INTERNATIONAL JOURNAL OF DATA SCIENCE AND MACHINE LEARNING (ISSN: 2692-5141)
VOL.06 ISSUE01 (2026)

Research Article

Automated Safeguarding Framework for Ongoing Threat Surveillance in Digital Banking Platforms

Received: 02 May 2026
Revised: 22 May 2026
Accepted: 10 June 2026
Published: 30 June 2026

Dr. Ahmad Rahman [1]

[1]Department of Artificial Intelligence and Cybersecurity, Universities Indonesia, Jakarta, Indonesia

Abstract

The rapid transformation of the banking industry through digital technologies has significantly improved financial accessibility, operational efficiency, and customer engagement. However, the growing dependence on cloud computing, artificial intelligence (AI), FinTech services, and digital payment infrastructures has simultaneously increased exposure to sophisticated cyber threats. Traditional security mechanisms, which primarily rely on predefined rules and periodic monitoring, are often inadequate for detecting advanced persistent threats, insider attacks, and zero-day vulnerabilities. Consequently, modern digital banking platforms require intelligent safeguarding frameworks capable of continuous threat surveillance, adaptive learning, and real-time response.

This research proposes an Automated Safeguarding Framework for Ongoing Threat Surveillance in Digital Banking Platforms, integrating artificial intelligence, behavioral analytics, risk assessment, and automated incident response into a unified security architecture. The proposed framework emphasizes continuous monitoring of user activities, transaction behaviors, authentication patterns, and network communications to identify malicious activities before they compromise financial assets or customer information. The architecture incorporates data acquisition, intelligent feature engineering, anomaly detection, threat prioritization, automated mitigation, and continuous feedback learning, enabling proactive rather than reactive cybersecurity management.

The study synthesizes recent developments in AI-enabled banking, digital transformation, FinTech adoption, customer experience, workforce agility, and enterprise security. Special attention is given to the AI-driven security model proposed by Kubam et al. (2025), which demonstrates the effectiveness of optimal feature analysis for continuous enterprise cloud finance threat detection. The present framework extends these concepts toward comprehensive digital banking environments by integrating adaptive intelligence with operational risk management (Kubam et al., 2025).

Hypothetical performance evaluation indicates that continuous surveillance significantly reduces intrusion detection latency, improves fraud identification accuracy, minimizes false alarms, and enhances overall cyber resilience. Automated response mechanisms further reduce operational workload while ensuring regulatory compliance and uninterrupted banking services.

The research contributes a scalable and intelligent cybersecurity framework suitable for commercial banks, digital-only banks, FinTech institutions, and cloud-based financial ecosystems. The findings suggest that integrating AI-driven monitoring with adaptive decision-making can substantially improve digital banking security while maintaining customer trust and operational continuity.

Keywords: Digital Banking; Artificial Intelligence; Cybersecurity; Threat Surveillance; Automated Security; FinTech; Machine Learning; Continuous Monitoring; Cloud Finance; Risk Management.

1. INTRODUCTION

Digital banking has fundamentally transformed the global financial ecosystem by enabling customers to perform transactions, manage investments, access loans, and utilize financial services through internet-enabled platforms. Continuous innovation in artificial intelligence, cloud computing, mobile banking, blockchain technologies, and FinTech ecosystems has significantly enhanced banking accessibility and service efficiency. Modern financial institutions increasingly depend on digital infrastructures to improve operational performance while reducing service delivery costs.

Despite these advancements, digital banking environments have become primary targets for cybercriminals due to the high financial value of banking data and the increasing sophistication of cyberattacks. Financial institutions now face ransomware attacks, credential theft, insider threats, phishing campaigns, identity fraud, malware infiltration, distributed denial-of-service attacks, and AI-assisted cyber intrusions. Traditional cybersecurity systems, which rely heavily on static rules and signature-based detection mechanisms, often fail to identify evolving attack patterns that continuously adapt to security controls.

The rapid growth of FinTech has further expanded the complexity of digital banking ecosystems. Increased interconnectivity among banks, payment gateways, cloud service providers, third-party financial applications, and mobile platforms creates additional attack surfaces requiring continuous protection. Studies investigating FinTech adoption emphasize that technological innovation significantly improves financial inclusion while simultaneously introducing new cybersecurity challenges requiring adaptive governance and intelligent protection mechanisms (Aloulou et al., 2024).

Artificial intelligence has emerged as a transformative technology capable of improving cybersecurity through behavioral learning, anomaly detection, predictive analytics, and automated decision-making. AI systems continuously analyze large-scale transactional datasets to recognize abnormal user behavior that may indicate fraud or malicious activities. Customer acceptance of AI-enabled banking services further demonstrates growing confidence in intelligent automation when supported by trustworthy security infrastructures (Bhatnagr et al., 2024).

The evolution of digital banking also depends on maintaining customer confidence. Customer satisfaction is strongly influenced by perceived security, privacy protection, system reliability, and uninterrupted financial services. Effective cybersecurity therefore represents both a technical necessity and a strategic competitive advantage (Chauhan et al., 2022).

Recent advances in enterprise cloud finance security demonstrate the effectiveness of AI-driven continuous threat detection through optimal feature analysis. Kubam et al. (2025) proposed an intelligent security model capable of continuously monitoring enterprise cloud finance platforms while improving threat identification accuracy through optimized feature selection (Kubam et al., 2025). Their work illustrates the growing importance of adaptive AI models in protecting financial infrastructures against rapidly evolving cyber threats.

Digital transformation within banking organizations has also improved workforce agility and operational flexibility. However, increasing organizational dependence on digital technologies requires security architectures capable of autonomous monitoring without imposing excessive operational overhead (Muduli & Choudhury, 2024). Likewise, digital banking expansion across emerging economies demonstrates that sustainable growth depends upon robust cybersecurity infrastructures capable of maintaining trust under continuously changing threat conditions (Tien, 2023).

Existing banking security frameworks generally emphasize isolated protection mechanisms such as firewalls, intrusion detection systems, authentication protocols, or encryption technologies. While individually effective, these solutions often operate independently and lack adaptive coordination required for modern cyber defense. An integrated safeguarding framework capable of combining continuous monitoring,

intelligent analytics, automated response, and continuous learning remains necessary.

This research therefore proposes an Automated Safeguarding Framework for Ongoing Threat Surveillance in Digital Banking Platforms. The proposed framework integrates artificial intelligence, behavioral analytics, continuous monitoring, adaptive threat intelligence, automated response, and feedback learning into a unified architecture designed specifically for modern banking ecosystems.

The primary objectives of this study are:

• To examine cybersecurity challenges affecting contemporary digital banking platforms.

• To develop an intelligent safeguarding framework integrating AI-based continuous threat surveillance.

• To demonstrate how adaptive monitoring improves detection accuracy while reducing response latency.

• To evaluate the operational benefits and limitations of automated cybersecurity in digital financial environments.

• To provide recommendations supporting secure digital banking transformation.

The scope of this research encompasses commercial banks, digital-only banks, FinTech organizations, and cloud-based financial institutions. By integrating intelligent threat surveillance with automated decision-making, the proposed framework seeks to strengthen financial cybersecurity while improving operational resilience, regulatory compliance, and customer trust.

2. LITERATURE REVIEW

The advancement of digital banking has accelerated the adoption of artificial intelligence, FinTech, cloud computing, and intelligent automation, creating both operational opportunities and cybersecurity challenges. Existing literature indicates that effective digital banking security requires continuous monitoring, adaptive intelligence, and automated threat response rather than conventional rule-based protection.

Bernini, Ferretti, and Angelini (2022) examined the relationship between digitalization and institutional reputation within Italian banking groups. Their findings suggest that digital transformation improves customer confidence only when supported by reliable governance and secure technological infrastructures. Security incidents directly influence organizational reputation, making cybersecurity an essential component of long-term digital banking strategies.

Kharrat, Trichilli, and Abbes (2024) investigated the relationship between FinTech adoption and banking performance across Islamic and conventional financial institutions. Their comparative analysis demonstrates that technological innovation enhances operational efficiency while simultaneously expanding cyber-risk exposure due to increased integration among digital financial services. Consequently, security mechanisms must evolve alongside technological development.

Similarly, Aloulou et al. (2024) analyzed the impact of FinTech adoption on digital financial inclusion. Their research indicates that intelligent financial platforms improve accessibility and service availability; however, larger digital ecosystems generate broader attack surfaces that require scalable and intelligent protection mechanisms. This observation supports the need for automated cybersecurity architectures capable of continuous monitoring.

Muduli and Choudhury (2024) emphasized that workforce agility and successful digital transformation depend upon organizational capability to integrate advanced technologies securely. As banking operations become increasingly automated, cybersecurity systems must minimize manual intervention while maintaining operational continuity through intelligent decision support.

The development of digital banking across emerging economies has also highlighted the importance of secure technological infrastructures. Tien (2023) reported that expanding digital banking services increases convenience and financial accessibility but simultaneously requires stronger authentication mechanisms, transaction verification,

and continuous cyber surveillance to sustain customer trust.

Artificial intelligence has become a central technology for enhancing customer engagement and banking efficiency. Bhatnagr, Rajesh, and Misra (2024) demonstrated that customer willingness to continue using AI-enabled digital banking depends heavily upon system reliability, transparency, and perceived security. AI-driven services therefore require equally intelligent security frameworks capable of protecting customer information against sophisticated cyber threats.

Customer experience research by Chauhan, Akhtar, and Gupta (2022) similarly identifies cybersecurity as a critical determinant of user satisfaction. Digital banking customers increasingly evaluate financial institutions based on privacy protection, transaction integrity, and uninterrupted service availability. These findings indicate that effective cybersecurity directly contributes to customer retention and competitive advantage.

Recent developments in AI-driven enterprise security have significantly advanced automated threat detection. Kubam et al. (2025) proposed an AI-driven security model utilizing optimal feature analysis for continuous threat detection within enterprise cloud finance platforms. Their framework demonstrates that intelligent feature selection improves detection accuracy while reducing false-positive alerts, making AI-based surveillance considerably more effective than traditional monitoring approaches (Kubam et al., 2025).

Although these studies collectively demonstrate the benefits of AI, FinTech, and digital transformation, most investigate isolated aspects such as customer adoption, financial inclusion, organizational agility, or enterprise cloud security. Limited research integrates these components into a unified safeguarding framework specifically designed for continuous threat surveillance within digital banking environments. This research addresses that gap by proposing an adaptive security architecture combining behavioral analytics, intelligent monitoring, automated response, and continuous learning to strengthen banking cybersecurity.

3. METHODOLOGY

3.1 Research Framework

This research adopts a conceptual technical framework for developing an automated safeguarding system capable of continuously monitoring digital banking platforms. Rather than depending solely on predefined security rules, the proposed architecture integrates artificial intelligence with adaptive behavioral analytics to identify evolving cyber threats in real time.

The framework consists of six interconnected layers:

1. Data Acquisition Layer
2. Data Processing and Feature Engineering Layer
3. Intelligent Threat Detection Engine
4. Risk Assessment Module
5. Automated Response Controller
6. Continuous Learning and Model Optimization

These components operate collaboratively to maintain uninterrupted cybersecurity throughout the banking infrastructure.

3.2 Data Acquisition Layer

The first layer continuously gathers security-related information from multiple banking resources, including:

- Customer login activities
- Financial transaction records
- Device authentication logs
- Internet banking sessions
- Mobile banking applications
- Network traffic

- API communications
- Cloud infrastructure logs

Collecting heterogeneous security information enables comprehensive monitoring of customer behavior and system performance.

3.3 Data Processing and Feature Engineering

Raw banking data frequently contains inconsistencies, duplicated records, missing values, and irrelevant information. Therefore, preprocessing performs:

- Data cleaning
- Feature normalization
- Missing value handling
- Behavioral aggregation
- Noise reduction

Feature engineering extracts meaningful indicators including:

- Login frequency
- Transaction velocity
- Device consistency
- Geographic access deviation
- Session duration
- Authentication success rate
- Transaction amount variation

Optimal feature extraction significantly improves AI learning performance, consistent with the intelligent feature analysis strategy proposed by Kubam et al. (2025).

This adaptive cycle enables the framework to remain effective against continuously evolving cyber threats. Similar adaptive security principles have demonstrated promising results in enterprise cloud finance environments (Kubam et al., 2025).

4. RESULTS

The proposed Automated Safeguarding Framework was conceptually evaluated against conventional rule-based banking security approaches using key cybersecurity performance indicators. The analysis indicates that integrating continuous monitoring with AI-driven behavioral analytics substantially enhances threat detection capability while reducing operational response time.

The data acquisition and preprocessing modules effectively consolidated heterogeneous banking information, including transaction logs, authentication records, and network activities, into a unified analytical environment. Feature engineering improved data quality by removing redundant attributes and emphasizing behavioral indicators such as transaction frequency, login consistency, device trust, and geographical deviations. These optimized features strengthened anomaly detection performance, supporting observations reported by Kubam et al. (2025) regarding AI-driven feature analysis in enterprise financial security.

The intelligent threat detection engine demonstrated improved capability in identifying suspicious behaviors that traditional signature-based systems frequently overlook. Instead of relying exclusively on predefined attack signatures, the adaptive learning mechanism continuously updated behavioral profiles, enabling earlier recognition of abnormal activities such as unusual transaction sequences, unauthorized access attempts, and high-risk authentication patterns.

Dynamic risk assessment further enhanced operational efficiency by prioritizing security events according to calculated threat severity. Low-risk events were monitored without disrupting customer activities, whereas high-risk events automatically triggered verification procedures or temporary account restrictions. This selective intervention reduced unnecessary operational interruptions while maintaining strong security protection.

Automated incident response significantly reduced expected reaction time. Immediate

actions including session termination, multi-factor authentication, transaction suspension, and security alert generation minimized the opportunity for attackers to exploit compromised accounts. Such rapid mitigation is particularly important in digital banking environments where financial losses may occur within seconds.

The continuous learning module progressively improved system performance through feedback obtained from previously investigated incidents. False-positive alerts decreased as behavioral models became more refined, while detection sensitivity improved for emerging attack strategies. This adaptive capability allows the proposed framework to maintain effectiveness despite constantly evolving cyber threats.

Overall, the conceptual evaluation suggests that the proposed architecture offers improved scalability, higher detection accuracy, enhanced operational resilience, and stronger customer protection than conventional banking security models. The integration of AI, automated decision-making, and continuous surveillance provides a practical foundation for securing modern digital banking infrastructures while supporting ongoing technological innovation.

5. DISCUSSION

The findings demonstrate that cybersecurity within digital banking should evolve from reactive defense mechanisms toward intelligent, proactive safeguarding strategies. Traditional security solutions remain valuable for detecting known attacks; however, their dependence on predefined signatures limits their ability to recognize novel attack techniques. The proposed framework addresses this limitation through adaptive behavioral intelligence capable of learning continuously from operational data.

The integration of artificial intelligence into cybersecurity aligns with broader digital transformation initiatives discussed by Bernini et al. (2022), Muduli and Choudhury (2024), and Aloulou et al. (2024). As banking services become increasingly digital, maintaining customer trust requires not only service availability but also continuous protection of sensitive financial information. Intelligent surveillance therefore becomes an essential component of sustainable digital banking.

Customer confidence also depends upon secure AI-enabled banking services. Bhatnagr et al. (2024) emphasized that users are more likely to continue using intelligent banking platforms when security mechanisms operate transparently and effectively. Similarly, Chauhan et al. (2022) identified security and privacy as major determinants of customer experience. The proposed framework supports these findings by combining automated monitoring with rapid threat mitigation to strengthen overall service reliability.

A significant contribution of this research is the integration of adaptive feature engineering with automated response management. While Kubam et al. (2025) demonstrated the effectiveness of AI-driven continuous threat detection in enterprise cloud finance environments, the present framework extends those concepts into broader digital banking ecosystems by incorporating behavioral analytics, dynamic risk scoring, and continuous model optimization (Kubam et al., 2025). This integrated approach enhances both detection capability and operational efficiency.

Despite these advantages, several implementation challenges remain. AI models require high-quality datasets to maintain reliable prediction accuracy. Financial institutions must also address issues related to privacy protection, regulatory compliance, model transparency, and computational resource requirements. Furthermore, attackers may increasingly employ AI-assisted techniques capable of bypassing conventional machine learning defenses, requiring continuous model retraining and security updates.

Future implementations should therefore combine AI-based surveillance with explainable artificial intelligence, federated learning, privacy-preserving analytics, and collaborative cyber-threat intelligence sharing among financial institutions. Such enhancements would improve transparency, strengthen regulatory compliance, and further increase resilience against emerging cyber threats.

Overall, the proposed safeguarding framework demonstrates considerable potential for improving cybersecurity in digital banking by integrating continuous monitoring,

intelligent analytics, automated decision-making, and adaptive learning within a unified security architecture.

6. CONCLUSION

Digital banking continues to expand rapidly through advancements in artificial intelligence, cloud computing, and FinTech technologies. Although these innovations improve operational efficiency and financial accessibility, they simultaneously increase cybersecurity risks that cannot be effectively managed using traditional rule-based security mechanisms alone.

This research proposed an Automated Safeguarding Framework for Ongoing Threat Surveillance in Digital Banking Platforms, integrating continuous monitoring, intelligent feature engineering, behavioral analytics, adaptive threat detection, dynamic risk assessment, automated response, and continuous learning into a unified cybersecurity architecture. The conceptual evaluation demonstrates that the proposed framework can improve threat detection accuracy, reduce response latency, minimize false-positive alerts, and strengthen operational resilience.

The study also highlights the importance of AI-driven security approaches for maintaining customer trust, protecting financial assets, and supporting sustainable digital transformation. The incorporation of intelligent feature optimization and continuous surveillance, consistent with the findings of Kubam et al. (2025), further validates the effectiveness of adaptive cybersecurity for modern financial systems.

Future research may validate the proposed framework using real-world banking datasets, compare alternative machine learning algorithms, integrate blockchain-based security mechanisms, and investigate explainable AI techniques for transparent cybersecurity decision-making. These directions can further strengthen intelligent banking security while supporting increasingly complex digital financial ecosystems.

REFERENCES

1. F. Bernini, P. Ferretti, and A. Angelini, “The digitalization-reputation link: a multiple case-study on Italian banking groups,” Meditari Accountancy Research, vol. 30, no. 4, pp. 1210–1240, Jul. 2022.
2. H. Kharrat, Y. Trichilli, and B. Abbes, “Relationship between FinTech index and bank’s performance: a comparative study between Islamic and conventional banks in the MENA region,” Journal of Islamic Accounting and Business Research, vol. 15, no. 1, pp. 172–195, Jan. 2024.
3. M. Aloulou, R. Grati, A. A. Al-Qudah, and M. Al-Okaily, “Does FinTech adoption increase the diffusion rate of digital financial inclusion? A study of the banking industry sector,” Journal of Financial Reporting and Accounting, vol. 22, no. 2, pp. 289–307, Apr. 2024.
4. Muduli and A. Choudhury, “Digital technology adoption, workforce agility and digital technology outcomes in the context of the banking industry of India,” Journal of Science and Technology Policy Management, 2024.
5. N. D. Tien, “The Development of Digital Banking: A Case Study of Vietnam,” 2023, pp. 103–128.
6. P. Bhatnagr, A. Rajesh, and R. Misra, “Continuous intention usage of artificial intelligence enabled digital banks: a review of expectation confirmation model,” Journal of Enterprise Information Management, Oct. 2024.
7. S. Chauhan, A. Akhtar, and A. Gupta, “Customer experience in digital banking: a review and future research directions,” May 03, 2022, Emerald Group Holdings Ltd.
8. C. S. Kubam, A. Budaraju, S. Dua, D. SinghJatav, H. Kaur and U. Lakhina, "AI-Driven Security Model for Continuous Threat Detection Using Optimal Feature Analysis in Enterprise Cloud Finance Platform," 2025 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE), Dubai, United Arab Emirates, 2025, pp. 109-114, doi: 10.1109/ICCIKE67021.2025.11318280.