Navigating the Cloud: Security, Compliance, and Risk Challenges in SME Adoption

Nagaraju Kolli[1]

[1]PhD in Information Technology, University of the Cumberlands, Address: 6178 College Station Drive, Williamsburg, KY 40769.

E-mail: [1]kollinagaraju7@gmail.com

Abstract

Cloud computing is an area that can improve the digitalization, performance, and competitiveness of small and medium-sized enterprises. In some cases, however, the failure to embrace security, compliance, and risk management measures can hinder such benefits. Through previous research findings and qualitative studies available in the literature, this paper reviews various issues faced by SMEs after migrating to the cloud. As the analysis of key topics indicates, the subject matter of data breaches and data encryption is of considerable importance for data protection and security. The issues most critical to SMEs, especially with regard to regulatory compliance, are GDPR, PCI DSS, data sovereignty, and auditing. The inability to make internal reforms and integration difficulties of cloud solutions with current systems are hindering the implementation of IT policies. These problems are even more pronounced when there are limited funds and other resources, including a low budget, a lack of understanding of how to use cybersecurity tools, and poorly trained or experienced personnel. This essay calls for anticipatory, tailored cybersecurity measures, formal change management, and reskilling. In order to have a safer and more efficient SME cloud environment, the SMEs, the cloud service providers, and the lawmakers must come together in a multiparty initiative.

Keywords: GDPR, SMEs, PCI, DSS, cybersecurity, Cloud.

DOI: https://doi.org/10.36548/jitdw.2025.3.001
Received: 20.05.2025, received in revised form: 23.06.2025, accepted: 11.07.2025, published: 25.07.2025

1. Introduction

1.2 SMEs Must Use the Cloud

Its application of cloud computing technology has also transformed it, especially for medium and small enterprises. Even though the globe is made up of small and medium enterprises (SMEs), their size is not the same as that of large enterprises, and they barely have the same resources [1]. Small firms nowadays are able to use elastic infrastructure, robust software platforms, and extensive analytics capability that were previously only within the reach of large firms. The reason is that they will not incur capital-intensive on-premises IT costs but will be paying usage-based, on demand. This allows small and medium-sized businesses (SMEs) to go digital for their core competencies, outsource repetitive tasks, and offer sophisticated services that are customer-centric, without ever having dealt with large amounts of cash. Flexible computing capacity and power, memory, and network bandwidth can offer capacity to SMEs to scale up and down more scalably and flexibly than ever before. It will enable them to react in a timely manner to changes in the market, create new business models, and compete in the global market [9].

1.2 Cloud Vulnerabilities That Are Unique to SMEs

While it has some benefits, small and medium-sized enterprises (SMEs) are finding it difficult to embrace cloud technology due to limited resources. They are not even able to buy enterprise-grade cybersecurity software, hire third-party security testers, or hire experts; they have to resort to cheaper and less secure cloud solutions that raise operating expenses and subject them to the risk of huge liabilities in case of a breach. Because of the absence of dedicated security teams and specialized cloud architects, SMEs are unable to keep up with adequately developing systems, figuring out complicated compliance mandates, or responding to incidents. The task of a small group involves executing numerous various things at once, and they do not have time to execute patching, security training, or implement policies, further fueling this skill gap. Small and medium business enterprises lack sufficient chips during negotiations for a favorable deal in regard to Service Level Agreements and security arrangements with the biggest Cloud Service Providers. The coupling of the above factors and inconsistencies in the patching process, inadequately configured firewalls, and unmanaged Bring-Your-Own-Device workflows makes SMEs softer targets. This is because small businesses do not know how attractive they are to opportunistic threat actors because of the security by obscurity belief. This makes it hard for them to prepare

against attacks. The harms breaches inflict on SMEs, both financially and reputations-wise, can be so massive that they will no longer be able to recover and will need to close shop.

1.3 Problem Statement

Though its inherent limitations make it difficult to use safely and effectively, cloud computing may help small and medium-sized businesses save money, be more flexible in their operations, and come up with new ideas. Data security, privacy, and the laws governing cloud systems are all problematic [7]. Combining strong IT policies and procedures with outdated systems can be challenging for small and medium-sized enterprises (SMEs) [25]. Due to significant talent and financial constraints, many SMEs postpone or discontinue their cloud-based initiatives. By limiting small and medium-sized enterprises' access to cloud services and undermining their long-term competitiveness and resilience, this confluence of risks may exacerbate the digital divide [5].

1.4 Structure and Focus of the Research

The research paper examines the main security, compliance, IT policy, and resource issues related to the adoption of cloud technology by SMEs through a qualitative data set via semi-structured questionnaires, a thematic approach, and academic and industry research. Section 3 discusses the process of selecting participants, data collection, and the analysis of the data. The most critical findings are listed in Section 4 and are organized by the largest issues experienced by IT professionals and SME executives. In Section 5, these findings are applied to theoretical and empirical frameworks to examine their meaning. Section 6 provides SME decision-makers, lawmakers, and Cloud Service Providers with detailed instructions on ways to reduce risks and make cloud integration safer. Section 7 concludes by presenting the results of the study and proposals for further research.

2. Methodology Overview

The research methodology to be utilized involves qualitative research that allows for investigating the context-related complex problems that small and medium-sized enterprises (SMEs) encounter during their transition to cloud technology [10]. Through qualitative research, the complexity of the viewpoints of individuals is revealed, as well as problems that are not detected in surveys [27][30]. In this study, we consider the social and technological factors that

influence cloud adaptation, including corporate culture, lack of resources, and perception of risk. This is achieved through interviews with decision-makers of small and medium-sized businesses (SMEs) and IT professionals [10].

We employed a semi-structured method of data collection. Such interviews were structured sufficiently to maintain consistency while also providing the respondents the opportunity to discuss personal issues [10][30]. The most active individuals in making decisions about or implementing cloud technology in their firms were chosen for interviews to gather the opinions of those who were well-informed about both the strategic and operational dynamics of cloud adoption [10]. The respondents discussed various unpredictable issues, such as ad-hoc governance processes, emergent risks in security, and the numerous ways in which constrained resources and a lack of skills can affect the cloud experiences of companies due to the nature of the questions posed [30]. To ensure the selection of security and compliance parameters was rigorous, it was informed by best practices (NIST CSF, GDPR, PCI DSS) and was relevant to typical SME constraints. We strategically incorporated contrasts in company size, industry, and digital maturity to examine how such variables affected their security and compliance issues. The simulation environment included actual data on SMEs collected during interviews and utilized NVivo software to simulate the differences in data under various SME profiles, which can be compared using thematic coding.

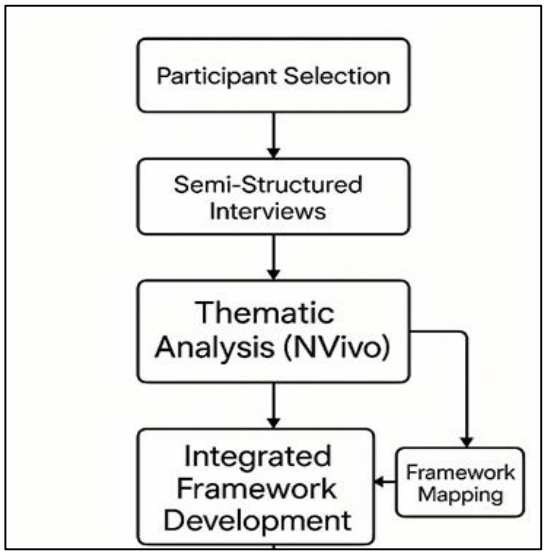

Figure 1. Integrated Frame Work Development

They coded the interview transcripts, generated topics, and refined them through an elaborate thematic analysis approach [32]. Initially, researchers paid attention to the data and created codes depicting significant concepts and patterns. These codes were then consolidated into

initial themes and enhanced over time as they represented a better interpretation of the data and made connections with the narratives of many participants [32]. NVivo software was also used to speed up coding, sorting, and searching of theme fragments to ensure greater rigor and user-friendliness of the analysis, as much quantitative information had to be analyzed without ignoring any detail [29]. The interview technique and the interpretation of themes were based on the Technology-Organization-Environment (TOE) framework and the Technology Acceptance Model (TAM) during the research [27][31]. These lenses enabled us to pose questions about the preparation of an organization, the perceived value of something, and the environmental pressures experienced by an organization. They also helped us unearth some issues specific to small and medium-sized businesses, such as time poverty and threat perception mismatch. Conclusions made in the study are founded on actual evidence, as the study involved theory-driven inquiry and thematic analysis by induction, making it a very rich study that offers a complete view of the cloud adoption issues that small and medium-sized entities encounter when they want to embrace security, compliance, policy, and resource matters.

3. Thematic Analysis of SME Cloud Adoption Issues

Our qualitative study identified four connected topics that represent SMEs' main cloud adoption challenges: security and data protection, compliance and regulation, IT policy implementation and integration, and resource allocation and training issues.

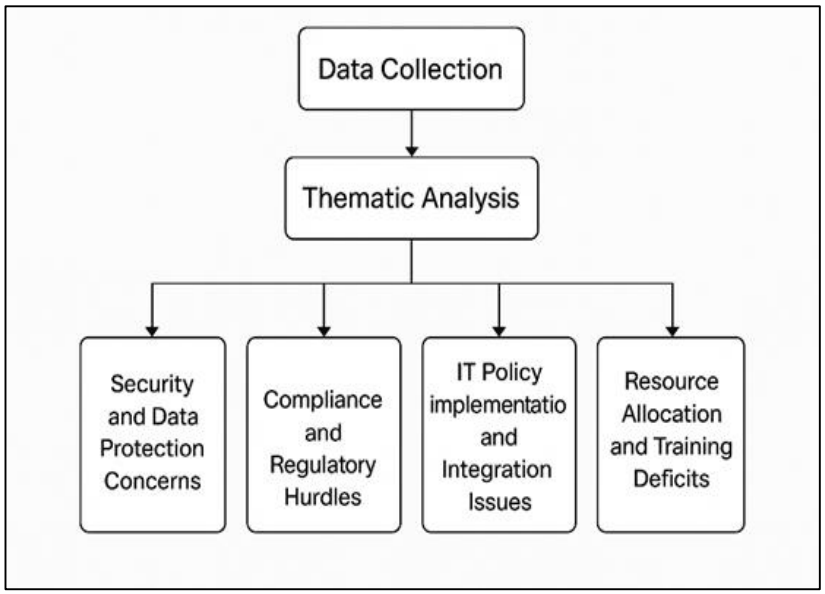

Figure 2. Qualitative Thematic Analysis Workflow

Figure 2 shows the Qualitative thematic analysis workflow which leading to the identification of four principal SME cloud-adoption challenges:

3.1 Data Security and Protection

The largest obstacle to adopting the SME cloud is security [5]. CSPs espouse the security of the infrastructure [14], but SMEs are vulnerable to a variety of threats- poorly configured systems leading to data compromise [18], lax authentication systems enabling unauthorized access [14], and exploding malware and ransomware attacks that can destroy operations and extort money [18 Phishing and social engineering exploit less-trained workers to circumvent technical defenses [2], and employees of SMEs both good and malicious pose internal security threats to sensitive data [1]. The main security threats that SMEs face by embracing cloud services are ransomware attacks, social engineering, account hijack and chain breach in the supply chain. Cloud services can be disabled by DoS attacks and disrupt the working of the companies [14]. Moreover, most SMEs are not even aware of their security status, and they are only able to implement weak security measures regarding encryption and protection policies of keys [18], which cripples CIA. The order of magnitude and the protocols needs a much better security rather than feeling the minor organizations are bound to be safe since the CSPs have their protection [17]. Unless an SME thinks differently, it tends to believe that CSPs take care of all possible levels of security leading to inappropriately configured policies and protection gaps of serious proportions [8].

3.2 Regulation and Compliance Issues

SMEs are denied resources and skills at the level of complex compliance requirements [7]. Sector-specific standards, such as PCI DSS in payments, and more general regulations, such as GDPR, can overwhelm SMEs with both technological and organizational demands [19]. Problems of data sovereignty impede adoption: retention of data across borders gives rise to legal wrangles and confusion over government access demands [11]. Many SMEs do not keep paperwork, tracking, and control documentation that can be used in formal compliance audits [15]. The challenge of making CSP-level certifications (e.g., FedRAMP) satisfy the needs of SMEs adds complexity [8], and reliance on third parties introduces vulnerabilities in supply chains that SMEs are not able to manage with due diligence. Issues of implementation and integration of IT policy persist. Cloud integration requires governance and strategic planning, but SMEs may not have IT rules that apply to the cloud [7]. The fear of job loss, insufficient change management, and a

cultural attachment to historical practices negatively affect the attempt to adopt something new [12]. The option of using the "lift-and-shift" approach, re-platforming, or refactoring to incorporate modern cloud services with fragile legacy systems necessitates careful dependency mapping, planning, and resources to engage in, which are often unavailable to small enterprises [25]. The absence of orderly change-management procedures, including stakeholder communication, training, and support, will exacerbate implementation delays and user dissatisfaction, preventing SMEs from accruing the benefits of cloud adoption [8].

3.3 Resource and Training Gaps

The SMEs are robbed of resources and knowledge due to compliance requirements [7]. The industry-based (i.e., PCI DSS in the case of payments) and the overall legislation (i.e., GDPR) might be too onerous for SMEs to bear [19]. Data sovereignty influences adoption: as long as data are housed in various jurisdictions in other countries, they create clashes of jurisdictions and confusion as to when governments have a right to access the information [11]. The majority of SMEs lack the paperwork, tracking, and control documentation to pass the formal compliance audit [15]. The risks that third-party dependencies pose to the supply chain are much greater than the capacity of SMEs to undertake due diligence, and greater complexity is a factor of concern when it comes to understanding that CSP-level certifications (e.g., FedRAMP) apply to SME requirements [8]. Problems arise in implementing and integrating IT policy. Cloud integration is linked with governance and requires quite a long-term planning, in which case SMEs are often denied the IT regulation regarding the cloud [7]. The three factors (fear of losing jobs, poor change management, and cultural attachment to past practices) make it impossible to have successful adoption efforts [12]. The choice of lift-and-shift, re-platforming, and refactoring models that will integrate legacy systems in a fragile state with currently offered modern cloud services should be accompanied by dependency mapping, as well as planning and resources capable of providing access to small enterprises [25]. The lack of organized change-management processes, such as stakeholder communication, training, and sustainability, aggravates delays in implementation and stakeholder dissatisfaction to the extent that SMEs fail to reap the benefits of the cloud [8].

4. Discussion

The theme analysis shows that small and medium-sized businesses (SMEs) face many problems when they try to use cloud services. There is a systemic vulnerability that cannot be

fixed one component at a time, as security issues, compliance burdens, policy and integration problems, and lack of resources and training are all profoundly connected.

4.1 Putting Together the Different Problems

All other issues are founded on a shortage of resources. Small and medium-sized enterprises (SMEs) are exposed to violations and unauthorized usage due to the fact that they lack sufficient funds or expertise to keep up stringent security controls [14]. The same constraints render it difficult to comply with stringent regulations from a technical as well as financial perspective, causing legal and reputational issues [15]. Also, an absence of skilled workers makes integration of legacy systems more difficult and delays the establishment of well-designed IT governance and change management [7]. Individuals often resist new processes since they are not well-trained or because of poor communication skills. Such challenges trace back to a lack of time and resources [8]. "Resource poverty" impacts technological configurations, individuals' capabilities, and organizational operation. This means that stand-alone solutions, like adding a new firewall, will likely be unsuccessful until broader capacity gaps are bridged.

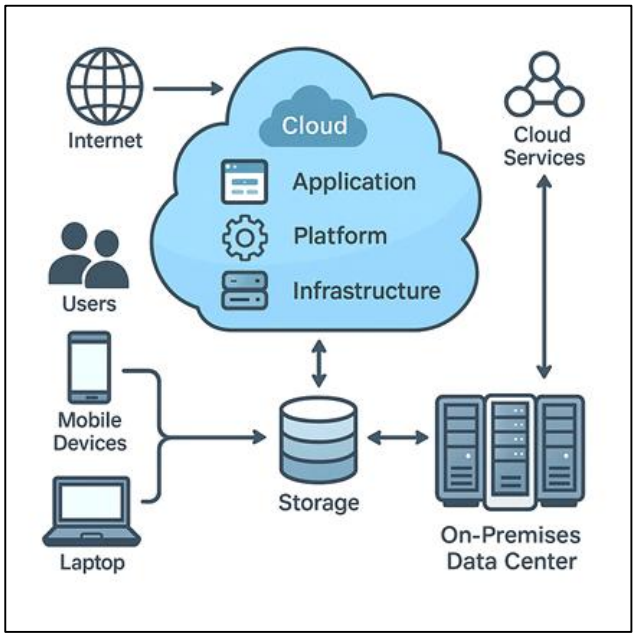

Figure 3. High-Level Cloud Architecture Diagram Showcasing the Key Components and Interactions

4.2 Comparing with Other Research and Literature

The barriers to cloud use identified in our research are the impediments widely reported in the literature on the topic [5][4]. Among them are concerns regarding security and privacy, high

costs, a lack of skilled workers, and compliance. The qualitative evidence, in turn, enhances what we already know by demonstrating how small and medium-sized businesses (SMEs) misunderstand the shared-responsibility model [8] and do not pay significant attention to opportunistic risks because they believe that their size makes them less conspicuous [17]. Most of the research has focused on early adoption decisions, so the problems and long-term effects of adoption are not as well researched [6]. Additionally, size, sector, and digital maturity are often not considered important because much of the research treats SMEs as a homogeneous group [17]. According to our research, more studies are required to gain insight into other types of SMEs and the impact of long-term cloud consumption on performance and resilience.

4.3 Differences Between SMEs and Their Environments

Not all SMEs are same. The resources of microenterprises, the ones of small businesses, and those of medium-sized businesses are rather different, they all have various rules that they must abide by, and technical sophistication [17]. The nature of business you are engaged in will also impact your risk profile and your integration strategy, e.g. a tech consultant who uses SaaS or a manufacturing firm using IaaS to monitor the production. Other factors like whether the places in urban cities have the internet or not may also influence the extent to which people are likely to adopt the cloud technology and the rate at which they do so [17]. The attitudes of leaders and the company culture impact the quality of the adoption as well: the firms that have leadership both supportive of the change and that promotes innovation are more able to adjust to a shift than the firms which are opposed to new ways of operating [11][12]. Such differences demonstrate the necessity of the modification of support programs and vendor services to be tailored to the requirements of the specific SME.

4.4 The Relationship Between SMEs and CSPs

Small and medium-sized businesses (SMEs) and cloud service providers (CSPs) simply do not mix, according to our results. CSPs promote simple, secure services and affordable prices; however, numerous small and medium-sized enterprises (SMEs) face the fact that they are not absolutely secure and need to pay additional fees. This is due to the fact that they lack knowledge about who is answerable to whom, and they do not have many bargaining chips [14][7]. People have less trust due to the fear of vendor lock-in and the lack of clarity regarding pricing mechanisms [16]. Security roles must be well circumscribed, Service Level Agreements must be

clear, and CSPs must be available in the form of packages and practical onboarding support that are tailored to meet the limitations of what smaller buyers can do.

4.5 Theoretical Implications

Combining our findings with those of the Technology-Organization-Environment (TOE) framework, we notice that organizational influences such as resources, skills, and the structure of governance play a vital role in the perceptions of SMEs regarding technological aspects of security, complexity, and compatibility, as well as pressure from the environment in terms of regulation, competitiveness, and vendor support [27]. Similarly, the sense of utility includes lower security risk and compliance demands, while the sense of simplicity is hindered by the incorporation of legacy systems and the absence of trained workers [31]. As demonstrated by our study, existing models need to be broadened to encompass resources and capacity to accurately reflect the experiences of SMEs in adopting cloud technology. The choice of deployment model for the cloud whether public, private, or hybrid has significant implications for the security of SMEs. Public clouds are scalable, yet they expose SMEs to multi-tenant risks. In summary, we require a comprehensive plan that can formulate technical safeguards, better prepare organizations, clarify legal routes, and foster collaboration between small businesses and cloud service providers to help them overcome the challenges surrounding cloud computing adoption. It is only through addressing these interrelated issues that SMEs can leverage the revolutionary nature of cloud computing.

5. Suggestions: How to Reduce the Risks of Small and Medium-Sized Businesses using the Cloud

To deal with security, compliance, integration, and resource challenges, SMEs, policymakers, and CSPs need to work together. Table 1 shows the best ways to do things.

Table 1. Recommended Cloud Adoption Best Practices for SMEs

Category	Recommendation	Key Supporting Actions / Examples
Cybersecurity Strategy	Adopt a Proactive, Risk-Based Approach	• Conduct regular risk assessments (e.g., NIST RMF) • Use security frameworks (e.g., NIST CSF, FISCCS) • Develop and test an incident response plan (NIST SP 800-61)

Technical Controls	Implement Layered Security Defenses	• Encrypt data at rest and in transit (AES-256, TLS 1.2+) • Enforce IAM with MFA, RBAC, least privilege • Apply regular patching, secure configurations, firewalls, WAFs • Backups
Compliance Management	Integrate Compliance into Operations	• Map applicable regulations (GDPR, HIPAA, PCI DSS) • Select CSPs with relevant certifications • Build controls into processes • Prepare documentation for audits
IT Policy & Integration	Establish Clear Governance & Plan Migration	• Define cloud usage policies (access, data handling, BYOD) • Conduct dependency mapping • Select migration strategy (6 Rs) • Plan for legacy integration or retirement
Change Management	Implement Structured Change Management	• Use established models (Kotter's 8-Step, ADKAR) • Secure leadership sponsorship • Communicate vision and benefits clearly • Provide ongoing support and feedback channels
Training & Awareness	Foster a Security-Aware Culture	• Deliver regular, role-based security training • Focus on common threats (phishing) • Use simulations and gamification • Reinforce learning through management support
Resource Management	Optimize Resources & Leverage Support	• Monitor and forecast cloud costs • Automate routine tasks • Engage Managed Security Service Providers (MSSPs) • Explore government funding and SME grants
Vendor Management	Choose CSPs Wisely & Manage Relationships	• Evaluate CSP security, compliance track record, and SLAs • Clarify shared-responsibility roles • Negotiate clear contract terms • Plan exit strategies to avoid lock-in

5.1 Cybersecurity for SMEs that is Proactive

SMEs ought to use risk-based security as opposed to reactive protection. The rankings of controls using controls recommended by NIST RMF or FISCCS frameworks are done by

ranking of the controls by important cloud assets, threats, and weaknesses through systematic risk assessments [4]. The data should be encrypted (e.g. AES-256), IAM should be complete (e.g. MFA, RBAC, least privilege), settings should be secure, firewalls should be deployed, and updates should be installed regularly [14]. Problems can be identified early through continuous monitoring and vulnerability checks performed with NSEMs that are lightweight or done by a CSP [14]. Lastly, recovery is possible after breaching, as a result of having an incident response plan and practicing it with ease [4].

5.2 Successful Change Management and Learning New Skills

Structured organizational change should be incorporated with technical steps. Formal change-management systems such as Kotter's 8-Step and ADKAR ensure that executives are on board, roles are defined, and staff is engaged [8]. Keeping people on board with the cloud by providing feedback loops and clearly communicating the aims and methods of adopting the cloud or the consequences of not doing so would reduce the chance that they act against it [8]. Employees of small and medium-sized businesses should always be trained on the relevant aspects of their jobs. Frequent practical seminars with information on phishing, password management, and data organization can ensure that people make fewer errors [1]. Through business training, individual consultancies, or government-supported projects, technical personnel can learn how to enter and protect the cloud [14].

5.3 Policy and Support Systems

Policymakers and industry organizations could simplify the process of adopting cybersecurity for individuals by offering grants or tax credits for investments and training [14]. Tips specific to small and medium-sized businesses (such as the simplified ENISA or NIST guides) and low-cost expertise (such as CISO-as-a-Service) are assisting organizations in becoming prepared [4]. They allow small businesses to save costs by using clear SLAs, better shared-responsibility documents, security bundles, and fixed-price packages that enable them to avoid surprise costs [7]. Standardized pre-approved cloud setups and transparent regulations regarding data sovereignty between neighboring countries will help small and medium-sized businesses easily comply with the regulations.

6. Future Directions

The potential results of the process of cloud adoption on the resilience of SMEs in the long term should be explored in future studies; sector-specific research and the possible impact of AI-based security tools should be discussed. Additionally, investigating the effectiveness of automated compliance systems and recommending specific policy changes can offer practical information to practitioners and policymakers.

7. Conclusion

SME migration to the cloud is challenging. SMBs enjoy many benefits, but they operate under challenges that necessitate them to thrive on competitive, low cost, efficiency, and scalability. The major issues include security, protection of data, adherence to laws, implementation of IT policies, integration of legacy systems, worldwide availability of resources, and absence of training. This research utilizes up-to-date and qualitative data collection. All these issues are interlinked, as noted in the study. SME capabilities and budgets do not allow them to implement thorough security practices or satisfy the requirements of sophisticated regulations, and move outdated systems and enhance security consciousness. Projections do not account for resources and are insecure. The discontents cannot be tackled at large because SMEs differ in size, sector, readiness to go digital, and location. It is important to monitor and reduce risks. SMEs should be keen on cybersecurity breaches backed by risk and technology controls as well as IT governance. The human element must be countered through cybersecurity awareness training and coordination of organizational change management for all employees. Efforts no matter how good cannot help SMBs address these issues. SMEs need to be advised, funded, and informed by policymakers. These aspects are supported by cloud providers, responsibility mapping, transparency, and service agreements. It is shown in one of the studies that SMEs are faced with issues regarding cloud services. Direction is situational and is crucial. The qualitative data of the study, coupled with the literature review, restrict the findings. Future research should examine the problems of SMEs, success in training and awareness, and long-term performance and resilience of cloud adoption.

References

[1] Duke IoW Team. (n.d.). Technology Adoption in Public Agencies. Duke Nicholas Institute. https://dukespace.lib.duke.edu/items/07f5b391-3e32-4fdf-a67e-790cd13fcda0

[2] Ssekakubo, J., Suleman, H., & Marsden, G. (n.d.). Issues of Adoption of Cloud Computing in SMES in Uganda: The Case Study of Kampala District. Social Science and Humanities Journal.

[3] Mun, Y. P., Khalid, H., & Nadarajah, D. (n.d.). Review of Technology Adoption Models and Theories. Journal of Information Systems and Technology Management. https://hal.science/hal-03741843/document

[4] Venkatesh, Viswanath, and Susan A. Brown. "A longitudinal investigation of personal computers in homes: Adoption determinants and emerging challenges." MIS quarterly (2001): 71-102.

[5] Zolas, Nikolas, Zachary Kroff, Erik Brynjolfsson, Kristina McElheran, David N. Beede, Cathy Buffington, Nathan Goldschlag, Lucia Foster, and Emin Dinlersoz. Advanced technologies adoption and use by US firms: Evidence from the annual business survey. No. w28290. National Bureau of Economic Research, 2021.

[6] Adam, Rubina & Kotzé, Paula & Van der Merwe, Alta. (2011). Acceptance of Enterprise Resource Planning Systems by Small Manufacturing Enterprises. ICEIS 2011 - Proceedings of the 13th International Conference on Enterprise Information Systems. 1. 229-238.

[7] Adane, Martin. "Business-driven approach to cloud computing adoption by small businesses." African Journal of Science, Technology, Innovation and Development 15, no. 2 (2023): 166-174.

[8] Oliveira, Tiago, Manoj Thomas, Goncalo Baptista, and Filipe Campos. "Mobile payment: Understanding the determinants of customer adoption and intention to recommend the technology." Computers in human behavior 61 (2016): 404-414.

[9] ResearchGate. (n.d.). Figure 1: The theoretical framework of innovation adoption based on SCT. https://www.researchgate.net/figure/The-theoretical-framework-of-innovation-adoption-based-on-SCT_fig1_235272333

[10] Al-rahmi, A. M., Shamsuddin, A., & Al-rahmi, W. M. (2019). META: A model for emerging technology adoption. Journal of Information and Knowledge Management, 18(02).

[11] Edward, M., & Bakkabulindi, F. E. K. (2014). A call for Return to Rogers' Innovation Diffusion Theory. Makerere Journal of Higher Education, 6(1), 61-76.

[12] Centre for International Business University of Leeds (CIBUL). (n.d.). Policy Implications from IDT4UKSME Project. University of Leeds.

[13] Lee, Yvonne, WeiLee Lim, and Ho Sai Eng. "A systematic review of UTAUT2 constructs' analysis among MSMEs in non-OECD countries." Journal of Science and Technology Policy Management 15, no. 4 (2024): 765-793.

[14] Guo, Qin & Huang, Wei. (2024). Analyzing the Diffusion of Innovations Theory. Scientific and Social Research. 6. 95-98. 10.26689/ssr.v6i12.8947.

[15] Alomari, Ali & Abdullah, Nasuha. (2023). Factors influencing the behavioral intention to use Cryptocurrency among Saudi Arabian public university students: Moderating role of financial literacy. Cogent Business & Management. 10.

[16] Alwreikat, Asma, Ahmed Maher Khafaga Shehata, and Mohammed Khair Abu Zaid. "Arab scholars' acceptance of informal scholarly communication tools: applying the technology acceptance model 2 (TAM2)." Global Knowledge, Memory and Communication 72, no. 1/2 (2023): 160-178.

[17] Rogers, Alan D. Examining small business adoption of computerized accounting systems using the technology acceptance model. Walden University, 2016.

[18] Diffusion of Innovations Theory. Investopedia. Retrieved from https://www.investopedia.com/terms/d/diffusion-of-innovations-theory.asp

[19] Rana, Nripendra P., and Yogesh K. Dwivedi. "Citizen's adoption of an e-government system: Validating extended social cognitive theory (SCT)." Government Information Quarterly 32, no. 2 (2015): 172-181.

[20] Thong, James YL. "An integrated model of information systems adoption in small businesses." Journal of management information systems 15, no. 4 (1999): 187-214.

[21] Plageras, Antonios, Apostolos Xenakis, Konstantinos Kalovrektis, and Denis Vavougios. "An Application Study of the UTAUT Methodology for the Flipped Classroom Model Adoption by Applied Sciences and Technology Teachers." Int. J. Emerg. Technol. Learn. 18, no. 2 (2023): 190-202.

[22] Priyadarshinee, Pragati. "Impact of Fog Computing on Indian Smart-Cities: An Empirical Study." (2021).

[23] Basu, Aveek, Sraboni Dutta, and Rohini Jha. "A comprehensive approach to study the adoption and implementation of cloud-based ERP among SMEs." International Journal of Business Information Systems 42, no. 3-4 (2023): 305-330.

[24] Williams, Michael D., Nripendra P. Rana, and Yogesh K. Dwivedi. "The unified theory of acceptance and use of technology (UTAUT): a literature review." Journal of enterprise information management 28, no. 3 (2015): 443-488.

[25] Taiminen, Heini Maarit, and Heikki Karjaluoto. "The usage of digital marketing channels in SMEs." Journal of small business and enterprise development 22, no. 4 (2015): 633-651.

[26] Singh, Gavin. "Technology Acceptance Model (TAM) and Use and Adoption of Technology by Small Business Owners in Queens, NY." (2022).

[27] Adane, Martin. "Cloud computing adoption: Strategies for Sub-Saharan Africa SMEs for enhancing competitiveness." African Journal of Science, Technology, Innovation and Development 10, no. 2 (2018): 197-207.

[28] Nan, Zhang, G. XUNHUA, and C. GUOQING. "IDT-TAM INTEGRATED MODEL FOR IT ADOPTION." (2008): 510-523.

[29] Soomro, K. A., Shah, N., & Memon, Z. A. (2023). Factors influencing the intention to adopt digitalization among SMEs in Europe. Asia-Pacific Journal of Business Administration, 16(2), 274-295.

[30] Wang, Y. M., Wang, Y. S., & Yang, Y. F. (2017). Understanding the Determinants of Blockchain Technology Adoption for Business Process Management. Proceedings of the 17th International Conference on Electronic Business. https://www.mdpi.com/2075-5309/12/10/1709

[31] Susanty, Aries & Puspitasari, Nia Budi & Siahaan, Geovany & Setiawan, Sigit & Syafrudin, Muhammad. (2025). Factors influencing the intention of textile and garment SMEs to adopt digital technologies and its impact on performance. Scientific Reports. 15.

[32] Techaisle. (n.d.). 5 SMB Cloud Adoption Lessons for Success. https://techaisle.com/cloud-reports/5-smb-cloud-adoption-lessons-for-success

[33] Yeboah-Boateng, Ezer Osei, and Kofi Asare Essandoh. "Factors influencing the adoption of cloud computing by small and medium enterprises in developing economies." International Journal of Emerging Science and Engineering 2, no. 4 (2014): 13-20.

[34] Ratten, Vanessa. "International consumer attitudes toward cloud computing: a social cognitive theory and technology acceptance model perspective." Thunderbird International Business Review 57, no. 3 (2015): 217-228.