operational consequences of utilizing the platform.	Functions concurrently and serves as a negative predictor of long-term adoption.
Perceived usefulness (PU)	Refers to the belief that a digital platform can improve a company's efficiency, productivity, market penetration, or other desired outcomes.	Serves as a predictor for sustainable adoption in relation to the direct Technology Acceptance Model.
Perceived ease of use (PEOU)	Thought that the digital platform can be easily learned and utilized, a concept referred to as perceived ease of use.	Positively related to perceived usefulness and serves as a direct predictor of long-term adoption within the Technology Acceptance Model.
Sustainable digital-platform adoption	Ensuring suitable levels of security, reliability, user-friendliness, and operational consistency through the ongoing, regular, and well-integrated utilization of digital platforms is crucial for lasting adoption.	Necessary outcome of the framework.
Platform category	Various distinctions arise concerning the platforms employed. These encompass e-commerce, fintech,	Focus lies on boundary conditions within the

and SME context	digital payments, social commerce, cloud systems, and supply-chain platforms, alongside considerations of infrastructure and resource limitations.	context, rather than on explicit moderators in the proposed model.
-----------------	--	--

Presented below is the Framework several propositions for future empirical testing:

P1: Perceived online security is positively associated with SME trust in digital platforms.

P2: Perceived online security is negatively associated with SME perceived risk in digital-platform use.

P3: Trust is positively associated with sustainable SME adoption of digital platforms.

P4: Perceived risk is negatively associated with sustainable SME adoption of digital platforms.

P5: Perceived usefulness is positively associated with sustainable SME adoption of digital platforms.

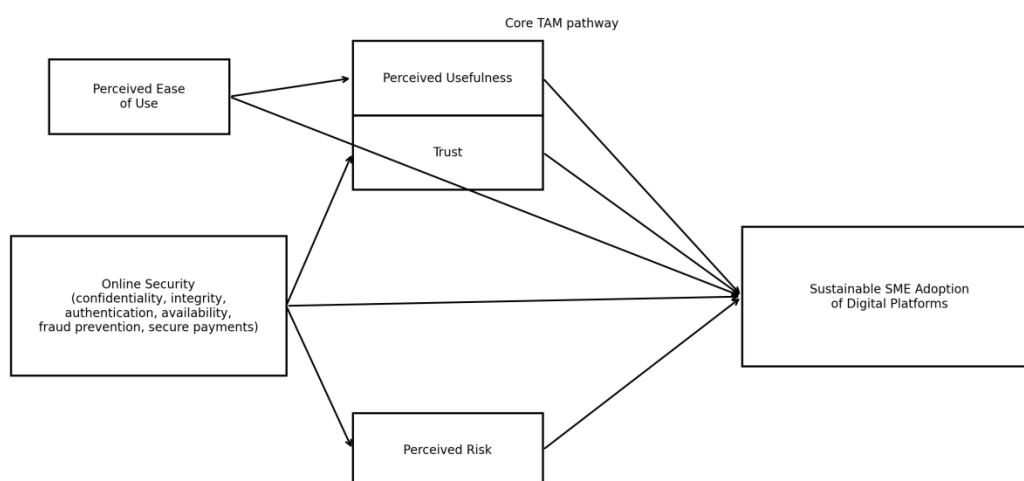
P6: Perceived ease of use is positively associated with sustainable SME adoption of digital platforms.

P7: Perceived ease of use is positively associated with perceived usefulness.

P8: Trust and perceived risk mediate the relationships between perceived online security and sustainable SME adoption of digital platforms

The roles of the constructions are clearly outlined by these propositions. Ensuring an online security is the foremost foundation. Mediating in a comparable manner are trust and perceived danger. One approach to predicting total addressable market is by examining the utility and user-friendliness of a product. Perceived ease of use also contributes to perceived usefulness. The dependent construct involves the sustainable adoption of digital platforms. Although the paper addresses various contextual factors including platform categorization, resource limitations, infrastructure, regulatory environment, and cybersecurity awareness, it does not formally designate these as moderators within the proposed model. One prevalent method for safeguarding online financial transactions is through the use of encryption.

Conceptual Framework



Trust and perceived risk are proposed parallel mediators; platform category and SME context are boundary conditions.

Figure 1. depicts a proposed conceptual framework connecting online security, TAM constructs, trust, perceived risk, and sustained SME digital-platform adoption.



Encryption Technologies

Encryption involves transforming data from a format that is easily understood to one that is encoded, ensuring that only individuals possessing the appropriate decryption keys can interpret it. This guarantees that essential information remains inaccessible to cybercriminals, even if they succeed in intercepting it during transit (Al-Rikabi, 2025). Banking, internet shopping, email, and cloud storage all rely on the principles of encryption technology. By bolstering confidentiality and minimizing the chances of data breaches, encryption protects sensitive consumer and financial information. Small and medium-sized enterprises are enhancing their digital security measures and fostering customer trust in online transactions through the implementation of encryption technologies.

Secure Socket Layer (SSL) Certificates

Secure Socket Layer (SSL) certificates are security protocols that establish encrypted communications between websites and web browsers. Websites that use SSL certificates use the “HTTPS” protocol, which means the data exchanged between the user and the website is secure (Murkomen, 2024). SSL certificates help secure sensitive data, such as passwords, payment information, and personal data, when it is exchanged over the internet. They also help verify website identities and reduce the risk of phishing and fraudulent websites. Generally, customers are more likely to do business on websites that show SSL security indicators because they view those sites as trustworthy and secure.

Multi-Factor Authentication (MFA)

Multi-factor authentication (MFA) is a security process where users are required to provide multiple forms of identification before they can access a system or complete a transaction. Multi-factor authentication (MFA) could involve combinations of passwords, fingerprints, facial recognition, security tokens, or one-time verification codes (Mohammed, Dziyauddin, & Latiff, 2023). MFA makes it far more difficult for cybercriminals to get into accounts or systems because they would have to bypass multiple layers of security. Hence, SMEs are increasingly adopting MFA to bolster online banking systems, cloud applications and customer accounts against cyber threats.

Antivirus Software and Firewalls

Firewall and antivirus software are important in cybersecurity because they protect computer systems and networks from malicious attacks. Firewalls monitor and control network traffic, blocking unauthorised communications, and antivirus software detects and removes harmful programs such as viruses, spyware, ransomware, and other malware (Arifin, Rosman, Radzi, Naw, & Alimin, 2024). Such tools can help SMEs to reduce their vulnerabilities, protect sensitive information and keep their business operations intact. Regular updates and constant monitoring of the systems also enhance the effectiveness of these security measures against ever-evolving cyber threats.

Safe Payment Gateways

Secure payment gateways are used to process online payments securely by encrypting payment details and ensuring the secure transmission of transaction data between customers, merchants, and financial institutions. Payment gateways help to minimize the risk of fraud and guarantee that financial transactions are processed in a secure manner (Al-Rikabi, 2025). Secure payment gateways instill confidence in SMEs involved in e-commerce and foster online purchasing behaviour. Whereas, popular payment gateways usually offer additional fraud detection and risk management features that add further security to the transactions.

Blockchain Technology Transaction Verification

Blockchain technology is being introduced as an innovative way to secure online transactions (Onileowo, 2024). Blockchain uses distributed digital ledgers to record and verify transactions in a transparent and secure manner. Blockchain records are spread across multiple systems and cannot be easily altered; thus, the



technology helps reduce fraud, improve transparency, and improve data integrity (Al-Rikabi, 2025). Moreover, blockchain-based transaction verification plays a significant role within financial services, supply chain management and digital payment systems. It offers SMEs more secure transactions, reduced operational risks and more trust from customers and business partners. In general, when SMEs perceive these security mechanisms as reliable and effective, they tend to trust digital platforms more and adopt digital technologies for business operations. Robust online security safeguards businesses from cyber threats and instils customer confidence, operational efficiency and sustainable digital transformation.

INFLUENCE OF ONLINE SECURITY ON SME ADOPTION OF DIGITAL PLATFORMS

The reviewed body of work collectively suggests that multiple direct relationships are involved when assessing the effects of internet security. Security measures foster a sense of assurance, subsequently enhancing trust and reducing perceived risk. These interconnected elements, along with practicality and user-friendliness, play a significant role in shaping continued acceptance, as suggested by a more credible interpretation. The subsequent sections delve into these paths and their tangible repercussions.

The way SMEs perceive, adopt, and continue to use digital platforms is significantly influenced by the security of online transactions. As e-commerce, mobile payments, cloud-based services, and online banking continue to expand, the significance of cybersecurity has surged for SMEs. These businesses face the pressing challenge of integrating technology while safeguarding their operations. Establishing trust, reducing risk, fostering customer confidence, adhering to regulations, evaluating costs, and ensuring usability are all interrelated elements influenced by transaction security.

Developing Trust and Confidence

Trust and confidence are two of the most important factors through which the security of online transactions affects the adoption of digital platforms by SMEs. Trust is a basic necessity in digital business environments, as transactions take place in the absence of physical interaction among buyers, sellers, and service providers. SMEs are more likely to trust digital platforms' security (Miracle, 2024), which helps them feel more confident that financial transactions and sensitive business data are protected from cyber threats.

Secure systems also provide SMEs with peace of mind that their finances, customer data and operations are not vulnerable to unauthorised access. This sense of security helps SMEs leverage digital platforms to conduct business activities such as online sales, digital marketing, and e-payments. For instance, the adoption of e-commerce by SMEs is enhanced by the availability of secure payment methods, such as encrypted gateways, which help reduce concerns about online fraud and payment interception (Mohammed, Dziyauddin, & Latiff, 2023). Similarly, secure digital banking helps SMEs embrace digital financial products such as account management, loan applications, and fund transfers. The lack of security measures can discourage SMEs from using digital systems, as they fear losing money, falling victim to identity theft, damaging their reputation, and losing customer trust. The perception of these risks directly affects willingness to use digital platforms and underscores the importance of perceived security in decisions to adopt them (Bassey, Oscar, Ebong, Oyekunle, & Matthew, 2025).

Mitigating Cybersecurity Risks

Security of online transactions is also considered a factor in the uptake of SMEs, as it minimises their susceptibility to cybersecurity risks. In a digital business environment, you'll face common cyber threats such as phishing, ransomware, hacking, spyware attacks, and payment fraud. The absence of advanced cybersecurity systems and expertise from SMEs makes them more susceptible to these threats (Arifin, Rosman, Radzi, Nawi, & Alimin, 2024). If SMEs feel that digital platforms are not safe to use, they might avoid them or limit their use, hindering digital transformation. But strong security systems greatly reduce risks of data breaches, unauthorised access, financial fraud and operational disruptions.



To create safer digital environments, technologies such as firewalls, intrusion detection systems, and encryption tools employ real-time monitoring and other methods to mitigate cyber risks (Al-Rikabi, 2025). As a consequence, SMEs are more at ease with digital technologies and more inclined to integrate them into their daily business as the risk of cyber-attacks diminishes. This indicates that one way security affects adoption behaviour is through risk reduction.

Building Customer Confidence and Business Image

Another factor that relates to online security and SMEs' adoption of digital platforms is customer trust. In digital markets, consumers are more inclined to purchase from organisations that they consider have a positive track record for protecting personal and financial data. SMEs recognise that customer trust directly impacts sales performance, brand reputation, and the sustainability of the business in the long run (Bassey, Oscar, Ebong, Oyekunle, & Matthew, 2025).

Security features such as HTTPS encryption, verified payment gateways, and secure login systems are essential for instilling confidence in customers that their data is safe. Customers will be more likely to make online transactions and engage with a business again if they feel safe. The growing level of customer trust makes it more attractive for SMEs to invest and use digital platforms to fulfil market expectations and stay competitive in digital spaces (Rampaul, 2025). This enhanced customer confidence serves as a reinforcement, further strengthening SMEs' willingness to adopt secure digital technologies.

Regulatory Compliance

Another driver for SME adoption of secure digital platforms is regulatory compliance. Governments and financial institutions across the world have established strict rules to safeguard consumer information, ensure transactions, and combat cybercrime. These standards include laws regarding data protection, electronic transactions and financial compliance (Tu, Kubatko, Melnyk, Li, Kovalov, & Yaremenko, 2025). SMEs can comply with these legal obligations and avoid penalties for non-compliance by using secure digital platforms. The consequences of not complying with regulatory requirements can include fines, legal action, and reputational damage, which can negatively affect business sustainability. Thus, SMEs prefer platforms that are already equipped with security and compliance features, thereby eliminating the need for in-house development and the costs of regulatory compliance (Miracle, 2024). In this regard, regulatory pressure can be considered an external motivator that drives SMEs to adopt secure digital systems.

Price Considerations

Cost-related factors can also affect an SME's willingness to adopt; however, security in online transactions can help strike a balance and make adoption more likely. Cybersecurity is a matter of investments, for example, in software, hardware, training your employees, updating systems and other professional services from consultants. These expenses can be prohibitive for many SMEs with small budgets (Mohammed, Dziyauddin, & Latiff, 2023). While some SMEs may see the value in digital transformation, they are still dissuaded from adopting digital platforms by the associated high costs or the complexity of security solutions. However, SMEs are more inclined to implement security solutions that are affordable, scalable and easy to use. This has lowered the cost of barriers and increased adoption rates among SMEs, as digital platforms offer cloud-based security services and built-in security features. Therefore, cost-effectiveness is an important moderator of the relationship between security adoption behaviour and security.

Reliability and User-Friendliness

Perceived Ease of Use and System Reliability are important factors affecting SMEs' adoption of Secure Digital Platforms. SMEs are more likely to adopt technologies that provide robust security without introducing undue complexity or slowing business processes. Security systems are considered to be inefficient, and if they are too complicated or too intrusive, they are not used (Cram, Proudfoot, & D'arcy, 2017). The top digital platforms feature good security and usability. Safety isn't all that matters, as user experience is enhanced by smooth multi-factor authentication, automated fraud detection, and quick, secure payment processing. SMEs are more



confident and inclined to use digital technologies if the systems are reliable and operate consistently, without downtime or security issues (Bassey, Oscar, Ebong, Oyekunle, & Matthew, 2025). So, alongside usability and reliability, security will ensure it isn't a barrier to adoption but an enabler of digital transformation.

BARRIERS TO SME ADOPTION DESPITE SECURITY MEASURES

Despite significant progress in online security and the availability of numerous protective technologies, Small and Medium Enterprises (SMEs) still face numerous challenges that impede the full adoption of digital platforms. Such challenges are particularly pronounced in developing economies, where structural, financial and technical constraints often hinder the effectiveness of cyber security measures. Understanding these challenges is important for explaining why, despite the availability of security solutions, SMEs may still be reluctant to adopt digital systems (Onileowo, Muharam, Ramily, & Khatib, 2021).

Lack of Awareness About Cybersecurity

One of the most critical challenges impeding SME adoption of digital platforms is the low cybersecurity awareness among business owners and employees. Many SMEs lack sufficient knowledge of cyber risks, security protocols, and safe digital practices to operate safely in digital environments. Hence, they may underestimate the probability or consequences of cyberattacks such as phishing, malware infections and data breaches (Miracle, 2024). This lack of awareness often leads to poor security behaviour such as weak password practices, failure to keep software updated, and failure to properly secure sensitive business data. As Al-Rikabi (2025) pointed out, human error remains a leading cause of security breaches in organisations, especially in small businesses with limited training programmes. SMEs often lack formal policies or guidelines on cyber security, making them even more vulnerable. Even with advanced security tools in place, without sufficient awareness, effective protection cannot be guaranteed, undermining confidence in digital platforms and slowing adoption rates.

Lack of Financial Resources

Financial constraints also pose a major barrier to SMEs' adoption of secure digital platforms. Many SMEs have limited budgets and focus on immediate operational needs like inventory, staffing, and production rather than investing in cybersecurity. Mohammed, Dziyauddin, & Latiff (2023) state that many security systems, such as encryption tools, firewalls, secure servers, and monitoring systems, require significant investment. SMEs should also be aware of the ongoing costs involved, such as software updates, subscription fees, maintenance costs, and cybersecurity insurance, in addition to the initial setup costs. These costs can deter SMEs from fully investing in digital security infrastructure. As a result, some SMEs use minimal or outdated security measures, leaving them more vulnerable to cyber risks. This financial limitation directly affects their willingness to adopt or increase the use of digital platforms, even when they are economically beneficial in the long run.

Lack of Technical Expertise

Another important challenge is the lack of technical expertise in SMEs. The vast majority of small businesses lack the IT departments and cybersecurity professionals with the expertise to properly manage their digital systems. This shortage of qualified personnel hinders their ability to deploy, monitor and maintain secure digital platforms (Tu, Kubatko, Melnyk, Li, Kovalov, & Yaremenko, 2025). Cybersecurity systems must be continually updated, configured, and monitored to be effective. SMEs may lack the skills to identify vulnerabilities or to respond promptly to security incidents. This raises the likelihood of system crashes and data breaches. Furthermore, non-technical users may struggle to manage complex security systems, leading to improper use or misconfiguration. This technical gap diminishes the effectiveness of security measures and hampers SME confidence in digital platforms, slowing adoption.

Ever-Changing Cyber Threats

The dynamic nature of cyber threats continues to be a challenge to SME digital adoption. Cybercriminals are continually creating more sophisticated attack techniques, including advanced phishing, ransomware-as-a-



service, AI-based attacks, and zero-day exploits. SMEs find it challenging to maintain updated and effective security systems in the face of these emerging threats (Al-Rikabi, 2025). SMEs may have strong security in place, but new vulnerabilities can emerge, rendering those protections less effective. This ongoing evolution creates uncertainty and fear among SME owners about the security of digital platforms. Miracle (2024) highlights that the ever-changing nature of cyber threats requires continuous investment in improving cybersecurity, including employee training and system monitoring. However, SMEs are often unable to keep pace with these developments due to a lack of resources, which undermines their confidence in adopting digital technologies.

Infrastructural Constraints

Infrastructure limitations, especially in developing economies, are another major barrier to SME adoption of secure digital platforms. For the proper functioning of digital systems, stable internet connectivity and a reliable electricity supply are essential. However, in many areas, internet outages, slow connections, and power cuts are common, affecting the operations of digital platforms (Bassey, Oscar, Ebong, Oyekunle, & Matthew, 2025). Unstable infrastructure can erode confidence in digital systems as SMEs may be concerned about transaction failures, data loss or system downtime when they need to perform critical business operations. Real-time security monitoring systems and cloud-based cybersecurity solutions are also affected by weak connectivity. In addition, the lack of digital infrastructure may discourage SMEs from investing in advanced technologies, as the return on investment may seem uncertain. This slows down the adoption of secure digital platforms and limits the benefits of digital transformation.

STRATEGIES FOR IMPROVING SME ADOPTION THROUGH BETTER SECURITY

There is a need not only to provide secure technologies but also to ensure that there is institutional, financial, and educational support for increasing SMEs' use of digital platforms. Since the security of online transactions plays a major role in adoption decisions, measures to further raise awareness and security, lower costs, and build trust are crucial to increasing SMEs' participation in the digital economy. These approaches include joint actions from governments, financial institutions, technology providers and SMEs.

Government Support

Government intervention is vital in improving SME uptake of secure online platforms. Policies are a tool that governments can use to foster a positive cybersecurity culture, digital literacy, and safe online business practices. The best practice is to create SME-specific cybersecurity awareness programs. Such schemes are designed to raise awareness among business owners and employees of common cyber risks, including phishing, ransomware, and online fraud, as well as ways to avoid them (Tu, Kubatko, Melnyk, Li, Kovalov, & Yaremenko, 2025). Furthermore, governments can incentivise to lessen the cost burden that comes with implementing cybersecurity systems. The main reason many SMEs are reluctant to use digital platforms is the cost of implementing security infrastructure, software, and training. To promote greater adoption of secure technologies, these financial barriers can be lowered through subsidies, tax reliefs and digital transformation grants (Bassey, Oscar, Ebong, Oyekunle, & Matthew, 2025). Moreover, by providing funding for e-commerce platforms, cloud services, and secure payment systems, SME digitalisation grants can help integrate secure digital systems. Government initiatives for digital support for SMEs have a substantial positive impact on SME competitiveness and digital transformation, especially in emerging economies, as shown (Rampaul 2025).

Training and Education

Training and education are critical to boosting SMEs' confidence and capability to access secure digital platforms. A lack of cybersecurity understanding is a challenge for many SMEs, making them more vulnerable to cyberattacks and reducing their willingness to adopt digital systems. Structured training programs can help address this knowledge gap and enhance safe digital practices. SMEs should be educated on important topics such as fraud prevention, password security, and safe internet use. Fraud prevention training is used to identify

suspicious emails, phishing attempts and fraudulent websites. Training on password management promotes the use of complex and distinctive passwords and secure authentication techniques. Safe online practice training will ensure that employees are aware of how to use online platforms safely and responsibly and how to handle sensitive data (Arifin, Rosman, Radzi, Nawi, & Alimin, 2024). With effective training, cybersecurity awareness can be promoted and human error, a major factor in security breaches, reduced. The more knowledgeable SMEs are about cybersecurity threats and solutions, the more confident they are in implementing digital platforms. Knowledge of cybersecurity threats and solutions significantly boosts their confidence in implementing digital platforms.

Affordable Security Solutions and Collaboration with Financial Institutions

Affordable and easy-to-use cybersecurity solutions are essential for SMEs to adopt as they enter digital platforms. Many SMEs face financial constraints and cannot afford enterprise-class security systems. Hence, it is important for technology providers to create customised, cost-effective security solutions that are effective for SMEs. SMEs can access cost-effective cybersecurity solutions through cloud-based services, subscription-based security software, and built-in security features of digital solutions. These solutions have the advantage of minimising the costs of large initial investments, and, when it comes to security services, they can be scaled according to the needs and budgets of SMEs (Mohammed, Dziyauddin, & Latiff, 2023). Cost-effective choices also keep things simple, making it easier for SMEs that are not technologically literate to implement and manage cybersecurity systems. These solutions reduce financial and technical constraints and promote the use of digital platforms.

The focus on collaborating with Financial Institutions cannot be undermined as this is aimed at enhancing SMEs performance and competitiveness in the dynamic environ. Another vital approach to building trust and leveraging digital platforms is cooperation among SMEs, banks, and fintech firms. Digital transactions are integral to financial institutions, especially in online banking, mobile payments, and electronic fund transfers. In turn, they directly impact SME confidence in improving security. By offering secure digital payment systems equipped with encryption, fraud detection, and real-time transaction monitoring, banks and fintech companies can build trust with SMEs. These systems help protect financial transactions from fraud and unauthorised access, ensuring their safe and efficient processing (Mohammed, Dziyauddin, & Latiff, 2023). Moreover, financial institutions can help SMEs by offering cybersecurity advice, secure payment methods, and customer protection policies. Through close collaboration with SMEs, these institutions can contribute to developing a more secure digital financial environment and promoting the use of digital platforms.

Continuous Security Updates

Regular security patches are crucial to ensure the systems are effective and to keep SMEs confident in digital platforms. Cyber-attacks are ever-changing and obsolete security infrastructures can be susceptible to new attacks. To stay resilient against the new vulnerability that emerges in the system, regular software updating, system patching and real-time monitoring is required (Al-Rikabi, 2025). Undoubtedly, automated security updates allow SMEs to remain secure without relying on in-depth technical expertise or manual effort. While continuous monitoring systems can also detect suspicious activities early and prevent potential cyberattacks before they cause significant damage.

Additionally, regular security updates also help foster trust and the ongoing use of digital technologies among SMEs, while maintaining platform security and keeping platforms up to date (Rampaul 2025). In general, it is essential to combine the various measures outlined below with government intervention, education and training, affordable cybersecurity solutions, collaboration within the financial sector, and continuous system updates to improve SME adoption of digital platforms. All of these strategies are geared toward solving the major barriers of cost, awareness, technical expertise, and trust. Improving these elements contributes to increased perceived security, reduced adoption resistance, and accelerated digital transformation of SMEs in the long run (Al-Rikabi, 2025).

CONCLUSION

The study integrative conceptual review reveals how SMEs can sustainably adopt digital platforms by integrating security within an enhanced framework of Technology Acceptance Model. Online security serves as a precursor to adoption, rather than functioning as a moderator or mediator, as posited by the central argument. The primary avenues that elucidate the entire concept revolve around trust and the perception of risk. If the platform boasts enhanced security, users are likely to develop greater trust in it, alleviating concerns regarding potential losses in aspects such as privacy, performance, finances, and operations. Perceived utility and ease of use serve as functional evaluations, yet these processes complement and enhance those assessments.

Furthermore, the framework clarifies the rationale behind the notion that security should not be viewed as a universal technical imperative applicable to all digital systems. Enhanced measures regarding identity verification, authorization processes, and the integrity of transactions are essential in the realms of financial technology, online banking, and digital payment systems. Additionally, cloud platforms require a focused approach to access management, confidentiality, availability, and recovery protocols. Meanwhile, digital supply-chain systems demand a commitment to integrity, availability, and the secure exchange of information. These criteria hold particular significance in the realms of e-commerce and social commerce. Although the concepts remain consistent, the security challenges adapt based on the context.

Investments in security do not guaranty continued adoption, as indicated by the analysis. Implementing and maintaining appropriate security presents significant challenges for SMEs. Factors contributing to this complexity include constrained resources, a general lack of cybersecurity awareness, inadequate technical expertise, aging infrastructure, strict regulatory requirements, and concerns regarding usability. Rather than perceiving these components as mere additional causal constructs that detract from the proposed mechanism, they are regarded as contextual conditions that envelop the primary model. In conclusion, the study offers a conceptually grounded framework along with nine propositions that could guide forthcoming empirical investigations. Future research could benefit from exploring different sectors of SMEs, various platform categories, and contexts within emerging economies to determine if the proposed direct and mediated correlations remain valid. Future studies can examine deeper into the various platforms and organizational capabilities that shape the robustness of the connections between security and adoption. Additionally, it is essential to explore whether trust and perceived risk play a mediating role in these interactions. To ensure that the digitalization of SMEs is secure, resilient, and sustainable, conducting such testing would provide more robust evidence for policymakers and actions in the digital business environment.

REFERENCES

1. Al-Rikabi, H. M. S. (2025). Network security and types of modern cyber-attacks on networks. *Power System Protection and Control*, 53(4), 168–175.
2. Arifin, M. S. M., Rosman, M. R. M., Radzi, S. M., Nawi, N. A. M. M., & Alimin, N. A. (2024). Information security behavior among Malaysian SMEs: Phishing, cybersecurity incident, human factors and risk mitigation. *Journal of Islamic*, 9(66), 640–650.
3. Bassey, I. B., Oscar, F., Ebong, G. N., Oyekunle, D., & Matthew, U. O. (2025). Impact of digital banking on financial inclusion for rural SMEs empowerments: A case study from EMEA region. *HAFED POLY Journal of Science, Management and Technology*, 6(2), 195–223.
4. Cram, W. A., Proudfoot, J. G., & D'arcy, J. (2017). Organizational information security policies: a review and research framework. *European Journal of Information Systems*, 26(6), 605–641.
5. Das, S., Kundu, A., & Bhattacharya, A. (2020). Technology adaptation and survival of SMEs: A longitudinal study of developing countries. *Technology Innovation Management Review*, 10(6).
6. Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13(3), 319–340.
7. Donbesuur, F., Ampong, G. O. A., Owusu-Yirenkyi, D., & Chu, I. (2020). Technological innovation, organizational innovation and international performance of SMEs: The moderating role of domestic institutional environment. *Technological Forecasting and Social Change*, 161, 120252.



8. Fundoni, M., Porcu, L., & Melis, G. (2023). Systematic literature review: Main procedures and guidelines for interpreting the results. *Researching and Analysing Business*, 55-72.
9. Madondo, E., & Dhoba, H. (2025). Leveraging social media for entrepreneurial success: A systematic review of the literature. *International Journal of Business Ecosystem & Strategy* (2687-2293), 7(3), 125–133.
10. Miracle, N. O. (2024). The importance of network security in protecting sensitive data and information. *International Journal of Research and Innovation in Applied Science*, 9(6), 259–270.
11. Mohammed, A. H. Y., Dziyauddin, R. A., & Latiff, L. A. (2023). Current multi-factor authentication: Approaches, requirements, attacks and challenges. *International Journal of Advanced Computer Science and Applications*, 14(1).
12. Murkomen, T. (2024). Performance, privacy, and security issues of TCP/IP at the application layer: A comprehensive survey. *GSC Advanced Research and Reviews*.
13. Nazari-Shirkouhi, S., Badizadeh, A., Dashtpeyma, M., & Ghodsi, R. (2023). A model to improve user acceptance of e-services in healthcare systems based on technology acceptance model: an empirical study. *Journal of Ambient Intelligence and Humanized Computing*, 14(6), 7919-7935.
14. Onileowo, T. T. (2024). Integrating blockchain technology with small and medium enterprises (SMEs) for economic development in Africa. *American International Journal of Business Management (AIJBM)*.
15. Onileowo, T. T., Muharam, F. M., & George, I. I. (2024). Unveiling the dynamic interplay of social media's influence on social entrepreneurship. *International Journal of Recent Research in Commerce Economics and Management (IJRRCEM)*, (11)2, 173-186.
16. Onileowo, T. T., Muharam, F. M., & Ramily, M. K. (2022). Financial structure and business development in Southwest Nigeria. *Journal of Hunan University Natural Sciences*, 49(10).
17. Onileowo, T. T., Muharam, F. M., Ramily, M. K., & Khatib, S. F. (2021). The nexus between innovation and business competitive advantage: A conceptual study. *Universal Journal of Accounting and Finance*, 9(3), 352–361.
18. Rampaul, K. (2025). Digital transformation and SME growth in emerging markets. *Journal of Emerging Markets and Management*, 1(1), 15–25.
19. Sujatha, R., & Karthikeyan, M. S. (2021). Determinants of e-commerce adoption: Evidence from small and medium-sized enterprises in India. *International Journal of Business and Society*, 22(2), 574–590.
20. Tu, Y. X., Kubatko, O., Melnyk, L., Li, R., Kovalov, B., & Yaremenko, A. (2025). Economic, institutional and environmental drivers of SMEs' development in the EU: Sustainable development goals perspective. *Environment, Development and Sustainability*, 27(8), 20101–20119.
21. Uche, D. B., Osuagwu, O. B., Nwosu, S. N., & Otika, U. S. (2021). Integrating trust into technology acceptance model (TAM), the conceptual framework for e-payment platform acceptance. *British Journal of Management and Marketing Studies*, 4(4), 34-56
22. Ursavaş, Ö. F. (2022). Unified theory of acceptance and use of technology model (UTAUT). In *Conducting technology acceptance research in education: Theory, models, implementation, and analysis* (111-133). Cham: Springer International Publishing.
23. Younas, A., Shahzad, S., & Inayat, S. (2022). Data analysis and presentation in integrative reviews: A narrative review. *Western Journal of Nursing Research*, 44(12), 1124-1133.