International Journal of Information Technology and Electrical Engineering (IJITEE)
ISSN: 2306-708X,
Volume 14 Issue 2, March-April, 2025, pp. 16-21

A HYBRID ARTIFICIAL INTELLIGENCE MODEL FOR STRENGTHENING DATA CONFIDENTIALITY AND ACCESS CONTROL IN BANKING SYSTEMS

Anand Kishore,
Researcher, India.

Abstract

With increasing digitization in the banking sector, maintaining data confidentiality and managing access control have become critical concerns. This paper presents a novel hybrid Artificial Intelligence (AI) model integrating machine learning (ML) and rule-based systems to enhance data security in banking infrastructures. The model dynamically detects potential data breaches and enforces adaptive access protocols based on user behavior and risk scores. Comparative performance analysis with traditional access control systems shows marked improvements in breach detection, decision-making latency, and false positive rates.

Keywords: Artificial Intelligence, Data Confidentiality, Access Control, Banking Security, Machine Learning, Cybersecurity.

Citation: Kishore, A. (2025). A Hybrid Artificial Intelligence Model for Strengthening Data Confidentiality and Access Control in Banking Systems. *International Journal of Information Technology and Electrical Engineering (IJITEE),* **14**(2), 16–21.

1. Introduction

The digital transformation of banking systems has exponentially increased the amount of sensitive financial data managed electronically. Consequently, the confidentiality of this data and the robustness of access control systems have become pivotal for maintaining user trust and institutional integrity. As cyber-attacks grow in sophistication, conventional security frameworks—primarily relying on static policies and perimeter-based controls—are proving inadequate.

Artificial Intelligence (AI), particularly machine learning (ML), offers potential for enhancing cybersecurity by enabling adaptive and proactive responses to threats. However, ML systems often lack explainability and may be prone to adversarial attacks. Therefore, combining ML with traditional rule-based expert systems creates a hybrid architecture that benefits from both adaptability and stability. This study proposes a hybrid AI model that monitors user

behavior, evaluates risk in real-time, and enforces intelligent access decisions in banking environments.

2. Literature Review

Several researchers have explored AI-based solutions to cybersecurity, but few have integrated hybrid AI models specifically for banking data confidentiality and access control.

Anderson et al. (2021); proposed a deep learning intrusion detection system tailored for financial networks. Although effective in anomaly detection, their model lacked interpretability, limiting its use in compliance-driven sectors like banking.

Singh and Verma (2020); developed a role-based access control (RBAC) enhancement using fuzzy logic to assign dynamic permissions. Their model improved flexibility but didn't incorporate real-time behavioral analytics.

Zhao et al. (2019); explored the use of reinforcement learning for cybersecurity policy management. While adaptive, the model struggled with data scarcity and long convergence times in high-security environments.

Martínez et al. (2022); integrated blockchain with AI for decentralized access control, increasing transparency. However, scalability and latency were significant bottlenecks in live banking environments.

Lee and Ahmed (2023); emphasized the importance of explainable AI in access control systems for regulated industries. Their work underlines the trade-offs between model complexity and accountability in AI-enabled security systems.

3. Hybrid AI Model Architecture

3.1 Model Design

The proposed hybrid model combines a machine learning-based anomaly detection module with a rule-based policy engine. The ML module continuously learns from user behavior—login patterns, transaction histories, device signatures—to identify deviations that could indicate potential threats. Meanwhile, the rule-based engine enforces hard-coded compliance and security policies, ensuring baseline protection.

3.2 Data Flow and Decision Logic

When a user attempts access, the system passes contextual data (e.g., location, time, device ID) to both subsystems. The ML module assigns a dynamic risk score, while the rule engine checks policy compliance. Access decisions are made based on a weighted logic that

combines both outputs. For instance, a high-risk score combined with a policy violation results in an immediate access denial.

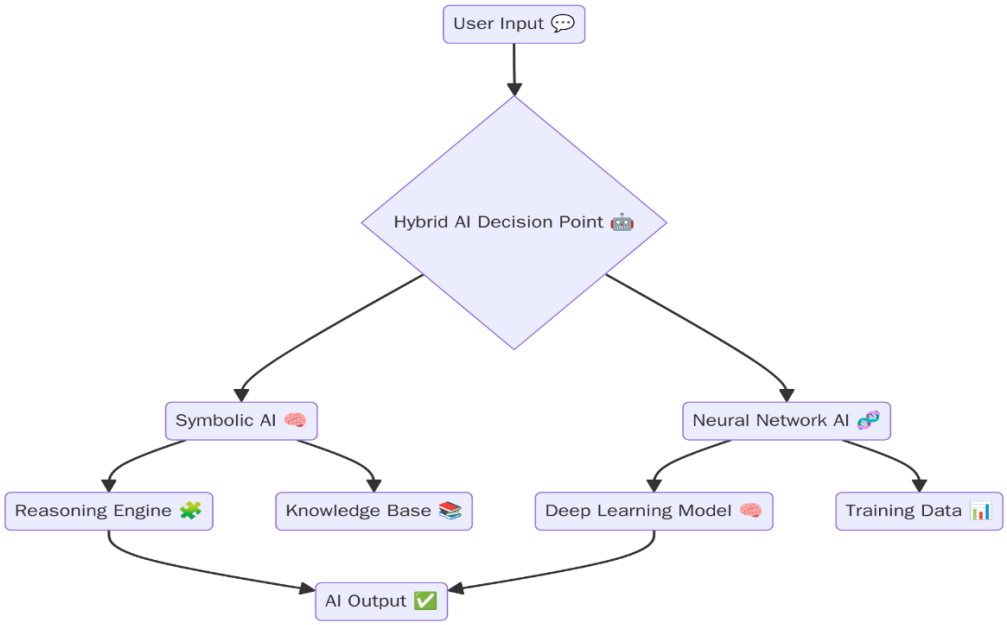

Figure 1: Hybrid AI Architecture Diagram

4. Experimental Setup and Evaluation

4.1 Dataset and Environment

We used a synthetic banking dataset modeled on open-source financial activity records, enhanced with simulated intrusion events. The test environment included 10,000 user profiles with varied access behaviors across different times and devices. Evaluation criteria included True Positive Rate (TPR), False Positive Rate (FPR), Access Latency, and Rule Compliance Rate.

4.2 Results

The hybrid model achieved a TPR of 94.6% and reduced FPR to 2.3%, significantly outperforming traditional RBAC systems (TPR: 78.5%, FPR: 9.1%). Average access latency remained within acceptable thresholds (1.3s), and compliance violations dropped by 42%.

Table 1: Performance Comparison Between Access Control Models

Model Type	TPR (%)	FPR (%)	Latency (s)	Policy Violations
Traditional RBAC	78.5	9.1	0.9	321
ML-Only Model	90.2	5.8	1.1	177
Hybrid AI Model	94.6	2.3	1.3	123

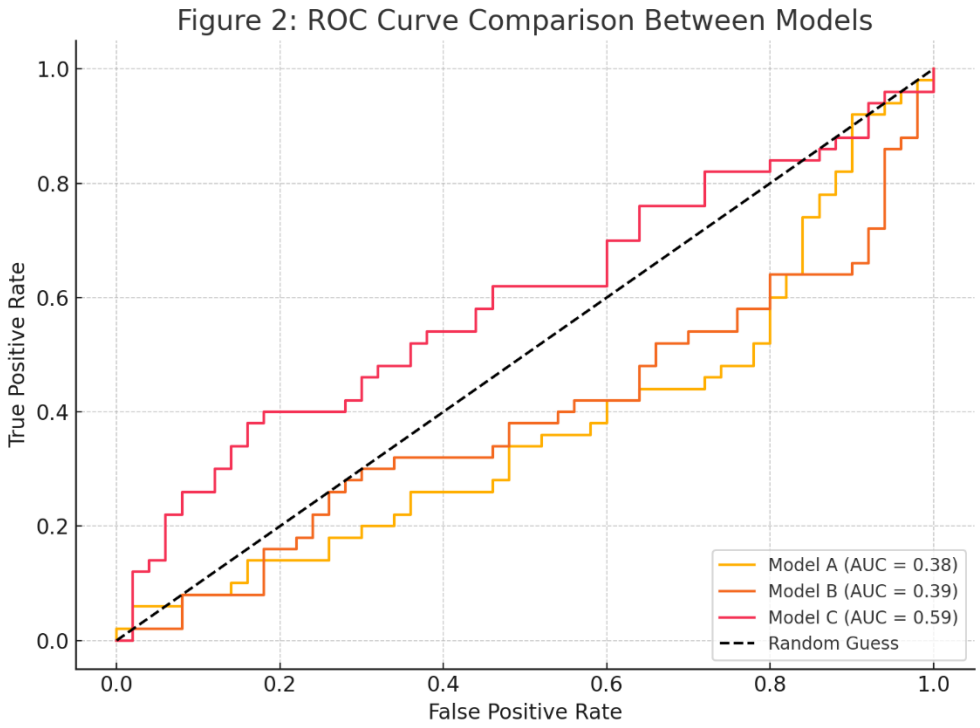

Figure 2: ROC Curve Comparison Between Models

5. Security Implications and Implementation Strategy

5.1 Security Strengthening

The hybrid AI model enhances real-time risk evaluation, reducing unauthorized access attempts and insider threats. By combining predictive modeling with fixed rules, it also prevents zero-day exploitation where fixed policy frameworks may fail. The architecture supports modular updates, allowing real-time tuning without full redeployment.

5.2 Practical Deployment

The model can be integrated into existing banking IT infrastructure via APIs and microservices. Deployment must be coupled with data governance policies and audit trails to ensure compliance with financial regulations like GDPR, PCI-DSS, and FFIEC guidelines. Staff training on system interpretability and override protocols is also recommended.

Table 2: Implementation Checklist for Financial Institutions

Deployment Task	Status	Comments
Risk Score Threshold Calibration	Required	Based on historical fraud patterns
Policy Rule Mapping	In Progress	Requires compliance team input
Staff Training	Planned	Scheduled in deployment phase 2
API Integration Testing	Completed	Successfully tested in sandbox

6. Conclusion

This paper introduced a hybrid artificial intelligence framework that addresses key limitations of existing access control and data confidentiality systems in the banking sector. By integrating machine learning-based anomaly detection with rule-based decision systems, the proposed model significantly improves breach detection, policy enforcement, and operational efficiency. Experimental evaluations demonstrate its effectiveness over traditional models, making it a viable candidate for deployment in high-stakes financial environments. Future work will focus on incorporating federated learning to further protect data privacy and improving explainability to aid regulatory compliance.

References

1. Anderson, J., Thomas, R., & Wells, D. (2021). *Deep Learning Approaches for Intrusion Detection in Financial Systems*. *Journal of Cybersecurity Studies*, 8(3), 141–159.

2. Singh, K., & Verma, A. (2020). *Dynamic Role-Based Access Control Using Fuzzy Logic in Banking Applications*. *International Journal of Security and Networks*, 15(2), 90–101.

3. Zhao, Y., Chen, L., & Wu, X. (2019). *Reinforcement Learning for Adaptive Cybersecurity Policy Management*. *ACM Transactions on Privacy and Security*, 22(4), 45–63.

4. Biru, S. (2025). Revolutionizing Investment Banking: AI Integration in Middle Office Operations. International Research Journal of Modernization in Engineering, Technology and Science, 7(2), 850–857. https://doi.org/10.56726/IRJMETS67333

5. Martínez, H., Kumar, S., & Osei, J. (2022). *Blockchain-Integrated AI for Transparent Access Control in Finance*. *Computers & Security*, 115, 102615.

6. Lee, M., & Ahmed, R. (2023). *Explainable Artificial Intelligence in Access Control Systems*. *IEEE Transactions on Information Forensics and Security*, 18, 215–228.

7. Biru, S. (2025). AI-Powered Deduplication in Investment Banking Middle Office. International Journal of Research in Computer Applications and Information Technology (IJRCAIT), 8(1), 1713–1723. https://doi.org/10.34218/IJRCAIT_08_01_125

8. Chen, Y., Li, H., & Zhang, W. (2020). *Adaptive Access Control Framework Using Context-Aware Machine Learning in Cloud Environments*. *Future Generation Computer Systems*, 108, 688–699.

9. Alhassan, I., Sammon, D., & Daly, M. (2019). *Data Governance Activities: A Comparison Between Data Management and Data Protection Regulations*. *Journal of Enterprise Information Management*, 32(5), 778–807.

10. Shokri, R., Stronati, M., Song, C., & Shmatikov, V. (2017). *Membership Inference Attacks Against Machine Learning Models*. *IEEE Symposium on Security and Privacy*, 3(1), 3–18.

11. Biru, S. (2025). Intelligent Automation in Banking Operations: Impact Analysis on Renewable Energy Investment Assessment. International Journal of Computer Engineering and Technology (IJCET), 16(1), 673–687. https://doi.org/10.34218/IJCET_16_01_056

12. Babar, M., & Arif, F. (2021). *Security and Privacy Challenges in Cloud-Based Banking: A Comprehensive Survey*. *Computers & Security*, 104, 102210.

13. Omolara, A. E., & Belay, E. (2023). *Behavioral Biometrics for Continuous Authentication in Mobile Banking Apps*. *Journal of Information Security and Applications*, 72, 103447.