Int Journal of Social Sciences Management and Entrepreneurship 10(1): 27-38 2026

ISSN 2411-7323

www.sagepublishers.com

DEVELOPMENT OF AN EASY-TO-USE CYBERSECURITY FRAMEWORK FOR SAFE AND EFFECTIVE IOT ADOPTION AMONG SMES IN NAIROBI COUNTY CBD, KENYA

[1] Ouma, Benard Okoth, [2]Mr. Nyairo Evanson, [3]Mr. Nyakoni Omwando

[1]Degree of Master of Science in Computer Information Systems of Kenya Methodist University

[2,3] Lecturers, Kenya Methodist University

ABSTRACT

Although the Internet of Things (IoT) provides SMEs with opportunities to enhance efficiency and competitiveness, adoption in developing-country contexts remains constrained by cybersecurity threats, financial limitations, organizational readiness gaps, and external environmental challenges. This study examined determinants of IoT adoption among SMEs operating within Nairobi County's Central Business District (CBD) and developed an easy-to-use cybersecurity framework to support safe and effective adoption. A descriptive survey design was used, with data collected from 393 SMEs through stratified sampling, producing 354 valid responses. Descriptive statistics, Pearson correlation analysis, and multiple regression modelling were employed to test the influence of cybersecurity and technological, financial, organizational, and external environmental factors on IoT adoption. The findings indicate that all determinants significantly influence IoT adoption, with organizational factors emerging as the strongest predictor, followed by cybersecurity and technological determinants, while financial and external environmental factors showed moderate but statistically significant effects. Based on these empirical results, the study developed a structured cybersecurity framework that translates statistically significant adoption determinants into a practical decision-support guide integrating organizational readiness, cybersecurity preparedness, financial feasibility, and external environmental support. The framework positions cybersecurity as a core enabler of adoption and provides SMEs with a pathway for secure, sustainable, and scalable IoT implementation. The study contributes context-specific empirical evidence and offers practical implications for SME managers, policymakers, and technology providers promoting secure IoT adoption in developing economies.

Keywords: cybersecurity framework; IoT adoption model; SMEs; digital innovation; regulatory environment; Kenya.

Background of Study

The Internet of Things (IoT) is increasingly transforming business operations by enabling sensor-based monitoring, automation and real-time analytics across sectors, allowing organizations to optimize operations and enhance decision-making (Tudor et al., 2024). Globally, IoT adoption continues to rise and is increasingly viewed as a strategic pillar of digital transformation because it can support efficiency improvement, customer engagement and value innovation (Lu, 2021; Munasser, 2024). SMEs are especially positioned to benefit from IoT-driven transformation because of their need for flexible and efficient systems that support cost-effective growth and responsiveness to market dynamics (Sallam et al., 2023).

In Kenya, SMEs represent a critical pillar of socioeconomic development, employment creation and national progress. However, SMEs often struggle to achieve full-scale digital transformation due to limited financial resources, inadequate infrastructure, and constrained organizational capacity (De Silva et al., 2021; Neyole et al., 2024). Although Nairobi County CBD provides a commercially vibrant environment with relatively advanced ICT infrastructure compared to other parts of Kenya, IoT adoption among SMEs remains low. This indicates the existence of persistent adoption barriers, including lack of technical expertise, limited access to financing, weak organizational readiness and uncertainty regarding regulatory environments (Ochieng et al., 2023; Peretz-Andersson et al., 2024).

Beyond these traditional barriers, cybersecurity threats pose a critical risk to IoT adoption sustainability. SMEs face increasing exposure to cyber incidents such as malware attacks, ransomware, phishing and data breaches, which may undermine business continuity, finances and reputation (Benjamin, 2024). IoT adoption increases this exposure because IoT ecosystems introduce multiple connected entry points, creating significant vulnerabilities if not properly secured. This makes cybersecurity not simply a risk to be managed after adoption, but a foundational requirement to enable safe and effective implementation. Consequently, without an adoption framework that integrates cybersecurity into implementation stages, SMEs risk adopting IoT in ways that may undermine rather than improve performance.

While prior studies have examined technology adoption barriers in SMEs, the existing scholarship provides limited actionable guidance on how SMEs in developing economies can integrate IoT solutions safely amid operational constraints. Specifically, there is limited evidence on adoption frameworks tailored to urban SME environments like Nairobi CBD that incorporate cybersecurity readiness assessment alongside organizational, financial and regulatory determinants. This knowledge gap implies that even when SMEs recognize the potential value of IoT, the absence of structured guidance prevents them from transitioning from intention to practical implementation.

Therefore, developing an easy-to-use cybersecurity-driven IoT adoption framework is critical to support SMEs in Nairobi CBD. Such a framework can offer SMEs structured steps for assessing readiness, planning adoption, implementing IoT controls and securing IoT ecosystems. This provides a practical mechanism through which SMEs can harness IoT opportunities while minimizing cybersecurity vulnerabilities and operational risks.

Statement of the Problem

The adoption of Internet of Things (IoT) technologies has become central to modern business competitiveness due to its capacity to support real-time analytics, automation and operational efficiency. Nevertheless, SMEs in Nairobi County's Central Business District (CBD) have not adopted IoT at the expected pace despite their potential to benefit from digital innovation (Lu, 2021). Multiple challenges hinder adoption, including financial limitations, inadequate infrastructure, limited access to digital financing, lack of technical expertise and escalating

cybersecurity threats (Benjamin et al., 2024; CAK, 2024). These barriers undermine SMEs' ability to design structured, secure and sustainable IoT integration processes.

Empirical evidence suggests that SMEs in Kenya experience persistent obstacles in digital transformation, particularly regarding device affordability, high internet costs, limited digital skills and cybersecurity risks (CAK, 2024; CIPE, 2021). Further, studies on digital business uptake in Nairobi reveal that a substantial proportion of SMEs lack formal digital strategies, which weakens their ability to implement advanced digital systems such as IoT in a structured manner (Noyele et al., 2024). As a result, IoT adoption is not only constrained by access challenges but also by the absence of systematic guidance on how SMEs can integrate IoT technologies safely while managing cyber risks.

Although previous studies (IOSR, 2023; CIPE, 2021) highlight digital adoption constraints in SMEs, there is limited research offering a structured and easy-to-use cybersecurity-driven framework that SMEs in Nairobi CBD can apply to support safe and effective IoT adoption. Without such a framework, SMEs remain exposed to implementation failure and security vulnerabilities, which may worsen operational and reputational risks rather than improve firm performance. Therefore, there is a need to develop a practical cybersecurity framework that integrates cybersecurity readiness assessment with key adoption determinants to support secure IoT diffusion among SMEs in Nairobi County CBD.

Purpose / Aim of the Study

The purpose of this study is to develop an easy-to-use cybersecurity framework that integrates cybersecurity, organizational, financial and regulatory determinants to support safe and effective adoption of Internet of Things (IoT) technologies among Small and Medium Enterprises (SMEs) in Nairobi County's Central Business District (CBD), Kenya.

Objectives of the Study

This study was guided by the following objectives:

1. To integrate key determinants influencing IoT adoption among SMEs in Nairobi County CBD into a structured adoption framework.
2. To develop an easy-to-use cybersecurity framework that supports safe and effective IoT adoption among SMEs in Nairobi County CBD.

Research Questions

1. What determinants should be prioritized in designing a safe IoT adoption framework for SMEs in Nairobi County CBD?
2. How can an easy-to-use cybersecurity framework be developed to facilitate safe and effective IoT adoption among SMEs in Nairobi County CBD?

Theoretical Framework (DOI Theory)

This study is guided by the Diffusion of Innovation (DOI) Theory developed by Rogers (2003), which explains how an innovation spreads through a social system over time via communication channels. DOI views adoption as a staged process involving knowledge, persuasion, decision, implementation, and confirmation. The theory further explains that adoption is influenced by the perceived characteristics of an innovation, namely relative advantage, compatibility, complexity, trialability, and observability.

IoT adoption among SMEs involves organizational decision-making under uncertainty, where firms must evaluate IoT value and determine whether adoption aligns with existing business processes and capabilities. Relative advantage explains how SMEs assess whether IoT improves efficiency, reduces costs, or strengthens customer engagement compared to traditional practices. Compatibility explains whether IoT aligns with SMEs' operational routines and infrastructure. Complexity addresses the perceived difficulty in implementing and maintaining IoT systems, while trialability and observability influence whether SMEs can test IoT solutions on a small scale and observe benefits within their business environment.

DOI is particularly suitable for informing the development of an easy-to-use cybersecurity framework because framework design must reflect adoption stages and address factors that reduce uncertainty and perceived complexity. By using DOI, the framework can guide SMEs through a structured pathway: awareness creation, persuasion through value demonstration, decision support, implementation safeguards (including cybersecurity), and reinforcement mechanisms for sustained IoT usage. Consequently, DOI provides a systematic theoretical basis for constructing a practical framework that enables safe and effective diffusion of IoT technologies among SMEs in Nairobi County CBD.

Empirical Review

The widespread IoT adoption has become famous in multiple industries. However, it still faces problems like usability, scalability, and cybersecurity issues as most organizations choose to use it rather than others. IoT allows institutions to increase the effectiveness of operations, service levels, and data-driven resolutions for businesses in several ways. However, the effective incorporation of IoT would need a trusted and easy-to-deploy framework to cut deployment expenses and attract users. In simple terms, the Technology Acceptance Model (TAM) identifies two main factors that drive technology adoption: perceived ease of use and perceived usefulness. When it comes to IoT, businesses are more likely to adopt technologies that are easy to use and clearly demonstrate practical benefits, especially if they don't require advanced technical skills. Through achieving well-developed visual interfaces, setting up automatic configurations, and enabling the use of different devices, the organization will succeed in ease of use, resulting in the fast adoption of the tech (Faiz, Le, & Masli, 2024).

In the same breath, the Diffusion of Innovation (DOI) theory presupposes that IoT follows a progression influenced by first users, who determine the broader acceptance in the market by their activities. Masli (2024) states that companies with a strong innovative culture can implement IoT solutions better. Omoyiola (2019) also finds that relative advantages, compatibility, and trialability are among the main factors on which the adoption of IoT is based. Thus, any well-developed IoT framework should comprise piloting testing stages, knowledge-sharing mechanisms, and incremental scaling to be compatible with organizational needs.

From a strategic point of view, Resource-Based View (RBV) theory is based on the factors of firm-specific resources that result in a competitive advantage First, Zhukabayeva et al. (2025) propose that organizations with good digital infrastructure, the necessary qualified personnel, and IoT-specific capabilities such as cybersecurity measures, big data analytics, and edge computing are the beneficiaries at the end of the day. Meanwhile, a study by (Karthikeyan, 2024; Willie, 2024) has discovered that firms can make IoT applications highly efficient by adequately utilizing their unique IT resources, giving them the power to establish stable competitive differences.

According to Sallam et al. (2023), a structured IoT adoption framework should focus on simplified deployment strategies, user-centric designs, organizational readiness, and resource optimization to narrow the gap between IoT's theoretical potential and practical implementation. Research by De Silva et al. (2021) highlights the importance of aligning

technological innovations with business objectives to ensure long-term viability. Moreover, companies that integrate standardized IoT adoption processes, combined with effective resource utilization, experience higher efficiency in implementation (Udeh et al., 2024). By leveraging insights from prior research, this study aims to develop an accessible, scalable, and user-friendly IoT adoption framework that ensures sustainable adoption across various industry contexts.

Conceptual Framework

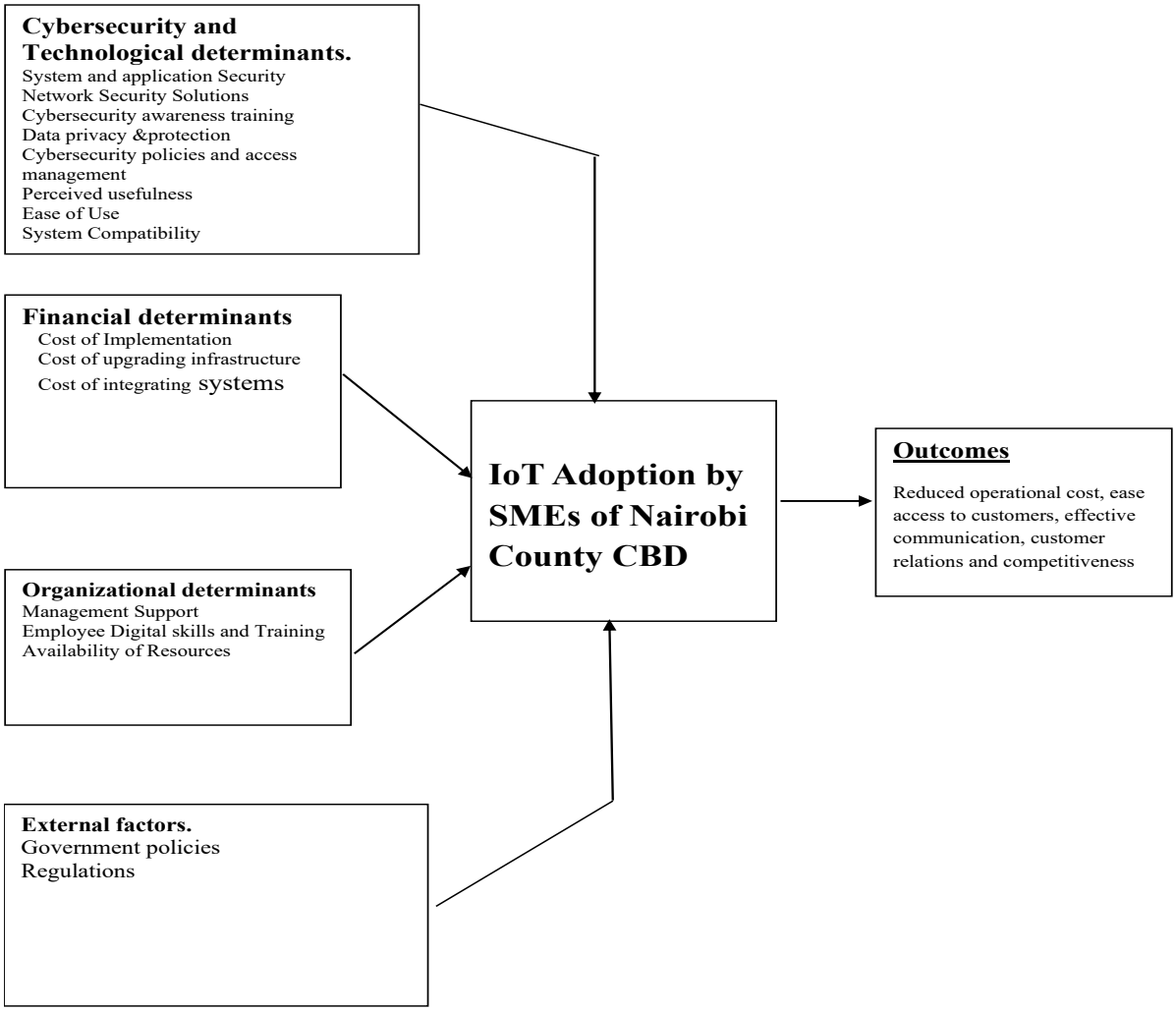


Figure 1: ***The conceptual framework: source (Benard, 2025)***

RESEARCH METHODOLOGY

This study employed a descriptive survey design combined with correlational research procedures to generate empirical evidence for the development of an easy-to-use cybersecurity-driven framework to support IoT adoption among SMEs in Nairobi County CBD. The descriptive survey design enabled systematic assessment of SMEs' status in relation to cybersecurity, financial, organizational, and regulatory determinants of IoT adoption while maintaining the natural business setting (Creswell & Creswell, 2023). The correlational component strengthened the methodological approach by establishing relationships among

adoption determinants and the level of IoT adoption, which is essential when developing a structured framework grounded in empirical predictor strength rather than assumptions (Gershman & Ullman, 2023).

The target population comprised 21,000 licensed SMEs operating in Nairobi CBD (KNCCI, 2021). Respondents were drawn from SME owners, senior managers, and IT decision-makers because they possess the responsibility and authority to implement technology-based change, manage resource allocation, and enforce internal cybersecurity governance (Padash, 2020). The study used stratified random sampling to ensure inclusion of SMEs from diverse business sectors, with a total sample size of 393 SMEs determined using Yamane's (1967) formula at a 5% precision level.

Primary data were collected through a structured questionnaire organized into sections measuring cybersecurity and technological determinants, financial determinants, organizational readiness determinants, external environmental determinants, and IoT adoption levels. A five-point Likert scale facilitated objective measurement of perceptions and readiness conditions across constructs. The questionnaire was pre-tested using a small subset of SMEs (approximately 10 SMEs) to refine items and improve clarity before full data collection. Instrument robustness was ensured through expert review to support content validity and Cronbach's alpha reliability testing to confirm internal consistency of measurement scales, with coefficients of 0.70 and above considered acceptable (Rosli et al., 2021). Data analysis was conducted using SPSS version 27, applying descriptive statistics, correlation analysis, and multiple regression modelling to generate evidence that informed development of the cybersecurity framework for safe IoT adoption.

RESULTS AND DISCUSSION

The study sought responses from 393 SMEs within Nairobi County's Central Business District to generate evidence necessary for the development of an easy-to-use cybersecurity framework for IoT adoption. A total of 362 questionnaires were returned, but 8 were incomplete and excluded from the dataset. This resulted in 354 valid questionnaires, representing an overall response rate of 90.1%. This return rate is considered exceptionally strong and provides adequate empirical support for the framework development process, since high response rates reduce non-response bias and strengthen representativeness of findings (Saunders et al., 2019).

Correlation Analysis

Pearson correlation analysis was conducted to examine the relationships between cybersecurity and technological factors, financial determinants, organizational readiness determinants, external environmental determinants, and IoT adoption among SMEs in Nairobi County CBD. Correlation coefficients were interpreted such that coefficients below 0.30 represent weak relationships, 0.30–0.49 represent moderate relationships, 0.50–0.69 represent strong relationships, and values of 0.70 and above represent very strong relationships. This analysis was important because it provides preliminary statistical evidence of association and supports the inclusion of predictors into regression models used to identify determinants with the strongest explanatory power for framework development (AlHogail, 2021; Kraus et al., 2021).

Table 1: Pearson Correlation Matrix of Study Variables

Variable		IoT Adoption	Cybersecurity & Technological	Financial Factors	Organizational Factors	External Environmental
IoT Adoption	Pearson Correlation	1				
	Sig. (2-tailed)					
	N	354				
Cybersecurity & Technological Factors	Pearson Correlation	.642**	1			
	Sig. (2-tailed)	.000				
	N	354	354			
Financial Factors	Pearson Correlation	.538**	.312	1		
	Sig. (2-tailed)	.000				
	N	354	354	354		
Organizational Factors	Pearson Correlation	.671**	.383	.147	1	
	Sig. (2-tailed)	.000	.074	.113		
	N	354	354	354	354	
External Environmental Factors	Pearson Correlation	.589**	.268	.196	.221	1
	Sig. (2-tailed)	.000	.123	.412	.098	
	N	354	354	354	354	354

Note: Correlation is significant at the 0.05 level (2-tailed).

The results demonstrated that all independent variables were strongly and positively associated with IoT adoption. Specifically, cybersecurity and technological factors were strongly correlated with adoption ($r = 0.642$, $p < 0.01$), indicating that higher cybersecurity awareness and technological readiness increase the likelihood of IoT adoption, consistent with the view that security considerations shape adoption decisions in connected digital systems (AlHogail, 2021). Financial factors were also strongly and positively correlated with IoT adoption ($r = 0.538$, $p < 0.01$), implying that access to financial resources, affordability of IoT systems, and return expectations encourage adoption, consistent with prior evidence that financing flexibility predicts technology uptake among SMEs in developing economies (Afolayan et al., 2022). Organizational factors exhibited the strongest relationship with IoT adoption ($r = 0.671$, $p < 0.01$), reinforcing the importance of internal capability, management support, staff readiness, and infrastructure preparedness as drivers of adoption (Kraus et al., 2021). External environmental factors were also strongly correlated with IoT adoption ($r = 0.589$, $p < 0.01$), suggesting that regulation, infrastructure availability, customer expectations, and vendor support exert significant influence on SMEs' decisions to adopt IoT (Rymaszewska et al., 2021).

Additionally, correlations among the independent variables were positive but largely moderate (below 0.50), indicating that while adoption determinants relate to each other, they do not exhibit excessive multicollinearity. This implies that each predictor reflects a distinct dimension of IoT adoption and is suitable for inclusion in multiple regression analysis. Therefore, the correlation analysis provided a strong preliminary justification for subsequent regression modelling to identify predictor strengths and guide development of the cybersecurity framework for safe IoT adoption (AlHogail, 2021; Kraus et al., 2021).

Develop an Easy-to-Use Cybersecurity Framework for IoT Adoption

The specific objective of the study was to develop an easy-to-use cybersecurity framework that supports safe and effective adoption of Internet of Things (IoT) technologies among Small and Medium Enterprises (SMEs) in Nairobi County Central Business District. A multiple regression analysis was carried out on cybersecurity and technological factors, financial factors, organizational factors, and external environmental factors to determine their combined effect on IoT adoption. The determination of the p-values, which were less than 0.05 and within the acceptable margin of error, was used to establish the significance of the results. The results from the multiple regression analysis formed the basis for the proposed cybersecurity framework for the study as indicated below.

Table 2: ANOVA Results

Model	Sum of Squares	df	Mean Square	F	Sig.
Regression	121.864	4	30.466	239.890	0.000
Residual	44.136	349	0.127		
Total	166.000	353			

a. Predictors: (Constant), Cybersecurity and Technological Factors, Financial Factors, Organizational Factors, External Environmental Factors

The ANOVA results indicate that the regression model is statistically significant ($F = 239.890$, $p < 0.05$), confirming that the independent variables jointly explain variations in IoT adoption among SMEs. The high F-statistic demonstrates that the combined model provides a substantially better fit than a model without predictors, thereby validating its appropriateness for hypothesis testing and inference. This finding is consistent with empirical evidence suggesting that technology adoption among SMEs is best explained through integrated analytical models that simultaneously account for technological capability, organizational readiness, financial capacity, and environmental context rather than single-factor explanations (Ghobakhloo & Ching, 2019; Venkatesh et al., 2022).

Table 3: Regression Coefficients

Variable	B	Std. Error	β (Standardized)	t-value	Sig.
Constant	0.412	0.168	,	2.452	0.015
Cybersecurity & Technological Factors	0.351	0.036	0.384	9.750	0.000
Financial Factors	0.226	0.033	0.248	6.848	0.000
Organizational Factors	0.402	0.039	0.436	10.308	0.000
External Environmental Factors	0.271	0.031	0.302	8.742	0.000

The findings in Table 2 and Table 3 indicate that cybersecurity and technological factors, financial factors, organizational factors, and external environmental factors are significant in influencing IoT adoption among SMEs as shown in the regression model below.

$$Y = 0.412 + 0.351X_1 + 0.226X_2 + 0.402X_3 + 0.271X_4$$

Where:

X_1 = Cybersecurity and Technological Factors
X_2 = Financial Factors
X_3 = Organizational Factors
X_4 = External Environmental Factors

As shown in Table 3, the coefficients of all independent variables are statistically significant at $p < 0.05$, indicating that improvements in these determinants lead to increased levels of IoT adoption among SMEs.

The regression results provide strong empirical justification for the structure and sequencing of the proposed easy-to-use cybersecurity framework for IoT adoption among SMEs in Nairobi County Central Business District. The statistical significance of all four determinants confirms that IoT adoption is influenced by a system of interacting organizational, technological, financial, and environmental factors.

Organizational factors emerged as the strongest predictor of IoT adoption ($\beta = 0.436$), indicating that internal readiness, including management support, employee digital skills, training, and availability of resources, forms the foundation for adoption. This suggests that SMEs must first establish internal capacity before engaging in IoT deployment.

Cybersecurity and technological factors demonstrated a strong and significant influence on IoT adoption ($\beta = 0.384$), confirming that secure, compatible, and usable systems directly affect adoption decisions. These finding positions cybersecurity readiness as a core determinant that must be embedded throughout the IoT adoption process.

Financial factors were also statistically significant ($\beta = 0.248$), indicating that cost considerations, access to finance, and expected returns influence the scale and sustainability of IoT implementation. However, their comparatively lower coefficient suggests a moderating role rather than a primary driving role.

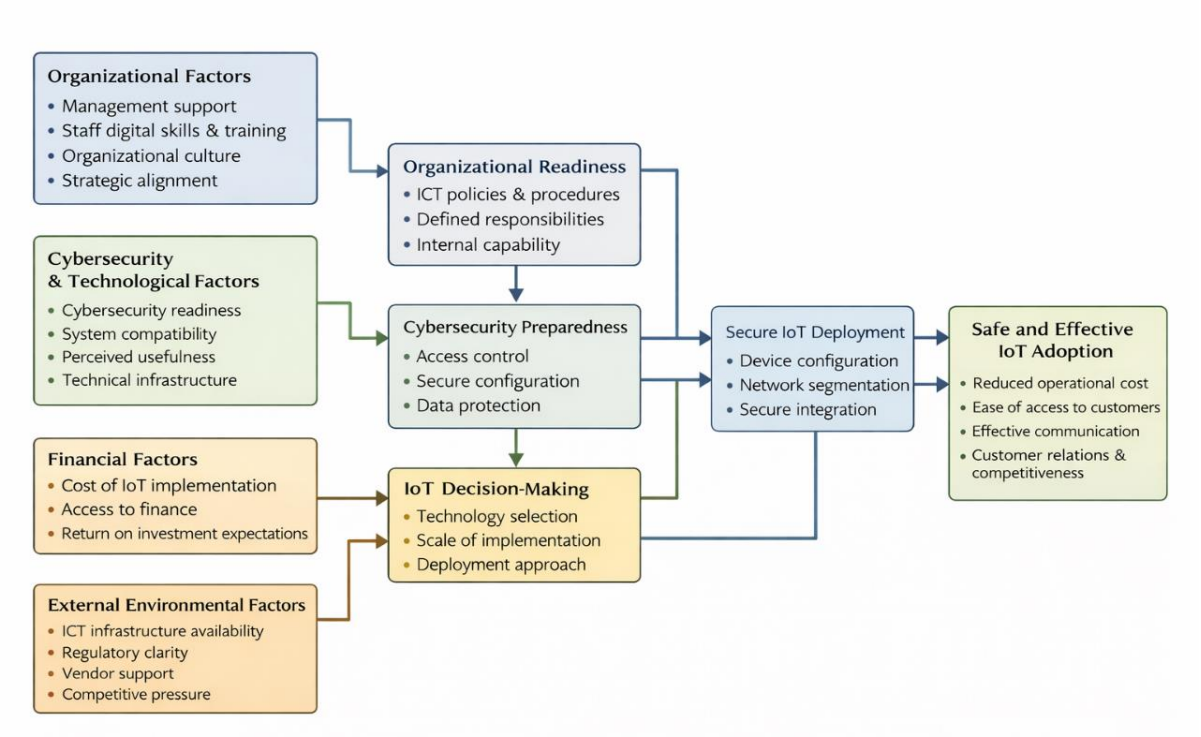
External environmental factors significantly influenced IoT adoption ($\beta = 0.302$), highlighting the importance of regulatory clarity, ICT infrastructure availability, and vendor support. These factors shape organizational confidence and reduce uncertainty associated with adoption.

Collectively, the regression results demonstrate that IoT adoption among SMEs is influenced by both direct and indirect relationships. Organizational readiness influences cybersecurity preparedness and financial decision-making; cybersecurity readiness directly influences adoption by reducing perceived risk; financial capacity determines feasibility and sustainability; and external environmental factors provide enabling conditions.

Based on the regression findings, organizational factors exert the strongest influence on IoT adoption by shaping internal readiness and decision-making capacity. Cybersecurity and technological factors directly influence adoption by mitigating risks associated with interconnected systems. Financial factors influence the scale and sustainability of IoT implementation, while external environmental factors influence adoption indirectly through regulatory certainty, infrastructure availability, and vendor ecosystems. These directional relationships informed the structure and flow of the proposed cybersecurity framework.

Based on the analysis above, an easy-to-use cybersecurity framework was proposed for SMEs operating within Nairobi County Central Business District. The framework integrates organizational readiness, cybersecurity preparedness, financial feasibility, and external environmental support to guide secure IoT deployment and usage. The proposed framework is presented in Figure 2.

Figure 2: Proposed Easy-to-Use Cybersecurity Framework for IoT Adoption among SMEs in Nairobi County CBD



In conclusion, the regression analysis confirms that IoT adoption among SMEs is significantly influenced by cybersecurity and technological factors, organizational readiness, financial capacity, and external environmental conditions. The proposed cybersecurity framework translates these empirical findings into a practical, structured, and easy-to-use guide to support safe and effective IoT adoption.

Discussion of Findings

The study findings provide strong empirical justification for developing an easy-to-use cybersecurity framework tailored to SMEs adopting IoT technologies. The coexistence of high cybersecurity awareness and only moderate adequacy of controls suggests that SMEs require practical guidance to operationalize security principles. Dutta and McCrohan (2021) observe that SMEs often struggle to translate abstract cybersecurity knowledge into actionable practices, a challenge amplified in IoT environments.

The significant predictive role of cybersecurity and technological readiness further underscores the need for structured guidance. ENISA (2020) emphasizes that baseline IoT security practices, such as asset management, secure configuration, and patching, are essential for reducing adoption risk. Fagan et al. (2020) similarly argue that lifecycle-based security controls enhance organizational confidence in adopting interconnected systems.

However, the findings also indicate that cybersecurity frameworks cannot operate in isolation. Ghobakhloo and Ching (2019) highlight that technology adoption outcomes depend on alignment across technological, organizational, and environmental dimensions. Faiz et al. (2024) further emphasize that frameworks lacking consideration of financial and organizational constraints are unlikely to be effective in SME contexts.

Accordingly, the proposed cybersecurity framework should be embedded within a broader IoT adoption readiness model that integrates cybersecurity practices with organizational capacity

building, financial feasibility, and external infrastructure conditions. Such an integrated approach aligns with contemporary information systems research advocating for holistic, capability-oriented adoption frameworks for SMEs (Venkatesh et al., 2022; Kraus et al., 2022).

Conclusions of the Study

The study concludes that IoT adoption among SMEs in Nairobi County Central Business District is a multidimensional process influenced by the interaction of cybersecurity and technological readiness, financial capacity, organizational preparedness, and external environmental conditions. Organizational factors emerged as the strongest determinant of IoT adoption, followed by cybersecurity and technological factors, external environmental factors, and financial factors. The high explanatory power of the regression model confirms that IoT adoption cannot be attributed to a single factor but requires alignment across internal capabilities and external ecosystem conditions. Overall, the study achieved its purpose by empirically establishing the determinants of IoT adoption among SMEs and providing a strong foundation for developing a practical, easy-to-use cybersecurity framework to support safe and effective IoT adoption.

Recommendations

The study recommends that SMEs in Nairobi County Central Business District prioritize strengthening cybersecurity and technological readiness as the foundational requirement for safe and sustainable IoT adoption. SME owners and top management should ensure that minimum cybersecurity controls are established before scaling IoT deployment. These controls include maintaining a clear inventory of IoT devices, enforcing secure system configurations and access controls, implementing routine system updates, and establishing simple incident response procedures. Because many SMEs operate under constrained technical capacity, the study emphasizes adoption of simplified, standardized, and low-complexity cybersecurity practices that are feasible for SMEs while still improving the security posture of IoT systems.

The study further recommends that technology providers and IoT vendors enhance SMEs' adoption capacity by offering solutions that are secure-by-default, easy to integrate with existing SME systems, and accompanied by simplified and practical implementation guidance. Vendors should also provide continuous support through security updates and maintenance services aligned with SME operating conditions. In addition, SMEs should build basic internal capacity by investing in continuous skills development, ensuring staff directly involved in IoT operations receive foundational training on device handling, data protection practices, and cybersecurity awareness. This improves correct system use, reduces avoidable security incidents, and strengthens trust in IoT technologies.

In terms of financial determinants, the study recommends that SMEs adopt structured financial planning when evaluating IoT investments. This includes conducting basic cost–benefit analysis to assess both startup and operational costs such as device acquisition, connectivity, maintenance, cybersecurity controls, and training. SMEs should also clearly define the expected operational gains and strategic benefits in order to reduce uncertainty regarding return on investment. At the ecosystem level, financial institutions, development partners, and policymakers should design affordable financing mechanisms tailored to SME technology adoption, including concessional loans, flexible repayment models, and technology-linked financing products that reduce upfront capital barriers. Integrating IoT investment support into broader SME digitalization and innovation programs is also recommended to scale adoption.

Regarding organizational determinants, the study recommends that SME leadership should frame IoT adoption as an organizational change initiative rather than a purely technical upgrade. Management support should be reflected through resource allocation for ICT training, clear assignment of responsibilities for IoT system management, and integration of digital

transformation initiatives into formal enterprise strategy. Establishing clear ownership of IoT systems and generated data enhances accountability and long-term sustainability. SMEs should also strengthen change management practices by involving staff early in adoption processes, communicating IoT benefits clearly, and providing training directly linked to staff tasks. Cross-functional collaboration should be encouraged to ensure IoT systems become integrated into core business workflows rather than functioning as isolated tools.

Finally, the study recommends strengthened external environmental support to improve IoT adoption conditions in Nairobi CBD. Government agencies and regulators should improve the clarity and accessibility of policies related to IoT adoption, data protection, and cybersecurity compliance to reduce uncertainty and increase SME confidence. Public institutions should also intensify awareness programs to ensure SMEs understand available incentives and digital adoption support initiatives. In addition, investment in reliable internet connectivity and broader ICT infrastructure within commercial zones such as Nairobi CBD should remain a priority for both government and service providers. The study also recommends building stronger collaboration networks among SMEs, technology vendors, and industry associations to improve access to shared expertise, resources, and best practices necessary for secure and effective IoT implementation.

REFERENCES

Benjamin, L. B., Adegbola, A. E., Amajuoyi, P., Adegbola, M. D., & Adeusi, K. B. (2024). Digital transformation in SMEs: Identifying cybersecurity risks and developing effective mitigation strategies. *Global Journal of Engineering and Technology Advances, 19*(2), 134–153. https://doi.org/10.30574/gjeta.2024.19.2.0084

Communications Authority of Kenya, & GSMA. (2024, October 22). *Driving digital transformation of the economy in Kenya* (GSMA report). https://www.gsma.com/aboutus/regions/subsaharanafrica/wpcontent/uploads/2024/05/spec_digi_africa_05_24.pdf

Creswell, J. W., & Creswell, J. D. (2023). *Research design: Qualitative, quantitative and mixed methods approaches*. Sage Publications Ltd. https://www.ucg.ac.me/skladiste/blog_609332/objava_105202/fajlovi/Creswell.pdf

De Silva, M., Al-Tabbaa, O., & Khan, Z. (2021). Business model innovation by international social purpose organizations: The role of dynamic capabilities. *Journal of Business Research, 125*, 733–749. https://doi.org/10.1016/j.jbusres.2019.12.030

Dutta, A., & McCrohan, K. (2021). Information security and privacy challenges in the Internet of Things: A review. *Information Systems Management, 38*(2), 86–103. https://doi.org/10.1080/10580530.2020.1816932

European Union Agency for Cybersecurity. (2020). *Guidelines for securing the Internet of Things*. ENISA. https://www.enisa.europa.eu

Faiz, F., Kazmi, S. H. A., Ahmad, M., & Amin, S. (2024). Determinants of digital technology adoption in innovative SMEs: Integrating TOE and DOI perspectives. *Technological Forecasting and Social Change, 198*, 123045. https://doi.org/10.1016/j.techfore.2023.123045

Gershman, S. J., & Ullman, T. D. (2023). Causal implicatures from correlational statements. *PLOS ONE, 18*(5), e0286067. https://doi.org/10.1371/journal.pone.0286067

Ghobakhloo, M., & Ching, N. T. (2019). Adoption of digital technologies in small and medium-sized enterprises: A systematic literature review. *Industrial Management & Data Systems, 119*(3), 465–490. https://doi.org/10.1108/IMDS-07-2018-0270

Kabaya, M., & Kageni, M. (2024). *Cyber security in the wake of the fourth industrial revolution in Kenya.* https://ypalumni.kippra.or.ke/wpcontent/uploads/2024/10/DP326.pdf

Karthikeyan, K. S., & Nagaprakash, T. (2024). Prioritizing IoT-driven sustainability initiatives in retail chains: Exploring case studies and industry insights. *EAI Endorsed Transactions on Internet of Things, 10*, 1–12. https://doi.org/10.4108/eetiot.4628

Kraus, S., Palmer, C., Kailer, N., Kallinger, F. L., & Spitzer, J. (2021). Digital transformation in SMEs: A systematic review. *Journal of Business Research, 126*, 325–348. https://doi.org/10.1016/j.jbusres.2020.12.068

Kraus, S., Durst, S., Ferreira, J. J., Veiga, P., Kailer, N., & Weinmann, A. (2022). Digital transformation in business and management research: An overview of the current status quo. *International Journal of Information Management, 63*, 102466.

Mugenda, O. M., & Mugenda, A. G. (2013). *Research methods: Quantitative and qualitative approaches*. Acts Press.

Munasser, H. (2024). *Understanding the adoption challenges of IoT among small to medium-size enterprises (SMEs): Study in Sweden* [Undergraduate thesis, Linnaeus University]. http://www.diva-portal.org/smash/get/diva2:1918587/FULLTEXT01.pdf

Neyole, J. misiko, Okwiri, S. M., & Mapema, N. (2024). Exploring the impact of cybersecurity threats on small and medium enterprises' performance: A case study of Kajiado County, Kenya. https://doi.org/10.20944/preprints202411.0237.v1

Oliveira, T., & Martins, M. F. (2011). Literature review of information technology adoption models at firm level. *The Electronic Journal of Information Systems Evaluation, 14*(1), 110–121.

Omoyiola, B. O. (2019). Factors affecting IoT adoption. *International Journal of Computer Engineering and Technology, 21*, 19–24. https://doi.org/10.9790/0661-2106011924

Peretz-Andersson, E., Tabares, S., Mikalef, P., & Parida, V. (2024). Artificial intelligence implementation in manufacturing SMEs: A resource orchestration approach. *International Journal of Information Management, 77*, 102781.

Rogers, E. M. (2003). *Diffusion of innovations* (5th ed.). Free Press.

Rosli, M. S., Saleh, N. S., Alshammari, S. H., Ibrahim, M. M., Atan, A. S., & Atan, N. A. (2021). Improving questionnaire reliability using construct reliability for researches in educational technology. *International Journal of Interactive Mobile Technologies, 15*(4), 109–116. https://doi.org/10.3991/ijim.v15i04.20199

Rymaszewska, A., Helo, P., & Gunasekaran, A. (2021). IoT powered servitization of manufacturing: Evidence from SMEs. *Journal of Manufacturing Technology Management, 32*(1), 92–116. https://doi.org/10.1108/JMTM-03-2020-0089

Sallam, K., Mohamed, M., & Wagdy, A. (2023). Internet of things (IoT) in supply chain management: Challenges, opportunities, and best practices. *Sustainable Machine Intelligence Journal, 2*, Article 22103. https://doi.org/10.61185/SMIJ.2023.22103

Saunders, M., Lewis, P., & Thornhill, A. (2019). *Research methods for business students* (8th ed.). Pearson Education.

Udeh, E., Amajuoyi, P., Adeusi, K., & Scott, A. (2024). The role of IoT in boosting supply chain transparency and efficiency. *Magna Scientia Advanced Research and Reviews, 12*, 178–197. https://doi.org/10.30574/msarr.2024.11.1.0081

Venkatesh, V., Thong, J. Y. L., Chan, F. K. Y., Hu, P. J. H., & Brown, S. A. (2022). Extending the unified theory of acceptance and use of technology: A multilevel perspective. *MIS Quarterly, 46*(1), 521–566. https://doi.org/10.25300/MISQ/2022/15897

Willie, M. (2024). Leveraging digital resources: A resource-based view perspective. *Golden Ratio of Human Resource Management, 5*(1), 01–14.

Yamane, T. (1967). *Statistics: An introductory analysis* (2nd ed.). Harper and Row. https://books.google.co.ke/books/about/Statistics.html?id=Wr7rAAAAMAAJ&redir_esc=y

Zhukabayeva, T., Amanzholova, S., & Suleimenov, I. (2025). Cybersecurity readiness and IoT adoption in SMEs. *Computers & Security, 134*, 103435.