JOURNAL OF BUSINESS AND SOCIAL SCIENCES
eISSN:2805-5187 | Vol.2025, Issue 3, No.4

Strengthening Ghana's Banking Security through IoT: Implications for Achieving SDG Goals

Adade Sedom Percy[1], Emmanuel Ofotsu Kwesi Bannor[1], Doris Enimil[1]
Khan Sarfaraz Ali[2*] , Ida Hindarsah[3]

[1]Faculty of Data Science and Information Technology,
INTI International University, Malaysia
[2]Faculty of Business, INTI International University, Malaysia
[3]Universitas Pasundan, Bandung, Indonesia

Email: khan.sarfarazali@newinti.edu.my*, ida.hindarsah@unpas.ac.id

Abstract

The use of the Internet of Things (IoT) in Ghana's banking sector has enormously enhanced efficiency in operations and customer service delivery. The digitalization process, however, poses considerable cybersecurity threats. This study investigates the impact of IoT on Ghanaian banks' cybersecurity with emphasis on the prominent risks, challenges, and strategic interventions. According to secondary data extracted from top banking reports and qualitative analysis by IT security professionals, we have prevalence of threats such as distributed denial-of-service (DDoS) attacks, unauthorised access, and data breaches. The findings quote the highest priority need for robust cybersecurity measures, continuous risk assessment, and government-initiated regulatory structures to offset risks of IoT deployments in financial institutions. The findings reference the greatest need for efficient cybersecurity measures, continued risk evaluation, and regulatory-driven frameworks being initiated by governments in order to offset vulnerabilities of IoT installations in financial institutions It is in line with Sustainable Development Goal 9 (Industry, Innovation, and Infrastructure), SDG 11 (Sustainable Cities and Communities), and SDG 16 (Peace, Justice, and Strong Institutions), as regards providing safe, resilient, and secure financial environments.

Keywords

Internet of Things (Iot), Cybersecurity, Banking Industry

Introduction

The development of Internet of Things (IoT) technologies has brought profound influences on banking institutions through its promotion of work efficiency, satisfaction to clients, and innovative digital services. With current banking environments, IoT facilitates digital services such as smart automatic teller machines based on biometric verification, online remote tracking of transactions in real-time and smart tracking systems coupled with mobile applications in order to promote interaction with clients. These technologies are being adopted

Submission: 15 October 2025; **Acceptance:** 21 December 2025 **Available online:** December 2025

ever more in the financial sector in Ghana as part of broader digitalization efforts to facilitate financial inclusion, operational transparency, and customization of services [1, [2].Use of IoT in banking systems, however, provides a complex security setup. Unlike traditional IT systems, IoT networks consist of heterogeneous devices that have limited processing power and limited security configurations. This increases the attack surface, exposing financial institutions to a range of cyber threats like unauthorized data access, data tapping, device tampering, and Distributed Denial-of-Service (DDoS) attacks: This is particularly a risky scenario in emerging economies like Ghana, where institutional and infrastructure lacunae may jeopardize the safe adoption of IOT -based solutions. Since the banking sector continue to digitize, it is important to understand the relationship between IOT deployment and cybersecurity threats for policymakers, technology vendors, and banks seeking to secure digital finance systems.

Literature review

The security concerns of IoT within the banking sector have been extensively documented across international and regional literature. Researchers have pointed out that the majority of IoT devices, especially those in financial services, lack the essential security features such as end-to-end encryption, secure boot, and regular firmware updates [3]. These loopholes leave IoT networks vulnerable to fraudulent activities such as spoofing, eavesdropping, and botnet assaults, with potential consequences of money data compromises and institutions' loss of reputation. Within the Ghanaian context, the weaknesses of IoT banking are augmented by structural constraints.

Firstly, the national ICT infrastructure although developing still suffers from erratic internet connectivity, substandard data centre facilities, and poor device interoperability, which collectively hinder safe IoT deployment [4]. Moreover, there is no regulation for handling specialized security requirements of IoT technology. Although Ghana has enacted the Data Protection Act and a national cybersecurity policy was approved, no specialized regulation of IoT exists, and such security procedures in financial institutions are not standard. Also, the human skills base for cybersecurity in Ghana is marred by a critical shortage of skills, particularly in IoT device security, risk analysis, and monitoring of threats in real-time.

This scarcity restricts the capacity of banks to actively counter forthcoming threats and to effectively react to incidents. Studies further show that insufficient investment and budgetary limitations on security infrastructure rank among the reasons for delay or incompleteness in implementing best practices in IoT cybersecurity [5, 6]. In conclusion, literature identifies that while IoT has tremendous potential to drive innovation in Ghanaian banks, its integration must go hand in hand with effective security frameworks, professional personnel, and aligned regulatory management to neutralize associated cyber threats.

Theoretical and Conceptual Framework

The figure 1 below adopts the Technology–Organization–Environment (TOE) framework to explain how IoT adoption interacts with cybersecurity readiness in the banking sector. The TOE model identifies three major contexts that influence institutional technology adoption and implementation success:

1. Technological Context – The availability, compatibility, and perceived complexity of IoT systems determine how securely banks can integrate them into existing networks.

2. Organizational Context – Institutional leadership, technical capacity, and financial resources affect cybersecurity preparedness and risk mitigation strategies

3. Environmental Context – Regulatory oversight, competitive pressures, and technological infrastructure shape how banks respond to cybersecurity challenges.

By situating the study within this framework, the research recognizes that IoT cybersecurity readiness depends not only on technical safeguards but also on institutional policies, human capacity, and external regulatory environments. The TOE perspective aligns closely with the socio-technical systems theory, which emphasizes the interdependence between technology, people, and organizational structures in achieving secure and sustainable innovation.

Theoretical and Conceptual Framework

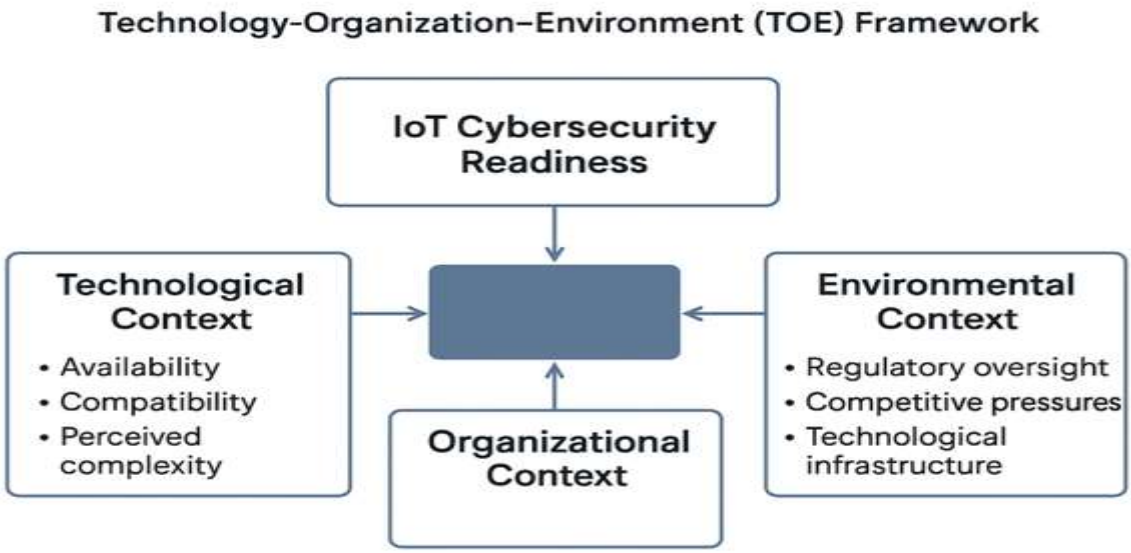

Figure 1: Technology-organisation-environment

Methodology

This study employed a mixed-method research design that incorporated both qualitative and quantitative approaches to data collection to explain the effects of Internet of Things (IoT) on cybersecurity within Ghana's banking sector. The study was structured into two main phases: (1) Document Analysis of publicly published reports on cybersecurity, and (2) Semi-Structured Expert Interviews. These converging methods enabled triangulation and enhanced the robustness of the findings.

Phase 1: Document Analysis*:*
10 publicly available cybersecurity and IT audit reports were obtained from leading Ghanaian commercial banks. These reports, including risk disclosure reports, data breach incident reports, and internal policy reports (where publicly disclosed), were analysed using content analysis. Each report was assessed with a checklist of common IoT-related threats, including:

1. DDoS vulnerabilities: DDoS exposures happen when attackers attack numerous hijacked systems employed to flood networks or servers, leading to downtime and disruption.
2. Device authentication practices: Device authentication controls block unauthorized access through permitting only authorized and trusted devices to attempt to join the system.
3. Encryption standards for connected endpoints: Encryption protocols for endpoint devices attached ensure that data in transit is protected because it becomes useless to the attackers, ensuring confidentiality and integrity.
4. Real-time monitoring capabilities: Real-time monitoring features provide continuous detection of threat or abnormal activity on devices and networks
5. Incident response preparedness: Cyberattack readiness allows companies to find, block, and bounce back from cyber-attacks quickly in an effort to minimize damages.

Table 1: IoT Cybersecurity Checklist (Phase 1: Document Analysis)

Checklist Item	Description
DDoS vulnerabilities	Assessment of exposure to Distributed Denial-of-Service attacks.
Device authentication practices	Evaluation of authentication measures for IoT devices.
Encryption standards for endpoints	Review of encryption methods securing connected endpoints.
Real-time monitoring capabilities	Examination of monitoring systems for real-time threat detection.
Incident response preparedness	Analysis of preparedness and procedures for responding to incidents.

The analysis produced baseline data on existing vulnerabilities, defence systems, and compliance levels with national and international cybersecurity requirements. It generated baseline information of existing vulnerabilities, methods of defence, and levels of compliance against national and global cybersecurity standards.

Phase 2: Semi-structured Interviews

Semi-structured interviews were conducted from a total of twelve (12) IT and cybersecurity practitioners from five core Ghanaian financial institutions. Respondents in the interviews included Chief Information Security Officers (CISOs), Chief Information Technology Infrastructures, and security analysts. The interview questions were structured around three main themes as shown in table 2 below:

Table 2: Themes and Focus Areas from Semi-Structured Interviews (Phase 2)

Theme	Focus Areas
IoT Adoption Practices	Current practices of IoT use in operations (e.g., ATMs, monitoring, access).
Cybersecurity Concerns	Specific areas of vulnerability and recent attacks linked to IoT devices.
Mitigation and Preparedness	Existing defense measures, incident response, and regulatory compliance efforts.

It was applied to extract prevailing patterns, match qualitative results to document results, as well as detect underlying organizational and infrastructural issues.

Data Analysis and Integration

Data from document analysis and semi-structured interviews were integrated using a risk impact matrix to prioritize threats and cross-thematic mapping to align qualitative insights with policy frameworks. This approach revealed gaps between policy and practice in institutional cybersecurity governance, showing that while policies emphasized encryption and authentication, practitioners highlighted weaknesses in incident response and real-time monitoring. The methodological framework (Figure 1) illustrates these sequential phases and their integration.

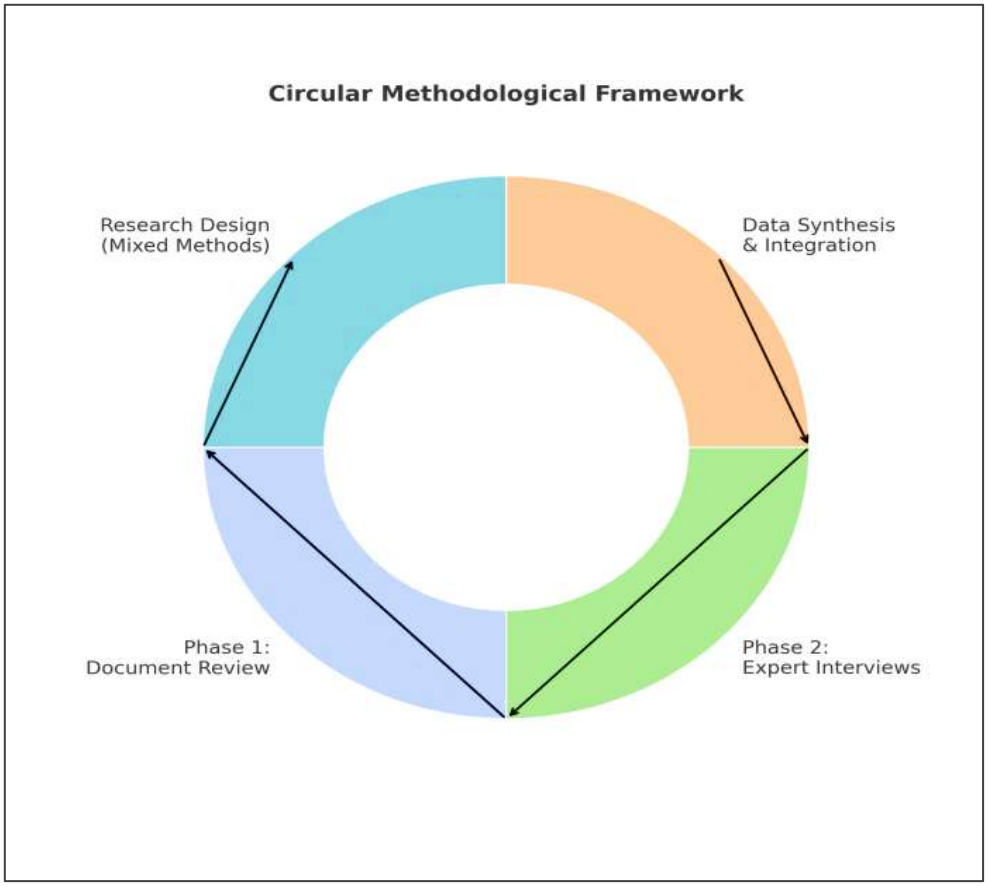

Figure 2: Methodological Framework

This incremental stepwise strategy ensured rigor, triangulation, and relevance of context, providing a holistic description of complex interactions between integration of IoT and cybersecurity in Ghana's banking operations.

Result and discussion

Key IoT-Related Cybersecurity Threats

The deployment of Internet of Things (IoT) devices in Ghanaian banks has significantly facilitated business efficiency, convenience to customers, and data-driven business decisions. Through thematic analysis of expert interviews as well as institutional cybersecurity audit reports, a variety of high-priority IoT-associated threat actors were unearthed. Central among these are:

Unsanctioned Access as well as Weak

IoT devices used in ATM networks, smart surveillance, and mobile banking are frequently poorly defended against strong authentication measures. Weak passwords and default passwords enhance unauthorized access possibilities.

Data Breach and Leakage

IoT devices gather sensitive customer information (e.g., history of transactions, biometrical identification). Weak encryption and insecure transmission channels facilitate interception and leakage of data.

Distributed Denial of Service (DDoS) Attacks

Compromised IoTs are widely employed as botnet mechanisms for DDoS assaults globally, which may interfere with basic banking operations as well as user digital platform availability.

Ransomware and Malware Attacks

IoT devices that are not patched create backdoors for ransomware exploitation, immobilizing essential systems and extorting funds for recovery.

Third-Party Vendor Threats: Some of the Ghanaian banks' IoT offerings are provided and maintained through third-party vendors. This in itself exposes financial institutions to supply chain threats and backdoors.

Insider Threats: Employees who have access to IoT networks could deliberately or inadvertently open systems to attack as a result of negligence, phishing vulnerabilities, or collaboration with outside actors.

Levels of Perceived Risk from IoT-Related Threats in Ghana's Banking Industry

According to institutional self-assessments and expert judgments, perceived levels of these threats were ranked from 1 (very low) to 10 (very high) Table 2 summarize Perceived Risk Levels of IoT-Related Threats in Ghana's Banking Industry.

Table 3: IoT-Related Cybersecurity Risk Perceptions in Ghana's Banking Industry

Threat	Risk Level (1–10)
Unauthorized access & weak authentication	9
Data breaches & leakage	8
DDoS attacks	7
Ransomware & malware infiltration	8
Third-party vendor risks	6
Insider threats	7

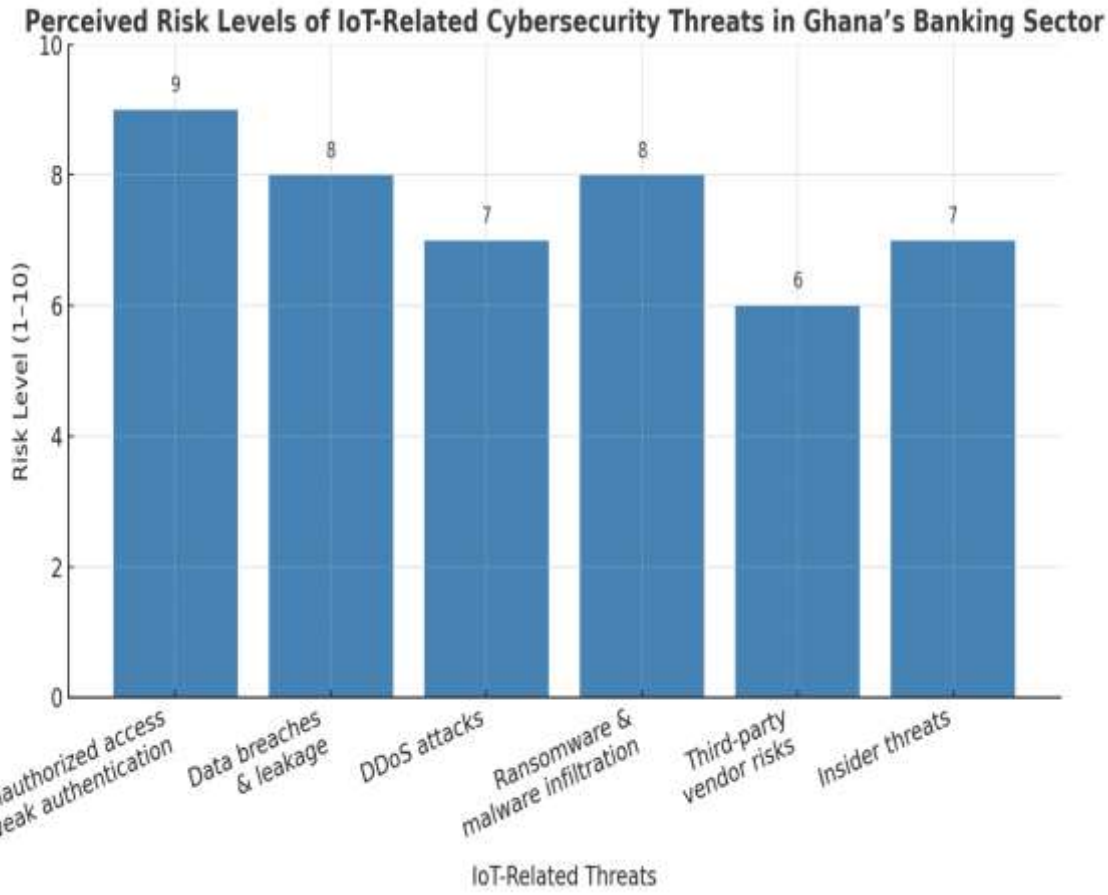

Figure 3: Perceived Risk Levels of IoT-Related Threats in Ghana's Banking Sector

The research uncovered a few high-priority cybersecurity risks relating to IoT integration in Ghanaian banks. Observations were based on thematic analysis of subject matter expert interviews and institutional cybersecurity audit reports, which called out such IoT deployments while facilitating efficiency and innovation conversely expand banks' attack surface [6-8]. The most commonly cited in figure 2 above illustrating risks were unauthorized access and poor authentication mechanisms (9/10), which subject IoT-enabled systems to credential-based assault as well as identity spoofing. Data leakage and breach (8/10) were similarly a significant concern, especially considering high amounts of sensitive customer and financial information processed by banks. Experts similarly highlighted ransomware and malware intrusion risks (8/10), which have a potential to capitalize on IoT device vulnerabilities to crash core financial operations. Distributed Denial-of-Service (DDoS) assaults (7/10) and insider attack (7/10) were assessed as moderately serious though nevertheless critical, representing external and internal attack methods, respectively. Lastly, third-party vendor risk (6/10) was noted as a result of a reliance upon outside service providers for IoT products, which tend to bring in vulnerabilities beyond bank's direct control. Individually, these results indicate Ghanaian banks need to implement strong IoT-focused cybersecurity frameworks, intertwining technical protections with governance controls, in order to manage risk in a rapidly digitalized financial atmosphere. Figure 3: illustrates Inadequate Standardized Security Procedures.

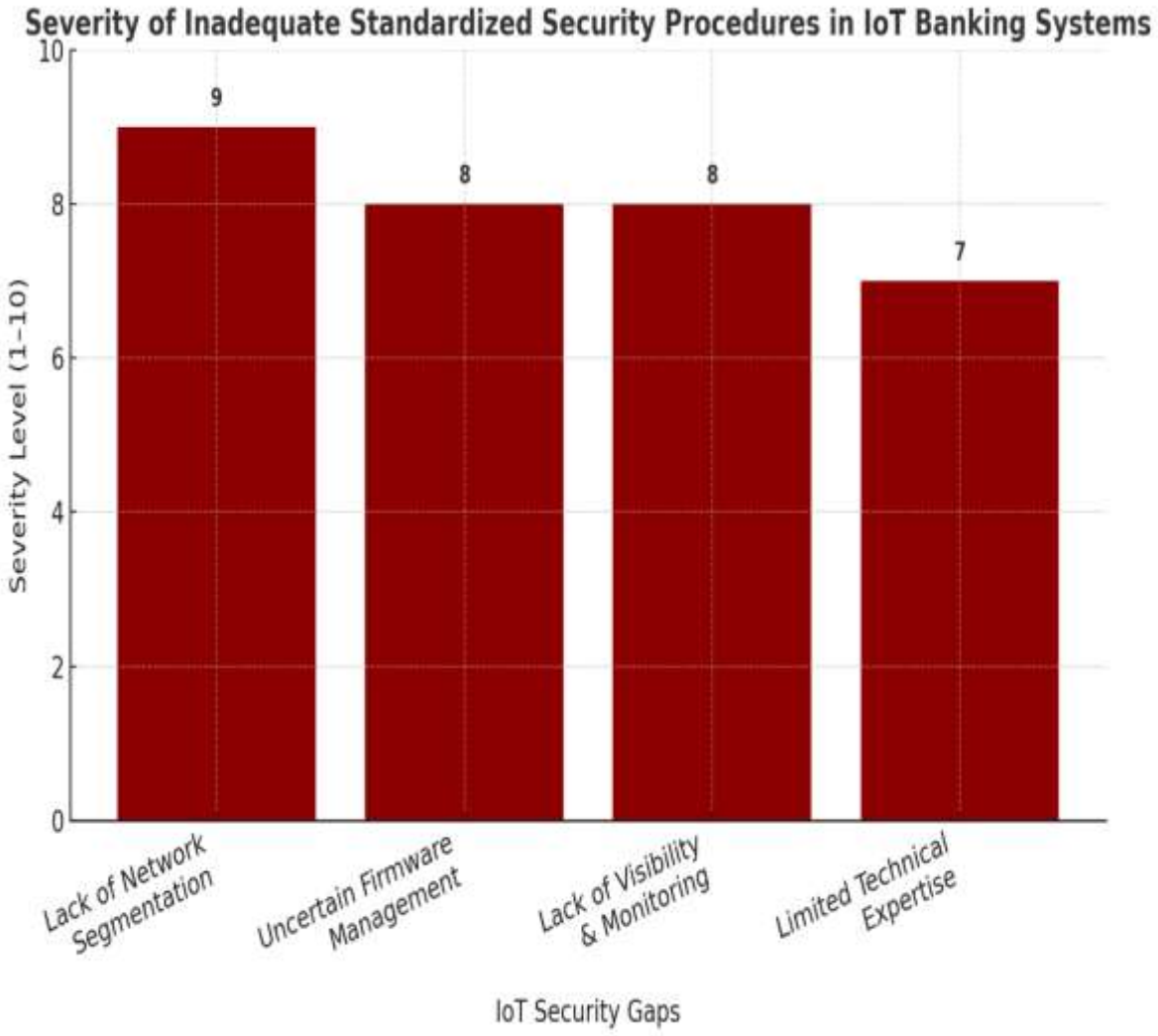

Figure 4: Inadequate Standardized Security Procedures

Documentation and interview analysis bring out prominently as a core concern a deficiency in standard procedures for managing Ghanaian bank IoT infrastructure. Even as there is greater IoT system use, there is no overarching framework that prescribes on-boarding, set-up, or lifecycle management of such equipment. The analysis highlighted a few recurring gaps:

Lack of Network Segmentation (Severity = 9/10)

Most banks operate flat network structures where IoT devices share the same domain as core banking applications. This design flaw allows lateral movement across networks, meaning a compromised IoT sensor could grant attackers access to sensitive databases or transaction servers.

Uncertain Firmware Management (Severity = 8/10)

The IoT devices don't have centralized update mechanisms, thus outdated firmware is in use for an extremely long time. This exposes banks to known and fixed vulnerabilities in later revisions.

Lack of Monitoring and Visibility (Severity = 8/10)

Fewer have in-place, real-time visibility into what IoT devices are doing. Lacking a counterpoint of control, anomalies and unauthorized logins may well go unnoticed, driving up mean time to detect (MTTD) and mean time to respond (MTTR).

Limited Skills in Technovation (Severity = 7/10)

Surveys discovered that IT staffs are not adequately educated in IoT cybersecurity specializations. Employees are highly educated in traditional IT and networking, yet no proper expertise exists in embedded matters or in IoT protocols. These failures are characteristic of systemic technical and regulatory standardization shortcomings. The BoG publishes generic cybersecurity best practices, yet no regulatory mandate is specifically reserved for IoT in banking specifically. This omission in regulatory action broadens institutional anomalies and widens risk exposures

Regulatory and Infrastructural Concerns

The uptake of Internet of Things (IoT) technologies by financial services in Ghana is outpacing the emergence of regulatory safeguarding, exposing stark chasms in national cybersecurity management. There is currently no bespoke IoT-specific cybersecurity policy for Ghana. Existing legislations, as the Data Protection Act, 2012 (Act 843), are primarily focused on privacy and management of personal data but fall short in addressing the advanced, real-time security requirements posed by IoT infrastructures [8]. Without comprehensive IoT-specific legislations, individual financial institutions operate in regulatory silos, implementing varied security processes with varying levels of effectiveness. This fragmentation of regulation constrains sector-wide cooperation in incident management, intelligence exchange, and best practice implementation. Apart from the law gap, infrastructural constraints heavily erode IoT deployments' security resilience:

Erratic Electricity Supply: Inconsistent power infrastructure disrupts continuous system presence, prevents security updates, and complicates real-time threat scans.

Limited Broadband Coverage: Broadband- empowered devices utilize high-bandwidth, guaranteed links to facilitate firmware updates, intrusion detection, as well as analysis in clouds. The narrow coverage of broadband links in urban centers and suburbs inhibits banks from installing or supporting such service in a secure manner [8].

Resource Constraints in Regulators: The likes of the Bank of Ghana (BoG) and the National Communications Authority (NCA) lack an IoT security regulation department, which means that more complexity and enforcement of tailored cybersecurity have to be practiced. Such regulatory as well as physical constraints aggregate to be a significant impediment to the protection of Ghana's digital financial systems that need to be confronted by both government and industry stakeholders simultaneously[9-10].

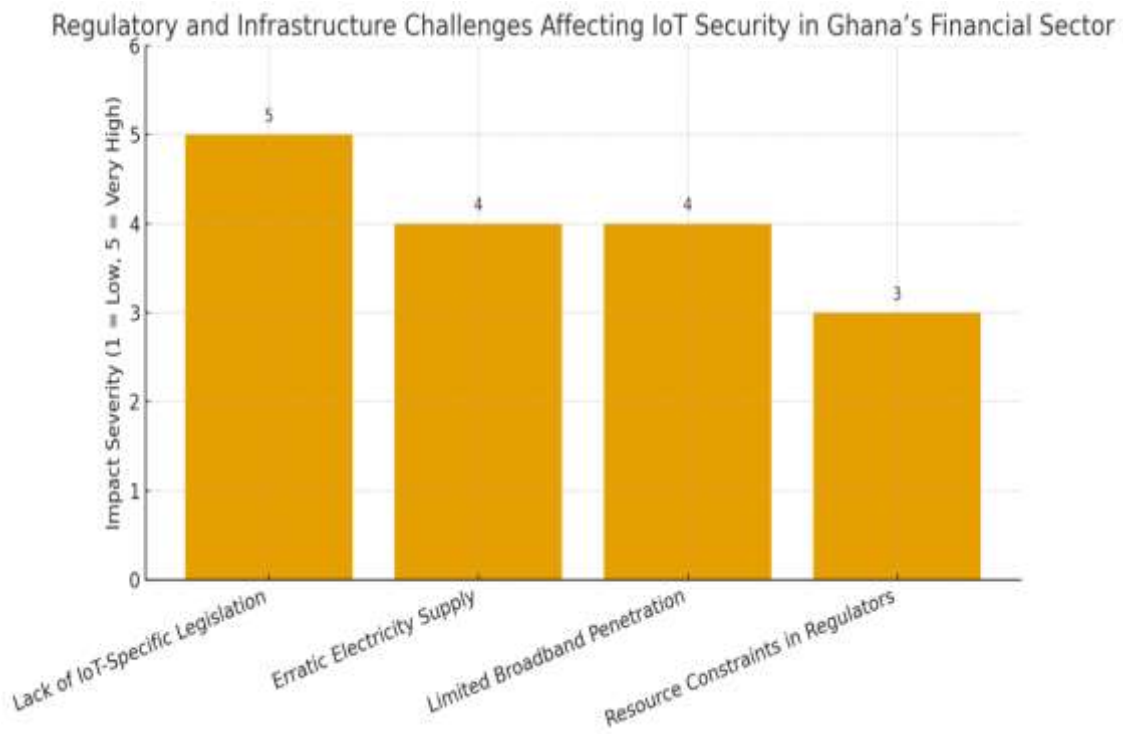

Figure 5: Regulatory and Infrastructure Challenges

Recommendations

To bolster Ghana's financial sector cyber posture against burgeoning use of Internet of Things (IoT) deployments, a number of strategic measures must be taken. First, it will be required to establish a National IoT Cybersecurity Framework:There is a need for a government-initiated, industry-made framework with immediate effect, to harmonize, reduce regulatory silos, and establish institutional trust. BoG, NCA, CSA, academia, industry, and cyber security professionals should spearhead this initiative. The framework must set out minimum security requirements across IoT devices and vendors so that secure coding, device authentication, and protocol-based life cycle management become universal. It must also establish certification of financial IoT systems, so as to provide confidence to stakeholders regarding trust in such systems. Periodic, defined cyber security audits must also be made mandatory across financial institutions in order to enhance accountability and compliance. Standardization with international best practices such as ITU recommendations, ISO/IEC 30141 reference architecture, and NIST Cybersecurity Framework will keep Ghana's policies interoperable and current at a global level. The suggestion directly corresponds with SDG 9 (Industry,Innovation, and Infrastructure) by enhancing innovation infrastructure, and SDG 16 (Peace, Justice, and Strong Institutions) by enhancing regulatory quality and institutional trust.

Second, there should be permanent AI-driven threat detection and surveillance programs developed by banks.

Utilization of AI-driven intrusion detection systems (IDS) and machine learning-based analytics will enhance institutions' capacity to detect anomalies in IoT networks in real time. Through normal behavior profiling, such systems will automatically detect anomalies that may be attributable to cyber threats and prevent spread of malware and insider threats. On top of this, centralized Security Operations Centers (SOCs) also need to be developed, with IoT-centric dashboards that offer a snapshot of branch, ATM, and other smart device activity. In tandem, real-time monitoring also needs to be ingrained in inter-bank sharing of threat intelligence systems, which will bolster sectoral resilience. This proposal assists in contributing to SDG 9 in terms of encouraging technological innovation and to SDG 16 by strengthening institutional resilience against cybercrime.

Third, banks must take notice of device-level hardening policies in securing IoT devices embedded in their operations.

Endpoints like biometric authentication terminals, security surveillance cameras, ATMs that are intelligent, as well as payment kiosks, are key nodes in bank networks and of significant concern to cybercriminals. Such endpoints receive daily firmware updates to address vulnerabilities and keep them resilient against new and emerging threats. Furthermore, mandatory end-to-end encryption will ensure confidentiality and integrity of data in transit. User authentication and computer access should require multi-factor authentication (MFA) and decrease unauthorized access risks drastically. A zero-trust architecture must also be implemented; in this model, no endpoint or computer is implicitly trusted, thus lowering lateral threat movement risks in institutional networks. The above methods of hardening devices are in line with SDG 9 by enabling innovation in a secure manner and with SDG 16 by minimizing risks of identity theft, financial crime, and fraud.

Finally, establishing the capacity to control and promoting public–private partnerships are essential for effective cybersecurity management.

Regulatory bodies such as BoG and NCA must establish specialist IoT Cybersecurity Units with the mandate to track compliance, incident response, and the overall development of the cybersecurity ecosystem. Due to funding limitations, public–private partnerships must be encouraged, with banks, telcos, and FinTech firms jointly investing in cybersecurity capacity building and technological research. Knowledge transfer schemes, by collaborating with foreign cybersecurity institutions and research academies, can assist in the exchange of knowledge and the development of localized solutions. Tax reliefs or subsidies must be provided to institutions that exceed the minimum level of IoT cybersecurity standards, thereby inducing compliant behaviour and innovation. This recommendation has a strong bearing on SDG 17 (Partnerships for the Goals) in that it believes in multi-stakeholder partnerships between government, the private sector, and international actors towards building a resilient and secure financial system.

Limitations and Future Research Directions

This study has certain limitations that open avenues for future research. First, data collection was primarily qualitative, relying on secondary reports and expert interviews,

which may not capture the full range of IoT-related cybersecurity experiences across all financial institutions. Future research should include broader quantitative surveys or longitudinal analyses to validate these findings statistically. Second, the study focused solely on the Ghanaian banking sector; future studies may extend to fintech, insurance, and telecommunications sectors to enhance generalizability. Lastly, as IoT and AI-driven cybersecurity evolve rapidly, future investigations should explore adaptive regulatory frameworks and real-time AI-based monitoring models that strengthen cybersecurity resilience in developing economies.

Conclusion

The universal uptake of Internet of Things (IoT) technologies in Ghana's financial services industry both presents transformative opportunities and significant cybersecurity issues. On the positive side, IoT-driven technologies such as biometric-based verification systems for customers, intelligent automated teller machines (ATMs), and real-time data analysis are capable of revolutionizing financial service provision. IoT-advanced technologies can enhance business operation efficiency, improve the customer experience, and strengthen consumer trust in digital banking platforms. In turn, the same innovations expose the financial sector to hitherto unforeseen risks. Cyber-attacks such as distributed denial-of-service (DDoS) attacks, large-scale data breaches, and unauthorized access to IoT devices can jeopardize financial stability, undermine institutional credibility, and reduce consumer confidence unless countered by deliberate policy and technical means. This study indicates the necessity of general institutional preparedness to manage such threats in effective manner. Central to such preparedness is consolidating artificial intelligence (AI)-powered monitoring solutions that are in a position to pre-emptively detect, analyze, and respond to cyber threats prior to their escalation. Just as critical is implementing standardized device protocols, which will promote interoperability between different IoT systems while strengthening resilience against illegal exploitation. In addition, institutions need to come up with preemptive incident response frameworks that allow for fast containment and recovery from cybersecurity incidents, hence limiting the potential for systemic disruption. On top of institutional reforms, regulatory and infrastructural reforms are essential in filling the existing governance and operational gaps. Currently, Ghana does not have a specific IoT cybersecurity law specifically addressing the specific risks inherent in smart devices within financial systems. This lack of coverage generates gaps that need to be filled by legal and regulatory provisions at the country level. Likewise, infrastructural issues, in the form of unreliable electricity supply and weak broadband penetration, limit safe and efficient utilization of IoT technologies. Those issues must be resolved at both country as well as institutional levels in order to support sustainable utilization of IoT. Long-term success of Ghana's banking sector with IoT-driven transformation will hinge upon security-by-design principles being implemented across all stages of the lifecycle of IoT deployment. Security considerations need to be designed-in at every step, from procurement and installation, to real-time monitoring and maintenance, and finally into secure decommissioning at the end of the lifecycle. Through such integration, institutions ensure that security is a consideration and not after-thought but instead integral to financial innovation. In addition, synchronization of such strategies with United Nations Sustainable Development Goals (SDGs) also enhances global transferability and long-term sustainability of IoT adoption. Specific. SDG 9 (Industry, Innovation, and Infrastructure) expressly calls upon strengthening Ghana's infrastructure in support of financial innovation, SDG 16 (Peace, Justice, and Strong Institutions). places strong emphasis upon robust regulatory regimes and trusted institutions, and SDG 17 (Partnerships for the Goals) outlines value proposition of multi-stakeholder

collaborations that include government, private sector firms, academia, and international partners. Ultimately, Ghana's financial system of the future is a function of successful multi-stakeholder collaborations. Regulators, banks, governments, technology firms, and cyber security professionals will all need to be involved in taking sound digital financial system from concept to reality. Public-private collaboration, regular debate, and compliance with international norms will be key in sustaining public confidence as well as financial integrity in a more interconnected digital economy. If this advice is followed, Ghana's financial sector will be in good stead to harness the potential of IoT as a force of innovation, efficiency, as well as resilience and reduce the cybersecurity risks that come with technological change.

Acknowledgements

There is no grant or funding bodies to be acknowledged for preparing this paper.

References

Albayati, H., 2024. Investigating undergraduate students' perceptions and awareness of using ChatGPT as a regular assistance tool: A user acceptance perspective study. *Computers and Education: Artificial Intelligence*, *6*, p.100203. https://doi.org/10.1016/j.caeai.2024.100203

Aouedi, O., Vu, T.H., Sacco, A., Nguyen, D.C., Piamrat, K., Marchetto, G. and Pham, Q.V., 2024. A survey on intelligent Internet of Things: Applications, security, privacy, and future directions. *IEEE communications surveys & tutorials*. 1-1 https://doi.org/10.1109/COMST.2024.3430368

C. Fan, S. Ghaemi, H. Khazaei, and P. Musilek, ‘‘Performance evaluation of blockchain systems: A systematic survey,’’ IEEE Access, vol. 8, pp. 126927–126950, 2020, https://doi.org/10.1109/ACCESS.2020.3006078

K. Gai, J. Guo, L. Zhu, and S. Yu, ‘‘Blockchain meets cloud computing: A survey,’’ IEEE Commun. Surveys Tuts., vol. 22, no. 3, pp. 2009–2030, 3rd Quart., 2020, https://doi.org/10.1109/COMST.2020.2989392

Khan, M.A. and Salah, K., 2018. IoT security: Review, blockchain solutions, and open challenges. *Future generation computer systems*, *82*, pp.395-411. https://doi.org/10.1016/j.future.2017.11.022

Kumar, V., Sharma, K.V., Kedam, N., Patel, A., Kate, T.R. and Rathnayake, U., 2024. A comprehensive review on smart and sustainable agriculture using IoT technologies. *Smart Agricultural Technology*, *8*, p.100487. https://doi.org/10.1016/j.atech.2024.100487

Laghari, A.A., Wu, K., Laghari, R.A., Ali, M. and Khan, A.A., 2022. Retracted article: A review and state of art of internet of things (IoT). *Archives of Computational Methods in Engineering*, *29*(3), pp.1395-1413. https://doi.org/10.1007/s11831-021-09622-6

S. Sicari, A. Rizzardi, L. Grieco, and A. Coen-Porisini, “Security, Privacy and Trust in Internet of Things: The Road Ahead,” Computer Networks, vol. 76, pp. 146–164, 2015. https://doi.org/10.1016/j.comnet.2014.11.008

Sarker, I.H., Khan, A.I., Abushark, Y.B. and Alsolami, F., 2023. Internet of things (iot) security intelligence: a comprehensive overview, machine learning solutions and research directions. *Mobile Networks and Applications*, *28*(1), pp.296-312. https://doi.org/10.20944/preprints202203.0087.v1

Schiller, E., Aidoo, A., Fuhrer, J., Stahl, J., Ziörjen, M. and Stiller, B., 2022. Landscape of IoT security. *Computer Science Review*, *44*, pp.1-18. https://doi.org/10.1016/j.cosrev.2022.100467