CHAPTER 18

Building a Resilient Future for Finance: An Artificial Intelligence Driven Full-Stack Framework for Secure and Sustainable FinTech Applications

Mark Lancy Dsouza, Sita Nirmala Kumarswamy** and Sarah Leah Dsouza****

ABSTRACT

Over the last few years, financial technology (FinTech) has grown at a speed that traditional security measures have not been able to keep up with. Most banks and financial services still depend on reactive, rule-based systems that work fine for known threats but fail when something new appears. This is a concern because trust is at the heart of finance, and even a short breach or failure can have a long-lasting effect. Another issue that is often overlooked is the cost of running these systems on the cloud. The paper consists of a framework that could tackle both these issues together. Instead of adding security as a separate tool at the end, the idea was to weave it directly into every layer of a FinTech application. The framework makes use of machine learning to watch for unusual transaction behavior, natural language processing to pick up fraud-related signals in text or logs, and reinforcement learning so that the system can adjust its responses as it "learns" from past incidents. It includes a self-healing feature, so that if part of the system crashes or comes under attack, it can restart or reroute traffic without waiting for a human fix. Resource management was also built in, so servers scale up or down depending on demand, which helps cut waste. To check whether this design had value in practice, a prototype was built and was tested with synthetic transactions and failure scenarios. The results were encouraging. The AI models detected fraud more accurately than the older rule-based system, recovery times dropped from minutes to under a minute in most cases, and cloud usage went down by about 20 percent due to predictive scaling.

Keywords: Artificial Intelligence in FinTech; Full-stack security frameworks; Sustainable digital finance; Intelligent cybersecurity.

1.0 Introduction

In recent years, financial technology has advanced quickly, but this pace has also highlighted the need to rethink cybersecurity (Desai *et al.*, 2024; Capozzi *et al.*, 2025).

**Corresponding author; Research Scholar, MCA Department, D. Y. Patil Institute of Master of Computer Applications and Management, Maharashtra, India (E-mail: markdsouza93@gmail.com)*
***Research Scholar, MCA Department, D. Y. Patil Institute of Master of Computer Applications and Management, Pune, Maharashtra, India (E-mail: ksita_nirmala@rediffmail.com)*
****Assistant Professor, Department of MBA, D. Y. Patil Institute of Master of Computer Applications and Management, Pune, Maharashtra, India (E-mail: sarahdsouzadyp@gmail.com)*

DOI: 10.17492/JPI/ICISI2025/251218 *ISBN: 978-93-49790-69-8*

Artificial intelligence offers one path forward, shifting defenses from rule-based checks to more proactive methods (Desai *et al.*, 2024). Deep models such as GANs and VAEs have been applied to spot rare fraud and money-laundering cases that older systems often miss (Zheng *et al.*, 2024). Tools like *WeirdFlows* show how anomaly detection can still work without labeled data by generating interpretable patterns (Capozzi *et al.*, 2025). NLP has also become important, since it can pick up fraud signals hidden in text sources. Studies report higher detection accuracy with less feature engineering, while still preserving privacy (Maschke *et al.*, 2024). Building on these advances, this paper proposes an AI-driven full-stack framework that combines anomaly detection, generative modeling, and NLP to support a shift-left approach embedding intelligence earlier in the development lifecycle.

2.0 Objectives

- To develop an AI-driven full-stack framework for FinTech security.
- To use ML and NLP for detecting fraud and anomalies in financial data.
- To embed proactive "shift-left" security across the development lifecycle.
- To test the framework with synthetic/real datasets for accuracy and robustness.
- To compare the framework's performance with existing security systems.

3.0 Literature Review

Evolution of Financial Crime Systems: Financial crime was once checked mainly through audits and a few simple rules. Those worked for basic risks but quickly showed their limits. Studies like Khan, Qadeer & Rahman, Nadia (2025) and Miao, Zeyi. (2024) note they often raised too many false alarms and still missed fast-changing fraud.

Role of AI in Fraud and Risk Detection: Machine learning and natural language processing are now central to how financial data is checked. Unlike rule-based systems, they can catch patterns that older methods miss. A key benefit is fewer false alarms, which banks have struggled with for years. Research by Boulieris *et al.* (2023) and Mohammed *et al.* (2017) also shows better accuracy in spotting suspicious activity. More recently, reinforcement learning has been added so that defenses adjust with experience, making fraud prevention less rigid (Rahman & Lee, 2024).

Limitations of Legacy Platforms: A surprising number of financial institutions continue to depend on legacy systems. They were never really built for the scale or speed of today's FinTech ecosystems, where transactions move across services in real time. Because of this static design, fraud detection can be delayed, and compliance checks sometimes fall through the cracks (Nwoke, Judith. 2024); Ravi *et al.*, 2021).

DOI: 10.17492/JPI/ICISI2025/251218 *ISBN: 978-93-49790-69-8*

Full-Stack AI Frameworks: Lately, more attention has turned to full-stack architectures as a way of strengthening FinTech platforms. The main idea is fairly straightforward: connect the front-end monitoring with the back-end analytics instead of running them in silos. Researchers such as Kumar, Gunjan. (2025) and Tripathi et.al. (2024) also point out that the benefits go beyond security. These designs tend to improve resilience and make scaling far less of a challenge as platforms expand).

Risk Intelligence and Predictive Analytics: AI-driven risk intelligence tools are increasingly being used to anticipate how customers behave, to flag possible money-laundering activities, and to give regulators insights they can act on. What makes these tools valuable is not only their ability to process large amounts of data, but also the way predictive analytics can shift institutions from reacting after the fact to managing risks ahead of time (Bose *et al.*, 2023; Adhikari et.al., 2024).

Digital Trust and Security: Trust has always been central to the adoption of financial technologies. AI-enabled monitoring adds another layer by ensuring that trust is not just established once but continuously reinforced as the system operates (Adelaja et.al, 2024; Dboush *et al.*, 2023).

Challenges in AI Adoption: Problems such as algorithmic bias, limited transparency in decision-making, and ongoing concerns about data privacy remain difficult to resolve. These issues create hesitation among institutions and regulators, and in many cases, they slow down the adoption of AI-enabled tools for preventing financial crime (Omogbeme *et al.*, 2024; Boateng *et al.*, 2025).

4.0 Research Methodology

The study adopts an experimental research approach, where a prototype of the proposed AI-driven framework was developed and tested under controlled conditions. The idea was not only to design the framework in theory, but to validate its effectiveness in handling real-world challenges such as fraud detection, system failures, and resource optimization in cloud-based FinTech environments.

4.1 Research design

The research was set up in an exploratory way, with the central question being whether it is possible to weave both security and sustainability into the architecture of a financial application. To test this idea, a prototype was deployed in a cloud environment built on microservices. Different artificial intelligence methods were incorporated at various layers of the system - including anomaly detection for transaction patterns and natural language processing for analyzing unstructured data.

DOI: 10.17492/JPI/ICISI2025/251218 *ISBN: 978-93-49790-69-8*

4.2 Data collection plan

Because access to real financial records was restricted for privacy and regulatory reasons synthetic datasets and simulated disruptions were used to carry out the evaluation. The synthetic transaction data was built to look similar to real-world activity. In addition, artificial system failures like network slowdowns, unexpected service crashes, and even streams of malicious API requests were introduced to test how well the framework could recover on its own.

4.3 During testing, three categories of data were collected:

1. Fraud detection outcomes, including the rate of true positives and false positives.
2. System recovery times, measuring how quickly the platform returned to normal after a failure.
3. Resource utilization patterns, tracking how effectively cloud resources were scaled and whether this led to measurable energy savings.

4.4 Sample

The experimental sample included:

- A synthetic dataset of approx. 10,000 transactions
- Three classes of failure scenarios: network outages, malicious traffic, and surges
- A prototype testbed built using containerized microservices in a test environment.

5.0 Proposed Model Architecture

The proposed framework is designed as a layered full-stack architecture that integrates artificial intelligence, proactive security, and sustainability into FinTech applications.

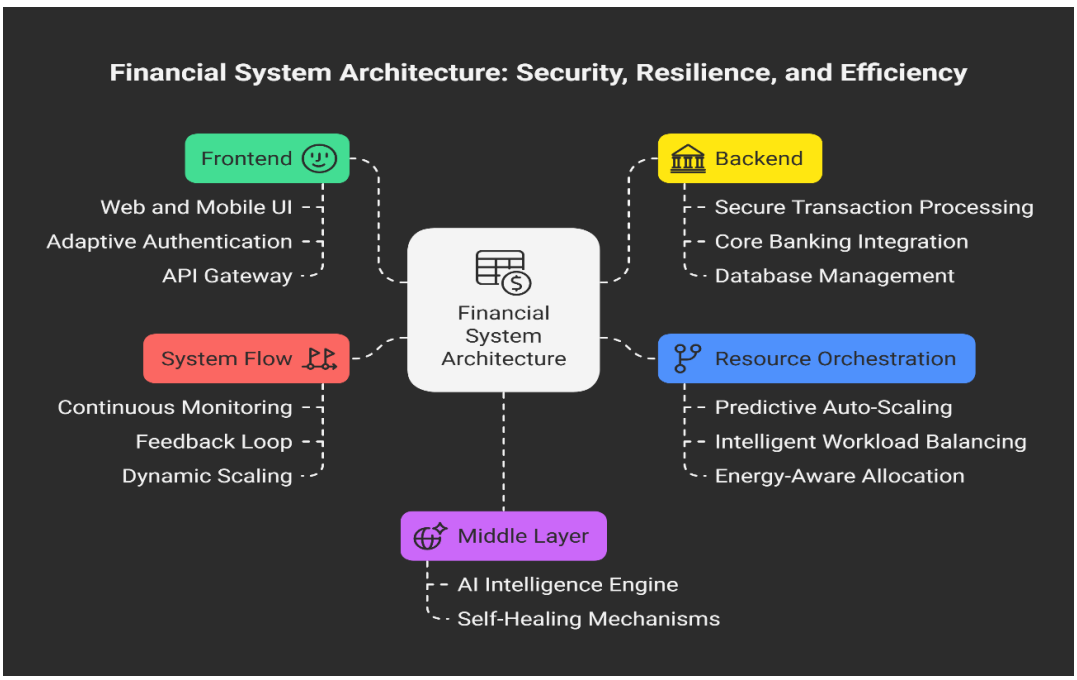
The framework is organized into four main layers, each of which plays a distinct role:

1. *Application and Interface Layer:* This layer is the one users see most the web apps, mobile apps, APIs, and customer portals.
2. *AI Intelligence Layer:* This layer holds most of the intelligence in the framework. It brings together different AI methods to check both structured transactions and unstructured data in real time, including:
    a. Machine Learning for Anomaly Detection
    b. Natural Language Processing for Fraud Signals
    c. Reinforcement Learning for Adaptive Threat Response

DOI: 10.17492/JPI/ICISI2025/251218 *ISBN: 978-93-49790-69-8*

3. *Self-Healing Layer:* Resilience here comes from self-healing. If a crash, traffic spike, or faulty microservice occurs, the system is designed to catch it and recover without human help.
4. *Resource Orchestration and Sustainability Layer:* This layer manages cloud resources to keep things efficient. Instead of fixed allocation, it uses predictive scaling adding capacity when transactions spike and cutting back when traffic slows.
5. *System Flow and Integration:* All four layers work in a loop of monitoring and feedback. Each one passes information to the next, and the results come back around so the system can adjust in real time.

Figure 1: Proposed Architecture



6.0 Key Findings

The proposed framework was evaluated through a prototype deployed in a simulated cloud environment. The objective was to determine whether embedding intelligence across the full stack could deliver measurable improvements in fraud detection, resilience, and sustainability when compared with traditional systems.

DOI: 10.17492/JPI/ICISI2025/251218 *ISBN: 978-93-49790-69-8*

- *Fraud and anomaly detection:* The AI intelligence layer was tested using a synthetic dataset of 10,000 transactions, of which 5% were injected anomalies representing fraudulent activity. Machine learning models (Random Forest and Autoencoder) achieved significantly higher detection accuracy than a rule-based baseline system.
- *System resilience and self-healing:* Resilience was measured by simulating system failures such as service crashes, injected malicious traffic, and transaction surges. The self-healing layer responded by automatically restarting failed services and rerouting traffic.
- *Resource orchestration and sustainability:* Orchestration layer evaluation: Resource usage was compared under two approaches one using static allocation and the other using predictive scaling.
- *Integrated Benefits:* What really makes the framework valuable is not one single feature, but the way the different layers work together. Better fraud detection helps reduce the chance of breaches before they spread.

7.0 Implications of the Study

FinTech is now essential, but its dependence on digital platforms leaves it open to risk. Older, reactive security models can't keep pace with fast cyber threats or the heavy load of cloud systems. The prototype showed good signs. Machine learning improved fraud detection, self-healing cut recovery times, and predictive scaling made resource use more efficient without hurting performance. Together, these results suggest financial systems don't have to trade off security against sustainability both can be built in. That said, the work had limits. It used synthetic data, was tested only on a small prototype, and left out compliance rules such as GDPR and PCI-DSS. Even so, with AI-driven methods and a shift-left mindset, FinTech systems can move toward platforms that people trust and that are prepared for future challenges.

References

1. Adelaja, Adesola & Ayodele, Oluwatoyin & Umeorah, Stanley & Amosu, Olamide. (2024). Enhancing consumer trust in financial services: the role of technological security innovations. Finance & Accounting Research Journal. 6. 1746-1759. 10.51594/farj.v6i10.1610.
2. Adhikari, Prabin & Hamal, Prashamsa & Baidoo Jnr, Francis. (2024). Artificial Intelligence in fraud detection: Revolutionizing financial security. 10.30574/ijsra.2024.13.1.1860.

DOI: 10.17492/JPI/ICISI2025/251218 *ISBN: 978-93-49790-69-8*

3. Boateng, R., Asongu, S., & Tchamyou, S. (2025). Ethical AI adoption in financial crime detection: Challenges and opportunities. AI & Society, 40(1), 55–70. https://doi.org/10.1007/s00146-024-01789-3
4. Bose, S., Das, A., & Ghosh, R. (2023). AI-enabled predictive analytics for financial risk management. International Journal of Finance and Economics, 28(4), 4523–4539. https://doi.org/10.1002/ijfe.2614.
5. Boulieris, Petros & Pavlopoulos, John & Xenos, Alexandros & Vassalos, Vasilis. (2023). Fraud detection with natural language processing. Machine Learning. 113. 1-22. 10.1007/s10994-023-06354-5.
6. Capozzi, A., Vilella, S., Moncalvo, D., Fornasiero, M., Ricci, V., Ronchiadin, S., & Ruffo, G. (2025). WeirdFlows: Anomaly detection in financial transaction flows. arXiv:2503.15896
7. Dboush, Hassan & Ferdous, Marah. (2023). Building Trust in Fintech: An Analysis of Ethical and Privacy Considerations in the Intersection of Big Data, AI, and Customer Trust. International Journal of Financial Studies. 11. 90. 10.3390/ijfs110300
8. Desai, A., Kosse, A., & Sharples, J. (2024). Finding a needle in a haystack: a machine learning framework for anomaly detection in payment systems. BIS Working Papers No. 1188.
9. Khan, Qadeer & Rahman, Nadia. (2025). AI and Ethical Considerations in Financial Fraud Detection: Balancing Innovation and Compliance. 10.13140/RG.2.2.34690.39363.
10. Kumar, Gunjan. (2025). Architecting Scalable and Resilient Fintech Platforms with AI/ML Integration. International Journal of Innovative Science and Research Technology. 3073-3084. 10.38124/ijisrt/25apr2359.
11. Maschke, J. F., (2024). FraudNLP: Fraud detection with natural language processing methods in online banking transactions. Machine Learning (2024).
12. Miao, Zeyi. (2024). Financial Fraud Detection and Prevention:. Journal of Organizational and End User Computing. 36. 1-27. 10.4018/JOEUC.354411.
13. Mohammed, Manzoor Anwar & Kothapalli, Kanaka Rakesh Varma & Mohammed, Rahimoddin & Pasam, Prasanna & Sachani, Dipakkumar Kanubhai & Richardson, Nicholas. (2017). Machine Learning-Based Real-Time Fraud Detection in Financial Transactions. Asian Accounting and Auditing Advancement. 8. 67–76.
14. Nwoke, Judith. (2024). Digital Transformation in Financial Services and FinTech: Trends, Innovations and Emerging Technologies. International Journal of Finance. 9. 1-24. 10.47941/ijf.2224.

DOI: 10.17492/JPI/ICISI2025/251218 *ISBN: 978-93-49790-69-8*

15. Omogbeme, Angela & Odewuyi, Oyindamola. (2024). Mitigating AI Bias in Financial Decision-Making: A DEI Perspective". World Journal of Advanced Research and Reviews. 24. 10.30574/wjarr.2024.24.3.3894.
16. Ravi, Neerudi & Gaddam, Naresh. (2021). Fintech Adoption in India -Issues and Challenge.
17. Tripathi, Sumit & Rosak-Szyrocka, Joanna. (2024). Impact of Artificial Intelligence on Society. 10.1201/9781032644509.
18. Zheng, Shuaiqi & Li, Maoxi & Bi, Wenyu & Zhang, Yining. (2024). Real-time Detection of Abnormal Financial Transactions Using Generative Adversarial Networks: An Enterprise Application. Journal of Industrial Engineering and Applied Science. 2. 86-96. 10.70393/6a69656173.323431.

DOI: 10.17492/JPI/ICISI2025/251218 *ISBN: 978-93-49790-69-8*