Economic Sciences
https://economic-sciences.com
ES (2025) 20(3S), 01-06 | ISSN:1505-4683

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

Aditi Rohan Kulkarni[1], Dr. Smrity Prasad[2], Dr. Gautam Sen[3], Dr. Avneesh Kumar[4], Kumari Tripti[5], Dr. Harshitha Y S[6]

[1]Assistant Professor, Guru Gobind Singh college of engineering and research centre, Nashik, Maharashtra, India
aditimulay197@gmail.com

[2]Assistant Professor, Department of Statistics and Data Science, CHRIST University, Bengaluru - 560029
Smritykashvi@gmail.com

[3]Assistant Professor in Commerce, Sundarban Hazi Desarat College, University of Calcutta, West Bengal, India, 743611, gautam_sen@hotmail.com

[4]Assistant Professor, Department of Commerce, Mahatma Gandhi Central University, Motihari, Bihar, India
avneesh@hotmail.com

[5]Research Scholar, Department of Commerce, Mahatma Gandhi Central University, Motihari, Bihar, India
tunitripti427@gmail.com

[6]Assistant Professor of Business and Management, CHRIST University Bengaluru

Abstract: *The use of IoT devices has become widespread in banking operations ranging from smart ATMs to better biometric systems, but with it comes enhanced risks to cyber threats. This empirical research scrutinises these risks, as well as device exploitation and DDoS attacks, and assesses the countermeasures such as Hidden Markov Models and ISO/IEC 27001. The research also emphasizes the decision-making process of using multiple layers of security to combat emerging threats by using case studies. The study offers the following implications for financial institutions to protect IoT systems: technical advancement and strong protection measures in the age of growing connectivity.*

Keywords: *Banking sector, IoT security, Cybersecurity, Smart ATMs, Biometric authentication, ISO/IEC 27001, Hidden Markov Model, DDoS attacks, Layered security, Digital innovation.*

Introduction

Banking sectors have benefited greatly from IoT devices which are now in abundance in organizations to improve organizational efficiency and customer relations. Smart ATMs, biometric authentication modules, and advanced surveillance systems have emerged as IoT-based systems that facilitate transactions and security processes in a manner that benefits customers. But this is also a connected environment that poses great cybersecurity risks to the banks. Smart devices connected through IoT are usually in danger of having their networks, information, and services hacked (Kannan, 2024). The emergence of IoT has increased the exposure of threats for hackers and the financial sector becomes one of the most exposed to innovative hacking approaches.

Some of the most urgent threats are attacks that can be aimed at smart ATMs and connected devices. These devices while providing complex processes are often easily compromised by poor security features including poor encryption standards or outdated operating systems. These are the challenges that the sector needs to meet head-on as IoT plays out in the future of banking (Sekar, 2022). The purpose of this study is to identify the risks that IoT poses to the banking industry – with special emphasis on smart ATMs and connected devices – and to determine measures that can enhance their security. Thus, this study aims to fulfil the existing knowledge gap in the literature by discovering the present gaps and providing strong solutions to increase the security of the banking sector while enhancing the use of advanced technologies.

Literature Review

1. IoT Integration in Banking

IoT has greatly impacted the banking sector by making it real-time and improving customer's experiences. Smart ATMs are one of the representative IoT applications of the banking sector, which means that banking offers financial services and multi-functional transaction capabilities around the clock. Smart surveillance, and biometric systems with the help of IoT have increased the overall operational performance and security (Kariapper et al., 2020). However, their integration increases inherent risks

Economic Sciences
https://economic-sciences.com
ES (2025) 20(3S), 01-06 | ISSN:1505-4683

including vulnerability to Distributed Denial of Service (DDoS) attacks and data breaches.

2. Security Threats of IoT Applications

New research shows that IoT devices have basic, if not no inherent security measures, and are the weakest links for banks' networks. Key vulnerabilities include:

Unsecured Interfaces: Management systems of IoT devices web-based are often attacked by hackers, which provide access to the control of crucial systems.

Data Encryption Deficiencies: A large number of IoT gadgets send their data openly without any form of encryption, meaning that the financial data are at risk (Shalaby et al., 2021).

Software Obsolescence: Devices with old firmware versions still in use can be easily attacked because they contain unaddressed vulnerabilities.

These risks were elaborated in researches which described that even such components as insecure encryption and inadequate passwords in IoT systems could bring catastrophe.

3. Theoretical Models and Threat Analysis

Security frameworks like the HMM for behavioral analysis give more understanding into how to identify anomalous behaviors in devices. These models with the help of machine learning (ML) can forecast and prevent probable security risks. Further, the Internet of Things Cybersecurity Improvement Act emphasizes the need to have standardized security for securing IoT devices at the bare minimum (Khan et al., 2023).

4. Loss of Customer Information and Lessons on IoT Breaches in Banking

Recent case studies demonstrate the severity of IoT-related cyber-attacks:

DDoS Attacks: As a result of malicious IoT devices, hackers flooded the banking servers and caused down time. The kind of attacks are usually cover-up for other complex ones that target the theft of sensitive data.

ATM Skimming and Jackpotting: Attacking IoT-based ATMs with malware, hackers have stolen money or even programmed the machine to release money improperly.

These occurrences highlight the importance of a preventive strategy to managing IoT risks in financial organisations.

5. Mitigation Strategies

Mitigation strategies involve enhancing security across multiple layers:

Device-Level Security: Biometric authentication, strong encryptions and constant updates of the software to counter existing risks.

Network Monitoring: Real-time threat detection is possible with the help of Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS).

Standardization and Regulation: The initiatives that help to achieve these objectives are the implementation of normative structures such as ISO/IEC 27001 (Vittala et al., 2024).

Proactive Stress Testing: Regular tests of systems against scenarios can help to uncover some of the vulnerabilities and what action needs to be taken.

6. Trends Related to IoT Security

To improve the security of the IoT, AI and blockchain technology are promising paths for the integration of IoT. Real-time threat identification is made possible by AI, while the transparency and unalterability of transactions are due to blockchain (Rao and Deebak, 2023). However, the adoption of these technologies requires a huge capital investment and infrastructure readiness.

Economic Sciences
https://economic-sciences.com
ES (2025) 20(3S), 01-06 | ISSN:1505-4683

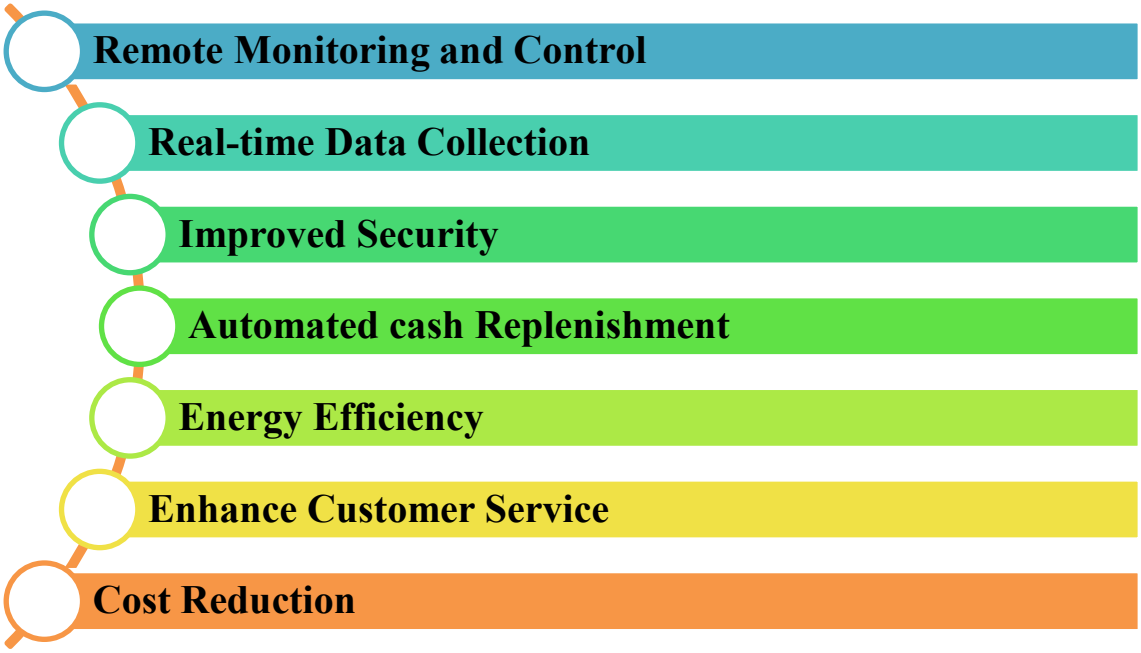

Figure 1: IoT Based ATM Security System
(*Source: Created by the Author*)

From discussions of threats, case studies, and novel security approaches, this literature review highlights the two-fold nature of IoT as a threat and as a resource in banking. Secure Internet of Things banking for the future relies on innovation matched with the right investments in the protection of the sector.

Data and Variables

As a source of data, this research paper relies on secondary qualitative data sourced from various published articles, business news, and case studies related to IoT security threats in the banking industry. The use of a qualitative approach allows the exploration of patterns, threats, and their mitigations related to IoT-enabling systems like smart ATMs and biometric devices. This research focuses on the following variables: IoT devices deployed in banking systems; the kind of cybersecurity threats; and, the efficacy of the recommended measures. The contextual evidence is obtained from analysing case studies of IoT security breaches, whereas the Hidden Markov Model, as well as IoT-centric cybersecurity standards such as ISO/IEC 27001, are examined critically (Marani et al., 2023). These variables will be used to generate empirical results and provide an understanding of the correlation between IoT vulnerabilities and the usage of effective security measures in financial organizations.

Methodology and Model Specification

The approach used in this empirical research paper is based on a critical analytical model derived from secondary qualitative data. This research relies on previous works, theories and models to analyze the threats and safeguards in the IoT integrated banking environment. The methodology integrates two primary components:

1. Analytical Models for Understanding Business and Management

This paper explores theoretical and applied models that address IoT security concerns:

Hidden Markov Model (HMM): This is a behavioral analysis tool that is used to identify problems with IoT devices usage. It estimates possible compromises by pointing out irregularities in the course of business as usual.

IoT Security Frameworks: Regulations like ISO/IEC 27001 are quoted to set basic security parameters for IoT devices, and align with the standards.

Cybersecurity Improvement Act Principles: These guidelines help in critically evaluating the need to

Economic Sciences
https://economic-sciences.com
ES (2025) 20(3S), 01-06 | ISSN:1505-4683

have special measures for security and regulation for every device in the financial institutions.

2. Data Analysis Approach

The literature review of the study utilizes secondary qualitative data from case studies, reports, and incident analyses. All these data sources are systematically reviewed in order to identify such factors such as ATM skimming, DDoS attacks, and insecure interfaces. Special emphasis is placed on real-world incidents of smart ATMs and networked devices compromise to find common trends and countermeasures.

3. Focus of Empirical Results

The empirical results will examine:

- Patterns of IoT-related security breaches in the banking sector.
- The success of risk management measures such as encryption, identity authentication, and intrusion prevention mechanisms.
- Case studies for comparison of the application of models such as HMM in assessing the effectiveness of the chosen approach.

The methodology is an improvement over the existing models and qualitative data as it is a critical synthesis of the two, offering a sound approach to comparing IoT security risks and solutions in the banking industry. In the subsequent empirical analysis, the findings of the theoretical analysis will be further supported by the analysis of the practical implementation of the derived concepts.

Empirical Results

1. IoT Risk Factors in the Context of Banking Industry

Smart devices improve IoT systems' operational processes while simultaneously posing security risks. The vulnerabilities identified include:

- **Device Exploitation:** Smart ATMs and other IoT devices are vulnerable to malware injection and unauthorized access because of low encryption levels.
- **Network Exposure:** Devices with weak security open the rest of the network to the hacker by allowing them to launch Distributed Denial of Service (DDoS) attacks and data breaches (George et al., 2024).
- **Biometric System Risks:** Despite the sophistication of IoT biometric systems there are issues like spoofing or misuse of stolen biometric data.

2. Mitigation Strategies: Evaluation and Effectiveness

There are a number of models and frameworks that relate to these vulnerabilities. Their implementation is evaluated below, with emphasis on practical application in the banking context:

Table 1: Evaluation of IoT Security Models and Strategies for the Banking Sector

Model/Strategy	Description	Application in Banking	Effectiveness
Hidden Markov Model (HMM)	Behavioral analysis model for detecting anomalies in device usage.	Applied to monitor smart ATMs and detect irregular transaction patterns.	High effectiveness in detecting abnormal patterns but requires advanced analytics infrastructure.
ISO/IEC 27001 Framework	Standardized guidelines for IoT device security and risk management.	Used to implement security protocols across devices, ensuring compliance.	Strong framework for risk mitigation but requires consistent updates to address evolving threats.
Biometric Authentication	Integration of fingerprint and facial recognition for enhanced security.	Secures ATMs and account access with multi-layered verification.	Reduces risk of unauthorized access but vulnerable to advanced spoofing techniques.

Economic Sciences
https://economic-sciences.com
ES (2025) 20(3S), 01-06 | ISSN:1505-4683

Intrusion Detection Systems	Systems for real-time monitoring and prevention of unauthorized access.	Deployed in IoT networks to detect and block malicious activity.	High accuracy in threat identification but requires continuous monitoring and system updates.
Data Encryption Protocols	Ensures secure transmission of data across IoT networks.	Protects sensitive customer and transaction data in ATMs and banking systems.	Effective against data interception but dependent on the strength and frequency of encryption updates.

(Source: Author's compilation)

3. Analysis of Case Studies

Case Study 1: Denial of Service Attacks on Banking Networks

A financial institution was once attacked by DDoS in which contaminated IoT devices flooded the financial institution's servers thus, straining the customers' services (Cloudflare, 2024). The bank reduced the effects of the attack through implementing the network level Intrusion prevention systems and traffic management by use of cloud based scrubbing service. This approach corresponded with the methodologies proposed, illustrating the importance of anticipatory network management.

Case Study 2: IoT-enabled ATM Skimming

IoT vulnerabilities in ATMs were targeted by cybercriminals who injected malware to steal card data. The measures that proved possibility of such attacks were biometric authentication and constant firmware updates, which showed that layered security measures were efficient (trendmicro, 2019).

Case Study 3: Biometric System Spoofing

Some IoT biometric systems of a bank were vulnerable to spoofing attacks. The use of behavioral analysis employing HMM alongside the combination of complex encryption protocols enhanced the security of these systems to minimize cases of misuse (Sultana, 2012).

4. Comparative Analysis of Mitigation Strategies

The results stress the contingency of the mitigation measures used in the study. There are several approaches to use in SO: behavioral models, including HMM, provided high accuracy in anomaly detection; standardized frameworks, including ISO/IEC 27001, provided wide-spectrum risk management (Roy et al., 2024). Biometric authentication is more secure than the traditional methods but the technology used in this method needs to improve the countermeasures for spoofing. The comparative analysis also shows that it is necessary to use a multilayered approach to respond to various threats.

5. Analysis of the Effects of the Crisis on the Banking Sector

This paper's findings suggest that there is a need to design an IoT security framework that includes monitoring, compliance, and encryption. Financial institutions need to ensure that the security systems are updated on a regular basis and the technologies like the AI-based analytics tools are adopted for better security. ISO/IEC 27001 framework can be thus used as reference for sound risk management and provide the necessary support for the secure implementation of IoT devices in the banking sector (Yaacoub et al., 2023).

The findings of this critical evaluation offer practical recommendations for managing IoT security issues, which makes it possible to discuss more sophisticated solutions in the banking context further.

Conclusion

The use of IoT in the banking sector has greatly improved operations but has opened up new security risks. This research outlines principal threats including; network exploitation and biometric spoofing, and the most efficient ways of moderating them; HMM, biometric authentication, and regulations. It becomes clear that a layered security approach is becoming unavoidable, in order to promote innovation while strengthening the protection mechanisms. More than that, future efforts should be directed towards the implementation of AI-based anomaly detection and the use of block chain as a way of increasing transparency and security. Moreover, emerging IoT security measures and real-time modification of system requirements are critical to addressing new challenges for secure banking in the context of IoT.

References

1. Kannan, Y., 2024. Impact of Internet of Things (IoT) devices on Network Security at Financial Institutions. *Authorea Preprints*.
2. Sekar, J., 2022. Innovative approaches to cloud security in IOT-enabled banking systems. *World Journal of Advanced Research and Reviews*, *23*, pp.822-828.
3. Kariapper, R.K.A.R., Razeeth, M.S., Pirapuraj, P. and Nafrees, A.C.M., 2020, December. Effectiveness of ATM and bank security: three factor authentications with systemetic review. In *Journal of Physics: Conference Series* (Vol. 1712, No. 1, p. 012007). IOP Publishing.
4. Shalaby, A., Gad, R., Hemdan, E.E.D. and El-Fishawy, N., 2021. An efficient multi-factor authentication scheme based CNNs for securing ATMs over cognitive-IoT. *PeerJ Computer Science*, *7*, p.e381.
5. Khan, H.U., Malik, M.Z., Nazir, S. and Khan, F., 2023. Utilizing bio metric system for enhancing cyber security in banking sector: A systematic analysis. *IEEE Access*.
6. Rao, P.M. and Deebak, B.D., 2023. Security and privacy issues in smart cities/industries: technologies, applications, and challenges. *Journal of Ambient Intelligence and Humanized Computing*, *14*(8), pp.10517-10553.
7. Vittala, K.P., Ahmad, S.S., Seranmadevi, R. and Tyagi, A.K., 2024. Emerging Technology Adoption and Applications for Modern Society Towards Providing Smart Banking Solutions. In *Enhancing Medical Imaging with Emerging Technologies* (pp. 315-329). IGI Global.
8. Marani, M., Soltani, M., Bahadori, M., Soleimani, M. and Moshayedi, A., 2023. The role of biometric in banking: A review. *EAI Endorsed Transactions on AI and Robotics*, *2*(1).
9. George, A.S., Baskar, T. and Srikaanth, P.B., 2024. Cyber threats to critical infrastructure: assessing vulnerabilities across key sectors. *Partners Universal International Innovation Journal*, *2*(1), pp.51-75.
10. Cloudflare. (2024). *Famous DDoS Attacks*. Retrieved November 29, 2024, from https://www.cloudflare.com/learning/ddos/famous-ddos-attacks/
11. www.trendmicro.com. (2019). *Banks Under Attack: Tactics and Techniques Used to Target Financial Organizations - Security News*. [online] Available at: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/banks-under-attack-tactics-and-techniques-used-to-target-financial-organizations.
12. Sultana, A., Hamou-Lhadj, A. and Couture, M., 2012, June. An improved hidden markov model for anomaly detection using frequent common patterns. In *2012 IEEE International Conference on Communications (ICC)* (pp. 1113-1117). IEEE.
13. Roy, A., Dhar, A. and Tinny, S.S., 2024. Strengthening IoT Cybersecurity with Zero Trust Architecture: A Comprehensive Review. *Journal of Computer Science and Information Technology*, *1*(1), pp.25-50.
14. Yaacoub, J.P.A., Noura, H.N., Salman, O. and Chehab, A., 2023. Ethical hacking for IoT: Security issues, challenges, solutions and recommendations. *Internet of Things and Cyber-Physical Systems*, *3*, pp.280-308.