IoT Security in the Banking Sector: Mitigating the Vulnerabilities of Connected Devices and Smart ATMs

Jaya Chandra Srikanth Gummadi

Senior Software Engineer, Lowes Companies Inc., Charlotte, North Carolina, USA

E-mail for correspondence: Jayachandrasrikanth7@gmail.com

https://doi.org/10.18034/abr.v13i3.737

ABSTRACT

This paper examines banking IoT and innovative ATM security issues and solutions. IoT technologies improve operational efficiency and consumer interaction but can increase cyberattacks, physical tampering, and data breaches in financial systems. The research aims to identify vulnerabilities, review security measures, and provide ways to minimize banking sector-connected device hazards. The research synthesizes peer-reviewed publications, industry reports, and regulatory directives using secondary sources. The main results show that missing security standards, obsolete legacy systems, and human factors are key risks, whereas AI, ML, blockchain, and biometrics may improve Security. Physical Security and data protection rules are also stressed in the research. Policy implications include uniform security frameworks, better regulatory supervision, and ongoing security assessments. To combat increasing threats, financial institutions must work with technology suppliers and governments to create comprehensive security standards and incorporate new technologies. In conclusion, IoT adoption in banking offers excellent prospects, but strong security measures are needed to secure sensitive financial systems and retain client confidence in an increasingly linked world.

Key words: IoT Security, Banking Sector, Smart ATMs, Connected Devices, Cybersecurity, Vulnerabilities, Risk Mitigation, Data Protection

INTRODUCTION

The Internet of Things (IoT) has transformed businesses with unparalleled connection and automation. IoT gadgets like linked ATMs, digital kiosks, and biometric identification systems have improved banking processes and consumer experiences (Devarapu, 2020; Talla et al., 2021; Thompson et al., 2019). However, the security risks of IoT systems increase with deployment. Financial data is sensitive, and banks are vital to the global economy, making them attractive targets for cyberattacks (Talla et al., 2022). IoT and financial Security convergence is complicated and urgent, requiring thorough research and effective mitigation (Devarapu, 2021; Rodriguez et al., 2020; Sachani et al., 2022; Talla, 2022; Talla et al., 2023).

Banking's IoT dependence creates particular risks. Because they are commonly placed in distant places, connected ATMs are vulnerable to physical tampering and remote hacking. IoT-based payment systems and consumer interface points may also be used to hack financial networks (Narsina et al., 2019; Narsina et al., 2022; Onteddu et al., 2022; Roberts et al., 2020; Rodriguez et al., 2021). DDoS assaults, ransomware, and IoT malware threaten banking system confidentiality, integrity, and availability (Devarapu et al., 2019). Beyond financial damages, such breaches may damage consumer confidence and regulatory compliance.

Due to their architecture, banking IoT systems are challenging to secure. Many IoT devices lack computer power, making encryption and security procedures difficult. Because devices and manufacturers vary, security requirements vary, leaving vulnerabilities for hostile actors. Legacy systems, which typically coexist with IoT in banking, introduce obsolete vulnerabilities, worsening Security (Kothapalli et al., 2019; Dhameliya et al., 2021; Goda, 2020; Gummadi, 2022; Mullangi et al., 2023; Narsina et al., 2021).

Mitigating these risks requires technical and organizational changes. Technologically, secure device design, network segmentation, and improved encryption algorithms are essential (Gummadi et al., 2020; Mullangi et al., 2018). Banks must promote cybersecurity knowledge among workers, customers, and third-party providers. Regulators must also adapt to the fast rise of IoT in banking, stressing responsibility and resilience.

This article analyses banking IoT and smart ATM vulnerabilities and their repercussions. It also evaluates mitigating methods and suggests new IoT security measures. By solving these problems, the banking industry can balance IoT expansion with asset protection.

IoT security in banking is essential since it might affect financial stability and consumer confidence. As IoT use grows, so does the need to address its vulnerabilities. Our results and suggestions will help safeguard banking sector IoT networks and ensure their sustainability and dependability in the face of emerging cyber threats.

Statement of the Problem

Because of the growing adoption of Internet of Things (IoT) technology, banks now provide seamless connections, automation, and tailored consumer experiences. These innovations have improved operational efficiency and consumer happiness, from smart ATMs and biometric identification to IoT-enabled payment solutions. However, IoT devices in banking systems have created security vulnerabilities that threaten data privacy, financial stability, and customer confidence. IoT devices' low processing capacity, variable security mechanisms, and vulnerability to physical and cyber-attacks make this problem crucial (Gummadi et al., 2021; Kamisetty, 2022; Mallipeddi, 2022).

Despite increased awareness of IoT security concerns in banking, current research and solutions fail to handle the intricacies. Most IoT security literature covers broad businesses or situations without addressing banking's unique needs and concerns (Kamisetty et al., 2021; Maddula, 2023). Although banking cybersecurity investigations are vast, they typically ignore IoT-enabled device and system concerns. This discrepancy exposes a research gap that requires dedicated attention to IoT security and banking.

The vulnerability of linked ATMs, increasingly installed in varied and distant areas, is a significant issue (Kothapalli, 2021). Malware, illegal access, and physical interference may endanger bank data and impair services at smart ATMs (Maddula, 2018). Bank IoT systems generally use third-party hardware and software, which exposes them to supply chain risks and vendor security issues. No consistent security standards for IoT devices make it harder for banks to create comprehensive security frameworks.

This paper examines IoT device and smart ATM vulnerabilities in the banking sector, evaluates current security solutions, and proposes creative risk mitigation techniques. The study focuses on IoT in banking to give practical insights that fill knowledge and practice gaps. The project aims to establish strong security frameworks that balance IoT growth with banking system security. Addressing these concerns is crucial. Banking is essential to global economic stability. IoT-enabled banking system security breaches may cause financial losses, reputational harm, and regulatory consequences. As banking adopts IoT technology, hackers will have more opportunities to exploit them. This research contributes to IoT security discourse by making focused suggestions to increase banking system resilience against upcoming attacks. This paper addresses the research gap and proposes banking-specific solutions to improve IoT security awareness and implementation. The results will benefit researchers, politicians, and bankers working to build a safe and sustainable financial IoT ecosystem.

Methodology of the Study

This secondary data-based research examines banking IoT devices, smart ATM vulnerabilities, and risk mitigation techniques. A thorough analysis of peer-reviewed scholarly publications, industry reports, white papers, and IoT security and banking regulatory requirements underpins the study. The paper analyses the threat environment, mitigation measures, and IoT security trends by synthesizing reputable sources. The secondary data review integrates multiple viewpoints and ideas from earlier research to help comprehend current practices' complexity and shortcomings. This technique guarantees the investigation is objective and uses facts to suggest practical and unique answers. The results will inform banking IoT security discussions.

Understanding IoT Risks in Banking Systems

Innovative financial services, increased operational efficiency, and better client experiences are revolutionary advantages of incorporating Internet of Things (IoT) technology into banking systems (Kothapalli, 2022). However, significant hazards are associated with this technological transformation, jeopardizing financial infrastructure's resilience, Security, and dependability. Developing successful tactics to safeguard sensitive financial data and maintain client confidence requires understanding these threats.

Cybersecurity Threats in IoT Ecosystems: Fraudsters increasingly target IoT devices in financial systems because of their inherent weaknesses. Due to their frequent lack of strong security features like firewalls or sophisticated encryption, these devices are vulnerable to ransomware, malware penetration, and Distributed Denial of Service (DDoS) assaults. For example, IoT-based linked ATMs may be used to get illegal access to financial networks, allowing hackers to steal client data or interfere with regular business operations. Furthermore, IoT devices with lax authentication procedures may provide hackers access points to private networks (Ammirato et al., 2019).

Physical Security Risks: Unlike conventional banking systems, smart ATMs and IoT-enabled equipment are often placed in distant or unsupervised areas. This geographic dispersion increases the danger of theft or physical tampering. Attackers may install skimming devices, change hardware, or insert malicious code by physically accessing these devices and taking advantage of open ports (Kundavaram et al., 2018). These physical flaws jeopardize the gadgets and the more extensive financial system they comprise.

Supply Chain Vulnerabilities: IoT ecosystems in banking often involve multiple suppliers for hardware, software, and connection services. Because every vendor and component in the supply chain may have different security levels, this variety creates serious concerns. Third-party providers' poorly executed security measures may give hackers entry points to undermine the system as a whole. Furthermore, these threats are made worse by the absence of established standards for IoT devices, which results in uneven and disjointed security procedures (Sholla et al., 2018).

Data Privacy and Compliance Challenges: Large volumes of sensitive data, such as transaction details, biometric identifiers, and personal financial information, are generated and processed by IoT devices. The risk of breaches is increased when such data is sent and stored across networked systems. In addition to violating client privacy, banks risk legal and regulatory repercussions if they fail to safeguard this data appropriately. Complex IoT ecosystems make it more challenging to comply with data protection laws like the Payment Card Industry Data Security Standard (PCI DSS) and the General Data Protection Regulation (GDPR) (Ammirato et al., 2019).

Legacy Systems and IoT Integration: The cohabitation of contemporary IoT technology and older systems makes Security more difficult in banking. When combined with IoT devices, legacy systems become vulnerable since they are often incompatible with modern security measures. Attackers may use these antiquated systems as entry points to infiltrate the banking network.

The first step in creating a safe and robust infrastructure is comprehending the many hazards connected to IoT devices in the banking industry. Supply chain risks, cybersecurity threats, physical vulnerabilities, data privacy issues, and legacy system integration influence the complex threat environment. By identifying and fixing these weaknesses, financial organizations may better safeguard their assets, uphold compliance, and win over their clients' confidence (Lykou et al., 2019).

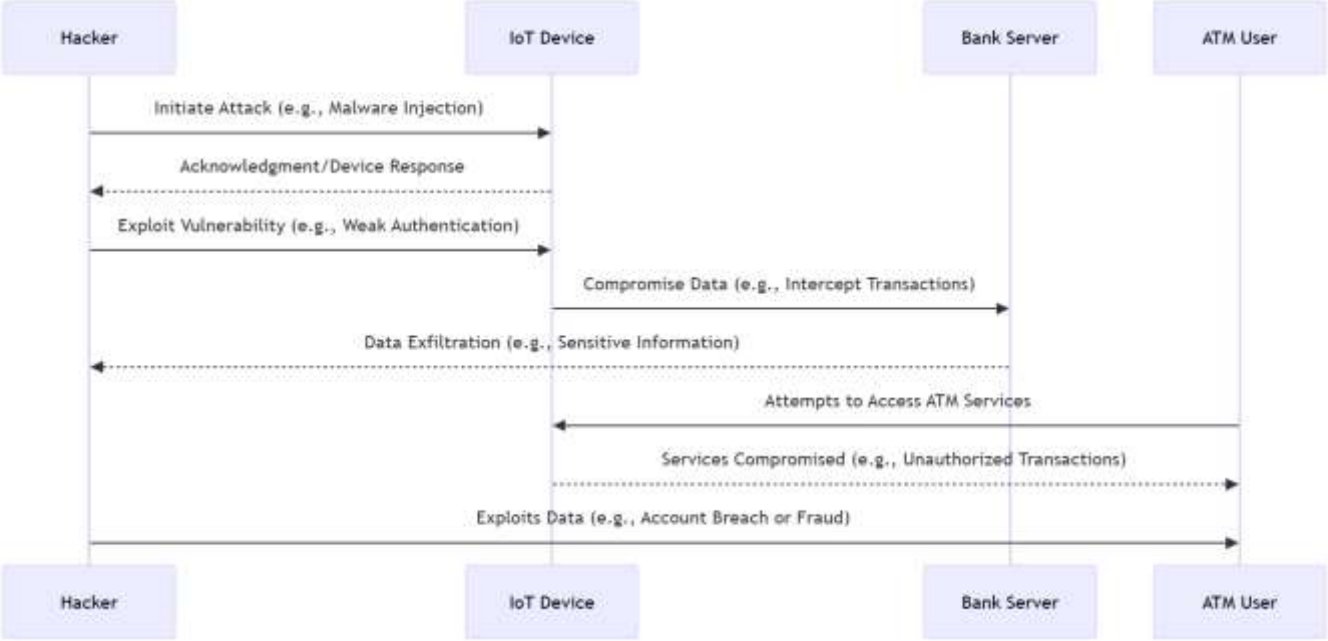
Hacker
IoT Device
Bank Server
ATM User
Initiate Attack (e.g., Malware Injection)
Acknowledgment/Device Response
Exploit Vulnerability (e.g., Weak Authentication)
Compromise Data (e.g., Intercept Transactions)
Data Exfiltration (e.g., Sensitive Information)
Attempts to Access ATM Services
Services Compromised (e.g., Unauthorized Transactions)
Exploits Data (e.g., Account Breach or Fraud)
Hacker
IoT Device
Bank Server
ATM User

Figure 1: Workflow of an IoT Attack on Smart ATMs

Figure 1 shows the sequential course of a cyberattack directed against a smart ATM. Four parties are involved: the hacker who starts the assault, the compromised IoT device, the bank server, and the ATM user whose data is ultimately in jeopardy. The procedure includes beginning the attack, using the Internet of Things device, compromising private information, and stealing the data.

Mitigation Strategies for Connected Device Vulnerabilities

IoT's emergence in the banking industry has brought about previously unheard-of levels of ease and creativity, but it has also revealed serious weaknesses that require strong security measures. A comprehensive strategy incorporating cutting-edge technology, organizational best practices, and regulatory compliance is needed to mitigate these risks. This chapter examines practical methods for protecting smart ATMs and other connected devices inside the financial ecosystem.

Implementing Robust Authentication Mechanisms: Robust authentication mechanisms are one of the fundamental methods for protecting IoT devices. Biometric verification and multi-factor authentication (MFA) may significantly improve the Security of smart ATMs and other linked financial equipment. To guarantee only allowed access, MFA combines the user's knowledge (password), possessions (OTP or token), and identity (facial recognition or fingerprint). Device-level authentication should also be used by IoT devices to stop illegal connections to the banking network (Hussein et al., 2018).

Data Encryption and Secure Communication Protocols: Encryption is essential for both data in transit and at rest to prevent sensitive financial data from being intercepted. IoT devices should use secure communication protocols like Transport Layer Security (TLS) and end-to-end encryption standards like AES-256 to protect data from hackers. Encrypted channels must also be used for over-the-air patching and secure firmware upgrades to stop malicious code from being injected during updates (Saxena & Al-Tamimi, 2017).

Network Segmentation and Zero Trust Architecture: To prevent hackers from accessing the whole system even if one component of the financial network is hacked, network segmentation entails splitting the network into separate parts. This is especially helpful for keeping critical financial systems and IoT devices apart. Furthermore, every person and device trying to access resources—within or outside the network perimeter—must undergo stringent identity verification when using a zero-trust security paradigm.

Enhanced Physical Security for IoT Devices: Physical Security is as important as cybersecurity for IoT devices like smart ATMs. Implementing monitoring systems, secure ATM enclosures, and tamper-resistant hardware may discourage physical tampering. Furthermore, safeguards against exploitation during physical breaches include features like automated shutdowns in response to unwanted access attempts. To guarantee device integrity, routine maintenance, and inspections should be carried out (Alhothaily et al., 2017).

Regular Security Audits and Penetration Testing: Banks should conduct penetration and security audits regularly to find weaknesses in their IoT environment. By identifying flaws in network design, software, and device settings, these proactive evaluations assist organizations in fixing problems before hackers can exploit them. Artificial intelligence (AI)-Powered continuous monitoring systems can identify irregularities in real time and provide prompt warnings for any dangers.

Vendor and Supply Chain Security: To mitigate supply chain risks, banks must impose stringent security standards on IoT device suppliers and manufacturers. This entails performing third-party risk assessments, adhering to industry standards, and ensuring devices are free of pre-installed vulnerabilities. Provisions for regular security support and timely upgrades should be included in vendor contracts.

Compliance with Regulatory Standards: Strong IoT security in banking requires adherence to industry requirements like the PCI DSS and GDPR. Compliance frameworks recommend operational resilience, device security, and data protection. Continuous protection is ensured by regular upgrades to security procedures by changing legislation (Chun, 2019).

Table 1: Encryption Protocols for IoT Security

Encryption Protocol	Key Length	Application in IoT	Strength	Potential Weaknesses
AES (Advanced Encryption Standard)	128, 192, or 256 bits	Secure communication for IoT devices, such as smart ATMs and sensors.	High	Vulnerable if keys are poorly managed or weak passwords are used.
RSA (Rivest-Shamir-Adleman)	1024–4096 bits	Encryption of data transmissions and secure key exchange in IoT systems.	Strong	Computationally intensive; less efficient for devices with limited resources.
ECC (Elliptic Curve Cryptography)	160–521 bits	Lightweight Security for resource-constrained IoT devices.	High	Relies on secure implementation; flawed configurations may lead to vulnerabilities.

TLS/SSL (Transport Layer Security)	Varies (uses AES, RSA, or ECC internally)	Secure data transfer between IoT devices and servers.	High	Susceptible to downgrade attacks or vulnerabilities in older protocol versions.
ChaCha20	256 bits	Lightweight encryption for real-time IoT communications.	High	Relatively new; lacks the extensive testing history of AES.
SHA-256 (Secure Hash Algorithm)	256 bits (hash function, not encryption)	Data integrity verification and secure authentication.	High	Vulnerable if combined with weak protocols or used for encryption instead of hashing.
DES/3DES (Data Encryption Standard)	56 bits (DES), 168 bits (3DES)	Legacy systems in IoT devices, though now largely obsolete.	Moderate	DES is easily broken; 3DES is computationally inefficient for modern use.
Quantum-Safe Algorithms	Varies (under development)	Anticipated use in future IoT systems to counter quantum computing threats.	Potentially High	Experimental; limited adoption and performance data.

Table 1 provides an overview of IoT systems' main encryption methods. It focuses on their technical details, common usage in IoT settings, security advantages, and possible vulnerabilities an attacker may exploit.

Smart ATMs and IoT-connected equipment have weaknesses that must be mitigated using a multipronged strategy that combines cutting-edge technology, organizational awareness, and regulatory compliance. Banks may lower the risks associated with IoT adoption by putting strong authentication, encryption, network segmentation, and vendor security procedures into place.

Future Trends in Smart ATM Security

Smart ATM security is becoming crucial as the banking industry adopts digital transformation. Due to technological breakthroughs and the growing complexity of cyber threats, future developments in smart ATM security are anticipated to include creative solutions that mix cutting-edge hardware, software, and process automation. This chapter examines the new developments that will influence smart ATM security in the future.

Biometric Authentication Advancements: Biometric authentication is an increasingly important component of smart ATM security. Compared to conventional PIN-based systems, technologies like fingerprint scanning, face recognition, and iris scanning provide higher Security. Vein recognition and behavioral biometrics, which examine distinctive user characteristics like typing speed or locomotion, may represent future developments in biometrics. These technologies provide additional protection by guaranteeing that only authorized users may access ATM services (Komulainen & Makkonen, 2018).

Blockchain for Transaction Security: Blockchain technology has potential uses in improving ATM security. Blockchain lowers the risk of fraud and manipulation by ensuring the integrity of transaction data via a decentralized, immutable ledger. Blockchain networks' openness increases system confidence, and smart contracts help automate and safeguard transaction processes. The incorporation of blockchain technology into ATM networks has the potential to improve Security as its use expands greatly.

Edge Computing for Real-Time Threat Mitigation: Instead of depending on centralized cloud services, edge computing processes data closer to the source. This translates into faster security threat detection and response for smart ATMs. Edge computing enhances real-time threat prevention and lowers latency via local data analysis. Additionally, it reduces the need for constant internet access, increasing resilience against network outages and assaults directed at centralized servers.

Quantum Cryptography for Enhanced Encryption: Conventional encryption techniques could be at risk as quantum computing advances. Data sent between ATMs and financial networks may be secured using unbreakable encryption provided by quantum cryptography, which uses the ideas of quantum physics. Quantum cryptography is still in its infancy but is anticipated to be a key component of ATM security systems.

Self-Healing Systems and Predictive Maintenance: Future smart ATMs will include self-healing features to fix hardware and software flaws automatically. IoT sensors and artificial intelligence (AI) enable predictive maintenance to detect malfunctions or tampering efforts before they happen. This proactive strategy lowers the chance of device breakdown or exploitation, improves system dependability, and decreases downtime.

Enhanced Physical Security with IoT Sensors: IoT sensors will enhance ATM physical security. These sensors can monitor the surroundings, spot manipulation, and notify security personnel of unwanted entry attempts. To prevent physical assaults, future ATMs could have cutting-edge surveillance features like motion detectors and face recognition cameras (Maurya & Sastry, 2017).

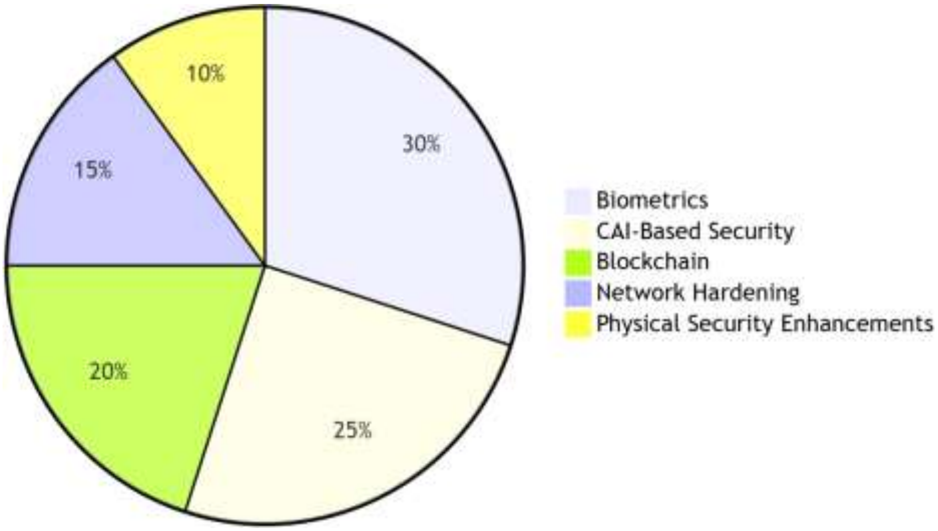

Figure 2: Proportion of Future Security Measures in Smart ATMs

The pie chart in Figure 2 shows the percentage of future security features in smart ATMs, emphasizing the relative importance of various security aspects. Biometrics, AI-Based Security, Blockchain, Network Hardening, and Physical Security Enhancements are among the segments that demonstrate how resources and efforts are allocated to counter new threats and improve ATM security.

Proactive threat detection, improved user authentication techniques, and the smooth integration of cutting-edge technology will be key components of smart ATM security in the future. The combined efforts of AI, biometrics, blockchain, quantum cryptography, and IoT-driven advancements will produce a strong security foundation for smart ATMs. By adopting these trends, the banking industry can guarantee safe, dependable, and customer-focused ATM services in an increasingly interconnected world.

MAJOR FINDINGS

The use of IoT technology in banking, notably smart ATMs and other linked equipment, has created Security, privacy, and operational integrity problems. A complete review of the issues and solutions revealed numerous key vulnerabilities and mitigation measures for banking IoT system security.

IoT Devices in Banking Present Unique Security Challenges: IoT devices, particularly smart ATMs, are susceptible owing to their low processing capability, which prevents complex security mechanisms. Cyber dangers like malware, ransomware, DDoS assaults, and physical threats like tampering and theft threaten this equipment. Smart ATMs are vulnerable to abuse because of their geographic dispersion and remote implementation.

The Lack of Unified Security Standards Increases Risks: Security requirements vary due to the variety of IoT devices and vendors. Due to fragmentation, attackers may use weak holes in less secure gadgets to enter financial ecosystems. Typically coupled with contemporary IoT technology, legacy systems increase security threats due to antiquated protocols and hard-to-fix flaws.

Technological Advancements Are a Challenge and an Opportunity: AI, ML, and blockchain may improve banking IoT security. Blockchain assures transaction data integrity and transparency, while AI and ML identify anomalies and forecast threats in real-time. However, these technologies are sophisticated, expensive, and require specialized skills, which may slow their acceptance in the near term.

Human Factors and Organizational Practices Influence Security: According to the research, human aspects are crucial to IoT security. IoT systems are vulnerable due to poor authentication, training, and consumer and staff cybersecurity awareness. Lack of engagement between financial institutions and third-party suppliers increases supply chain risks, emphasizing the necessity for strong vendor management and Security.

Physical Security Remains a Critical Concern: Despite cybersecurity advances, physical attacks on IoT devices, especially smart ATMs, remain a problem. Hardware tampering, skimming, and illegal access remain dangers. IoT sensors, tamper-resistant designs, and automated notifications for unwanted access are used to solve these issues.

Regulatory Compliance Is Vital but Complex: Securing banking IoT systems requires GDPR and PCI DSS compliance. As IoT innovation accelerates, legal frameworks evolve slowly, leaving institutions susceptible. Compliance must be updated to reflect new risks and technology.

The results emphasize the necessity for a diversified banking IoT security strategy. Technology and new solutions may improve Security, but fragmented standards, human factors, and physical weaknesses require collaboration among financial institutions, regulators, and technology vendors. Banks can develop a safe, robust, and future-ready IoT ecosystem by addressing these facts.

Limitations and Policy Implications

This research on banking IoT security is thorough yet constrained by secondary data. The lack of primary data or case-specific analysis limits insights into real-world implementations and strategy efficacy. IoT technology and cyber threats evolve quickly, so some conclusions may become obsolete when new vulnerabilities and solutions arise. Policymakers must establish security protocols for banking IoT devices and prioritize strong encryption, authentication, and vendor accountability laws. Given cyber threats' cross-border nature, worldwide IoT security standards need international coordination. Finally, to mitigate IoT threats, banks should be motivated to invest in regular security assessments and future technologies like AI and blockchain.

Conclusion

IoT technology has entirely transformed banking operations, improving client engagement, efficiency, and convenience. However, flaws in IoT devices, such as smart ATMs, seriously threaten the Security and integrity of financial institutions. This research examined these vulnerabilities and identified issues such as supply chain vulnerabilities, physical tampering, cyberattacks, and difficulties with regulatory compliance. A diversified strategy is necessary to counter these challenges. IoT security may be improved by integrating cutting-edge technologies like blockchain, quantum cryptography, artificial intelligence, and machine learning. Risk mitigation techniques are essential, including strong authentication procedures, encryption methods, network segmentation, and ongoing monitoring. Furthermore, proactive steps like predictive maintenance, frequent audits, and physical security upgrades are necessary for protecting IoT-enabled financial equipment. Notwithstanding these solutions' promise, the report acknowledges several drawbacks, such as inconsistent security standards, human error, and the dynamic character of IoT risks. These difficulties highlight how crucial it is for financial institutions, IT companies, and legislators to collaborate to create uniform frameworks and regulations.

In conclusion, even if IoT technologies provide the banking industry with many innovative prospects, their implementation must be matched with strong security protocols. By resolving the weaknesses and adopting new trends, the banking sector can create a robust IoT ecosystem that guarantees client trust, operational integrity, and long-term sustainability in a more interconnected world.

References

Alhothaily, A., Alrawais, A., Song, T., Lin, B., Cheng, X. (2017). QuickCash: Secure Transfer Payment Systems. *Sensors*, *17*(6), 1376. https://doi.org/10.3390/s17061376

Ammirato, S., Sofo, F., Felicetti, A. M., Raso, C. (2019). A Methodology to Support the Adoption of IoT Innovation and its Application to the Italian Bank Branch Security Context. *European Journal of Innovation Management*, *22*(1), 146-174. https://doi.org/10.1108/EJIM-03-2018-0058

Ammirato, S., Sofo, F., Felicetti, A. M., Raso, C. (2019). The Potential of IoT in Redesigning the Bank Branch Protection System: An Italian Case Study. *Business Process Management Journal*, *25*(7), 1441-1473. https://doi.org/10.1108/BPMJ-04-2018-0099

Chun, S-H. (2019). E-Commerce Liability and Security Breaches in Mobile Payment for e-Business Sustainability. *Sustainability*, *11*(3), 715. https://doi.org/10.3390/su11030715

Devarapu, K. (2020). Blockchain-Driven AI Solutions for Medical Imaging and Diagnosis in Healthcare. *Technology & Management Review*, *5*, 80-91. https://upright.pub/index.php/tmr/article/view/165

Devarapu, K. (2021). Advancing Deep Neural Networks: Optimization Techniques for Large-Scale Data Processing. *NEXG AI Review of America*, *2*(1), 47-61.

Devarapu, K., Rahman, K., Kamisetty, A., & Narsina, D. (2019). MLOps-Driven Solutions for Real-Time Monitoring of Obesity and Its Impact on Heart Disease Risk: Enhancing Predictive Accuracy in Healthcare. *International Journal of Reciprocal Symmetry and Theoretical Physics*, *6*, 43-55. https://upright.pub/index.php/ijrstp/article/view/160

Dhameliya, N., Sai Sirisha Maddula, Kishore Mullangi, & Bhavik Patel. (2021). Neural Networks for Autonomous Drone Navigation in Urban Environments. *Technology & Management Review*, *6*, 20-35. https://upright.pub/index.php/tmr/article/view/141

Goda, D. R. (2020). Decentralized Financial Portfolio Management System Using Blockchain Technology. Asian Accounting and Auditing Advancement, 11(1), 87–100. https://4ajournal.com/article/view/87

Gummadi, J, C. S. (2022). Blockchain-Enabled Healthcare Systems: AI Integration for Improved Patient Data Privacy. *Malaysian Journal of Medical and Biological Research*, *9*(2), 101-110.

Gummadi, J. C. S., Narsina, D., Karanam, R. K., Kamisetty, A., Talla, R. R., & Rodriguez, M. (2020). Corporate Governance in the Age of Artificial Intelligence: Balancing Innovation with Ethical Responsibility. *Technology & Management Review*, *5*, 66-79. https://upright.pub/index.php/tmr/article/view/157

Gummadi, J. C. S., Thompson, C. R., Boinapalli, N. R., Talla, R. R., & Narsina, D. (2021). Robotics and Algorithmic Trading: A New Era in Stock Market Trend Analysis. *Global Disclosure of Economics and Business*, *10*(2), 129-140. https://doi.org/10.18034/gdeb.v10i2.769

Hussein, W. N., Kamarudin, L. M., Hussain, H. N., Zakaria, A., Ahmed, R. B. (2018). The Prospect of Internet of Things and Big Data Analytics in Transportation System. *Journal of Physics: Conference Series*, *1018*(1). https://doi.org/10.1088/1742-6596/1018/1/012013

Kamisetty, A. (2022). AI-Driven Robotics in Solar and Wind Energy Maintenance: A Path toward Sustainability. *Asia Pacific Journal of Energy and Environment*, *9*(2), 119-128. https://doi.org/10.18034/apjee.v9i2.784

Kamisetty, A., Onteddu, A. R., Kundavaram, R. R., Gummadi, J. C. S., Kothapalli, S., Nizamuddin, M. (2021). Deep Learning for Fraud Detection in Bitcoin Transactions: An Artificial Intelligence-Based Strategy. *NEXG AI Review of America*, *2*(1), 32-46.

Komulainen, H., Makkonen, H. (2018). Customer Experience in Omni-channel Banking Services. *Journal of Financial Services Marketing*, *23*(3-4), 190-199. https://doi.org/10.1057/s41264-018-0057-6

Kothapalli, S. (2021). Blockchain Solutions for Data Privacy in HRM: Addressing Security Challenges. *Journal of Fareast International University,* 4(1), 17-25. https://jfiu.weebly.com/uploads/1/4/9/0/149099275/2021_3.pdf

Kothapalli, S. (2022). Data Analytics for Enhanced Business Intelligence in Energy-Saving Distributed Systems. *Asia Pacific Journal of Energy and Environment*, *9*(2), 99-108. https://doi.org/10.18034/apjee.v9i2.781

Kothapalli, S., Manikyala, A., Kommineni, H. P., Venkata, S. G. N., Gade, P. K., Allam, A. R., Sridharlakshmi, N. R. B., Boinapalli, N. R., Onteddu, A. R., & Kundavaram, R. R. (2019). Code Refactoring Strategies for DevOps: Improving Software Maintainability and Scalability. *ABC Research Alert*, *7*(3), 193–204. https://doi.org/10.18034/ra.v7i3.663

Kundavaram, R. R., Rahman, K., Devarapu, K., Narsina, D., Kamisetty, A., Gummadi, J. C. S., Talla, R. R., Onteddu, A. R., & Kothapalli, S. (2018). Predictive Analytics and Generative AI for Optimizing Cervical and Breast Cancer Outcomes: A Data-Centric Approach. *ABC Research Alert*, *6*(3), 214-223. https://doi.org/10.18034/ra.v6i3.672

Lykou, G., Anagnostopoulou, A., Gritzalis, D. (2019). Smart Airport Cybersecurity: Threat Mitigation and Cyber Resilience Controls. *Sensors*, *19*(1). https://doi.org/10.3390/s19010019

Maddula, S. S. (2018). The Impact of AI and Reciprocal Symmetry on Organizational Culture and Leadership in the Digital Economy. *Engineering International*, *6*(2), 201–210. https://doi.org/10.18034/ei.v6i2.703

Maddula, S. S. (2023). Evaluating Current Techniques for Detecting Vulnerabilities in Ethereum Smart Contracts. *Engineering International*, *11*(1), 59–72. https://doi.org/10.18034/ei.v11i1.717

Mallipeddi, S. R. (2022). Harnessing AI and IoT Technologies for Sustainable Business Operations in the Energy Sector. *Asia Pacific Journal of Energy and Environment*, *9*(1), 37-48. https://doi.org/10.18034/apjee.v9i1.735

Maurya, A. K., Sastry, V. N. (2017). Fuzzy Extractor and Elliptic Curve Based Efficient User Authentication Protocol for Wireless Sensor Networks and Internet of Things. *Information*, *8*(4), 136. https://doi.org/10.3390/info8040136

Mullangi, K., Anumandla, S. K. R., Maddula, S. S., Vennapusa, S. C. R., & Mohammed, M. A. (2018). Accelerated Testing Methods for Ensuring Secure and Efficient Payment Processing Systems. *ABC Research Alert*, *6*(3), 202–213. https://doi.org/10.18034/ra.v6i3.662

Mullangi, K., Dhameliya, N., Anumandla, S. K. R., Yarlagadda, V. K., Sachani, D. K., Vennapusa, S. C. R., Maddula, S. S., & Patel, B. (2023). AI-Augmented Decision-Making in Management Using Quantum Networks. *Asian Business Review*, *13*(2), 73–86. https://doi.org/10.18034/abr.v13i2.718

Narsina, D., Devarapu, K., Kamisetty, A., Gummadi, J. C. S., Richardson, N., & Manikyala, A. (2021). Emerging Challenges in Mechanical Systems: Leveraging Data Visualization for Predictive Maintenance. *Asian Journal of Applied Science and Engineering*, *10*(1), 77-86. https://doi.org/10.18034/ajase.v10i1.124

Narsina, D., Gummadi, J. C. S., Venkata, S. S. M. G. N., Manikyala, A., Kothapalli, S., Devarapu, K., Rodriguez, M., & Talla, R. R. (2019). AI-Driven Database Systems in FinTech: Enhancing Fraud Detection and Transaction Efficiency. *Asian Accounting and Auditing Advancement*, *10*(1), 81–92. https://4ajournal.com/article/view/98

Narsina, D., Richardson, N., Kamisetty, A., Gummadi, J. C. S., & Devarapu, K. (2022). Neural Network Architectures for Real-Time Image and Video Processing Applications. *Engineering International*, *10*(2), 131-144. https://doi.org/10.18034/ei.v10i2.735

Onteddu, A. R., Rahman, K., Roberts, C., Kundavaram, R. R., Kothapalli, S. (2022). Blockchain-Enhanced Machine Learning for Predictive Analytics in Precision Medicine. *Silicon Valley Tech Review,* *1*(1), 48-60. https://www.siliconvalley.onl/uploads/9/9/8/2/9982776/2022.4

Roberts, C., Kundavaram, R. R., Onteddu, A. R., Kothapalli, S., Tuli, F. A., Miah, M. S. (2020). Chatbots and Virtual Assistants in HRM: Exploring Their Role in Employee Engagement and Support. *NEXG AI Review of America, 1*(1), 16-31.

Rodriguez, M., Shajahan, M. A., Sandu, A. K., Maddula, S. S., & Mullangi, K. (2021). Emergence of Reciprocal Symmetry in String Theory: Towards a Unified Framework of Fundamental Forces. *International Journal of Reciprocal Symmetry and Theoretical Physics*, *8*, 33-40. https://upright.pub/index.php/ijrstp/article/view/136

Rodriguez, M., Sridharlakshmi, N. R. B., Boinapalli, N. R., Allam, A. R., & Devarapu, K. (2020). Applying Convolutional Neural Networks for IoT Image Recognition. *International Journal of Reciprocal Symmetry and Theoretical Physics*, *7*, 32-43. https://upright.pub/index.php/ijrstp/article/view/158

Sachani, D. K., Anumandla, S. K. R., Maddula, S. S. (2022). Human Touch in Retail: Analyzing Customer Loyalty in the Era of Self-Checkout Technology. *Silicon Valley Tech Review, 1*(1), 1-13.

Saxena, S., Al-Tamimi, T. A. S. M. (2017). Big Data and Internet of Things (IoT) Technologies in Omani Banks: A Case Study. *Foresight: the Journal of Futures Studies, Strategic Thinking and Policy*, *19*(4), 409-420. https://doi.org/10.1108/FS-03-2017-0010

Sholla, S., Mir, R., Chishti, M. (2018). Eventuality of an Apartheid State of Things: An Ethical Perspective on the Internet of Things. *International Journal of Technoethics*, *9*(2), 62-76. https://doi.org/10.4018/IJT.2018070106

Talla, R. R. (2022). Integrating Blockchain and AI to Enhance Supply Chain Transparency in Energy Sectors. *Asia Pacific Journal of Energy and Environment*, *9*(2), 109-118. https://doi.org/10.18034/apjee.v9i2.782

Talla, R. R., Addimulam, S., Karanam, R. K., Natakam, V. M., Narsina, D., Gummadi, J. C. S., Kamisetty, A. (2023). From Silicon Valley to the World: U.S. AI Innovations in Global Sustainability. *Silicon Valley Tech Review, 2*(1), 27-40.

Talla, R. R., Manikyala, A., Gade, P. K., Kommineni, H. P., & Deming, C. (2022). Leveraging AI in SAP GTS for Enhanced Trade Compliance and Reciprocal Symmetry Analysis. *International Journal of Reciprocal Symmetry and Theoretical Physics*, *9*, 10-23. https://upright.pub/index.php/ijrstp/article/view/164

Talla, R. R., Manikyala, A., Nizamuddin, M., Kommineni, H. P., Kothapalli, S., Kamisetty, A. (2021). Intelligent Threat Identification System: Implementing Multi-Layer Security Networks in Cloud Environments. NEXG AI Review of America, 2(1), 17-31.

Thompson, C. R., Talla, R. R., Gummadi, J. C. S., Kamisetty, A (2019). Reinforcement Learning Techniques for Autonomous Robotics. *Asian Journal of Applied Science and Engineering*, *8*(1), 85-96. https://ajase.net/article/view/94

--0--

How to cite this article

Gummadi, J. C. S. (2023). IoT Security in the Banking Sector: Mitigating the Vulnerabilities of Connected Devices and Smart ATMs. *Asian Business Review*, *13*(3), 95-102. https://doi.org/10.18034/abr.v13i3.737