Volume 12, No.7, July 2025
*Journal of Global Research in Mathematical Archives*
ISSN 2320 – 5822
RESEARCH PAPER
Available online at http://www.jgrma.com

# A SURVEY OF MACHINE LEARNING MODELS FOR INFRASTRUCTURE RESILIENCE IN FINTECH APPLICATIONS

**Dr. Jvalantkumar Kanaiyalal Patel[1]**

[1] Assistant Professor, Shri Manilal Kadakia College of Commerce, Management, Science and Computer Studies, Ankleshwar
jvalant007@gmail.com

**Abstract:** The survey will consider how machine learning (ML) models can be used to improve infrastructure resilience in Fintech applications. With rising complexity, data volumes, and cybersecurity threats to Fintech systems, ML offers substantial basis to the maintenance of operational continuity, prevention of fraud, anomaly detection, and real-time risk management. Such abilities are essential in ensuring system consistency and flexibility in busily developing digital financial landscapes. The paper examines different types of ML models, supervised learning, unsupervised learning, reinforcement learning and their use in fraud detection, the detection of anomalies, cybersecurity and recovery of disasters. The deployment architectures like cloud-native systems and federated learning are also discussed in terms of the advantages in scale and data secrecy. Along with this, the unification of ML with innovation-based technologies, such as blockchain and generative artificial intelligence (AI), indicates the prominence of the key indicators of system integrity, digital trust, and financial inclusion. An adequate literature research signifies the availability of the research on such topics as banking efficiency, decentralized protocols and AI-driven digital transformation. The paper also provides a comparison of strengths, challenges and future potential of ML-driven solutions in Fintech infrastructure. The survey sums up, stating that explainable AI, adaptive learning frameworks, and cross-border compliance mechanisms are needed to strengthen intelligent, resilient, and inclusive financial systems.

**Keywords:** Fintech, Infrastructure Resilience, Fraud Detection, Anomaly Detection, Cybersecurity, Real-Time Analytics, Blockchain Integration, Federated Learning, Predictive Modeling.

## 1 INTRODUCTION

Financial technology, or fintech, is revolutionizing how institutions, corporations and individuals interact with financial services [1][2]. Fintech transformations, such as tokens, artificial intelligence-powered risk estimates, blockchain, and digital payments are shaking up the traditional paradigm of the financial sphere [3]. The heightening degree of complexity and interdependence of financial markets has made infrastructure and financial resilience in the face of economic shocks even more crucial. Financial resilience is the capacity of people, institutions and economies to endure and recover from financial crises, market volatility and external shocks [4]. The global financial crisis of 2008 and the COVID-19 pandemic of 2020 have shown that conventional financial systems possess many weaknesses and crucial flaws. This explains the necessity of adaptive measures which are aimed at reducing risks, guaranteeing financial stability, and providing fast economic recovery.

Fintech is a critical tool in enhancing financial resilience with its new functions to manage risks, analyze in real-time, and access liquidity. The digital lending networks, decentralized financial systems (DeFi), and predictive analytics help individuals and businesses manage the factors of economic uncertainty more effectively. Moreover, fintech-powered solutions promote financial inclusion, as it guarantees that underserved and marginalized groups can access basic financial services, especially in crisis situations. In the fast-growing field of financial technology (FinTech), efficiency of operations has emerged as one of the most important attributes of the companies that want to preserve a competitive advantage. The complexity and the volume of transactions have soared as the industry keeps expanding, propelled by the rising digitization of the financial services [5]. Although this growth is positive, there has been an increase in the fraud occurrence on fintech companies that are quite challenging.

In order to address this, a lot of companies now resort to use of sophisticated technologies like artificial intelligence (AI) and data-informed insight that provide them with effective tools to detect fraud and also increase the efficiency of their operations. Rule-based systems have been used traditionally to detect fraud whereby suspicious events are reported on basis of programmed rules [6]. Even though these systems have proved to be effective to some degree, they tend to be very rigid, and fail to swiftly adapt to any emerging fraud strategies and also may end up producing a high frequency of false positives. Using machine learning (ML) algorithms, ML can be important in maintaining business continuity, avoiding fraud, and handling risk [7]. Conventional rule based fraud detection systems are losing effectiveness in countering the advanced threats, and in most instances they produce high false positives [8]. On the contrary, the ML algorithms review large amounts of transactional data, identify real-time anomalies, and adapt to emerging fraud patterns, improving detecting accuracy [9]. Predictive risk analysis is also supported by data-led information in customer behavior and market trends.

This integration reduces manual work, false alerts, and processes, allowing FinTech companies to scale efficiently without compromising their security. Fraud prevention is one area where ML enhances capabilities, but it also promotes resilience and better decision-making in general. These technologies continue to shape more innovation, cost and service quality, and thus they be an important source in dealing with risk and remaining competitive in the FinTech industry, which is quite dynamic [10]. Since the utilization of digital infrastructures, as well as the sophistication of financial ecosystems, grows [11], ML models become the most significant aspect of enhancing fintech systems' resilience [12][13]. The ML-driven approaches based on a data-centric approach provide management of vulnerabilities on a dynamic basis, disruption response, and adjustment to the evolving risks in real time.

ML models do not only assist in keeping the processes running without any interruptions, identifying the person that defrauds another, but also provide conditions when governments can mitigate the risks due to the ability to make informed decisions. By cataloguing and discussing various ML practices in the area of infrastructure resilience for fintech systems, this survey aims to analyze and identify the potential and applications of ML in the field of finance, introducing such systems as secure, resilient, and high-efficiency-based frameworks.

### 1.1 Structure of the Paper

The structure of this paper is as follows: Section 2 discusses the fundamentals of infrastructure resilience in Fintech. Section 3 explores the role of ML in Fintech. Section 4 focuses on ML models applied to resilience-oriented applications. Section 5 provides a review of existing literature. Finally, Section 6 concludes the paper and outlines potential directions for future research.

## 2 FUNDAMENTALS OF INFRASTRUCTURE RESILIENCE IN FINTECH

Financial resilience is the capacity of people, organizations, and economies to endure financial shocks and bounce back from emergencies [14]. Traditional financial systems often struggle to maintain stability during economic downturns, as seen in past global financial crises and disruptions caused by events such as the COVID-19 pandemic. Fintech solutions have emerged as vital mechanisms that improve financial resilience through enhanced risk management, improved access to financial services, and increased transparency in financial transactions. Key fintech innovations such as real-time digital payments, decentralized finance (DeFi), automated credit scoring, and predictive analytics have enabled financial institutions and consumers to make more informed financial decisions. These technologies contribute to resilience by ensuring continuous financial transactions, reducing dependency on physical banking infrastructure, and offering alternative credit sources for individuals and businesses during periods of economic distress, as shown in Figure 1.

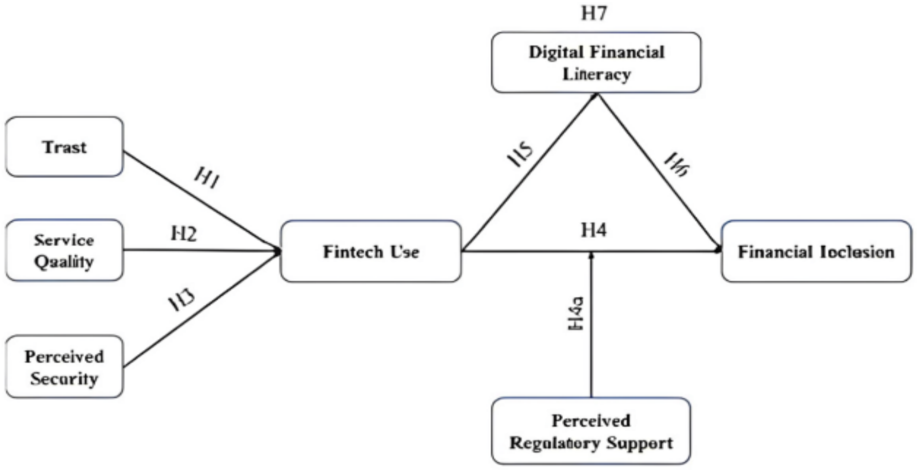


Figure 1: The Role of Fintech in Financial Resilience

### 2.1 Challenges in Fintech Infrastructure

Fintech infrastructure is facing growing challenges, including cyber threats, system failures, and increasing transaction volumes. Addressing these risks requires resilient frameworks, advanced technologies, and scalable solutions to ensure operational reliability and compliance with regulations.

#### 2.1.1 Cyber Threats:

The increasing severity of cyber-attacks is demonstrated by a PwC survey that indicated 67% of businesses had at least one cyberattack in the previous year [15]. Companies are employing frameworks that address risks through anticipation, defense, recovery, and adaptation, in order to develop resiliency. Key strategies include investing in cybersecurity technologies, educating employees, preparing contingency plans, and conducting regular monitoring. Strategic and tactical resilience models are necessary to fully address system vulnerabilities.

#### 2.1.2 System Failure

System failures in fintech describe any unforeseen breakdowns /disruptions malfunctions within the technological infrastructure upon which the financial technology services are operating. Such failures may be due to computer glitches, hardware faults, communication interruptions, database problems, disruptions from external service providers, security breaches, or human errors, and could result in an inability to access financial transactions or services, delays, or the incorrect delivery of transactions or services [16] These outages are dangerous to the operationality, credibility, financial stability, and regulatory compliance. It requires robust resilience systems, including redundancy, real-time capabilities, fault tolerance, and disaster recovery plans.

### 2.1.3 Transaction Load

In the FinTech sector, optimizing systems integration is essential for managing and enhancing transaction volumes. Effective integration strategies contribute to scalability, efficiency, and security, key aspects for handling high transaction loads and ensuring seamless operation [17]. By addressing these areas, financial technology companies can better cope with growing demands and maintain high standards of service. Scalability is a fundamental consideration in managing increasing transaction volumes. To scale systems effectively, FinTech organizations need to adopt strategies that ensure their infrastructure can handle both current and future demands.

### 2.1.4 Compliance and Regulatory Constraints

Compliance and regulatory limitations in fintech can be described as a complex set of legal, institutional, and policy implications that fintech businesses must follow to operate within the financial system in a legal and ethical manner [18]. Such restrictions are issued by government bodies, central banks, financial oversight authorities and global standards organizations and are meant to facilitate consumer protection, information confidentiality, asset stability, anti-cash laundering (AML), terrorism financing (CTF), cybersecurity and responsible innovation.

## 3 MACHINE LEARNING IN FINTECH

Fintech's use of ML facilitates real-time decision-making, predictive analytics, and intelligent automation. It transforms financial services by enhancing risk assessment, fraud detection, and customer personalization. Through supervised, unsupervised, and reinforcement learning models, ML drives efficiency, scalability, and resilience, making it a core component of modern Fintech infrastructure and operations.

### 3.1 Role of ML in Fintech

The FinTech sector had a significant uptake of ML methods between 2016 and 2020. The increased popularity of predictive analytics, one of the key elements of ML, contributed to data-driven decision-making in the financial processes [19]. The popularizing of supervised and unsupervised learning algorithms impacted the examination of consumer behavior and risk evaluation.

### 3.1.1 Real-Time Analytics

Fintech businesses and other organizations now tackle cybersecurity in a whole different way thanks to advanced analytics and ML [20] The ability to anticipate, identify, and respond to cyberattacks in a timely manner is necessary, to safeguard sensitive financial data, ensure regulatory compliance, and support consumer faith, given the Trojan Horse of cyberattacks. The fintech industry faces a more complex and varied cyber environment as it expands. Advanced analytics and ML are being used by fintech companies to improve their threat detection and risk management skills as well as fortify their cybersecurity frameworks in response to these changing dangers shown in Figure 2. That illustrates the use of data analytics to fight cybercrime.


Figure 2: Data Analytics in Combating Cybercrime

In cybersecurity, predictive modelling is one of the most important uses of ML and advanced analytics. Predictive models are able to predict potential cyber threats and avoid their occurrence by employing the history and statistical metrics to inform organizations well in advance, thus creating a possibility to act preventively and minimize the risks. Predictive modelling is used in the fintech industry to identify potential weaknesses and emerging threats by analyzing vast volumes of transaction data, user behavior patterns, and network traffic.

 

### 3.1.2 Fraud Detection and Anomaly Detection

The definition of a fraud is "an intentionally deceptive action designed to deny a victim a right or to provide the Perpetrator with an unlawful gain." Since fraud is an adaptive crime, it is difficult to detect, which is why extensive financial records are necessary. An accumulation of transactions from the financial network traffic over a given time period is represented by a dataset. A fraud appears in these databases as an anomaly that is different from the typical records. Techniques were applied to anomaly detection in the field of ML to find such patterns. Generally speaking, anomaly detection methods make it possible to find frauds in big databases. It has been demonstrated that they are effective in classifying anomalous data in these kinds of aggregations. They are indeed a logical alternative to handle fraud detection issues because of these benefits.

## 3.2 Categories of Machine Learning (ML) Models Used

Fintech infrastructure's resilience is greatly increased by ML models, which provide intelligent, data-driven decision-making [21]. These models are typically categorized into supervised, unsupervised, and reinforcement learning, each serving unique functions within complex financial systems.

### 3.2.1 Supervised Learning:

Supervised learning models play a vital role when it comes to predictive maintenance, anomaly detection, and fraud prevention, and these techniques are based on historical, labeled data to predict the failure or risk. Such methods include DT, SVM, RF, and neural networks, which are commonly used to classify events and predict system behavior under various operating conditions.

### 3.2.2 Unsupervised Learning:

These models can be used to analyze unlabeled data to find hidden patterns in the data so that a fintech system can determine new threats or abnormal transactions even when classified beforehand. The most popular algorithms for identifying anomalies and critical data points are K-means clustering, DBSCAN, and principal component analysis (PCA).

### 3.2.3 Reinforcement Learning:

Adaptive System management uses reinforcement learning and agents engage in a continuous interaction with dynamic environments until they learn their best policies. It facilitates resource placement, real-time planning and optimization of fault-tolerant systems such as Q-learning and Deep Q-Networks (DQN).

### 3.2.4 Combined Approach:

These categories of ML, when combined, create a strong background towards the reinforcement of resiliency of both human and technical infrastructures in fintech, making the systems more flexible, productive, and responsive in underdeveloped financial systems.

## 3.3 Machine learning (ML) Deployment Architectures in Fintech Systems

The scalable, secure, and efficient ML deployment architecture provides modern fintech systems the ability to ensure resilience and performance in their operations. Such strategies as cloud-native applications and federated learning have flexibility, cost-efficiency, and data privacy, which makes them suitable for the dynamic financial landscape.

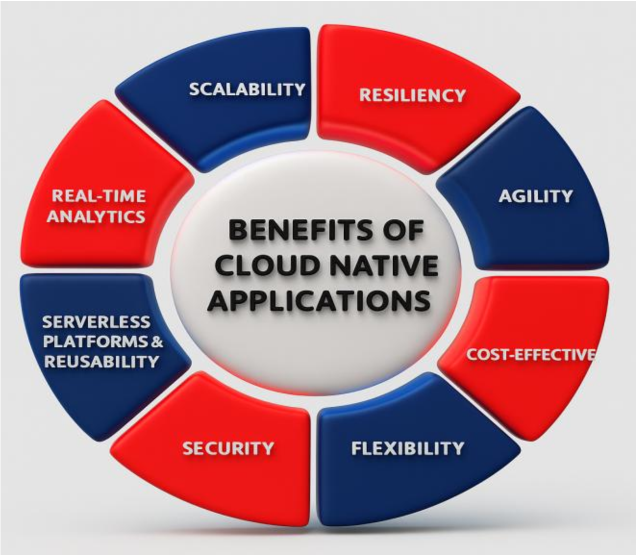


Figure 3: Benefits of Cloud Native Application

 

#### 3.3.1 Cloud-Native

The cloud-native applications are software programs created on the basis of taking full advantage of the benefits of the environment of cloud computing. These apps are built on significant patterns, such as containerization, microservices, and DevOps practices, among others [22]. Applications that run in the cloud have certain characteristics that help them: dynamic scaling, fault tolerance, and optimal use of cloud resources. Figure 3 illustrates Cloud Native Applications' advantages. Advantages of Cloud-Native Applications for FinTech are as follows:

#### 3.3.2 Scalability and Flexibility:

Cloud-based applications are capable of scaling up or down very quickly, which helps to increase efficient resource utilization and reduce total cost of ownership by only using the resources they need at any particular time. This flexibility is a useful quality of fintech companies that experience irregular workloads or surges of using their services during the season.

#### 3.3.3 Cost-Efficiency:

Fintech companies may save on operational costs using the pay-per-use cloud computing paradigm as they can avoid the over-provisioning of resources by avoiding the costly capital investments, with cloud-native applications being self-scalable to the point of provisioning resources, exemplifying the case of less waste and more efficiency.

#### 3.3.4 Federated Learning

Federated Learning is an ML technique that uses a scalable framework spanning several devices and domains to train models on decentralized data. Its main objective is to protect privacy and advance the efficiency of FinTech applications [23]. It's seen as a realistic strategy for growing AI and ML applications without sacrificing security. According to financial experts, federated learning has great promise for boosting the expansion and efficiency of financial technology.

## 4 ML MODELS FOR RESILIENCE-ORIENTED APPLICATIONS

The ML models play an important role in making Fintech infrastructures more resilient because the systems are learning to recognize conditions, cope with and respond to disturbance. The models are useful in detecting anomalies, cybersecurity, preventing fraud, and recovery of disasters by analyzing the data and providing predictions in real-time. This knowledge area looks into some of the critical ML-powered applications that support stability and continuity of the Fintech system.

### 4.1 Anomaly Detection Models

The detection of anomalies is one of the most essential components of the identification of possible threats and fraudulent practices in FinTech systems. The different methods that are used are the statistical, ML, and DL methods, which may have different benefits in the detection of anomalies. Detection of such deviations in terms of expected financial behaviors is performed with the help of statistical approaches, which include z-score analysis and hypothesis testing [24]. These approaches include the establishment of tolerance levels to differences in transaction value changes, user patterns or system parameters. Although the methods are useful when the task is to detect simple anomalies, they are usually not flexible to change accordingly to complex and changing threats. To overcome these shortcomings, many ML algorithms, e.g., Isolation Forests, One-Class SVM, and Local Outlier Factor, can be employed to learn normal behavior and raise alerts in deviations. The algorithms can work with high-dimensional data and detect minute anomalies which may not be detected by standard statistical means.

#### 4.1.1 Autoencoders, Isolation Forest, One-Class SVM

Isolation Forest and One-Class SVM models found anomalous patterns in transaction data, e.g. incorrect amount of products or delivery time, that may be related to fraud or logistics of the supply chain [25]. Every transaction was captured in blockchain platform and this can be used to train ML models that can be used to detect any abnormal activity in real time.

#### 4.1.2 Cybersecurity and Intrusion Detection

The fast implementation of online banking systems has exposed people to different online frauds. These are threats that exploit the vulnerabilities on systems and they tend to cause huge financial and reputation losses. Phishing, ransomware, data breaches, and account takeovers are among the most eminent threats as demonstrated in Figure 4 below.

 


Figure 4: Cybersecurity risks and fraud

The importance of ML in risk analysis has become crucial to financial institutions, as it offers them the means to identify and prevent possible threats to business successfully. The main ideas of the ML utility in this field include the notions of supervised learning, unsupervised learning, and reinforcement learning, as well as niche algorithms, including anomaly detection, clustering, and DL. Cybersecurity risk analysis using ML has changed the way financial institutions respond and detect threats. Intrusion detection systems (IDS) and behavioral analysis systems are important ML-based tools that promptly detect unusual activities and eliminate real-time risks [26]. One of the most evident ML uses in cybersecurity is the IDS. Such systems keep track of the activities in the network and detect malicious actions which can affect the integrity of the system. Typical IDS can only identify threats defined by a set of predefined signatures and thus tend not to detect new attacks. ML has been used to improve IDS systems and allow them to classify unknown threats based on patterns.

#### 4.1.3 Fraud Detection and Transaction Monitoring

ML use in the fintech sector has revolutionized fraud detection and allowed financial institutions to address the varied and increasingly complicated challenges of fraud. To identify fraud, a variety of ML models were chosen [5]. Numerous supervised and unsupervised learning methods were taken into consideration, including clustering algorithms (e.g., K-means, DBSCAN), LR, DT, RF, SVM, neural networks, and others. These algorithms create models that can differentiate between authentic and fraudulent transactions by using past transactional data and other pertinent characteristics. explains that the capacity of ML to adjust to changing fraud tendencies is one of its main benefits. To keep ahead of new risks, ML models may be updated and trained on fresh data as fraudsters constantly come up with new strategies. ML is used in a variety of finance fields for fraud detection in the real world.

#### 4.1.4 Disaster Recovery and Infrastructure Continuity

Disaster recovery and infrastructure continuity are vital for sustaining uninterrupted fintech operations during disruptions like cyberattacks, hardware failures, or natural disasters. Manual recovery processes are time-consuming and subjective, and they usually cause data loss and prolonged downtime [27]. Automated disaster recovery plans are more efficient and reliable since they involve reduced downtimes and continuity of system functions.

There is also the issue of load forecasting which provides a better continuity by predicting the various computational and transactional requirements. With SVM, neural networks, and gradient boosting, which are all models of ML, fintech platforms can dynamically scale resources to avoid system overloads [28]. Reinforcement learning also allows making changes in real-time leading to increased flexibility and resiliency. These methods in combination reinforce the fintech infrastructure against shocks.

## 5 LITERATURE OF REVIEW

In this section, a literature review of ML models of infrastructure resilience in Fintech applications be provided with a focus on integration of AI and blockchain, as well as advanced analytics. The analyzed articles dwell upon the topic of efficiency analysis, security, decentralization, digital transformation in the banking system.

Zeng (2025) a better solution towards the analysis of the effectiveness of Chinese commercial banks using computer technology and fintech. To begin with, preprocessing is undertaken in order to examine the effectiveness of Chinese commercial banks, deriving important characteristic parameters out of the information. Subsequently, a multi-chimera identification network tailored for Chinese commercial banks is introduced. This network is first pre-trained, and then it is adjusted to fit the particular purpose of locating Chinese commercial banks, thereby facilitating the research on the efficiency analysis strategy. The efficiency of the suggested approach is verified through the use of simulation technologies [29].

 

Devi, Chauhan and Jain (2025) explores the revolutionary impact of these financial technologies on the banking sector of India, concentrating in particular on Housing Development Finance Corporation (HDFC), India's top private bank. This paper starts with the introduction of Fintech in the banking sector how these advanced technologies, Digital payment technologies, mobile banking, and big data analytics have replaced India's old banking system. This study also examines the emergence of fintech in the banking industry, including blockchain integration, quicker payments, and financial inclusion [30].

Li et al. (2025) examines the impact of integrating blockchain technology on incentive structures (e.g., data sharing, compliance with standards, and collaborative efforts), as well as the resulting implications for supply chain resilience. Recognizing the rising interest in blockchain applications, identify a critical gap in understanding how firms' cooperative and competitive dynamics serve as boundary conditions in this area. Grounded in Transaction Cost Economics and Goal Interdependence Theory, empirically tested hypotheses using structural equation modelling with data from 285 Chinese firms [31].

Chatterjee, Das and Rawat (2024) an approach to address these challenges using Generative AI and blockchain integration to make Fintech systems more resilient. Sophisticated ML algorithms identify and stop data manipulation in the suggested systems. Real-time system security monitoring, anomaly identification, and threat detection are all accomplished with generative AI. Then, in order to improve the overall robustness of systems, use blockchain technology. Through block validation, control distribution across decentralized networks, and secure transaction reliability, blockchain technology improves financial services' dependability [32].

Vishwakarma et al. (2024) the current FinTech system, user financial information is stored centrally. In the centralized system, the information security risks are high. Thus, a decentralized system is required for better security, trust and safety management in the FinTech information system. Blockchain is a decentralized technology that can solve the issues of traditional FinTech applications like banking. In the blockchain, consensus protocols are responsible for maintaining a consistent copy of the blockchain at each node of the blockchain network. However, these protocols are not suitable for regular currency transactions due to high latency and low throughput. Therefore, to achieve reliability, low latency, and high throughput, have introduced a new protocol called FinBlock. In FinBlock, the pipeline concept is introduced in blockchain to increase the transaction throughput [33].

Pillai et al. (2023) financial literacy gap requires lifetime learning to begin at a young age. Through the elimination of middlemen, fintech enhances access to financial services. Notwithstanding present efforts, there remains a gap that Fintech tools can help close. The solutions include chatbots, robo-advisory services, gamification software, and mobile banking devices. When combined with an increase in smartphone ownership, fintech's growing use in developing countries has the potential to completely transform financial inclusion and digital literacy. Research on teaching materials for digital financial literacy, how digitalization affects financial decision-making, and how financial institutions support the development of digital financial literacy is crucial [34].

Singh et al. (2022) shown that people's perceptions of online networks had changed considerably from those of conventional cable networks. This change has gradually impacted the acceptance of new technologies throughout the world, especially AI, which is now revolutionizing a number of industries. Financial companies be able to introduce innovative products and services, completely rethink their business models, and above all have an impact on customer experience initiatives thanks to AI. Agile fintech companies that utilize cutting-edge technology to augment or even replace human labor with sophisticated algorithms compete with banks in this second machine age. To maintain a significant competitive edge, banking companies must embrace AI and incorporate it into their business strategy [35].

Table 1 presents a summary of the literature review, highlighting each study’s focus, approach, key findings, challenges, and proposed future directions.

Table 1: Comparative Analysis of Literature Review on ML Models for Infrastructure Resilience in Fintech Applications

| Reference | Study On | Approach | Key Findings | Challenges | Future Direction |
|---|---|---|---|---|---|
| Zeng (2025) | Efficiency analysis of Chinese commercial banks | Multi-chimera identification network with ML pretraining & fine-tuning | Enhanced bank efficiency analysis using ML; validated via simulations | Model complexity and domain adaptation | Expand multi-chimera models for real-time fintech monitoring |
| Devi, Chauhan and Jain (2025) | Fintech’s impact on Indian banking (HDFC) | Descriptive analysis of Fintech tools like ML, big data | Improved banking performance, financial inclusion, and customer experience | Resistance to digital adoption, legacy systems | ML-based personalization, predictive banking analytics |
| Li et al. (2025) | Blockchain and incentive structure in supply chains | Structural Equation Modeling with 285 Chinese firms | Blockchain improves resilience via security, cost-efficiency | Limited understanding of firm dynamics with blockchain | Integrate ML for predictive resilience and adaptive incentives |
| Chatterjee, Das and Rawat (2024) | AI & Blockchain integration in Fintech resilience | Generative AI + blockchain for threat/anomaly detection | ML improves system monitoring, security, data integrity | Scalability of AI models, latency in blockchain validation | Real-time ML deployment with scalable blockchain architecture |

 

| | | | | | |
|---|---|---|---|---|---|
| Vishwakarma et al. (2024) | Decentralization in Fintech systems | Novel FinBlock protocol with pipelining in blockchain | Increased throughput & reliability in Fintech transactions | Latency & consensus protocol inefficiencies | ML-integrated consensus mechanisms for adaptive performance |
| Pillai et al. (2023) | Financial literacy and Fintech tools | ML-powered gamification, robo-advisors, chatbots | ML promotes digital financial inclusion and literacy | Access to digital resources in emerging regions | AI-driven educational platforms and adaptive learning tools |
| Singh et al. (2022) | AI transformation in banking | ML & AI-driven automation, smart analytics | Improved customer service, data analysis, and cost-efficiency | AI adoption barriers, regulatory risks | Human-AI collaboration models, explainable AI in finance |

## 6 CONCLUSION AND FUTURE WORK

This survey examined ML models as pivotal enablers of infrastructure resilience in Fintech applications. By analyzing their role in fraud detection, anomaly recognition, cybersecurity, and disaster recovery, highlighted how ML-driven systems enhance operational continuity, threat mitigation, and decision-making in dynamic financial environments. The reviewed literature shows how ML integrates with blockchain, cloud-native frameworks, and analytics to create secure, adaptive, and intelligent Fintech infrastructures. Real-time analytics, predictive modeling, and decentralized architectures have emerged as critical components for tackling systemic challenges such as cyber threats, transaction overload, and regulatory compliance. From enhancing efficiency in banking systems to reinforcing supply chain security and promoting financial literacy, the convergence of ML and emerging technologies fosters greater inclusivity, transparency, and resilience in digital finance. Comparative studies further demonstrate that ML not only automates risk management but also drives innovation and competitive differentiation in the Fintech sector.

Future research should explore hybrid ML models that combine explainable AI with real-time decision systems, especially under high-frequency transactional stress. Additionally, integrating ML with federated learning and edge computing could further address data privacy and latency issues. Investigating cross-border compliance automation using AI-driven rule engines will also be crucial for global Fintech resilience.

## REFERENCES


[1] N. Malali, “AI Ethics in Financial Services: A Global Perspective,” *Int. J. Innov. Sci. Res. Technol.*, vol. 10, no. 2, 2025, doi: 10.5281/zenodo.14881349.

[2] A. Adwani, “Fintech Innovations and Financial Resilience: A Framework for Crisis Management,” *Multidiscip. Res. Nexus Ideas Mod. World*, no. February, 2025, doi: 10.59646/mrnc5/321.

[3] S. Garg, “AI, Blockchain and Financial Services: Unlocking New Possibilities,” *Int. J. Innov. Res. Creat. Technol.*, vol. 8, no. 1, p. 1, 2022, doi: 10.5281/zenodo.15537568.

[4] S. Robbins, “Operational Efficiency in FinTech : Leveraging AI and Data-Driven Insights for Operational Efficiency in FinTech : Leveraging AI and Data-Driven Insights for Fraud Detection,” no. August, 2024, doi: 10.13140/RG.2.2.12384.08965.

[5] H. P. Josyula, “Fraud Detection in Fintech Leveraging Machine Learning and Behavioral Analytics,” *Research Square*. pp. 1–23, Nov. 2023. doi: 10.21203/rs.3.rs-3548343/v1.

[6] B. Stojanović *et al.*, “Follow the Trail: Machine Learning for Fraud Detection in Fintech Applications,” *Sensors*, vol. 21, no. 5, p. 1594, Feb. 2021, doi: 10.3390/s21051594.

[7] N. Malali, “Exploring Artificial Intelligence Models for Early Warning Systems with Systemic Risk Analysis in Finance,” in *2025 International Conference on Advanced Computing Technologies (ICoACT)*, IEEE, Mar. 2025, pp. 1–6. doi: 10.1109/ICoACT63339.2025.11005357.

[8] M. Ononiwu, T. Azonuche, F. Onum, and O. Enyejo, “Machine Learning Approaches for Fraud Detection and Risk Assessment in Mobile Banking Applications and Fintech Solutions,” *Int. J. Sci. Res. Scince, Eng. Technol.*, vol. 10, no. 4, pp. 371–390, 2023, doi: https://doi.org/10.32628/IJSRSET.

[9] R. Q. Majumder, “A Review of Anomaly Identification in Finance Frauds Using Machine Learning Systems,” *Int. J. Adv. Res. Sci. Commun. Technol.*, pp. 101–110, Apr. 2025, doi: 10.48175/IJARSCT-25619.

[10] A. Desai, A. Kosse, and J. Sharples, “Finding a Needle in a Haystack: A Machine Learning Framework for Anomaly Detection in Payment Systems,” *Bank Canada Staff Work. Pap.*, vol. 24, no. 15, 2024.

[11] B. Chaudhari and S. C. G. Verma, “Synergizing Generative AI and Machine Learning for Financial Credit Risk Forecasting and Code Auditing,” *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, vol. 11, no. 2, 2025.

[12] A. Oluokun, A. Ige, and M. Ameyaw, “Building cyber resilience in fintech through AI and GRC integration: An exploratory Study,” *GSC Adv. Res. Rev.*, vol. 20, pp. 228–237, 2024, doi: 10.30574/gscarr.2024.20.1.0245.

[13] H. Xu, K. Niu, T. Lu, and Siyang Li, “Leveraging artificial intelligence for enhanced risk management in financial services: Current applications and future prospects,” *Eng. Sci. Technol. J.*, vol. 5, no. 8, pp. 2402–2426, Aug. 2024, doi: 10.51594/estj.v5i8.1363.


 

[14] G. Kumar, "Architecting Scalable and Resilient Fintech Platforms with AI/ML Integration," *Int. J. Innov. Sci. Res. Technol.*, pp. 3073–3084, 2025, doi: 10.38124/ijisrt/25apr2359.

[15] M. F. Safitra, M. Lubis, and H. Fakhrurroja, "Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity," *Sustainability*, vol. 15, no. 18, 2023, doi: 10.3390/su151813369.

[16] M. Campbell-Verduyn and M. Lenglet, "Imaginary failure: RegTech in finance," *New Polit. Econ.*, vol. 28, no. 3, pp. 468–482, 2023, doi: 10.1080/13563467.2022.2140795.

[17] A. G. Adeleke, T. O. Sanyaolu, C. P. Efunniyi, L. A. Akwawa, and C. F. Azubuko, "Optimizing systems integration for enhanced transaction volumes in Fintech," *Financ. Account. Res. J.*, vol. 4, no. 5, pp. 345–363, Dec. 2022, doi: 10.51594/farj.v4i5.1511.

[18] S. Obeng, T. V. Iyelolu, A. A. Akinsulire, and C. Idemudia, "The Transformative Impact of Financial Technology (FinTech) on Regulatory Compliance in the Banking Sector," *World J. Adv. Res. Rev.*, vol. 23, no. 1, pp. 2008–2018, Jul. 2024, doi: 10.30574/wjarr.2024.23.1.2184.

[19] P. Kamuangu, "Advancements of AI and Machine Learning in FinTech Industry (2016-2020)," *J. Econ. Financ. Account. Stud.*, vol. 6, no. 1, pp. 23–31, 2024, doi: 10.32996/jefas.2024.6.1.3.

[20] E. Kokogho, R. Okon, B. M. Omowole, C. P.-M. Ewim, and O. C. Onwuzulike, "Enhancing cybersecurity risk management in fintech through advanced analytics and machine learning," *Int. J. Front. Sci. Technol. Res.*, vol. 8, no. 1, pp. 001–023, Jan. 2025, doi: 10.53294/ijfstr.2025.8.1.0023.

[21] H. Wang, X. Chen, J. Du, and K. K. Lai, "Classification of FinTech Patents by Machine Learning and Deep Learning Reveals Trends of FinTech Development in China," *Math. Probl. Eng.*, vol. 2022, 2022, doi: 10.1155/2022/1852447.

[22] P. Chintale, L. Korada, A. Mahida, P. Ranjan, and G. Desaboyina, "Risk Management Strategies for Cloud-Native Fintech Applications," *Adv. Eng. Sci.*, vol. 52, no. 05, 2020.

[23] B. Dash, P. Sharma, and A. Ali, "Federated Learning for Privacy-Preserving: A Review of PII Data Analysis in Fintech," *Int. J. Softw. Eng. Appl.*, vol. 13, no. 4, pp. 1–13, 2022, doi: 10.5121/ijsea.2022.13401.

[24] D. Kumar, "Innovative FinTech Security : Federated Learning and Anomaly Detection Innovative FinTech Security : Federated Learning and Anomaly Detection Techniques," no. September, 2024, doi: 10.13140/RG.2.2.29129.35681.

[25] T. Rahman *et al.*, "Blockchain Applications in Business Operations and Supply Chain Management by Machine Learning," *Int. J. Comput. Sci. Inf. Syst.*, vol. 09, no. 11, pp. 17–30, Nov. 2024, doi: 10.55640/ijcsis/Volume09Issue11-03.

[26] M. Williams, M. F. Yussuf, and A. O. Olukoya, "Machine Learning for Proactive Cybersecurity Risk Analysis and Fraud Prevention in Digital Finance Ecosystems," *Int. J. Eng. Technol. Res. Manag.*, vol. 5, no. 12, pp. 160–177, 2021.

[27] A. Mahida, "An Automated Disaster Recovery Strategies for Fintech Infrastructure," *J. Eng. Appl. Sci. Technol.*, vol. 5, no. 3, pp. 1–4, Jun. 2023, doi: 10.47363/JEAST/2023(5)236.

[28] A. A. Abayomi, A. C. Uzoka, O. T. Odofin, O. S. Adanigbo, and J. C. Ogeawuchi, "Predictive Infrastructure Scaling in Fintech Systems Using AI-Driven Load Balancing Models," vol. 4, no. 6, pp. 2393–2401, 2024.

[29] Y. Zeng, "Research on Application and Optimization of Fintech and Computer Technology in Chinese Commerial Bank Efficiency Analysis," in *2025 7th International Congress on Human-Computer Interaction, Optimization and Robotic Applications (ICHORA)*, IEEE, May 2025, pp. 1–5. doi: 10.1109/ICHORA65333.2025.11017257.

[30] P. Devi, R. Chauhan, and R. Jain, "An Application of Fintech is Revolutionary in Indian Banking Sector: W.R.T. to HDFC Bank," in *2025 International Conference on Intelligent Control, Computing and Communications (IC3)*, IEEE, Feb. 2025, pp. 59–62. doi: 10.1109/IC363308.2025.10957709.

[31] X. Li, H. Zhao, A. Mehrotra, R. Gugnani, and V. Agarwal, "Harmonizing Fintech and Supply Chain Resilience: Unveiling the Role of Blockchain Integration, Incentives, and Resilience," *IEEE Trans. Eng. Manag.*, pp. 1–38, 2025, doi: 10.1109/TEM.2025.3578098.

[32] P. Chatterjee, D. Das, and D. B. Rawat, "A Generative AI Approach for Ensuring Data Integrity Security Resilience in Fintech Systems," in *2024 IEEE 24th International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW)*, 2024, pp. 168–173. doi: 10.1109/CCGridW63211.2024.00027.

[33] L. Vishwakarma, A. Kumar, J. Madugunda, and D. Das, "FinBlock: Secure and Fast Transaction Confirmation with High Throughput for FinTech Application," in *2024 IEEE Wireless Communications and Networking Conference (WCNC)*, 2024, pp. 1–6. doi: 10.1109/WCNC57260.2024.10571189.

[34] D. Pillai, A. S. Singh, T. Bhosale, and A. Doifode, "A Perspective on the Application of Fintech as a Gateway for Financial Literacy," in *2023 International Conference on Information Technology (ICIT)*, 2023, pp. 811–814. doi: 10.1109/ICIT58056.2023.10225810.

[35] A. K. Singh, P. M. Sharma, M. Bhatt, A. Choudhary, S. Sharma, and S. Sadhukhan, "Comparative Analysis on Artificial Intelligence Technologies and its Application in FinTech," in *2022 International Conference on Augmented Intelligence and Sustainable Systems (ICAISS)*, 2022, pp. 570–574. doi: 10.1109/ICAISS55157.2022.10010573.


 