

Cybersecurity Threats and Mitigation Strategies in Cloud-Based Retail and E-Commerce Platforms: A Systematic Literature Review

Ademola Moruf Ojo, Ridwan Kolapo, Temitope Olufunmi Atoyebi

Department of Information Technology, Faculty of Computing, Nile University of Nigeria, Abuja, Nigeria.

DOI: <https://doi.org/10.51244/IJRSI.2026.1308000190>

Received: 29 August 2026; Accepted: 03 September 2026; Published: 14 September 2026

ABSTRACT

Retail and e-commerce in the cloud have driven modern digital commerce, encompassing online stores, mobile payments, marketplace participation, logistics, customer analytics, real-time payment services, and more. This transformation has introduced additional cybersecurity challenges across websites, mobile applications, APIs, seller dashboards, cloud storage, customer databases, payment workflows, third-party integrations, and identity systems. This paper systematically highlights cybersecurity threats and corresponding mitigation strategies affecting cloud-based retail and e-commerce platforms. The methodology involved a qualitative, systematic literature review using PRISMA principles and a Parsifal-managed review process. The search covered seven electronic sources and yielded 1,340 records. Of these, 102 full-text studies were considered for inclusion, and the final synthesis included 35 peer-reviewed journal articles and conference papers published from 2021 to 2026. The results indicate that phishing, account takeover, credential stuffing, cloud misconfiguration, insecure APIs, payment fraud, fake listings, insider misuse, malware, ransomware, distributed denial-of-service attacks, data leakage, bot abuse, business-logic abuse, and supply-chain compromise are the most significant threats. Nigerian e-commerce platforms need to focus more on trust-building strategies, scam prevention, data protection maturity, payment confidence, identity security, and early incident response, while global platforms should adopt a scalable Zero Trust strategy, AI-assisted detection, seller ecosystem governance, API security, privacy engineering, and supply-chain resilience. The research outlines a cyber-resilience approach framed by NIST CSF 2.0 functions, structured around them, and aligned with ISO/IEC 27001:2022 controls without exception.

Keywords: Cloud security, e-commerce cybersecurity, NIST CSF 2.0, ISO/IEC 27001:2022, Zero Trust Architecture, AI-driven threat detection, Nigerian e-commerce, online retail security.

INTRODUCTION

In digital business, retail, and e-commerce, cloud-based platforms have grown exponentially in importance. The latest platforms not only enable online sales but also support mobile payments, marketplace participation, logistics coordination, customer analytics, real-time payment systems, seller ecosystems, cloud storage, and application programming interfaces (APIs). These tools help businesses adapt and improve efficiency, but they also create challenges from multi-source cybersecurity threats across interconnected cloud services and customer-facing systems [1], [2], [12].

Cloud-based retail stores must contend with a multifaceted cybersecurity attack surface spanning websites, mobile applications, APIs, seller dashboards, cloud storage, customer databases, payment workflows, third-party integrations, and identity systems. Cloud security literature highlights vulnerabilities such as inadequate authentication and access control, poor data protection, insufficient monitoring, misconfiguration, and reliance on other cloud services, which are frequently the main concerns. Adopting cloud-native services increases risk through microservices, containers, APIs, orchestration, and distributed workloads [1], [2], [8], [12]. In e-commerce, cybersecurity vulnerabilities can disrupt customer, seller, and worker operations, payment services, business processes, data protection, and organizational trust. Current e-commerce research identifies potential concerns such as phishing, compromised accounts, transaction fraud, payment manipulation, fake listings, and social engineering. Studies on fraud detection point to transaction monitoring, behavioral analysis, and machine-

learning methods for combating emerging fraud trends [6], [7], [9]. Phishing is significant to this topic because fraudsters may create fake websites, messages, login pages, delivery notifications, and refund communications, and may also impersonate customer-support representatives of well-known retail brands. Recent studies on phishing detection focus mainly on URL analysis, webpage-content analysis, machine learning, and deep learning, while also addressing data quality, adversarial adaptation, generalization, and real-world deployment [4], [5], [10].

Identity and access management is another major area of cybersecurity. Weak authentication, compromised credentials, excessive privileges, and inadequate access controls can lead to unauthorized access and contribute to account takeovers and other cybercrimes. Zero Trust research notes that distributed and cloud environments should adopt continuous verification, least privilege, and identity-oriented access control as key principles [11].

The aim of the study is to conduct a systematic literature review on Cyber Security Threats and Mitigation Strategies in Cloud-Based Retail and E-Commerce Platforms

The objectives of the study are to:

1. Review, based on peer-reviewed literature published between 2021 and 2026, how e-commerce brand impersonation and credential phishing affect cloud-based retail and e-commerce platforms.
2. Assess how phishing risk manifests across selected Nigerian and global e-commerce platforms, focusing on customers, sellers, account access, payment workflows, and trust.
3. Evaluate mitigation strategies, including user awareness, multi-factor authentication, secure account recovery, anti-phishing detection, AI-assisted monitoring, Zero Trust Architecture, DevSecOps, and incident response.
4. Recommend a framework-aligned anti-phishing solution mapped to NIST CSF 2.0 and ISO/IEC 27001:2022 for cloud-based retail and e-commerce platforms.

LITERATURE REVIEW

The article highlights the integration of cloud computing security with multiple issues, including authentication, access control, privacy, data protection, monitoring, service availability, governance, and risk management, all of which recent studies examined. Al Nafea and Almaiah focused on stronger authentication, data protection, monitoring, and risk-aware governance, while Alouffi et al. synthesized cloud threats and, for general controls, emphasized the need for layering [1], [2].

The main reason IaaS, PaaS, and SaaS have different security requirements is that security is a shared responsibility between providers and users. Thus, Parast et al. emphasized the need for controls addressing data security, access control, and shared responsibility [8]. Cloud-native architectures also introduce additional risks associated with microservices, containers, APIs, orchestration, and distributed workloads. Theodoropoulos et al. identified the following as crucial components of cloud-native security: secure design, runtime monitoring, API protection, DevSecOps, and supply-chain awareness [12].

E-commerce faces the persistent cybersecurity challenge of fraud. Rodrigues et al. note that fraud prevention benefits from transaction monitoring, behavioral analysis, machine learning, and platform-level controls. Mutemi and Bação noted that the inflation of fraudsters' patterns is a difficult-to-tackle issue; machine-learning methods require high-quality data, continuous validation, and integration with operations, even with static controls [7], [9]. Liu et al. again highlighted ongoing cybersecurity problems in e-commerce, especially regarding user trust, privacy, and transaction security [6].

Recent studies on phishing have focused on URL classification, webpage content analysis, feature extraction, and machine learning and deep learning. For example, Catal et al. reviewed deep-learning techniques for phishing detection, while Do et al. offered a taxonomy of deep-learning techniques and addressed issues such as adversarial behavior, data quality, and deployment. Furthermore, Safi and Singh provided a detailed review of

phishing website detection and reported hybrid approaches that combine URL, content, and machine-learning features [4], [5], [10].

Identity-centered security is particularly applicable to cloud-based retail because of the multitude of parties, such as customers, sellers, administrators, employees, vendors, and third parties, who interact with and use the common digital services. Syed and his colleagues found Zero Trust Architecture to be a model that focuses on continuous validation, least-privilege access, and identity-centered access control for distributed and cloud-based settings [11].

Security is a crucial component of both software development and operations. According to Akbar et al., implementing DevSecOps requires four essential prerequisites: organizational readiness, automation, secure development practices, and management support [3]. These prerequisites complement one another, highlighting that cloud-based retail cybersecurity requires coordinated governance, identity protection, secure development, monitoring, detection, and response, rather than relying on isolated controls.

Integrating these evidence streams within a retail-focused cloud context remains a significant research gap. Existing studies largely focus on cloud security, e-commerce fraud, phishing detection, or Zero Trust, often in isolation. Fewer studies examine combinations of these topics and consider customers, sellers, payment workflows, APIs, cloud services, and platform governance. To address this gap, the document brings together categories of threats, platform exposure, mitigation strategies, and cyber resilience priorities for selected e-commerce platforms in Nigeria and globally [1], [6], [7], [9], [11], [12].

The literature identifies the integration of these areas within cloud-based retail and e-commerce as the primary gap. It also lacks comparative discussions of cybersecurity priorities between Nigerian and global platforms. This research addresses these gaps through threat classification, platform comparison, mitigation mapping, and framework-aligned strategic recommendations.

METHODOLOGY

Research Format

This research followed a qualitative systematic literature review design. This approach was chosen because, unlike methods that collect data from respondents through instruments such as interviews, surveys, or laboratory experiments, this study focuses on collecting, assessing, and synthesizing prior literature, making primary data collection through those methods unnecessary. The review's major characteristics were the dynamic application of PRISMA principles and the thematic categorization of the resulting data into cybersecurity threats, vulnerabilities, relevant platform components, mitigation strategies, and framework alignment.

Review Management

The use of Parsifal software for the systematic literature review was a significant part of the process. The review management process included formulating research questions, developing the search strategy and inclusion and exclusion criteria, selecting studies, extracting data, assessing quality, and synthesizing findings.

Search Strategy and Data Sources

The systematic review focused on peer-reviewed journal articles and conference papers published between 2021 and 2026. I searched IEEE Xplore, ACM Digital Library, SpringerLink, ScienceDirect, Wiley Online Library, Google Scholar, and Scopus. Search terms included cloud security, e-commerce cybersecurity, phishing, fraud, insider threats, Zero Trust Architecture, DevSecOps, AI-driven detection, and cyber resilience.

Inclusion and Exclusion Criteria

The included studies were published between 2021 and 2026; were peer-reviewed journal articles or conference papers; covered cloud security, e-commerce cybersecurity, phishing, fraud, insider threats, Zero Trust, DevSecOps, or AI-driven detection; were relevant to the research questions; and provided evidence suitable for

thematic and framework-aligned analysis. I excluded studies outside the imposed limits, such as scope, time, or evidence requirements.

Study Selection Process

The review followed the PRISMA framework, including identification, duplicate checking, title and abstract screening, full-text eligibility assessment, and final inclusion. In total, the identification stage yielded 1,340 records from seven sources. I checked for duplicates using titles, authors, publication years, DOIs, and publication venues. After title and abstract screening, 102 studies proceeded to full-text eligibility assessment. We evaluated full texts against the inclusion and exclusion criteria, quality threshold, and relevance to the research question. Altogether, the process retained 35 peer-reviewed journal articles and conference papers published between 2021 and 2026 for synthesis.

PRISMA Flow Diagram for Study Selection

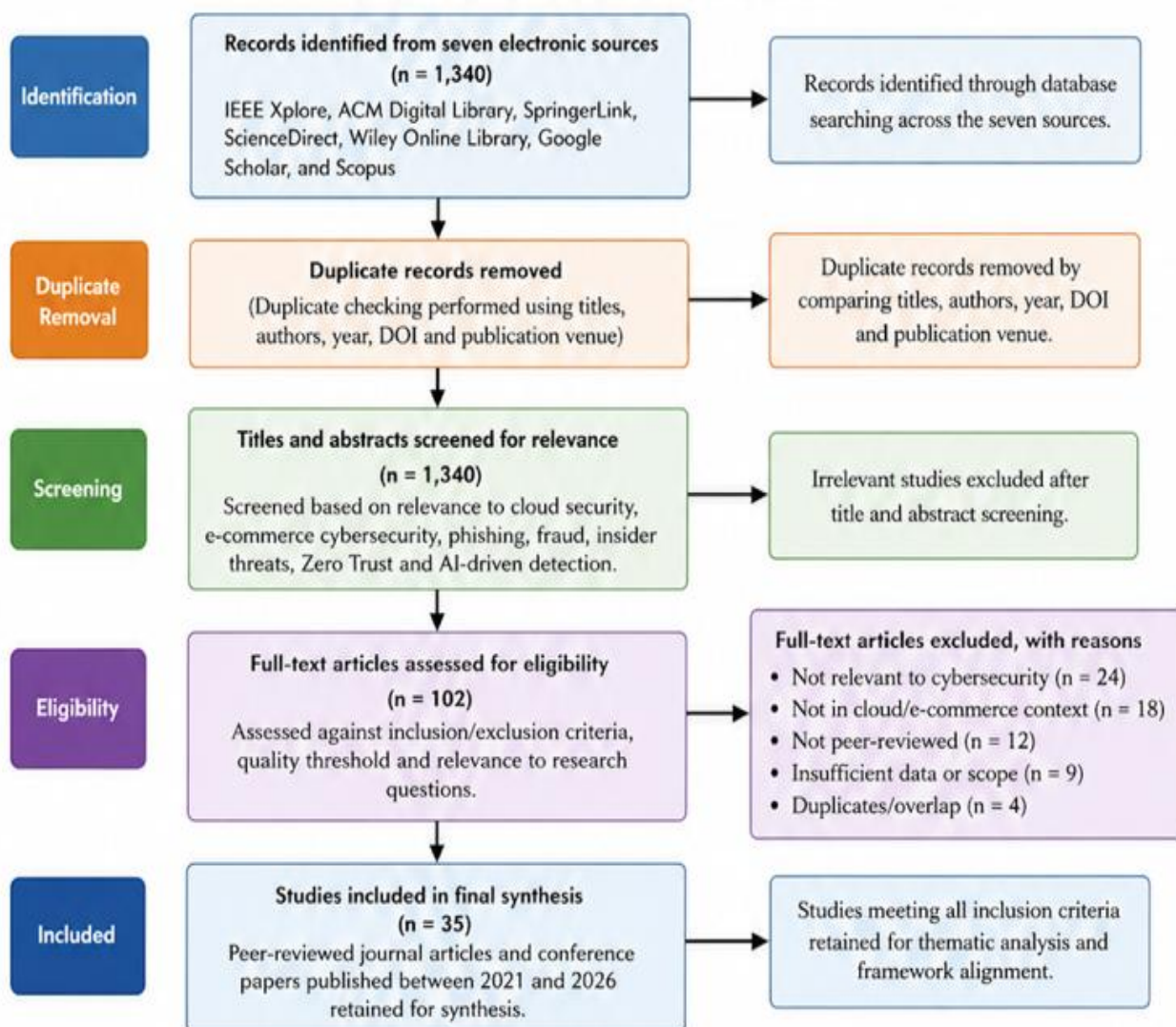


Figure 1. PRISMA Flow Diagram for Study Selection

Data Extraction and Analysis

Data extraction aligned with the study objectives and research questions. The extraction process was based on the study source, research focus, cybersecurity threat category, vulnerability, affected component, mitigation strategy, platform relevance, framework alignment, findings, and limitations. Thematic analysis grouped the evidence into major categories: threats, vulnerabilities, platforms, mitigation strategies, and framework-aligned cybersecurity actions. The findings were then mapped to the NIST CSF 2.0 functions and ISO/IEC 27001:2022.

Quality Assessment

The study included a quality assessment to evaluate the studies' relevance and methodological value. The assessment criteria were relevance to the research objectives, methodological clarity, strength of evidence, applicability to cloud-based retail and e-commerce, framework relevance, and limitations.

RESULTS AND DISCUSSION

Cybersecurity Threats and Cloud-Architecture Vulnerabilities

The literature review identified a broad range of cyber threats targeting cloud-based retail and e-commerce platforms. The most common threats include phishing, account takeover, credential stuffing, cloud misconfiguration, insecure APIs, payment fraud, fake listings, insider misuse, malware, ransomware, distributed denial-of-service attacks, data leakage, bot abuse, business-logic abuse, and supply-chain compromise.

Cloud misconfiguration is a major vulnerability because cloud environments require users to regularly manage permissions, access controls, storage configurations, network settings, identity policies, logging, and service integrations. Weak configurations can expose sensitive customer and company information.

Insecure APIs also matter greatly because e-commerce platforms rely heavily on APIs for functions such as payments, logistics, mobile applications, seller services, customer support, analytics, and third-party integrations. Weak authentication, lack of authorization, validation, or monitoring can expose the system to unauthorized access and data leakage.

Identity compromise was also identified as a major risk area. Credential theft, weak authentication mechanisms, excessive privileges, poorly designed recovery processes, and inadequate access management can lead to account takeover, fraud, insider misuse, and unauthorized access. Therefore, the findings indicate that the cybersecurity threats affecting cloud-based retail are interconnected.

Nigerian and Global Risk Platform Comparison

The investigation covered selected Nigerian and global platforms. Nigeria's group included Jumia Nigeria, Konga, Jiji Nigeria, Slot Systems Limited, and Supermart Nigeria. The global group included Amazon Bazaar, AliExpress, Walmart, and eBay.

The research clearly shows parallels between Nigerian and global platforms in the types of cyber threats they face, but their implementation priorities differ. Nigerian platforms require greater emphasis on customer trust, scam prevention, identity security, payment confidence, data protection maturity, seller and account protection, and incident readiness. Global platforms need more on-the-spot handling of scalable security automation, Zero Trust implementation, AI-assisted detection, API resilience, seller ecosystem governance, privacy engineering, supply-chain resilience, and transparent incident communication.

Rationale for Platform Selection

The rationale for platform selection is that the Nigerian and global platforms listed in Table 1 are chosen as Contextual cases for the systematic synthesis are drawn from the two geographic regions specified in the study: selected e-commerce platforms in Nigeria and selected global platforms (Amazon Bazaar, AliExpress, Walmart, and eBay), alongside the Nigerian platforms (Jumia Nigeria, Konga, Jiji Nigeria, Slot Systems Limited, and Supermart Nigeria). This choice allows comparison of how the threat categories identified in the literature might manifest across different e-commerce environments, focusing on customers, sellers, account access, payment workflows, trust, cloud services, APIs, and platform governance. Therefore, the platform selection serves as a purposive analytical sample for intra-review comparison rather than a statistically representative sample of the entire Nigerian or global e-commerce platform groups. The comparison should not be construed as a ranking of cybersecurity maturity or incident occurrence.

Table 1. Nigerian and Global Platform Risk Comparison

Dimension	Nigerian Platforms	Global Platforms
Platforms	Jumia, Konga, Jiji, Slot Systems, Supermart	Amazon Bazaar, AliExpress, Walmart, eBay
Main Risks	Scams, fake listings, phishing, payment fraud, data protection maturity	Large-scale fraud, seller abuse, cross-border privacy, API exposure, supply-chain risk
User Context	Mobile-first access, varied digital literacy, local payment realities	Global users, broad seller ecosystems, stronger regulatory pressure
Priority Controls	Trust building, scam prevention, MFA, fraud monitoring, incident readiness	Zero Trust, AI-assisted detection, API security, privacy engineering, supply-chain governance

Empirical Validation and Evidentiary Limitation

The study is primarily a qualitative systematic literature review; it does not measure the extent to which individual cybersecurity attacks occurred or the degree to which they occurred on the platforms discussed in this study. The study does not include an incident-level dataset, platform telemetry, vulnerability scans, penetration test results, or forensic evidence for the selected companies. Thus, the outlined threat categories should be understood as literature-derived conclusions and as risk categories suitable to platform contexts, not as measured incidents reported for those platforms. Presenting the number of platform-specific incidents or assessing severity would require more independent, verifiable empirical evidence beyond this review's scope.

Framework-Aligned Mitigation Strategies

The research indicates that cloud-based retail cybersecurity requires a combination of strategies, not just standalone technical controls. The most relevant countermeasures include Zero Trust Architecture, AI-driven threat detection, DevSecOps, identity and access management, API security, cloud configuration governance, fraud analytics, incident response, and recovery planning.

These countermeasures can apply across customer accounts, seller dashboards, cloud services, APIs, payment systems, logistics integrations, and organizational operations. The research's strategic framework is based on the NIST CSF 2.0, which organizes cybersecurity actions into Govern, Identify, Protect, Detect, Respond, and Recover, while ISO/IEC 27001:2022 aligns controls for implementation.

Framework-Aligned Cyber Resilience Model

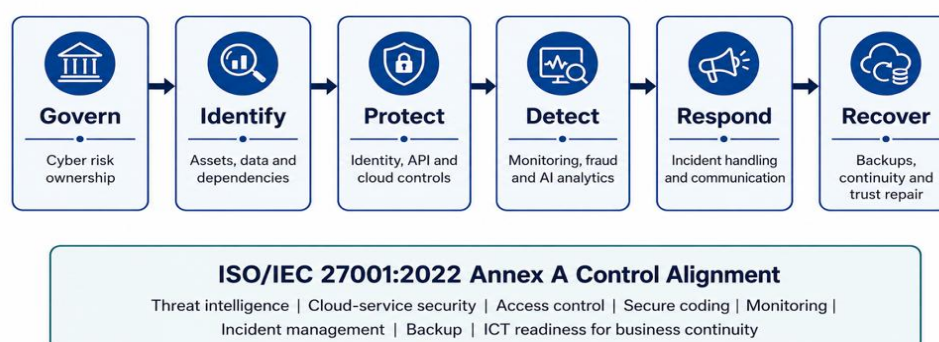


Figure 2. Framework-Aligned Cyber Resilience Model

Strategic Recommendations

Govern: Companies should have cybersecurity leadership at the executive level, along with policies, accountability structures, risk management responsibilities, and a supplier oversight plan in place.

Identify: Companies should maintain records of all assets and related information, map critical data flows, document cloud usage, evaluate attack surfaces, and assess risk across customer accounts, seller dashboards, payment systems, APIs, mobile apps, cloud storage, and third-party integrations.

Protect: Protection strategies ought to include identity and access management, multi-factor authentication, least-privilege access, encryption, secure coding, API security, cloud configuration management, seller verification, and cybersecurity awareness.

Detect: Detection should integrate fraud analytics, cloud monitoring, threat intelligence, AI-assisted detection, suspicious-login analysis, anomaly detection, and continuous security monitoring.

Respond: Platforms should have incident management plans, clear escalation procedures, stakeholder communication processes, investigation capabilities, and coordinated containment measures.

Recover: Recovery actions should focus on restoring service, recovering backups, reconciling orders and transactions, ensuring business continuity, conducting restoration testing, capturing lessons learned, and rebuilding customer trust.

Discussion of Key Security Gaps

The research results identified several problems affecting the security of cloud-based retail and e-commerce systems. The first was a governance issue: cybersecurity lacked sufficient executive ownership and enterprise-level risk management attention.

The second issue is an identity gap involving weak authentication, compromised credentials, and excessive access privileges, caused by inadequate account protection. The third is a cloud-configuration gap, including weaknesses in permissions, access control, storage, monitoring, and visibility.

The fourth is an API security gap, stemming from weak authentication, authorization, validation, monitoring, and rate control. The fifth is a detection gap, in which platforms may lack sufficient behavioral analytics, fraud monitoring, cloud visibility, threat intelligence, and AI-assisted detection.

The sixth is an incident-response and recovery gap, marked by untested procedures, weak communication, poor planning, and little or no post-incident improvement. The research findings and contributions align with the four goals of distinguishing and evaluating threats and vulnerabilities, contrasting with global platforms from Nigeria, evaluating mitigation, and, lastly, providing NIST/ISO-compliant recommendations.

CONCLUSION

This research paper presents a systematic review of cybersecurity threats and mitigation strategies affecting cloud-based retail and e-commerce platforms. The review included 35 articles from peer-reviewed journals and conference papers published between 2021 and 2026. These articles were selected using the PRISMA-defined process from among 1,340 items, with 102 items awaiting full-text eligibility assessment.

According to the research, online retail and e-commerce platforms offered on a cloud basis are exposed to interconnected threats, including phishing, account takeover, credential stuffing, cloud misconfiguration, insecure APIs, payment fraud, fake listings, employee misappropriation, malware, ransomware, distributed denial-of-service, data leakage, bot abuse, business-logic abuse, and supply-chain compromise.

The comparative analysis found that Nigerian platforms and their international counterparts face the same categories of cybersecurity threats, but differences in impact lead to different priorities. Nigerian online platforms face primary challenges around customer trust and scam prevention, including identity security, payment confidence, data protection maturity, and incident readiness. Global platforms prioritize adopting scalable Zero Trust, AI-based detection, API resilience, seller ecosystem governance, privacy engineering, supply-chain resilience, and open incident communication practices.

The investigation also found that assigning full cybersecurity responsibility to a single technical control is unrealistic. A resilient cloud-based retail environment requires integrated governance, asset identification, identity protection, secure cloud configuration, API security, AI-assisted detection, fraud analytics, incident response, recovery planning, and continuous improvement.

The core point is that the framework enables a cyber-resilience approach that distributes actions across the NIST CSF 2.0 functions of Govern, Identify, Protect, Detect, Respond, and Recover, while ISO/IEC 27001:2022 is used for control alignment and implementation.

The next stage of cyber-resilience research should prioritize empirical validation of the proposed cyber-resilience model over a literature synthesis. The research should first focus on basic, authorized, platform-level case studies that examine real-world incidents, phishing reports, account takeover attempts, fraud, API exposures, and cloud-security incidents on a specific platform to collect measurable data on severity and frequency. Second, the initiative should include a controlled study of exploratory generative-AI phishing and how opposing facets of human behavior respond, integrating machine learning models for detection, user awareness, auto-classification, and incident-response controls. Third, the focus should be on serverless cloud vulnerabilities and their impact on e-commerce, which relies on event-driven services, APIs, identity controls, logging, and third-party integrations. Fourth, long-term studies should assess AI-assisted detection, Zero Trust controls, DevSecOps practices, and incident-response capabilities over time, along with false positives, model drift, operational cost, and recovery performance. Fifth, the Nigerian dimension should call for collaborative empirical research involving cybersecurity professionals, platform operators, sellers, and users to determine whether the priorities identified in this survey align with operational experience. These studies would provide empirical data to validate, refine, and quantify the framework proposed in this research.

REFERENCES

1. Al Nafea, R., & Almaiah, M. A. (2021). Cyber security threats in cloud: Literature review. In 2021 International Conference on Information Technology (ICIT) (pp. 779–786). IEEE. <https://doi.org/10.1109/ICIT52682.2021.9491638>
2. Alouffi, B., Hasnain, M., Alharbi, A., Alosaimi, W., Alyami, H., & Ayaz, M. (2021). A systematic literature review on cloud computing security: Threats and mitigation strategies. *IEEE Access*, 9, 57792–57807. <https://doi.org/10.1109/ACCESS.2021.3073203>
3. Akbar, M. A., Smolander, K., Mahmood, S., & Alsanad, A. (2022). Toward successful DevSecOps in software development organizations: A decision-making framework. *Information and Software Technology*, 147, Article 106894. <https://doi.org/10.1016/j.infsof.2022.106894>
4. Catal, C., Giray, G., Tekinerdogan, B., Kumar, S., & Shukla, S. (2022). Applications of deep learning for phishing detection: A systematic literature review. *Knowledge and Information Systems*, 64(6), 1457–1500. <https://doi.org/10.1007/s10115-022-01672-x>
5. Do, N. Q., Selamat, A., Krejcar, O., Herrera-Viedma, E., & Fujita, H. (2022). Deep learning for phishing detection: Taxonomy, current challenges and future directions. *IEEE Access*, 10, 36429–36463. <https://doi.org/10.1109/ACCESS.2022.3151903>
6. Liu, X., Ahmad, S. F., Anser, M. K., Ke, J., Irshad, M., Ul-Haq, J., & Abbas, S. (2022). Cyber security threats: A never-ending challenge for e-commerce. *Frontiers in Psychology*, 13, Article 927398. <https://doi.org/10.3389/fpsyg.2022.927398>
7. Mutemi, A., & Bação, F. (2024). E-commerce fraud detection based on machine learning techniques: Systematic literature review. *Big Data Mining and Analytics*, 7(2), 419–444. <https://doi.org/10.26599/BDMA.2023.9020023>

8. Parast, F. K., Sindhav, C., Nikam, S., Yekta, H. I., Kent, K. B., & Hakak, S. (2022). Cloud computing security: A survey of service-based models. *Computers & Security*, 114, Article 102580. <https://doi.org/10.1016/j.cose.2021.102580>
9. Rodrigues, V. F., Policarpo, L. M., da Silveira, D. E., da Rosa Righi, R., da Costa, C. A., Barbosa, J. L. V., Antunes, R. S., Scorsatto, R., & Arcot, T. (2022). Fraud detection and prevention in e-commerce: A systematic literature review. *Electronic Commerce Research and Applications*, 56, Article 101207. <https://doi.org/10.1016/j.elerap.2022.101207>
10. Safi, A., & Singh, S. (2023). A systematic literature review on phishing website detection techniques. *Journal of King Saud University - Computer and Information Sciences*, 35(2), 590–611. <https://doi.org/10.1016/j.jksuci.2023.01.004>
11. Syed, N. F., Shah, S. W., Shaghaghi, A., Anwar, A., Baig, Z., & Doss, R. (2022). Zero Trust Architecture (ZTA): A comprehensive survey. *IEEE Access*, 10, 57143–57179. <https://doi.org/10.1109/ACCESS.2022.3174679>
12. Theodoropoulos, T., Rosa, L., Benzaid, C., Gray, P., Marin, E., Makris, A., Cordeiro, L., Diego, F., Sorokin, P., Di Girolamo, M., Barone, P., Taleb, T., & Tserpes, K. (2023). Security in cloud-native services: A survey. *Journal of Cybersecurity and Privacy*, 3(4), 758–793. <https://doi.org/10.3390/jcp3040034>