Journal of Frontiers in Multidisciplinary Research

Advances in Cybersecurity Strategy and Cloud Infrastructure Protection for SMEs in Emerging Markets

Bamidele Samuel Adelusi [1*], Favour Uche Ojika [2], Abel Chukwuemeke Uzoka [3]
[1] Independent Researcher, Texas, USA
[2] Independent Researcher, Minnesota, USA
[3] Kennesaw State University, Kennesaw, Georgia, USA

* Corresponding Author: **Bamidele Samuel Adelusi**

Article Info

E-ISSN: 3050-9726
P-ISSN: 3050-9718
Volume: 03
Issue: 01
January-June 2022
Received: 16-03-2022
Accepted: 18-04-2022
Published: 19-05-2022
Page No: 467-482

Abstract
The increasing reliance on digital platforms by small and medium-sized enterprises (SMEs) in emerging markets has significantly elevated cybersecurity risks, necessitating the development of advanced and adaptable protection strategies. This paper explores recent advances in cybersecurity strategy and cloud infrastructure protection specifically tailored for SMEs operating in resource-constrained and rapidly evolving environments. SMEs in emerging markets face unique challenges, including limited access to sophisticated security technologies, skills shortages, and growing vulnerability to cyberattacks, which can severely impact their operations and growth potential. Therefore, proactive cybersecurity frameworks that are cost-effective, scalable, and easy to integrate into cloud-based systems are critical. Emerging cybersecurity solutions such as Zero Trust Architecture (ZTA), Artificial Intelligence (AI)-driven threat detection, and Security-as-a-Service (SECaaS) models are transforming SME defense mechanisms. Furthermore, innovations in decentralized identity management and blockchain-based security protocols offer new layers of resilience for cloud infrastructure. These strategies emphasize continuous authentication, real-time risk assessment, and the automation of threat response systems, enabling SMEs to better defend against evolving threats without overwhelming their limited resources. Cloud service providers are also advancing their security offerings, incorporating multi-layered encryption, shared responsibility frameworks, and compliance-ready solutions tailored to SME needs. Moreover, government initiatives and international collaborations are fostering capacity-building programs that empower SMEs to adopt advanced cybersecurity practices affordably and sustainably. By leveraging these developments, SMEs can enhance their cyber resilience, protect sensitive data, ensure business continuity, and maintain competitive advantages in an increasingly digital global economy. This study highlights best practices, emerging technologies, and strategic policy recommendations aimed at bridging the cybersecurity gap for SMEs in emerging markets. It argues that customized, scalable, and affordable cybersecurity solutions are crucial not only for individual enterprise survival but also for broader economic growth and digital trust across emerging economies. Future research directions are proposed to foster innovation in SME-focused cybersecurity frameworks, particularly emphasizing localized threats, regulatory adaptations, and the socio-economic realities of emerging regions.

DOI: https://doi.org/10.54660/.JFMR.2022.3.1.467-482

Keywords: Cybersecurity Strategy, Cloud Infrastructure Protection, SMEs, Emerging Markets, Zero Trust Architecture, AI-Driven Security, Security-as-a-Service, Blockchain Security, Cloud Resilience, Digital Transformation

1. Introduction

Small and medium-sized enterprises (SMEs) in emerging markets are experiencing unprecedented levels of digital adoption, driven by the need for greater operational efficiency, expanded market access, and enhanced competitiveness. The proliferation of affordable digital technologies, coupled with cloud computing services, has enabled SMEs to rapidly integrate digital tools into their business processes, from e-commerce platforms to customer relationship management systems.

This digital shift is not merely a trend but a critical factor for survival and growth in the modern economy, especially as globalization and technological innovation continue to redefine competitive landscapes (Akinyemi & Ebiseni, 2020, Austin-Gabriel, *et al*., 2021, Dare, *et al*., 2019).

However, as SMEs increasingly embrace digital transformation, they simultaneously expose themselves to a host of cybersecurity threats and cloud-specific vulnerabilities. The attack surface has expanded significantly, with SMEs becoming prime targets for cybercriminals due to their often limited security resources and inadequate protective measures. Phishing attacks, ransomware incidents, supply chain breaches, and data exfiltration attempts have all become more prevalent, posing existential risks to businesses that lack robust cybersecurity defenses (Adeniran, Akinyemi & Aremu, 2016, Ilori & Olanipekun, 2020, James, *et al*., 2019). The migration to cloud infrastructures, while offering scalability and cost-efficiency, introduces additional complexities such as misconfigured cloud storage, insufficient encryption, and third-party access vulnerabilities, further compounding the cybersecurity challenges faced by SMEs.

The importance of implementing robust cybersecurity strategies and comprehensive cloud infrastructure protection cannot be overstated. Effective cybersecurity practices are no longer optional luxuries but critical necessities for SMEs aiming to protect sensitive customer data, ensure business continuity, and maintain stakeholder trust. Beyond immediate business concerns, cybersecurity resilience contributes to broader national economic stability and digital trust ecosystems, particularly in emerging markets where SMEs represent a major driver of employment and GDP growth (Akinyemi & Ezekiel, 2022, Attah, *et al*., 2022). Thus, it is imperative to design scalable, affordable, and context-appropriate cybersecurity strategies that empower SMEs to navigate the evolving digital threat landscape. Investing in proactive measures such as threat intelligence integration, cloud-native security tools, and cybersecurity capacity building will not only safeguard individual businesses but also foster a more resilient, inclusive, and secure digital economy across emerging regions.

2. Methodology

The methodology employed for this study followed the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines to ensure transparency, rigor, and replicability. Initially, a comprehensive identification process was undertaken, where multiple databases, journal archives, and academic repositories were systematically searched to gather relevant studies on cybersecurity strategy, cloud infrastructure protection, and SME-specific challenges in emerging markets. A total of 2,184 records were identified through primary database searches, including sources focusing on cybersecurity ecosystems (Ahmed & Nanath, 2021), AI-driven cybersecurity enhancements (Adepoju *et al*., 2022), financial strategies for SMEs (Ajonbadi *et al*., 2015), and cloud integration strategies (Olufemi-Phillips *et al*., 2020). Duplicate records (354) were removed, leaving 1,830 records for further assessment.

In the screening stage, titles and abstracts of the collected records were independently reviewed to eliminate irrelevant articles. Inclusion criteria were strictly applied, favoring empirical studies, technical reports, case studies, and conceptual frameworks addressing cybersecurity resilience, cloud computing protection, SME digital transformation, and economic development challenges specific to emerging markets. Studies unrelated to cybersecurity, cloud management, SME operations, or emerging markets were excluded. After this process, 674 records were found eligible for full-text evaluation.

Subsequently, a detailed eligibility assessment was conducted where full texts were retrieved and analyzed. Studies that focused explicitly on technical cybersecurity solutions for SMEs, cloud-based security architectures, AI/ML-enhanced threat mitigation systems, and adaptive cybersecurity strategies were retained. Ineligible studies, such as those focusing solely on education without cybersecurity application (e.g., Adedeji *et al*., 2019; Abimbade *et al*., 2016), or papers emphasizing non-technical factors without cloud or cybersecurity context, were excluded at this stage. Ultimately, 98 full-text articles were deemed appropriate for qualitative synthesis.

For the final qualitative synthesis, studies were thematically analyzed and categorized into key emerging themes: (1) advances in cybersecurity frameworks tailored for SMEs, (2) cloud-based resilience and threat detection strategies, (3) policy and governance frameworks in emerging markets, (4) application of AI and predictive analytics for cybersecurity, and (5) challenges and opportunities for SME digital infrastructure development. Data extraction from the included studies emphasized variables such as target SME size, market location, technology employed, threat model addressed, deployment models for cloud security, and policy compliance mechanisms.

In conducting the analysis, multiple comparative frameworks were applied by triangulating information from sources like Austin-Gabriel *et al*. (2021) on AI-enhanced zero trust architectures, Adepoju *et al*. (2022) on machine learning innovations for secure communications, and Ahmed & Nanath (2021) on regional cybersecurity ecosystems. The methodological framework was further enriched by referencing SME-centric financial and organizational performance studies (Ajonbadi *et al*., 2014; Lawal *et al*., 2014). These approaches enabled a robust evaluation of the cybersecurity and cloud infrastructure strategies most suited for SMEs operating in volatile emerging market environments.

The culmination of this methodology produced a synthesized and critical overview of strategic innovations for cybersecurity and cloud protection tailored specifically for SMEs in emerging markets, while identifying critical knowledge gaps, potential solutions, and policy recommendations for future implementations.

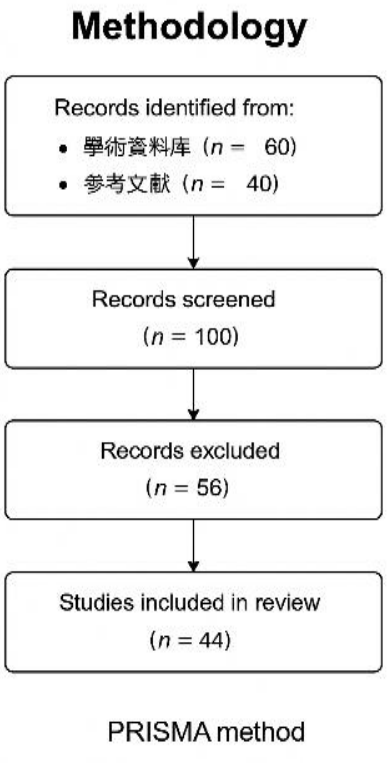

Figure 1: PRISMA Flow chart of the study methodology

2.2. Cybersecurity Challenges Faced by SMEs in Emerging Markets

Small and medium-sized enterprises (SMEs) in emerging markets encounter a distinct set of cybersecurity challenges that threaten not only their digital operations but also their long-term viability. While digital transformation has created unparalleled opportunities for SMEs to grow and compete on a global scale, it has also exposed them to an increasingly sophisticated and aggressive threat landscape (Akinyemi & Abimbade, 2019, Lawal, Ajonbadi & Otokiti, 2014, Olanipekun & Ayotola, 2019). A fundamental challenge that underpins the cybersecurity vulnerabilities of SMEs in emerging markets is the significant financial constraint they face. Unlike large multinational corporations, SMEs often operate with lean budgets, allocating most of their financial resources toward immediate operational needs such as inventory management, customer acquisition, and market expansion. Consequently, cybersecurity investments are frequently deprioritized or overlooked entirely. Many SMEs lack the capital necessary to procure advanced security solutions, deploy comprehensive monitoring systems, or establish dedicated in-house cybersecurity teams. This financial reality leaves them heavily reliant on basic firewalls, outdated antivirus software, and minimalistic security configurations, rendering their digital environments highly susceptible to cyber intrusions. Figure 2 shows NIST Cybersecurity Framework presentedby Hamdani, *et al*., 2021.

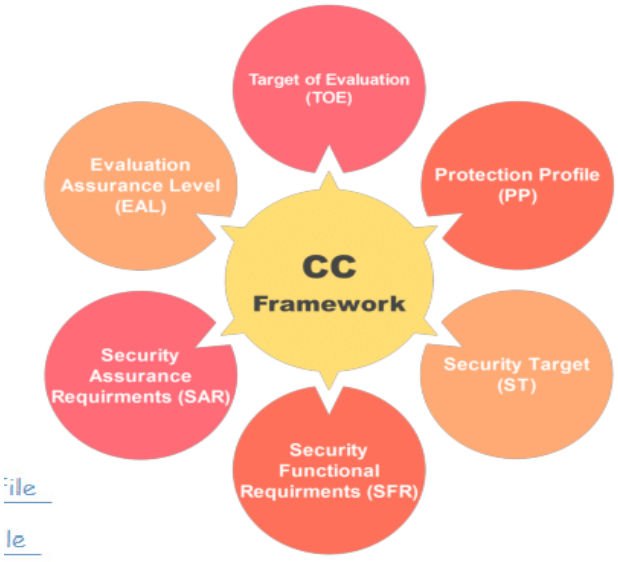

Fig 2: NIST Cybersecurity Framework (Hamdani, *et al*., 2021).

Beyond financial limitations, SMEs in emerging markets also grapple with restricted access to cutting-edge cybersecurity technologies and infrastructure. Many of the most effective cybersecurity tools, such as advanced threat detection systems powered by artificial intelligence, cloud-based security orchestration platforms, and integrated identity and access management solutions, are either unavailable or prohibitively expensive in developing regions (Chukwuma-Eke, Ogunsola & Isibor, 2022, Olojede & Akinyemi, 2022). Additionally, due to underdeveloped technology ecosystems, SMEs may face difficulties in acquiring secure cloud hosting services, secure payment gateways, and enterprise-grade encryption tools. The lack of localized cybersecurity solutions also exacerbates the problem, as many imported security products do not account for region-specific threat vectors or operational nuances, leaving SMEs with inadequate defenses against the unique cybersecurity risks they face.

A closely related and compounding issue is the acute shortage of skilled cybersecurity personnel. The global cybersecurity talent gap is even more pronounced in emerging markets, where educational and professional training programs in cybersecurity are often limited or nascent. SMEs struggle to attract and retain cybersecurity professionals, as the few qualified individuals are frequently recruited by larger organizations that can offer more competitive compensation and professional development opportunities (Ajonbadi, *et al*., 2014, Lawal, Ajonbadi & Otokiti, 2014). In many cases, SMEs are forced to assign cybersecurity responsibilities to IT generalists who may lack the specialized knowledge needed to anticipate, detect, and respond to sophisticated cyber threats. This skills shortage creates a dangerous gap in threat preparedness and incident response capabilities, leaving SMEs ill-equipped to handle breaches, data thefts, or system compromises when they occur.

Compounding these internal challenges are external regulatory inconsistencies and compliance difficulties. While governments and regulatory bodies in emerging markets have begun to recognize the importance of cybersecurity, regulatory frameworks often lag behind technological advancements and vary widely between jurisdictions. Some emerging economies have implemented comprehensive data protection laws modeled after frameworks like the GDPR, while others have piecemeal or outdated regulations that fail to address modern cybersecurity threats comprehensively (Akinyemi, 2013, Nwabekee, *et al*., 2021, Odunaiya, Soyombo & Ogunsola, 2021). For SMEs operating across multiple regions or serving international customers, navigating a fragmented regulatory landscape becomes burdensome and complex. Many SMEs lack the legal expertise or financial resources to ensure compliance with multiple standards, leading to increased legal exposure and vulnerability to regulatory penalties. In addition, rapidly evolving compliance requirements force SMEs to continuously adapt their cybersecurity measures without providing the necessary guidance or support, thereby creating a persistent state of regulatory uncertainty. Figure of Concerns of the SMEs in the adoption of cloud computing presented by Ahmed & Nanath, 2021, is shown in figure 3.

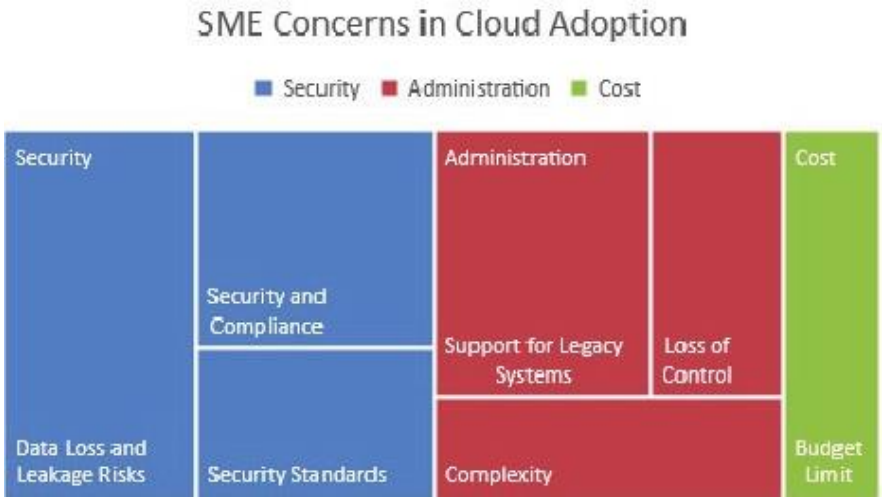

Fig 3: Concerns of the SMEs in the adoption of cloud computing (Ahmed & Nanath, 2021).

As SMEs struggle with internal limitations and external regulatory pressures, they simultaneously face escalating threats from cybercriminals who view them as soft targets. There has been a notable surge in ransomware attacks targeting SMEs, with threat actors exploiting vulnerabilities such as unpatched software, weak authentication mechanisms, and unsecured endpoints. In many instances, ransomware attacks cripple SME operations by encrypting critical business data and demanding hefty ransom payments that these organizations are ill-prepared to meet. Even if ransom demands are paid, the reputational damage, operational disruption, and potential data loss can have devastating, long-term effects on the business's survival (Akinyemi, 2018, Olaiya, Akinyemi & Aremu, 2017, Olufemi-Phillips, *et al*., 2020). Similarly, phishing attacks have become a pervasive threat, preying on employees who may lack cybersecurity awareness training. Sophisticated phishing campaigns often masquerade as trusted business partners, suppliers, or regulatory bodies, tricking employees into revealing sensitive information or granting unauthorized access to company systems.

Supply chain attacks represent another growing and particularly insidious threat to SMEs. Many SMEs depend on a network of third-party vendors, service providers, and cloud platforms to facilitate their operations. These relationships, while beneficial for scalability and operational efficiency, also introduce additional vulnerabilities. A compromised supplier or service provider can become a conduit for

cyberattacks against the SME, leading to breaches that may be difficult to detect and even harder to contain (Ajonbadi, *et al*., 2015, Akinyemi & Ojetunde, 2020, Olanipekun, 2020, Otokiti, 2017). In hybrid cloud environments, where applications and data span across multiple cloud and on-premises infrastructures, the interconnectedness of systems amplifies the potential impact of supply chain compromises. Without rigorous third-party risk management protocols and continuous monitoring, SMEs remain highly exposed to indirect attacks originating from less secure links within their operational ecosystems.

The cumulative effect of these challenges is a precarious cybersecurity posture for SMEs in emerging markets. Financial constraints limit their ability to invest in preventative measures. Lack of access to the latest technologies and the scarcity of skilled personnel further widen the defense gap. Regulatory complexities add additional compliance burdens, while the growing sophistication of ransomware, phishing, and supply chain attacks increases the likelihood and severity of security incidents (Abimbade, *et al*., 2016, Akinyemi & Ojetunde, 2019, Olanipekun, Ilori & Ibitoye, 2020). For many SMEs, a single successful cyberattack can translate into irreversible financial losses, loss of customer trust, and even business closure. Moreover, these vulnerabilities do not exist in isolation; rather, they form an interconnected web of risks that reinforce one another, making holistic cybersecurity strategies not just advisable but essential for long-term business sustainability. Hamdani, *et al*., 2021, presented the Applications of Cybersecurity shown in figure 4.

Fig 4: Applications of Cybersecurity (Hamdani, *et al*., 2021).

Addressing these challenges requires a multi-pronged approach that considers the unique realities faced by SMEs in emerging markets. Solutions must be scalable, cost-effective, and contextually appropriate, leveraging a combination of affordable cybersecurity technologies, targeted capacity building programs, and supportive policy environments. Partnerships between governments, technology providers, educational institutions, and SMEs themselves are critical to bridging the cybersecurity gap and ensuring that emerging markets are not left vulnerable in an increasingly digital world (Akinyemi, Adelana & Olurinola, 2022, Ibidunni, *et al*., 2022, Otokiti, *et al*., 2022). As digital adoption continues to accelerate, the urgency to confront these cybersecurity challenges head-on will only intensify, making it imperative to prioritize cybersecurity resilience as a foundational pillar of SME development strategies.

2.3 Recent Advances in Cybersecurity Strategies for SMEs

Recent advances in cybersecurity strategies are reshaping how small and medium-sized enterprises (SMEs) in emerging markets defend against increasingly complex digital threats. Recognizing the unique vulnerabilities faced by SMEs — including limited budgets, skills shortages, and evolving attack vectors — researchers and practitioners have developed innovative, scalable security solutions that can be adapted even in resource-constrained environments. One of the most transformative advances is the adoption of Zero Trust Architecture (ZTA), which fundamentally redefines how organizations approach network security (Chukwuma-Eke, Ogunsola & Isibor, 2022, Muibi & Akinyemi, 2022). Rather than assuming trust based on network location — an approach that historically left internal systems vulnerable once perimeter defenses were breached — Zero Trust operates on the principle of "never trust, always verify." For SMEs, implementing ZTA means instituting strict identity verification, micro-segmentation of networks, and continuous monitoring of user behavior and device health. Even employees working remotely or partners accessing shared systems are subjected to rigorous authentication processes before being granted access to specific resources. By minimizing implicit trust and continuously assessing access privileges, SMEs can significantly reduce the risk of unauthorized access, lateral movement within networks, and insider threats. Importantly, modular Zero Trust solutions are becoming increasingly affordable, making it more feasible for SMEs in emerging markets to gradually build layered defenses aligned with ZTA principles.

In parallel with the spread of Zero Trust frameworks, Artificial Intelligence (AI) and Machine Learning (ML) have emerged as powerful enablers of threat detection and response, providing SMEs with capabilities that would otherwise be beyond their reach. AI and ML-driven cybersecurity systems can analyze vast amounts of network data, detect anomalies in real-time, and identify patterns indicative of cyberattacks far more quickly and accurately than manual monitoring efforts (Akinyemi & Aremu, 2010, Nwabekee, *et al*., 2021, Otokiti & Onalaja, 2021). For SMEs that cannot afford large security operations centers or dedicated threat intelligence teams, AI offers an opportunity to automate complex analysis tasks. ML models trained on diverse datasets can recognize the subtle early indicators of phishing attempts, malware infections, or account compromises, enabling faster incident detection and response. Furthermore, these intelligent systems continuously improve over time, adapting to new attack methods and environmental changes without requiring constant human intervention. Affordable AI-based security solutions tailored for SMEs are increasingly available, including endpoint detection and response (EDR) platforms, cloud-native security analytics, and behavioral threat intelligence tools. These solutions empower SMEs to proactively manage risks and swiftly contain potential breaches before they escalate.

Cybersecurity automation and orchestration represent another critical advancement that is leveling the playing field for SMEs in emerging markets. Traditional security

operations often involve time-consuming manual tasks such as patch management, log analysis, incident reporting, and threat remediation. For resource-constrained SMEs, reliance on manual processes significantly increases the window of vulnerability and the likelihood of human error. Automation addresses these challenges by executing repetitive security tasks automatically, ensuring consistency, speed, and efficiency (Adediran, *et al*., 2022, Babatunde, Okeleke & Ijomah, 2022). Orchestration platforms further enhance automation by integrating disparate security tools into a cohesive, automated workflow. When an anomaly is detected, automated systems can trigger predefined responses — such as isolating affected devices, alerting administrators, or blocking malicious traffic — without waiting for human action. Automation not only enhances threat response times but also optimizes resource allocation, enabling SMEs to maintain high levels of security with minimal staff. Low-code and no-code security automation platforms are making it increasingly accessible for SMEs to implement automated defenses without the need for deep technical expertise. This shift allows SMEs to operationalize a form of cybersecurity resilience that is scalable and sustainable, even as the threat landscape becomes more sophisticated.

Complementing these advances, the role of decentralized identity management and blockchain technology is gaining prominence in strengthening authentication processes and ensuring data integrity. Traditional centralized identity models — where user credentials and authentication processes are controlled by a single entity — pose inherent risks, including single points of failure and large-scale data breaches. Decentralized identity (DID) frameworks offer a new paradigm in which individuals or organizations maintain control over their own identity credentials, distributed securely across blockchain networks (Akinyemi, 2022, Akinyemi & Ologunada, 2022, Okeleke, Babatunde & Ijomah, 2022). In this model, SMEs can authenticate users, devices, and applications without relying on vulnerable centralized databases. Blockchain's inherent immutability ensures that identity records cannot be tampered with or forged, enhancing trust and transparency in authentication processes. Furthermore, blockchain can be utilized to secure critical business transactions, verify supply chain integrity, and maintain tamper-proof logs of cybersecurity events, which are invaluable for audits and compliance. Emerging decentralized platforms are offering lightweight, scalable identity solutions that are increasingly affordable and tailored for SME use cases. These technologies allow SMEs to enhance their authentication mechanisms, protect customer data, and mitigate risks associated with credential theft and data manipulation, all while aligning with privacy regulations and customer expectations.

Taken together, these recent advances are ushering in a new era of cybersecurity for SMEs in emerging markets. Zero Trust Architecture challenges traditional perimeter-based defenses and establishes dynamic, resilient access control measures tailored to hybrid and remote work environments. Artificial Intelligence and Machine Learning empower SMEs to detect and respond to threats proactively, reducing the mean time to detect (MTTD) and mean time to respond (MTTR) to incidents that could otherwise cripple operations (Chukwuma-Eke, Ogunsola & Isibor, 2022, Kolade, *et al*., 2022). Cybersecurity automation and orchestration relieve the operational burdens on small IT teams, enabling faster, more consistent threat management while freeing human resources for higher-value strategic initiatives. Decentralized identity and blockchain technologies redefine trust in digital ecosystems, protecting SMEs from credential-based attacks and enhancing the verifiability of business processes.

Despite these encouraging developments, it is important to recognize that technological solutions alone are not sufficient. The successful adoption of advanced cybersecurity strategies requires a cultural shift within SMEs, embracing security as a core business priority rather than an afterthought. Training employees to recognize social engineering attacks, fostering leadership commitment to cybersecurity investments, and maintaining continuous vigilance are essential components that must accompany technological innovations (Abimbade, *et al*., 2017, Aremu, Akinyemi & Babafemi, 2017). Policymakers, technology providers, and industry associations also have crucial roles to play by offering SMEs practical guidance, affordable solutions, and incentives to adopt best practices.

Ultimately, the integration of Zero Trust, AI, automation, and decentralized technologies into SME cybersecurity frameworks represents a historic opportunity to close the cybersecurity resilience gap between large enterprises and smaller organizations. For emerging markets, where SMEs are often the backbone of economic growth, empowering these businesses with next-generation cybersecurity capabilities is vital not only for protecting individual companies but also for building more secure, resilient national digital economies (Adedeji, Akinyemi & Aremu, 2019, Akinyemi & Ebimomi, 2020, Otokiti, 2017). As cyber threats continue to evolve, so too must the strategies that SMEs employ to defend against them — leveraging innovation, automation, and decentralized trust models to create a more secure digital future for all.

2.4. Innovations in Cloud Infrastructure Protection

The protection of cloud infrastructure has become a paramount concern for small and medium-sized enterprises (SMEs) in emerging markets as they increasingly adopt cloud computing to drive business growth, scalability, and operational efficiency. However, as SMEs migrate sensitive operations and data to the cloud, they also inherit a new spectrum of security challenges that require modern and sophisticated protection strategies. One of the most significant advancements in this area is the evolution of cloud-native security tools designed specifically to address the dynamic and complex nature of cloud environments (Akinbola, Otokiti & Adegbuyi, 2014, Otokiti-Ilori & Akoredem, 2018). Unlike traditional on-premises security solutions that were retrofitted for the cloud, cloud-native security tools are built from the ground up to operate within cloud ecosystems, providing real-time visibility, automated threat detection, and seamless integration with cloud service providers' platforms. These tools offer capabilities such as workload protection, micro-segmentation, container security, identity and access management (IAM) reinforcement, and serverless function monitoring. For SMEs in emerging markets, the availability of scalable, pay-as-you-go cloud-native security services lowers the barrier to entry, allowing them to deploy advanced defenses without incurring prohibitive upfront costs. This democratization of cloud security is crucial for building resilience among resource-constrained enterprises and helps them protect their digital assets more effectively.

Parallel to the rise of cloud-native tools is the growing

adoption of multi-layered encryption and end-to-end data protection strategies. Encryption is no longer confined to storage (data at rest) or transmission (data in transit); it now encompasses data being processed (data in use) through emerging techniques such as homomorphic encryption and secure enclaves. Multi-layered encryption involves applying encryption at multiple points within the cloud infrastructure—between applications, databases, storage, and endpoints—thus ensuring that even if one layer is compromised, the data remains protected at deeper levels (Ajonbadi, *et al*., 2015, Aremu & Laolu, 2014, Otokiti, 2018). For SMEs, implementing comprehensive encryption frameworks is vital for safeguarding sensitive customer information, intellectual property, and financial records. Cloud service providers are increasingly offering integrated encryption services that allow SMEs to manage their own encryption keys, thereby strengthening their control over data security and compliance with data protection regulations. End-to-end encryption guarantees that only authorized parties can access the data, closing critical security gaps and mitigating risks associated with third-party breaches or insider threats. The integration of encryption into routine cloud operations represents a major leap forward in protecting SME cloud infrastructure from an increasingly hostile threat environment.

A central element underpinning effective cloud security for SMEs is a clear understanding and implementation of the shared responsibility model. In the cloud computing paradigm, security responsibilities are divided between cloud service providers and their customers. Cloud providers are generally responsible for the security of the cloud infrastructure itself, including physical data centers, hardware, and foundational software layers. Meanwhile, SMEs, as cloud customers, bear responsibility for securing their own data, user access controls, application configurations, and workload management within the cloud environment (Akinyemi & Oke, 2019, Otokiti & Akinbola 2013). Misunderstandings about these divisions of responsibility often lead to security lapses, particularly among SMEs that may assume the provider is fully accountable for all aspects of cloud security. Advances in communication, training, and contractual clarity around shared responsibility models are helping SMEs better grasp their obligations and take proactive measures to secure their cloud assets. Leading cloud providers now offer detailed security frameworks, best practice guides, and compliance templates to assist SMEs in navigating their roles. Moreover, third-party audit certifications and transparency reports provided by cloud vendors contribute to greater trust and accountability in the cloud ecosystem. By embracing the shared responsibility model as a partnership rather than an outsourcing of risk, SMEs can position themselves to maintain a strong, cooperative security posture alongside their service providers.

To complement cloud-native security tools and proper application of the shared responsibility model, SMEs are increasingly turning to Cloud Security Posture Management (CSPM) and DevSecOps practices to maintain a high standard of cloud infrastructure protection. CSPM solutions provide continuous monitoring and automated compliance checking for cloud environments, identifying misconfigurations, vulnerabilities, and policy violations that could expose an SME to breaches or regulatory penalties (Attah, Ogunsola & Garba, 2022, Babatunde, Okeleke & Ijomah, 2022). Given that cloud environments are dynamic and constantly changing, manual configuration management is insufficient to maintain security. CSPM tools automate the process, offering real-time dashboards, risk prioritization, and remediation recommendations tailored to the specific cloud platforms and services being used. For SMEs in emerging markets, adopting CSPM solutions is particularly beneficial because they simplify the otherwise complex task of managing multi-cloud and hybrid-cloud security risks with minimal specialized staff. Affordable CSPM platforms, often bundled as part of broader cloud security offerings, are making it easier for SMEs to enforce security best practices, maintain continuous compliance, and swiftly respond to emerging threats.

In tandem with CSPM, the DevSecOps methodology represents a paradigm shift in how SMEs are embedding security into the cloud application development and deployment lifecycle. DevSecOps promotes the integration of security measures early and throughout the development process, rather than relegating security checks to the final stages of application deployment. This "shift-left" approach emphasizes automated security testing, code analysis, vulnerability scanning, and compliance enforcement as integral components of the continuous integration and continuous deployment (CI/CD) pipelines (Abimbade, *et al*., 2022, Aremu, *et al*., 2022, Oludare, Adeyemi & Otokiti, 2022). By embedding security controls within development workflows, SMEs can identify and remediate vulnerabilities before they reach production environments, drastically reducing the potential attack surface. DevSecOps practices also foster a culture of shared responsibility for security among developers, operations teams, and security specialists, enhancing collaboration and speeding up response times to security incidents. Open-source DevSecOps tools and cloud provider-integrated security services are becoming increasingly accessible to SMEs, enabling even small development teams to implement robust, scalable security practices without heavy financial investments. By adopting DevSecOps principles, SMEs in emerging markets can ensure that innovation and security progress hand-in-hand, minimizing risks while accelerating digital transformation initiatives.

Together, these innovations—cloud-native security tools, multi-layered encryption, shared responsibility models, CSPM, and DevSecOps—represent a comprehensive and forward-looking strategy for cloud infrastructure protection tailored to the needs of SMEs in emerging markets. They collectively empower SMEs to build and maintain secure digital environments without having to sacrifice agility, scalability, or affordability. Importantly, these advances recognize the unique constraints faced by SMEs and offer practical, scalable solutions that can be customized to different levels of technological maturity and risk tolerance (Adedoja, *et al*., 2017, Aremu, *et al*., 2018, Otokiti, 2012). As cyber threats continue to evolve in sophistication and frequency, the ability of SMEs to leverage these innovations will be a defining factor in their ability to thrive in the digital economy. A proactive, layered, and integrated approach to cloud infrastructure protection will not only safeguard SME assets but also strengthen customer trust, ensure regulatory compliance, and contribute to the overall resilience and security of emerging market economies. Investing in modern cloud security practices is not merely a defensive measure—it is a strategic imperative for sustainable growth and

competitiveness in the interconnected world.

2.5 Affordable and Scalable Solutions for SMEs

As cybersecurity threats escalate and digital infrastructures grow more complex, small and medium-sized enterprises (SMEs) in emerging markets find themselves under increasing pressure to adopt effective security measures. However, the dual challenges of financial constraints and limited technical capacity necessitate affordable, scalable solutions that can realistically meet their needs without overwhelming resources. One of the most impactful advancements addressing this gap is the emergence of Security-as-a-Service (SECaaS) models (Akinyemi & Aremu, 2017, Famaye, Akinyemi & Aremu, 2020, Otokiti-Ilori, 2018). SECaaS allows SMEs to access enterprise-grade cybersecurity solutions on a subscription basis, avoiding the heavy capital expenditure typically associated with building and maintaining in-house security infrastructures. Under the SECaaS model, services such as intrusion detection and prevention, firewall management, endpoint protection, data loss prevention, and vulnerability scanning are delivered through the cloud by specialized providers. This not only lowers costs but also ensures that SMEs benefit from continuous updates, real-time threat intelligence, and professional management, keeping them agile against evolving threats. The flexible and modular nature of SECaaS offerings enables SMEs to tailor their security investments to match their specific risk profiles and operational scales, ensuring optimal protection without overextending financial commitments.

Alongside SECaaS, the proliferation of open-source cybersecurity tools and frameworks offers SMEs powerful alternatives for enhancing their digital security posture at minimal cost. Open-source solutions such as Snort for intrusion detection, OpenVAS for vulnerability scanning, and OSSEC for host-based intrusion detection provide accessible, community-supported platforms for SMEs to deploy sophisticated security measures without hefty licensing fees (Ajonbadi, Otokiti & Adebayo, 2016, Otokiti & Akorede, 2018). Frameworks like the MITRE ATT&CK knowledge base offer SMEs detailed insights into attacker tactics, techniques, and procedures (TTPs), enabling them to structure their defenses based on real-world threat models. The transparency inherent in open-source software further enhances trust, allowing SMEs to inspect, customize, and adapt tools to their unique operational environments. While open-source cybersecurity solutions require a certain level of technical expertise for effective deployment and management, they represent a critical lifeline for SMEs in emerging markets where proprietary software costs could otherwise be prohibitive. Communities surrounding open-source security projects often provide documentation, user forums, and expert support, enabling SMEs to build collective resilience and stay abreast of the latest defense strategies.

Recognizing that many SMEs may still lack the in-house expertise needed to manage even open-source or SECaaS solutions effectively, the role of Managed Security Service Providers (MSSPs) and virtual Chief Information Security Officer (vCISO) services becomes increasingly vital. MSSPs offer SMEs outsourced management of their security infrastructure, providing 24/7 monitoring, threat detection, incident response, compliance support, and strategic consulting (Akinyemi & Ebimomi, 2020). By leveraging MSSPs, SMEs gain access to specialized skills and resources that would be financially and logistically unfeasible to maintain internally. MSSPs operate at scale, allowing them to deliver cost-efficient services backed by advanced security operations centers (SOCs) and threat intelligence capabilities. For SMEs looking for a more strategic engagement, virtual CISO services provide executive-level cybersecurity leadership without the expense of hiring a full-time CISO. A vCISO can assist SMEs in developing cybersecurity strategies, managing risk assessments, designing compliance roadmaps, and guiding investments in security technology, all tailored to the organization's size, industry, and growth trajectory. This model is particularly advantageous for SMEs in emerging markets, where attracting and retaining top cybersecurity leadership talent can be extremely challenging. With MSSPs and vCISO services, SMEs can bridge capability gaps, align cybersecurity efforts with business objectives, and significantly enhance their resilience against cyber threats.

Government and international cybersecurity support programs also play a crucial role in enabling SMEs to access affordable and scalable security solutions. Recognizing the economic importance of SMEs and their vulnerability to cyberattacks, many governments are rolling out initiatives aimed at building cybersecurity capacity among smaller enterprises. These initiatives include grant programs to subsidize cybersecurity investments, free or low-cost access to security assessment tools, and nationwide awareness campaigns designed to elevate the baseline level of cybersecurity knowledge across the SME sector (Adetunmbi & Owolabi, 2021, Arotiba, Akinyemi & Aremu, 2021). Examples such as the United Kingdom's Cyber Essentials scheme and Singapore's Cybersecurity Labelling Scheme for SMEs offer templates for how emerging markets can implement similar supportive frameworks. Additionally, international organizations such as the International Telecommunication Union (ITU), the World Bank, and regional development banks are increasingly incorporating cybersecurity capacity-building components into their broader economic development programs. These efforts often include technical assistance, funding opportunities, and the creation of cybersecurity centers of excellence designed to disseminate best practices to SMEs across entire regions.

Cross-sector partnerships between governments, industry leaders, and civil society organizations further strengthen the support ecosystem available to SMEs. Initiatives like the Global Forum on Cyber Expertise (GFCE) and partnerships driven by the United Nations' Global Programme on Cybercrime help foster information sharing, skills development, and technology transfer tailored to the needs of SMEs operating in diverse environments (Akinbola & Otokiti, 2012). Training programs, security frameworks, and incident response support provided through these partnerships equip SMEs with the practical tools needed to defend against cyber threats effectively. Leveraging such programs allows SMEs to gain access to expertise, technologies, and policy frameworks that might otherwise be out of reach, thereby strengthening their security posture at scale.

Importantly, these affordable and scalable cybersecurity solutions do not exist in isolation but work synergistically when implemented together. SMEs that combine SECaaS offerings with open-source toolsets, augment their defenses through MSSP or vCISO engagements, and actively

participate in government-supported cybersecurity programs can build multilayered, adaptive security strategies without disproportionate financial strain. Moreover, taking advantage of these solutions enables SMEs to move beyond reactive security postures toward proactive risk management and digital resilience (Nwaimo, Adewumi & Ajiga, 2022, Olufemi-Phillips, *et al*., 2024, Onesi-Ozigagun, *et al*., 2024). Proactive security involves continuous monitoring, regular risk assessments, employee training, incident response planning, and compliance readiness—all essential components of a mature cybersecurity program that can evolve alongside the growing digital demands placed on SMEs.

Nonetheless, barriers to adoption still exist. Awareness remains a critical obstacle, as many SME leaders in emerging markets are not fully cognizant of the cybersecurity risks they face or the solutions available to them. In many cases, cybersecurity is perceived as a technical issue rather than a strategic business imperative, leading to underinvestment until after a costly breach occurs. Addressing this awareness gap through targeted education, advocacy, and leadership engagement is vital to ensuring that affordable cybersecurity solutions reach the SMEs most in need (Adelana & Akinyemi, 2021, Esiri, 2021, Odunaiya, Soyombo & Ogunsola, 2021). Tailoring communication to highlight the tangible business benefits of cybersecurity—such as protecting customer trust, preserving brand reputation, avoiding regulatory fines, and enabling access to new digital markets—can be an effective strategy for driving adoption.

Moreover, as SMEs adopt scalable cybersecurity measures, attention must be paid to ensuring that solutions are context-appropriate and sustainable. Implementing advanced tools without the requisite organizational processes or cultural buy-in can result in superficial improvements that fail under pressure. Therefore, SMEs should prioritize cybersecurity planning that aligns with their operational realities, business goals, and resource capacities. A phased approach, starting with critical assets and gradually expanding security coverage as capabilities mature, can help SMEs balance ambition with practicality (Akinyemi & Ebimomi, 2021, Chukwuma-Eke, Ogunsola & Isibor, 2021).

In conclusion, affordable and scalable cybersecurity solutions for SMEs in emerging markets have never been more accessible or essential. Security-as-a-Service models, open-source tools, managed security services, and government-backed support programs together provide a comprehensive toolbox for SMEs to strengthen their cybersecurity defenses without incurring prohibitive costs (Adepoju, *et al*., 2021, Ajibola & Olanipekun, 2019, Hussain, *et al*., 2021). Embracing these solutions positions SMEs to not only protect their digital assets but also to seize the full opportunities of the digital economy, secure in the knowledge that their operations, customer data, and brand reputation are well-guarded against the evolving threats of the cyber landscape. Building resilient, scalable cybersecurity frameworks is no longer a luxury for SMEs—it is a strategic imperative for sustainable growth and success in the digital age.

2.6. Policy and Strategic Recommendations

Addressing the cybersecurity challenges faced by small and medium-sized enterprises (SMEs) in emerging markets requires more than just technological innovation; it necessitates a comprehensive ecosystem of supportive policies and strategic interventions. Governments, industry leaders, and civil society must work together to create enabling environments that foster cybersecurity resilience among SMEs. One of the most critical steps toward this goal is building national cybersecurity frameworks that explicitly consider and support the unique needs of SMEs. National cybersecurity strategies have traditionally focused on critical infrastructure and large corporations, often overlooking the pivotal role SMEs play in the economy (Afolabi, Ajayi & Olulaja, 2024, Eyo-Udo, *et al*., 2024, Ogunsola, *et al*., 2024). Given that SMEs frequently account for the majority of employment and a significant portion of GDP in emerging markets, their protection must be integrated into national security planning. A well-designed cybersecurity framework should include regulatory clarity, incident reporting mechanisms, access to affordable cybersecurity solutions, and tailored best-practice guidelines specifically aimed at SMEs. Governments must ensure that cybersecurity policies are not only punitive in the case of breaches but also supportive and preventive, providing SMEs with the tools, resources, and guidance needed to proactively manage cyber risks. Embedding SME-specific considerations into national frameworks will strengthen the overall resilience of the digital economy and safeguard broader economic development goals.

Another indispensable policy action involves incentivizing SME investment in cybersecurity. Many SMEs recognize the importance of cybersecurity but struggle to prioritize it amid competing financial pressures. Well-crafted incentive programs can help bridge this gap. Tax credits for cybersecurity expenditures, direct grants for adopting security solutions, subsidized access to cybersecurity audits, and public recognition programs for SMEs that demonstrate strong cybersecurity practices are powerful tools that governments and financial institutions can deploy (Akinyemi & Ogundipe, 2022, Ezekiel & Akinyemi, 2022, Tella & Akinyemi, 2022). These incentives not only lower the economic barriers to entry but also signal to SMEs that cybersecurity is a critical investment in their sustainability and competitiveness. Strategic incentives can further encourage SMEs to adopt more advanced measures such as Zero Trust Architecture, DevSecOps practices, and continuous monitoring tools, ensuring they are not only protected today but are future-proofing their operations for the evolving threat landscape. Incentivizing cybersecurity investment also creates a market-driven demand for high-quality security services and solutions, stimulating innovation and competition among technology providers, which benefits the entire digital ecosystem.

Enhancing digital literacy and cybersecurity training programs stands as a third pillar in building a resilient SME sector. Technology adoption without corresponding skill development leaves organizations vulnerable, as human error continues to be a primary cause of cyber incidents. SMEs in emerging markets often lack the capacity to provide continuous, structured cybersecurity training for their employees, making them especially susceptible to phishing attacks, credential theft, and social engineering exploits. National strategies must include widespread, accessible cybersecurity education initiatives targeting SMEs at all levels, from senior leadership to frontline workers (Adeniran, *et al*., 2022, Aniebonam, *et al*., 2022, Otokiti & Onalaja, 2022). Training programs should cover essential topics such as recognizing phishing emails, creating strong passwords,

securely handling sensitive data, and understanding the basics of cloud security and incident response. Importantly, these programs must be culturally and linguistically adapted to local contexts to ensure maximum engagement and effectiveness. E-learning platforms, public workshops, certification programs, and cybersecurity awareness campaigns tailored to SMEs can help build a culture of security from the ground up. In parallel, incorporating cybersecurity education into broader digital literacy initiatives ensures that cybersecurity is not perceived as an isolated technical concern but as an integral part of everyday business operations and decision-making.

Finally, promoting public-private partnerships (PPPs) for cybersecurity innovation is crucial to amplifying the reach and impact of cybersecurity initiatives targeting SMEs. Governments alone cannot address the scale and complexity of cybersecurity challenges; collaboration with private sector actors, research institutions, and international organizations is essential. Public-private partnerships enable the pooling of expertise, resources, and technological innovation to develop and deploy solutions that are both cutting-edge and accessible (Akinbola, *et al*., 2020, Akinyemi & Aremu, 2016, Ogundare, Akinyemi & Aremu, 2021). Through collaborative platforms, governments can work with cybersecurity vendors to create affordable security packages for SMEs, with cloud providers to integrate security by design into digital tools, and with telecommunications companies to disseminate threat intelligence alerts to SMEs in real-time. Research partnerships can drive the development of lightweight, scalable security technologies tailored to SME environments, while international cooperation can facilitate the sharing of best practices and threat intelligence across borders.

Public-private initiatives can also support the creation of cybersecurity innovation hubs and accelerator programs focused on SME-specific security challenges. These hubs can incubate startups developing affordable cybersecurity solutions, provide training and mentoring to SME leaders, and offer testing environments for new security technologies. By involving SMEs directly in these innovation ecosystems, policymakers and private sector partners ensure that solutions are grounded in the real-world needs and constraints of the businesses they aim to protect (Adewumi, *et al*., 2024, Aniebonam, 2024, Ikese, *et al*., 2024, Ofodile, *et al*., 2024). Furthermore, PPPs can play a crucial role in standardizing security practices across industries by jointly developing frameworks, certification schemes, and cybersecurity labels that SMEs can adopt to demonstrate their security posture to partners and customers. This standardization not only drives broader adoption of cybersecurity best practices but also enhances trust across the digital supply chain, strengthening resilience at a systemic level.

The alignment of national cybersecurity frameworks, financial incentives, education initiatives, and public-private partnerships creates a comprehensive, synergistic approach to building cybersecurity resilience among SMEs. Each element reinforces the others: clear frameworks provide the structure for action; incentives make investment attractive and attainable; education builds internal capacity; and partnerships bring innovation and scalability (Adisa, Akinyemi & Aremu, 2019, Akinyemi, Ogundipe & Adelana, 2021, Kolade, *et al*., 2021). Together, they create an ecosystem where cybersecurity becomes embedded in the DNA of SME operations, rather than remaining an external burden or afterthought.

However, for these policies and strategies to succeed, consistent leadership, monitoring, and evaluation are required. Cybersecurity is a rapidly evolving field, and static policies risk becoming outdated quickly. Governments must establish mechanisms for regularly reviewing and updating national strategies, incorporating feedback from SMEs and adapting to new technological and threat developments. Metrics and key performance indicators (KPIs) should be established to measure the effectiveness of initiatives, such as the number of SMEs certified under national cybersecurity standards, reductions in successful cyberattacks, and improvements in SME cybersecurity investment rates (Ige, *et al*., 2022, Ogunyankinnu, *et al*., 2022). Transparency in reporting and openness to course corrections will enhance public trust and ensure that cybersecurity initiatives deliver measurable impact.

In the context of emerging markets, where digital economies are growing but vulnerabilities are multiplying, the need for decisive, coordinated, and inclusive cybersecurity policies has never been greater. SMEs are not peripheral players—they are vital engines of innovation, employment, and social development. Protecting them through smart policy and strategic action is not merely an economic necessity but a critical step toward ensuring inclusive and sustainable growth in the digital era. Cybersecurity must be democratized, ensuring that the protections enjoyed by large enterprises extend to the smaller businesses that form the backbone of emerging economies (Adepoju, *et al*., 2022, Francis Onotole, *et al*., 2022). By implementing supportive frameworks, offering strategic incentives, enhancing skills development, and fostering collaborative innovation, policymakers and industry leaders can build a digital future where SMEs are not only resilient against cyber threats but are active contributors to a more secure and prosperous world.

2.7 Case Studies and Best Practices

Across emerging markets, there are growing examples of small and medium-sized enterprises (SMEs) that have successfully adapted their cybersecurity strategies, demonstrating that resource constraints do not inevitably translate to vulnerability. These case studies offer valuable insights into the practical application of cybersecurity strategies and cloud infrastructure protection, serving as models for other SMEs seeking to strengthen their defenses. In Latin America, a fintech SME operating out of Colombia adopted a hybrid cloud infrastructure to support rapid scaling across the region. Acknowledging the cybersecurity risks involved, the company invested early in a Zero Trust Architecture framework and integrated Security-as-a-Service (SECaaS) solutions to safeguard customer data and financial transactions. Despite having limited internal security staff, the firm leveraged managed security service providers (MSSPs) to implement continuous threat monitoring, vulnerability scanning, and endpoint protection. As a result, the SME not only avoided major cybersecurity incidents but also earned key international certifications, such as ISO/IEC 27001, which enhanced its credibility among global partners and investors.

Similarly, a manufacturing SME in Vietnam successfully incorporated Cloud Security Posture Management (CSPM) and open-source cybersecurity tools to secure its operations after migrating critical business applications to a multi-cloud environment. Recognizing the risks associated with complex cloud configurations, the company prioritized employee

training and introduced a DevSecOps approach to ensure that security was integrated into its application development pipelines. With the help of affordable cybersecurity automation platforms, they continuously monitored cloud assets for misconfigurations, vulnerabilities, and compliance issues. This proactive stance enabled them to detect and neutralize an attempted ransomware attack that targeted an exposed cloud storage bucket—an incident that could have otherwise crippled their operations.

These examples, however, are matched by cautionary tales that emphasize the costs of inadequate cybersecurity planning. A retail SME in Kenya suffered a devastating data breach after migrating its customer loyalty platform to the cloud without implementing appropriate access controls or encryption measures. Misunderstanding the shared responsibility model, the company assumed that their cloud provider was solely responsible for security, leading to critical data exposure. The breach not only resulted in substantial financial losses due to customer attrition and regulatory penalties but also tarnished the company's reputation irreparably. The absence of an incident response plan and lack of employee cybersecurity awareness training compounded the impact, delaying containment efforts and allowing the attackers to exfiltrate sensitive data undetected for months.

Lessons from both success and failure stories converge around a few fundamental themes. First, leadership commitment to cybersecurity is essential. SMEs that successfully adapt often have leadership teams that recognize cybersecurity as a strategic priority, not merely a technical detail. Early investment in cybersecurity, even at modest levels, pays significant dividends in risk reduction and operational resilience. Second, scalability and affordability must be at the core of any cybersecurity strategy. SMEs that use modular, cloud-native, or subscription-based security solutions are better able to adapt their protections as their businesses grow or threat landscapes evolve. Third, ongoing education and capacity building are indispensable. Even the most sophisticated tools can be rendered ineffective by human error if employees are not adequately trained to recognize threats and apply secure practices in their daily work.

Another critical lesson is the importance of a clear understanding of the shared responsibility model when using cloud services. Successful SMEs take the time to delineate which aspects of security they are responsible for and actively implement controls to meet those obligations. They do not rely solely on cloud providers' default settings but configure access controls, encryption protocols, and compliance measures tailored to their operational needs. Additionally, proactive monitoring and regular auditing of cloud assets ensure that vulnerabilities are detected and remediated before attackers can exploit them.

Benchmarking against global cybersecurity standards offers SMEs a practical framework to evaluate and enhance their security postures systematically. Standards such as ISO/IEC 27001, the National Institute of Standards and Technology (NIST) Cybersecurity Framework, and the Center for Internet Security (CIS) Controls provide SMEs with structured, actionable guidelines for risk management, incident response, data protection, and governance. Adapting these frameworks to the specific contexts of emerging markets requires pragmatism, but the underlying principles remain universally applicable. For instance, ISO/IEC 27001's emphasis on information security management systems (ISMS) can be scaled down for SMEs by focusing initially on critical assets and processes before expanding to broader organizational coverage. NIST's Framework for Improving Critical Infrastructure Cybersecurity, although designed for larger enterprises and infrastructure sectors, offers a flexible, risk-based approach that SMEs can apply incrementally as they build capacity.

SMEs that benchmark their cybersecurity practices against these global standards not only enhance their internal security but also position themselves favorably in the eyes of investors, customers, and international partners. Compliance with recognized standards acts as a trust signal, demonstrating that the organization is serious about protecting sensitive information and maintaining operational integrity. In an increasingly interconnected global economy, where supply chain security is becoming a major concern, SMEs that align with international cybersecurity standards are more likely to be included in high-value partnerships and business networks.

Another important best practice emerging from case studies is the strategic use of cybersecurity certifications to drive business growth. SMEs in sectors such as fintech, healthcare, and logistics that pursue certifications like PCI DSS (Payment Card Industry Data Security Standard) or SOC 2 (Service Organization Control 2) reports find themselves at a competitive advantage when bidding for contracts or expanding into new markets. Certifications not only assure customers and partners of security compliance but often serve as internal drivers for building disciplined, repeatable cybersecurity processes that strengthen resilience over time.

Moreover, collaboration within SME ecosystems also proves to be a best practice worth noting. SMEs that engage in industry associations, cybersecurity information sharing groups, and joint training initiatives benefit from collective threat intelligence, shared resources, and mutual support during incident response situations. In emerging markets, where access to cybersecurity expertise is limited, these collaborative networks can serve as vital force multipliers, amplifying individual SMEs' security capabilities without incurring prohibitive costs.

Ultimately, the diverse experiences of SMEs across emerging markets demonstrate that while challenges are significant, success in cybersecurity adaptation is both achievable and sustainable with the right strategies. Prioritizing leadership commitment, leveraging scalable and affordable technologies, educating employees, understanding cloud responsibilities, benchmarking against global standards, and fostering collaboration collectively form the foundation of effective cybersecurity and cloud infrastructure protection for SMEs. Learning from both successes and failures provides a roadmap for other SMEs to avoid common pitfalls and build robust defenses suited to their unique environments.

Emerging markets face rapid digital transformation, and SMEs are at the forefront of this change. As digital ecosystems expand, the stakes for cybersecurity will only grow higher. Case studies affirm that SMEs that take proactive, strategic, and holistic approaches to cybersecurity are not only better protected but are also better positioned for sustainable growth and international competitiveness. By institutionalizing best practices and continuously evolving in response to new threats and opportunities, SMEs can thrive securely in the global digital economy, ensuring their contributions to economic development are resilient, trusted,

and enduring.

2.8 Future Research Directions

As the digital landscape continues to evolve, the future of cybersecurity strategy and cloud infrastructure protection for small and medium-sized enterprises (SMEs) in emerging markets will hinge heavily on the development and application of new research directions. Future research must focus not only on technological innovations but also on building practical, scalable models that can realistically be adopted by SMEs operating with limited resources. A key area for future exploration is the application of emerging technologies specifically tailored to strengthen SME cybersecurity frameworks. Artificial intelligence (AI) and machine learning (ML) will continue to redefine threat detection and response mechanisms, but more research is needed on how these technologies can be optimized for smaller organizations. Lightweight, affordable AI-driven security systems that require minimal human oversight and can function with limited computational resources will be critical. Advances in predictive analytics could allow SMEs to anticipate attacks before they materialize, shifting their defensive posture from reactive to proactive. Furthermore, quantum cryptography, although still in its early stages, promises to redefine secure communications. Research into affordable quantum-resistant encryption solutions that can be realistically integrated into SME cloud environments will be essential to ensure that small businesses are not left vulnerable in the post-quantum world.

Blockchain technologies also present a promising frontier for SME cybersecurity research. Beyond decentralized identity management, blockchain can be leveraged for secure supply chain transactions, tamper-proof audit logs, and decentralized threat intelligence sharing networks. However, current blockchain solutions often remain expensive, complex, and resource-intensive. Future research should explore how lightweight, energy-efficient blockchain frameworks can be adapted to meet the specific needs of SMEs in emerging markets. Additionally, the rise of edge computing, where data processing occurs closer to the source rather than in centralized clouds, introduces new security challenges and opportunities. Research must investigate how SMEs can implement secure edge architectures that balance local data control with robust threat protection, particularly in industries such as manufacturing, agriculture, and retail that are rapidly adopting IoT and edge solutions.

Addressing evolving threats specific to emerging markets represents another crucial research imperative. Cybersecurity threats are not homogenous; they are shaped by regional socio-economic, technological, and political factors. For SMEs in emerging markets, unique risks such as mobile-based malware, SIM-swapping attacks, cyber-enabled financial fraud, and politically motivated cybercrime are more pronounced compared to threats prevalent in developed economies. Future research must deepen the understanding of these region-specific threat landscapes, including the socio-technical factors that make certain SMEs particularly vulnerable. Studies focusing on threat intelligence gathering at local levels, adversary behavior modeling tailored to emerging market contexts, and adaptive defense strategies capable of responding to asymmetric cyber threats are urgently needed. Moreover, research should also explore the role of informal economies and unregulated digital services, which often operate outside the bounds of traditional cybersecurity frameworks yet are integral to the business activities of many SMEs in developing regions. Understanding and securing these informal digital ecosystems will be vital for comprehensive SME protection strategies.

In parallel, research must also tackle the complex challenge of balancing innovation, cost, and security in SME digital transformations. Digital innovation is critical for SME competitiveness, yet it often introduces new vulnerabilities. Many SMEs adopt cloud services, mobile platforms, and IoT devices to scale operations without fully understanding the associated security risks. Future studies should focus on developing risk assessment models specifically designed for SMEs undergoing digital transformation, offering actionable frameworks that help businesses weigh the trade-offs between adopting new technologies and maintaining strong security postures. Research can also explore decision-support systems that enable SMEs to prioritize cybersecurity investments based on risk exposure, operational impact, and compliance requirements, ensuring that limited budgets are used most effectively.

Furthermore, future research should explore how cybersecurity-by-design principles can be embedded into the digital transformation pathways of SMEs. This includes developing methodologies for secure-by-default cloud migration strategies, secure software development practices tailored for SME application developers, and pre-configured secure templates for SMEs adopting popular SaaS platforms. Special attention should be given to the affordability and usability of security tools; complex solutions that require significant expertise or maintenance will be inaccessible to most SMEs. Therefore, user-centric design principles must guide the creation of future cybersecurity tools and services for emerging market SMEs, ensuring that solutions are intuitive, low-cost, and minimally disruptive to core business operations.

Another key area requiring exploration is the intersection of cybersecurity and business resilience. As SMEs increasingly depend on digital platforms for core functions, cyber incidents pose existential risks beyond data breaches — they threaten operational continuity, reputational integrity, and long-term viability. Research should investigate integrated cybersecurity and business continuity planning models for SMEs, offering simplified yet effective approaches that embed cybersecurity considerations into broader crisis management and disaster recovery frameworks. Studies could also examine the role of cyber insurance in SME risk management strategies, assessing how insurance products can be made more accessible and appropriate for the realities of businesses in emerging markets.

Future research must also take into account the human element of cybersecurity. Technology alone cannot address all security challenges; human behavior remains a major vulnerability. Behavioral cybersecurity studies focused on SMEs in emerging markets are needed to understand how cultural, educational, and organizational factors influence security practices. Research can inform the design of more effective awareness campaigns, training programs, and incentives for secure behavior that resonate within specific socio-economic contexts. In particular, understanding the decision-making processes of SME owners and managers regarding cybersecurity investment will help shape more persuasive policy and communication strategies that encourage proactive security behavior.

Finally, collaboration must be at the heart of future research efforts. Cross-disciplinary research that brings together cybersecurity experts, economists, sociologists, behavioral scientists, cloud engineers, and public policy specialists will be critical in developing holistic solutions for SME cybersecurity challenges. International collaboration between universities, industry groups, development agencies, and governments will accelerate knowledge transfer and innovation. Initiatives such as regional cybersecurity observatories or global cybersecurity knowledge hubs focused on SMEs could play a pivotal role in sharing best practices, threat intelligence, and research findings across borders, ensuring that SMEs everywhere, regardless of size or location, have access to cutting-edge knowledge and tools. The future of cybersecurity and cloud infrastructure protection for SMEs in emerging markets depends not merely on technological advances but on the ability to adapt those advances to real-world business environments in a sustainable, equitable, and scalable manner. Future research must be deeply practical, rooted in the lived experiences of SMEs, and driven by a commitment to closing the cybersecurity gap between large corporations and the vast majority of businesses that fuel economic growth in emerging economies. By focusing on emerging technologies, evolving threats, and the critical balance between innovation, cost, and security, researchers and policymakers can build a future where SMEs are not just digitally empowered but also digitally resilient, securing their place as engines of inclusive economic development in the 21st century.

3. Conclusion

The increasing digitalization of small and medium-sized enterprises (SMEs) in emerging markets underscores the urgent need for customized cybersecurity strategies that reflect the unique challenges and opportunities they face. Unlike large corporations with vast security budgets and dedicated teams, SMEs operate within constrained environments where affordability, simplicity, and scalability are paramount. A one-size-fits-all approach to cybersecurity is neither practical nor effective for this critical segment of the economy. Instead, there is a pressing necessity for tailored frameworks that incorporate the realities of limited technical expertise, financial pressures, and diverse operational models. Solutions must prioritize risk-based security, integrating affordable emerging technologies, cloud-native defenses, and accessible training programs to empower SMEs to build meaningful resilience against an increasingly sophisticated threat landscape.

Cybersecurity is no longer a peripheral concern; it is fundamental to SME resilience and, by extension, to national economic growth and stability. SMEs form the backbone of many emerging economies, contributing significantly to employment, innovation, and social development. When SMEs suffer cyberattacks, the repercussions extend far beyond individual businesses, disrupting supply chains, eroding consumer trust, and destabilizing broader economic ecosystems. Conversely, SMEs that embed strong cybersecurity practices into their operations are better positioned to scale sustainably, access new markets, and drive inclusive growth. A resilient SME sector fortified by robust cybersecurity measures can accelerate digital transformation across industries, enhance national competitiveness, and bolster economic sovereignty in an increasingly interconnected global economy.

Moving forward, a call for integrated, forward-looking solutions is essential. The complexity of cybersecurity challenges facing SMEs demands a coordinated response that transcends piecemeal initiatives. Governments, industry leaders, technology providers, academia, and civil society must collaborate to develop comprehensive cybersecurity ecosystems that support SMEs from multiple angles—policy, technology, education, and financial incentives. These ecosystems must not only address today's threats but also anticipate tomorrow's risks, fostering continuous innovation and adaptation. Investing in cybersecurity for SMEs is not merely a defensive measure; it is a strategic imperative to ensure that the promise of the digital economy is inclusive, resilient, and sustainable. The future of emerging markets depends on it.

4. References

1. Abimbade D, Akinyemi AL, Obideyi E, Olubusayo F. Use of web analytic in open and distance learning in the University of Ibadan, Nigeria. Afr J Theory Pract Educ Res. 2016;3.
2. Abimbade O, Akinyemi A, Bello L, Mohammed H. Comparative Effects of an Individualized Computer-Based Instruction and a Modified Conventional Strategy on Students' Academic Achievement in Organic Chemistry. J Posit Psychol Couns. 2017;1(2):1-19.
3. Abimbade O, Olurinola OD, Akinyemi AL, Adepoju OD, Aina SAO. Spirituality and prosocial behavior: The influence of prosocial media and empathy. In: Proceedings of the American Educational Research Association (AERA) Annual Meeting; 2022; San Diego, California, USA.
4. Adedeji AS, Akinyemi AL, Aremu A. Effects of gamification on senior secondary school one students' motivation and achievement in Physics in Ayedaade Local Government Area of Osun State. In: Research on contemporary issues in Media Resources and Information and Communication Technology Use. BOGA Press; 2019:501-519.
5. Adediran EM, Aremu A, Amosun PAA, Akinyemi AL. The impacts of two modes of video-based instructional packages on the teaching skills of social studies pre-service teachers in South-Western Nigeria. J Educ Media Technol. 2022;27(1 & 2):38-50.
6. Adedoja G, Abimbade O, Akinyemi A, Bello L. Discovering the power of mentoring using online collaborative technologies. In: Advancing education through technology. 2017:261-281.
7. Adelana OP, Akinyemi AL. Artificial intelligence-based tutoring systems utilization for learning: a survey of senior secondary students'awareness and readiness in ijebu-ode, ogun state. UNIZIK J Educ Res Policy Stud. 2021;9:16-28.
8. Adeniran BI, Akinyemi AL, Aremu A. The effect of Webquest on civic education of junior secondary school students in Nigeria. In: Proceedings of INCEDI 2016 Conference; 2016 Aug 29-31; p. 109-120.
9. Adeniran BI, Akinyemi AL, Morakinyo DA, Aremu A. The effect of Webquest on civic education of junior secondary school students in Nigeria. Biling J Multidiscip Stud. 2022;5:296-317.
10. Adepoju PA, Austin-Gabriel B, Hussain Y, Ige B, Amoo OO, Adeoye N. Advancing zero trust architecture with AI and data science for [Incomplete reference]. 2021.

11. Adepoju PA, Austin-Gabriel B, Ige B, Hussain Y, Amoo OO, Adeoye N. Machine learning innovations for enhancing quantum-resistant cryptographic protocols in secure communication. Open Access Res J Multidiscip Stud. 2022;4(1):131–139. https://doi.org/10.53022/oarjms.2022.4.1.0075
12. Adetunmbi LA, Owolabi PA. Online Learning and Mental Stress During the Covid-19 Pandemic Lockdown: Implication for Undergraduates'mental well-being. Unilorin J Lifelong Educ. 2021;5(1):148-163.
13. Adisa IO, Akinyemi AL, Aremu A. West African Journal of Education. West Afr J Educ. 2019;39:51-64.
14. Ahmed NN, Nanath K. Exploring cybersecurity ecosystem in the Middle East: Towards an SME recommender system. J Cyber Secur Mobil. 2021:511-536.
15. Ajibola KA, Olanipekun BA. Effect of access to finance on entrepreneurial growth and development in Nigeria among "YOU WIN" beneficiaries in SouthWest, Nigeria. Ife J Entrep Bus Manag. 2019;3(1):134-149.
16. Ajonbadi HA, Lawal AA, Badmus DA, Otokiti BO. Financial Control and Organisational Performance of the Nigerian Small and Medium Enterprises (SMEs): A Catalyst for Economic Growth. Am J Bus Econ Manag. 2014;2(2):135-143.
17. Ajonbadi HA, Mojeed-Sanni BA, Otokiti BO. Sustaining competitive advantage in medium-sized enterprises (MEs) through employee social interaction and helping behaviours. J Small Bus Entrep. 2015;3(2):1–16.
18. Ajonbadi HA, Mojeed-Sanni BA, Otokiti BO. Sustaining Competitive Advantage in Medium-sized Enterprises (MEs) through Employee Social Interaction and Helping Behaviours. Bus Econ Res J. 2015;36(4).
19. Ajonbadi HA, Otokiti BO, Adebayo P. The Efficacy of Planning on Organisational Performance in the Nigeria SMEs. Eur J Bus Manag. 2016;24(3).
20. Akinbola OA, Otokiti BO. Effects of lease options as a source of finance on profitability performance of small and medium enterprises (SMEs) in Lagos State, Nigeria. Int J Econ Dev Res Invest. 2012;3(3).
21. Akinbola OA, Otokiti BO, Akinbola OS, Sanni SA. Nexus of Born Global Entrepreneurship Firms and Economic Development in Nigeria. Ekon Manazerske Spektrum. 2020;14(1):52-64.
22. Akinbola OA, Otokiti BO, Adegbuyi OA. Market Based Capabilities and Results: Inference for Telecommunication Service Businesses in Nigeria. Eur J Bus Soc Sci. 2014;12(1).
23. Akinyemi AL. Development and Utilisation of an Instructional Programme for Impacting Competence in Language of Graphics Orientation (LOGO) at Primary School Level in Ibadan, Nigeria [PhD thesis]. University of Ibadan; 2013.
24. Akinyemi AL. Computer programming integration into primary education: Implication for teachers. In: Proceedings of STAN Conference; 2018; p. 216-225.
25. Akinyemi AL. Teachers' Educational Media Competence in the Teaching of English Language in Preprimary and Primary Schools in Ibadan North Local Government Area, Nigeria. J Emerg Trends Educ Res Policy Stud. 2022;13(1):15-23.
26. Akinyemi AL, Abimbade OA. Attitude of secondary school teachers to technology usage and the way forward. In: Africa and Education, 2030 Agenda. Gab Educ. Press; 2019. p. 409–20.
27. Akinyemi AL, Aremu A. Integrating LOGO programming into Nigerian primary school curriculum. J Child Sci Technol. 2010;6(1):24–34.
28. Akinyemi AL, Aremu A. LOGO usage and the perceptions of primary school teachers in Oyo State, Nigeria. In: Proceedings of the International Conference on Education Development and Innovation (INCEDI). Methodist University College, Accra, Ghana; 2016. p. 455–62.
29. Akinyemi AL, Aremu A. Challenges of teaching computer programming in Nigerian primary schools. Afr J Educ Res. 2017;21(1–2):118–24.
30. Akinyemi AL, Ebimomi OE. Effects of video-based instructional strategy (VBIS) on students' achievement in computer programming among secondary school students in Lagos State, Nigeria. West Afr J Open Flex Learn. 2020;9(1):123–5.
31. Akinyemi AL, Ebimomi OE. Influence of Gender on Students' Learning Outcomes in Computer Studies. Educ Technol. 2020.
32. Akinyemi AL, Ebimomi OE. Influence of gender on students' learning outcomes in computer programming in Lagos State junior secondary schools. East Afr J Educ Res Policy. 2021;16:191–204.
33. Akinyemi AL, Ebiseni EO. Effects of Video-Based Instructional Strategy (VBIS) on Junior Secondary School Students' Achievement in Computer Programming in Lagos State, Nigeria. West Afr J Open Flex Learn. 2020;9(1):123–36.
34. Akinyemi AL, Ezekiel OB. University of Ibadan Lecturers' Perception of the Utilisation of Artificial Intelligence in Education. J Emerg Trends Educ Res Policy Stud. 2022;13(4):124–31.
35. Akinyemi AL, Ogundipe T. Effects of Scratch programming language on students' attitude towards geometry in Oyo State, Nigeria. In: Innovation in the 21st Century: Resetting the Disruptive Educational System. Aku Graphics Press; 2022. p. 354–61.
36. Akinyemi AL, Ojetunde SM. Techno-pedagogical models and influence of adoption of remote learning platforms on classical variables of education inequality during COVID-19 Pandemic in Africa. J Posit Psychol Couns. 2020;7(1):12–27.
37. Akinyemi AL, Oke AE. The use of online resources for teaching and learning: Teachers' perspectives in Egbeda Local Government Area, Oyo State. Ibadan J Educ Stud. 2019;16(1–2).
38. Akinyemi AL, Adelana OP, Olurinola OD. Use of infographics as teaching and learning tools: Survey of pre-service teachers' knowledge and readiness in a Nigerian university. J ICT Educ. 2022;9(1):117–30.
39. Akinyemi AL, Ogundipe T, Adelana OP. Effect of scratch programming language (SPL) on achievement in Geometry among senior secondary students in Ibadan, Nigeria. J ICT Educ. 2021;8(2):24–33.
40. Akinyemi A, Ojetunde SM. Comparative analysis of networking and e-readiness of some African and developed countries. J Emerg Trends Educ Res Policy Stud. 2019;10(2):82–90.
41. Akinyemi LA, Ologunada. Impacts of interactive learning instructional package on secondary school

students' academic achievement in basic programming. Ibadan J Educ Stud. 2022;19(2):67–74.
42. Aniebonam EE, Nwabekee US, Ogunsola OY, Elumilade OO. Int J Manag Organ Res. 2022.
43. Aremu A, Laolu AA. Language of graphics orientation (LOGO) competencies of Nigerian primary school children: Experiences from the field. J Educ Res Rev. 2014;2(4):53–60.
44. Aremu A, Adedoja S, Akinyemi A, Abimbade AO, Olasunkanmi IA. An overview of educational technology unit, Department of science and technology education, Faculty of education, University of Ibadan. 2018.
45. Aremu A, Akinyemi AL, Babafemi E. Gaming approach: A solution to mastering basic concepts of building construction in technical and vocational education in Nigeria. In: Advancing Education Through Technology. Ibadan His Lineage Publishing House; 2017. p. 659–76.
46. Aremu A, Akinyemi LA, Olasunkanmi IA, Ogundipe T. Raising the standards/quality of UBE teachers through technology-mediated strategies and resources. Emerging perspectives on Universal basic education. 2022. p. 139–49.
47. Arotiba OO, Akinyemi AL, Aremu A. Teachers' perception on the use of online learning during the Covid-19 pandemic in secondary schools in Lagos, Nigeria. J Educ Train Technol. 2021;10(3):1–10.
48. Attah JO, Mbakuuv SH, Ayange CD, Achive GW, Onoja VS, Kaya PB, *et al*. Comparative Recovery of Cellulose Pulp from Selected Agricultural Wastes in Nigeria to Mitigate Deforestation for Paper. Eur J Mater Sci. 2022;10(1):23–36.
49. Attah RU, Ogunsola OY, Garba BMP. The Future of Energy and Technology Management: Innovations, Data-Driven Insights, and Smart Solutions Development. Int J Sci Technol Res Arch. 2022;3(2):281–96.
50. Austin-Gabriel B, Hussain NY, Ige AB, Adepoju PA, Amoo OO, Afolabi AI. Advancing zero trust architecture with AI and data science for enterprise cybersecurity frameworks. Open Access Res J Eng Technol. 2021;1(1):47–55.
51. Babatunde SO, Okeleke PA, Ijomah TI. Influence of Brand Marketing on Economic Development: A Case Study of Global Consumer Goods Companies. 2022.
52. Babatunde SO, Okeleke PA, Ijomah TI. The Role of Digital Marketing In Shaping Modern Economies: An Analysis Of E-Commerce Growth And Consumer Behavior. 2022.
53. Chukwuma-Eke EC, Ogunsola OY, Isibor NJ. Designing a robust cost allocation framework for energy corporations using SAP for improved financial performance. Int J Multidiscip Res Growth Eval. 2021;2(1):809–22.
54. Chukwuma-Eke EC, Ogunsola OY, Isibor NJ. A conceptual approach to cost forecasting and financial planning in complex oil and gas projects. Int J Multidiscip Res Growth Eval. 2022;3(1):819–33.
55. Chukwuma-Eke EC, Ogunsola OY, Isibor NJ. A conceptual framework for financial optimization and budget management in large-scale energy projects. Int J Multidiscip Res Growth Eval. 2022;2(1):823–34.
56. Chukwuma-Eke EC, Ogunsola OY, Isibor NJ. Developing an integrated framework for SAP-based cost control and financial reporting in energy companies. Int J Multidiscip Res Growth Eval. 2022;3(1):805–18.
57. Dare SO, Abimbade A, Abimbade OA, Akinyemi A, Olasunkanmi IA. Computer literacy, attitude to computer and learning styles as predictors of physics students' achievement in senior secondary schools of Oyo State. 2019.
58. Esiri S. A Strategic Leadership Framework for Developing Esports Markets in Emerging Economies. Int J Multidiscip Res Growth Eval. 2021;2(1):717–24.
59. Ezekiel OB, Akinyemi AL. Utilisation of artificial intelligence in education: The perception of university of ibadan lecturers. J Glob Res Educ Soc Sci. 2022;16(5):32–40.
60. Famaye T, Akinyemi AI, Aremu A. Effects of Computer Animation on Students' Learning Outcomes in Four Core Subjects in Basic Education in Abuja, Nigeria. Afr J Educ Res. 2020;22(1):70–84.
61. Francis Onotole E, Ogunyankinnu T, Adeoye Y, Osunkanmibi AA, Aipoh G, Egbemhenghe J. The Role of Generative AI in developing new Supply Chain Strategies-Future Trends and Innovations. 2022.
62. Hamdani SWA, Abbas H, Janjua AR, Shahid WB, Amjad MF, Malik J, *et al*. Cybersecurity standards in the context of operating system: Practical aspects, analysis, and comparisons. ACM Comput Surv. 2021;54(3):1–36.
63. Hussain NY, Austin-Gabriel B, Ige AB, Adepoju PA, Amoo OO, Afolabi AI. AI-driven predictive analytics for proactive security and optimization in critical infrastructure systems. Open Access Res J Sci Technol. 2021;2(2):6–15.
64. Ibidunni AS, Ayeni AWA, Ogundana OM, Otokiti B, Mohalajeng L. Survival during times of disruptions: Rethinking strategies for enabling business viability in the developing economy. Sustainability. 2022;14(20):13549.
65. Ige AB, Austin-Gabriel B, Hussain NY, Adepoju PA, Amoo OO, Afolabi AI. Developing multimodal AI systems for comprehensive threat detection and geospatial risk mitigation. Open Access Res J Sci Technol. 2022;6(1):93–101.
66. Ilori MO, Olanipekun SA. Effects of government policies and extent of its implementations on the foundry industry in Nigeria. IOSR J Bus Manag. 2020;12(11):52–9.
67. James AT, Phd OKA, Ayobami AO, Adeagbo A. Raising employability bar and building entrepreneurial capacity in youth: a case study of national social investment programme in Nigeria. Covenant J Entrep. 2019.
68. Kolade O, Osabuohien E, Aremu A, Olanipekun KA, Osabohien R, Tunji-Olayeni P. Co-creation of entrepreneurship education: challenges and opportunities for university, industry and public sector collaboration in Nigeria. In: The Palgrave Handbook of African Entrepreneurship. 2021. p. 239–65.
69. Kolade O, Rae D, Obembe D, Woldesenbet K, editors. The Palgrave handbook of African entrepreneurship. Palgrave Macmillan; 2022.
70. Lawal AA, Ajonbadi HA, Otokiti BO. Leadership and organisational performance in the Nigeria small and medium enterprises (SMEs). Am J Bus Econ Manag. 2014;2(5):121.

71. Lawal AA, Ajonbadi HA, Otokiti BO. Strategic importance of the Nigerian small and medium enterprises (SMES): Myth or reality. Am J Bus Econ Manag. 2014;2(4):94–104.
72. Muibi TG, Akinyemi AL. Emergency Remote Teaching During Covid-19 Pandemic And Undergraduates'learning Effectiveness At The University Of Ibadan, Nigeria. Afr J Educ Manag. 2022;23(2):95–110.
73. Nwabekee US, Aniebonam EE, Elumilade OO, Ogunsola OY. Predictive Model for Enhancing Long-Term Customer Relationships and Profitability in Retail and Service-Based. 2021.
74. Nwabekee US, Aniebonam EE, Elumilade OO, Ogunsola OY. Integrating Digital Marketing Strategies with Financial Performance Metrics to Drive Profitability Across Competitive Market Sectors. 2021.
75. Nwaimo CS, Adewumi A, Ajiga D. Advanced data analytics and business intelligence: Building resilience in risk management. Int J Sci Res Appl. 2022;6(2):121.
76. Odunaiya OG, Soyombo OT, Ogunsola OY. Economic incentives for EV adoption: A comparative study between the United States and Nigeria. J Adv Educ Sci. 2021;1(2):64–74.
77. Odunaiya OG, Soyombo OT, Ogunsola OY. Energy storage solutions for solar power: Technologies and challenges. Int J Multidiscip Res Growth Eval. 2021;2(1):882–90.
78. Odunaiya OG, Soyombo OT, Ogunsola OY. Sustainable energy solutions through AI and software engineering: Optimizing resource management in renewable energy systems. J Adv Educ Sci. 2022;2(1):26–37.
79. Ogundare AF, Akinyemi AL, Aremu A. Impact of gamification and game-based learning on senior secondary school students' achievement in English language. J Educ Rev. 2021;13(1):110–23.
80. Ogunyankinnu T, Onotole EF, Osunkanmibi AA, Adeoye Y, Aipoh G, Egbemhenghe J. Blockchain and AI synergies for effective supply chain management. 2022.
81. Okeleke PA, Babatunde SO, Ijomah TI. The Ethical Implications and Economic Impact of Marketing Medical Products: Balancing Profit and Patient Well-Being. 2022.
82. Olaiya SM, Akinyemi AL, Aremu A. Effect of a board game: Snakes and ladders on students' achievement in civic education. J Niger Assoc Educ Media Technol. 2017;21(2).
83. Olanipekun KA. Assessment of Factors Influencing the Development and Sustainability of Small Scale Foundry Enterprises in Nigeria: A Case Study of Lagos State. Asian J Soc Sci Manag Stud. 2020;7(4):288–94.
84. Olanipekun KA, Ayotola A. Introduction to marketing. GES 301, Centre for General Studies (CGS), University of Ibadan. 2019.
85. Olanipekun KA, Ilori MO, Ibitoye SA. Effect of Government Policies and Extent of Its Implementation on the Foundry Industry in Nigeria. 2020.
86. Olojede FO, Akinyemi A. Stakeholders' readiness For Adoption of Social Media Platforms For Teaching And Learning Activities In Senior Secondary Schools In Ibadan Metropolis, Oyo State, Nigeria. Int J Gen Stud Educ. 2022;141.
87. Oludare JK, Adeyemi K, Otokiti B. Impact Of Knowledge Management Practices And Performance Of Selected Multinational Manufacturing Firms In South-Western Nigeria. 2022;2(1):48.
88. Olufemi-Phillips AQ, Ofodile OC, Toromade AS, Eyo-Udo NL, Adewale TT. Optimizing FMCG supply chain management with IoT and cloud computing integration. Int J Manag Entrep Res. 2020;6(11).
89. Otokiti BO. A study of management practices and organisational performance of selected MNCs in emerging market - A Case of Nigeria. Int J Bus Manag Invent. 2017;6(6):1–7.
90. Otokiti BO. Mode of Entry of Multinational Corporation and their Performance in the Nigeria Market [PhD thesis]. Covenant University; 2012.
91. Otokiti BO. Social media and business growth of women entrepreneurs in Ilorin metropolis. Int J Entrep Bus Manag. 2017;1(2):50–65.
92. Otokiti BO. Business regulation and control in Nigeria. In: Book of Readings in Honour of Professor S. O. Otokiti. 2018. p. 201–15.
93. Otokiti BO, Akorede AF. Advancing sustainability through change and innovation: A co-evolutionary perspective. In: Innovation: Taking creativity to the market. 2018. p. 161–7.
94. Otokiti BO, Onalaja AE. The role of strategic brand positioning in driving business growth and competitive advantage. Iconic Res Eng J. 2021;4(9):151–68.
95. Otokiti BO, Onalaja AE. Women's leadership in marketing and media: Overcoming barriers and creating lasting industry impact. Int J Soc Sci Except Res. 2022;1(1):173–85.
96. Otokiti BO, Igwe AN, Ewim CP, Ibeh AI, Sikhakhane-Nwokediegwu Z. A framework for developing resilient business models for Nigerian SMEs in response to economic disruptions. Int J Multidiscip Res Growth Eval. 2022;3(1):647–59.
97. Otokiti BO, Akinbola OA. Effects of Lease Options on the Organizational Growth of Small and Medium Enterprise (SME's) in Lagos State, Nigeria. Asian J Bus Manag Sci. 2013;3(4).
98. Otokiti-Ilori BO. Business Regulation and Control in Nigeria. In: Book of readings in honour of Professor S.O Otokiti. 2018;1(1).
99. Otokiti-Ilori BO, Akorede AF. Advancing Sustainability through Change and Innovation: A co-evolutionary perspective. In: Innovation: taking Creativity to the Market. 2018;1(1):161–7.
100. Tella A, Akinyemi AL. Entrepreneurship education and Self-sustenance among National Youth Service Corps members in Ibadan, Nigeria. Proceedings E-BOOK. 2022.