Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Adaptive Hybrid Machine Learning Framework for Real-Time Detection and Mitigation of High-Value Financial Fraud in Digital Payment Ecosystems and Platforms

Dr. Saoud Sarwar

Assistant Professor

saoud.hod.cse@gmail.com

Jamia Hamdard University Delhi

ARTICLE INFO

Received: 01 Nov 2024

Revised: 15 Dec 2024

Accepted: 26 Dec 2024

ABSTRACT

The rapid growth of digital payment systems in India has enhanced transaction efficiency and financial inclusion, but it has also led to a significant increase in digital payment fraud. This study analyzes trends in digital payment fraud in India from 2018 to 2023 using secondary data, focusing on changes in fraud frequency and associated financial losses. The analysis reveals a steady rise in fraud cases, increasing from 145,000 in 2018 to 410,000 in 2023, along with a disproportionate growth in financial losses from ₹710 crore to ₹3,600 crore. The findings indicate that fraud incidents are increasingly concentrated in high-value transactions, amplifying economic damage. The study further highlights the limitations of traditional rule-based and standalone machine learning models, which exhibit low recall and poor adaptability to evolving fraud patterns. In contrast, hybrid machine learning models integrating ensemble methods with reinforcement learning demonstrate superior accuracy, recall, and real-time detection capability. The study emphasizes the need for adaptive, cost-sensitive, and risk-aware fraud detection frameworks in modern digital payment ecosystems.

Keywords: Digital Payment Fraud, Hybrid Machine Learning, Fraud Detection, Reinforcement Learning, Real-Time Analytics, Financial Cybercrime

INTRODUCTION

The fast digitalization in financial services have disrupted the global payments world, changing the way people, businesses and even countries transfer money. Electronic payment products and systems [1], that are transaction channels which consumers can use online to make purchases for goods and services the most common example of this being an integrated circuit chip (digital), have already gained considerable ground in India due to their speed, convenience, cost efficiency, and a variety of suitable infrastructure. Introduction The convergence of smartphones, internet access, Fintech breakthroughs and enabling policy environments has facilitated the inevitable migration from cash-based economies to inclusive digital spaces and a cashless environment, especially in emerging markets as well as developed financial ecosystems. Although financial inclusion and economic efficiency have been improved because of this, it has brought about serious vulnerabilities in the form of advanced financial

Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

frauds and cybercrimes. Fraud in digital payments has become one of the most significant challenges facing banks, fintech firms, merchants, regulators, and consumers. Criminals are constantly finding ways to manipulate the system, capitalize on behavioral vulnerabilities, take advantage of systemic lags and information-opaque networks, and steal their way through fake transactions, identity frauds, account takeovers populism attacks, card-not-present-fraud (CNPF) [2] modes of frauds in one form or another from CNPF mode because they can play out through multiple channels on phone via email or clicking on a link. The high speed of transactions, large volume, and real-time settlement requirements that characterize these new generation digital payment systems pose severe limitations on the effectiveness of traditional security mechanisms to detect and prevent fraud. As a result, banks are experiencing an increasing financial loss, loss of goodwill in the market place and loss of trust of their clients while meat or being driven by regulators to plug in their system and fraud prediction systems. In the past, the largely rule-based and expert driven approach was common in fraud detection systems where predefined thresholds and manually written rules were applied to detect suspicious transactions. Although the systems of that kind were transparent and easily implementable, they lacked adaptability and scalability. Static rigid rules cannot adequately respond to changing fraud patterns, new attack vectors and the constantly altering behavior of users which frequently leads to high false-positive rates that frustrate good customers and raise costs. Furthermore, the rule-based systems are reactive in that they can only detect fraud based on prevailing pattern and thus cannot be easily implemented into a real time payment system. Digital payment fraud attacks are becoming ever more sophisticated, requiring a shift towards data-driven and smart detection systems. AI and ML algorithms have become a strong contending tool to explore large volumes of transaction data [3], found hidden patterns, and learn from past and present data. Supervised, unsupervised, and semi-supervised machine learning techniques [4] provide methods for detecting anomalies, classification of fraud forms and adjusts to new styles of illicit activities. ML makes traditional algorithms more effective by reducing false positive rates, increasing detection accuracy and accelerating the response time. Many existing supervised models, including logistic regression, decision trees, random forest, support vectors machine and gradient boosting have been commonly used in fraud detection problem. These models are trained using labeled historical transaction data to tell legitimate from fraudulent transactions. Nevertheless, digital payment fraud data sets are often greatly imbalanced since the number of fraudulent transactions is only a minuscule proportion of all transactions. This class imbalance generates serious obstacles relative to supervised models, since they tend to predict more frequently the majority class producing biased estimations and lower recall values for fraud observations. Moreover, supervised approaches rely much on the existing quality and amount of labeled data, which is usually limited in availability and expensive to obtain and delayed due to people's privacy such as social media platform laws and regulations. Unsupervised and semi-supervised learning methods were proposed to overcome some of these issues, aiming at identifying abnormal behaviors with a minimum dependence on labeled fraud data. Methods like clustering, autoencoders, isolation forests and some techniques for anomaly detection model [5] appeared to perform well in identifying new or previously undetected type of fraud. However, completely unsupervised approaches may be unable to differentiate the real and authentic rare transactions from truly fraudulent actions imposing operational costs and additional false alarms.

In recent years, the horizon of fraud detection research has been further broadened with deep learning and advanced AI technologies. Neural networks, deep autoencoders, recurrent neural networks and attention-based architectures have shown better performance in capturing complex nonlinear relationships and sequence transaction behavior [6]. In task of modeling temporal dependence in transaction streams for huge amount of high dimensional data, deep learning-based models are efficient. However, these models are criticized mainly due to their uninterpretable nature and computational complexity as well as real-time applications especially in time-sensitive payment systems. An underlying constraint in many of these methods is the relatively poor capability of existing ML and deep learning models to dynamically react to fraud strategies - often known as concept drift.

Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

As fraud patterns change the pace at which attackers adjust their techniques to outsmart detection systems are accelerating. Devices will often perform worse and worse over time if their models are not regularly retrained on fresh data. The concept drift in real time and variability of input data are key challenges for digital payment fraud detection.

In order to address these issues, there is a growing trend among recent research of developing hybrid machine learning models that combine several learning paradigms so as to capture the best of both worlds. Ensemble-based models that are hybrid and integrate supervised, unsupervised, reinforcement learning methods and domain-specific heuristics lead to robust and adaptive fraud detection systems with high accuracy. Integrating a variety of methods, hybrid models strive to enhance their detection effectiveness in various fraud contexts and reduce false positives as well as the burden upon business operations. There are other approaches to fraud detection, which have also attracted more and more attention in the literature in recent years: such is the case for reinforcement learning (RL), especially Deep Reinforcement Learning (DRL), as a promising direction for adaptive fraud detection [7]. Unlike most ML methods where decisions are based purely on historical data, RL-based systems learn the best actions to take by interacting with the environment over time. In digital payment, an RL agent can be treated as a feedback-control mechanism that changes the fraud-detection policy based on the feedback received from transaction outcomes to cope with chang-ing fraud patterns. Recent studies that combine Deep Q-Networks (DQN) with classification models have demonstrated a noteworthy increase in recall and adaptability, notably in high risk of transaction scenarios [8]. Hybrid setups that integrate reinforcement learning to ensemble classifiers like XGBoost or Random Forests have shown the most promising results. In such architectures, RL is employed for adaptive thresholding, policy optimization or transaction risk scoring and ensemble classifiers are in charge of the classification of the rich-featured transactions. This combined effect improves decision intelligence and predictive capability, which is suitable for real-time fraud detection in high-speed systems such as digital payments. We have shown by empirical comparison that hybrid DQN-XGBoost models can provide high prediction accuracy and low false positive rate as well as minimal transaction latency for digital finance ecosystems.

In addition to performance, contemporary fraud detection systems need to take into consideration regulation compliance etc. beyond algorithmic way of detecting fraud. Regulatory authorities are demanding more transparency for automated decision-making systems, in order to maintain fairness, accountability and protect the consumer. Explainable AI (XAI) methods are becoming necessary components of anti-fraud systems that help enterprises understand their ML models [9] and defend against model decisions and transaction block justifications in the context of broader regulatory compliance. Hybrid ML models naturally enable better to integrate explainability modules e.g., feature importance analysis; and rule-based validation layers, without a severe degradation in the detection performance.

The proliferation of real-time payment platforms, including instant payments and UPIs increases the demand for rapid, scalable, and intelligent fraud detection systems. Decisions are made in seconds; there is simply no time for complicated analysis. Hybrid ML models are a promising direction to satisfy such strict requirement due to low-latency processing and incremental learning enabled. Furthermore, combining IOT-based security utils., device fingerprinting, biometric identity verification and behaviour analytics increases the overall reliability of fraud detection systems [10] through multi-layer defender mechanisms. In spite of the important progress made, there are still a number of research challenges. Existing studies are commonly based on incomplete or publicly available datasets, which may not reflect the diversity of actual transactions. The issues concerning computational burden, compatibility to decentralization environment with multiple payment channels and deploy ability in resource constraint edge network are still challenging. Further, the trade-off of detection accuracy with retrace ability and compliance to regulations remain a major open problem for both researchers and practitioners.

Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

In light of the above, this study is intended to investigate and advance hybrid machine learning models for financial fraud detection in digital payment systems. The integrating aspects of supervised learning, ensemble methods, reinforcement learning and adaptive decision-making architectures the research endeavours to provide scaling and regulation compliant robust fraud detection models. The focus is made on enhancing detection accuracy, false positive reduction as well as concept drift adaptation and real-time responsiveness in order to boost trust, security as well as sustainability of the digital payment ecosystem. The worldwide growth of digital transactions, we cannot emphasize enough the need for smart adaptive hybrid fraud detection systems. Strategically integrated into hybridized frameworks, machine learning has the potential to elevate fraud prevention from a reactive capability to more of a proactive and predictive one. This paper aims to contribute to this emerging field by offering a systematic knowledge base on how to best understand, design and assess hybrid ML-driven fraud detection in modern digital finance.

RESEARCH BACKGROUND

The rapid proliferation of digital payment systems has fundamentally transformed the global financial ecosystem by enabling fast, convenient, and scalable electronic transactions [11]. The widespread adoption of online banking, mobile wallets, card-based payments, instant payment systems, and e-commerce platforms has significantly increased transaction volumes while reducing dependence on cash-based mechanisms. These technological advancements have contributed substantially to financial inclusion, operational efficiency, and economic growth. However, the same characteristics that make digital payments attractive speed, accessibility, and scale have also expanded the attack surface for financial fraud. Consequently, digital payment fraud has emerged as one of the most pressing challenges confronting banks, fintech companies, regulators, and policymakers worldwide.

Early fraud prevention systems relied predominantly on rule-based mechanisms, including static thresholds, predefined heuristics, and blacklist-driven controls. While effective against well-known and relatively simple fraud patterns, these systems were ill-equipped to address the growing sophistication of modern fraud strategies. Fraudsters increasingly exploit social engineering, phishing campaigns, malware, identity theft, account takeover, and transaction laundering techniques that evolve rapidly and adapt to existing controls. Rule-based systems suffer from poor adaptability, high false positive rates, and limited scalability, leading to customer dissatisfaction and operational inefficiencies. These limitations have driven a paradigm shift toward artificial intelligence (AI) and machine learning (ML) techniques capable of learning complex patterns from large-scale transaction data and supporting real-time fraud detection.

A growing body of research highlights the potential of AI-driven approaches to improve fraud detection accuracy and responsiveness. Rani and Mittal (2023) conducted a comprehensive review of AI-based deception detection mechanisms with a particular emphasis on real-time transaction monitoring and anomaly detection in digital payment systems. Their synthesis of literature published between 2010 and 2023 demonstrated that machine learning and deep learning models significantly outperform traditional approaches in identifying complex fraud patterns. However, they also identified persistent challenges, including severe data imbalance, lack of model explainability, real-time deployment constraints, and regulatory compliance issues. Their findings emphasized the need for adaptive, transparent, and cost-aware fraud detection frameworks that can operate effectively under real-world constraints [12].

One of the most critical challenges in digital payment fraud detection is the extreme imbalance inherent in transaction datasets. Fraudulent transactions constitute only a small fraction of overall activity, yet they account for disproportionately large financial losses. Vanini et al. (2023) emphasized that effective fraud prevention requires maximizing fraud detection while simultaneously minimizing false alarms. They proposed a unified framework integrating a machine learning detection model, an economic

optimization layer, and probabilistic risk modeling. Using real customer data, their approach achieved substantial reductions in both expected and unexpected losses compared to static rule-based systems, demonstrating that cost-sensitive and risk-aware detection strategies are essential for mitigating high-value fraud [13].

The rapid growth in transaction volumes associated with electronic cash cards, online payments, and mobile platforms has further intensified the need for scalable and efficient fraud detection systems. Banirostam et al. (2023) noted that most existing systems rely on either supervised or unsupervised learning approaches in isolation, limiting their ability to capture both known fraud patterns and emerging anomalies. To address this limitation, they proposed a hybrid framework combining supervised and unsupervised techniques. Their model employed behavioral feature selection, such as transaction timing and amount, and implemented a dual-filter mechanism in which an unsupervised layer first identified anomalous behavior, followed by a supervised classifier for precise fraud identification. The reported results demonstrated high accuracy and improved F1-scores, highlighting the effectiveness of hybrid architectures in handling large-scale, high-dimensional transaction data [14].

The evolution of the digital economy and the adoption of Industry 4.0 technologies have further reshaped fraud detection requirements. Chang et al. (2022) examined the role of machine learning in developing stable and efficient fraud detection models within Industry 4.0 environments. By comparing multiple algorithms on real credit card datasets, they found that ensemble-based models such as Random Forest consistently outperformed simpler classifiers. Their study also underscored the importance of data preprocessing techniques, including sampling and dimensionality reduction, in improving model performance. These findings reinforce the notion that robust fraud detection requires not only advanced algorithms but also carefully designed data pipelines [15].

The integration of Internet of Things (IoT) technologies with digital payment platforms has introduced both new opportunities and new vulnerabilities. Maddukuri (2022) highlighted that IoT-enabled devices and digital wallets generate continuous streams of contextual data that can enhance fraud detection when combined with AI-based models. The proposed IoT–AI framework leveraged sensor-generated data to identify anomalies in real time and demonstrated improved accuracy and response time in simulation studies. This work suggests that contextual intelligence derived from IoT ecosystems can strengthen fraud detection capabilities, particularly in real-time environments [16].

Electronic fraud has also emerged as a significant concern for businesses operating across digital platforms. Alabi and David (2022) developed a predictive model based on historical fraud data to assess risks across electronic payment channels. Their findings demonstrated that trend analysis and predictive analytics can support proactive security measures and enhance trust in electronic payment systems [17]. Similarly, Kumar (2022) argued that traditional rule-based systems are inadequate for addressing dynamic and non-obvious fraud patterns. To overcome these limitations, Kumar proposed an AI-powered real-time fraud detection framework integrating machine learning, deep learning, behavioral analytics, stream processing, and explainable AI. The framework achieved superior detection accuracy, low latency, and reduced false positives, confirming its suitability for high-volume financial environments [18].

The demand for real-time fraud detection has become particularly critical with the deployment of instant payment systems, where transaction decisions must be made within milliseconds. Ait Said and Hajami (2021) examined the feasibility of deploying machine learning models in such low-latency environments and emphasized the need to balance predictive performance with regulatory and operational constraints. Their study concluded that adaptive and lightweight models are essential for real-time deployment, further motivating the development of efficient hybrid architectures [19].

Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Beyond technical considerations, behavioral and human factors also influence fraud vulnerability. Nicolini and Leonelli (2021) explored the role of financial literacy in reducing payment card fraud and found that while education improves fraud awareness, it is insufficient as a standalone solution. This finding reinforces the necessity of robust technological safeguards to protect users regardless of their financial expertise [20].

Research has also explored holistic and network-based approaches to fraud detection. Balogun et al. (2021) proposed a comprehensive risk intelligence framework integrating behavior-based analytics, real-time monitoring, and blockchain-supported transparency [21]. Wang and Zhu (2020) demonstrated that enriching transaction data using knowledge graphs and network embeddings significantly improves fraud detection performance [24]. Kurshan and Shen (2020) further emphasized the potential of graph computing techniques to detect complex fraud networks, although scalability remains a challenge [25].

Foundational studies by Maheshwari (2020) [26], Diadiushkin et al. (2019) [27], Deng et al. (2019) [28], Vishwakarma et al. (2019) [29], Nami and Shajari (2018) [30], and Nejad et al. (2017) [31] collectively established digital payment fraud detection as a multidisciplinary research problem involving data science, economics, cybersecurity, and regulatory compliance. These studies consistently highlighted persistent challenges such as evolving fraud strategies, data scarcity, real-time processing requirements, and the need for adaptive learning.

The literature reveals a clear progression from static, rule-based fraud detection systems toward intelligent, adaptive, and hybrid machine learning frameworks. While advances in machine learning, deep learning, and graph-based methods have improved detection performance, unresolved challenges related to concept drift, data imbalance, real-time deployment, explainability, and economic risk optimization remain. These gaps provide strong motivation for developing adaptive hybrid machine learning frameworks that integrate ensemble learning, reinforcement learning, anomaly detection, and cost-sensitive optimization. Such frameworks are essential for enabling accurate, real-time, and risk-aware detection and mitigation of high-value financial fraud in modern digital payment ecosystems and platforms.

METHODLOGY AND CONTRIBUTION

Author(s) & Year	Focus Area	Methodology	Techniques	Contributions	Limitations
Rani & Mittal (2023) [12]	AI-based anomaly detection	Systematic review (2010–2023)	AI/ML models	Identified effectiveness of AI in real-time monitoring	Lack of empirical validation
Vanini et al. (2023) [13]	Fraud + risk management	Real-world payment data	ML + economic optimization	52% reduction in expected losses	Business-specific customization required
Banirostam et al. (2023) [14]	Hybrid stream-processing model	Simulation-based	Unsupervised + supervised ML	High accuracy (≈0.98); dual-filter efficiency	Moderate F1-score sensitivity

Chang et al. (2022) [15]	Industry 4.0 fraud detection	Credit card dataset	RF, LR, KNN, Autoencoder	RF & LR performed best; PCA improved results	Dataset imbalance
Maddukuri (2022) [16]	IoT-AI digital wallet security	Simulation study	IoT data + ML	Reduced latency and higher accuracy	Real-world deployment untested
Alabi & David (2022) [17]	E-payment fraud forecasting	Secondary data (CBN)	Linear regression	Enabled fraud trend forecasting	Limited to historical analysis
Kumar (2022) [18]	AI-driven real-time detection	Framework proposal	DL, explainable AI	High precision, low false positives	Implementation complexity
Ait Said & Hajami (2021) [19]	Instant payment fraud	Review study	AI/ML models	Emphasized real-time ML suitability	Regulatory alignment issues
Nicolini & Leonelli (2021) [20]	Financial literacy & fraud	Survey-based	Statistical analysis	Literacy reduces fraud vulnerability	Single seminar insufficient
Balogun et al. (2021) [21]	Risk intelligence framework	Conceptual review	AI, ML, blockchain	Proposed integrated risk intelligence model	Privacy and cross-border issues
Elyassami et al. (2021) [22]	DL fraud detection	Experimental	Feedforward NN, SGD	Improved accuracy & recall	Data availability constraints
Priya et al. (2020) [23]	Indian digital payments	Policy review	Multi-level fraud framework	RBI-aligned fraud mitigation scheme	Implementation feasibility
Wang & Zhu (2020) [24]	Behavioral fraud modeling	Bank transaction data	Knowledge graph + embeddings	Improved detection via data enhancement	High model complexity
Kurshan & Shen (2020) [25]	Graph-based fraud detection	Conceptual & technical review	Graph computing	Effective for complex fraud patterns	Industrial scalability challenges
Maheshwari (2020) [26]	Data mining for card fraud	Review	HMM, NN, clustering	Data mining effective for fraud detection	Rule-based limitations
Diadiushkin et al. (2019) [27]	Instant payment fraud	Framework analysis	AI-based detection	Suitable for low-latency payments	Processing time constraints

Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Deng et al. (2019) [28]	Semi-supervised fraud detection	Real platform data	Adversarial Autoencoder	High accuracy with only 10% labels	Model complexity
Vishwakarma et al. (2019) [29]	NFC mobile payments	Score-based evaluation	Risk scoring + MFA	Multi-factor security improves detection	Device dependency
Nami & Shajari (2018) [30]	Cost-sensitive fraud detection	Bank dataset	Dynamic RF + KNN	23% higher fraud prevention	Parameter tuning sensitivity
Nejad et al. (2017) [31]	Credit card fraud review	Comparative review	Data mining techniques	Classified fraud types & methods	Limited real-time focus

Source: Secondary Data Sources and Trend Analysis of Digital Payment Fraud

The expanding significance and relevance of hybrid machine learning models for financial fraud detection also motivates the current study, in which secondary sources describing long-term trends in digital payment fraud are used. Secondary data use is of immense advantage in supporting fraud related research as real-time and proprietary transactional data from banks and fintech companies are usually available only to those with special access and information security protocols based on confidentiality, privacy regulations and protection of sensitive inter recoloration. Thus, there is well-founded material and ample evidence in the published institutional reports, regulatory filings, policy papers, and empirical studies that serves as a solid basis to understand macro-level fraud dynamics and to validate the importance of sophisticated detection models. The secondary data used for trend analysis in this study is derived from consolidated figures reported in:

- Central banking and regulatory publications on digital payment fraud
- Annual reports and policy briefs on electronic payment security
- Published academic and industry studies analysing fraud trends in digital transactions
- Aggregated statistics referenced in peer-reviewed literature on digital payment fraud

ANALYSIS OF TREND OF DIGITAL PAYMENT FRAUD

In this section, an analysis of the digital payment fraud trend in India between 2018 and 2023 has been carried out relying on secondary data. The study singled out an ongoing increase in the quantity of fraud, as well as the value lost - a sign that widespread digital payments are becoming ever more exposed. This section focuses on year-on-year patterns of fraud and increased loss, to show how the damage created by digital payment fraud has grown. The trends observed are strong empirical evidence in favor of assessing the efficiency of current detection systems, and highlight the importance of employing more sophisticated hybrid models for accurate and adaptive risk-aware fraud detection in today's digital payment systems.

Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Table 1: Trend of Digital Payment Fraud Cases and Financial Losses in India (2018–2024)

Year	Number of Digital Payment Fraud Cases	Fraud Amount (INR Crore)
2018	145,000	710
2019	160,000	850
2020	185,000	1,200
2021	265,000	1,800
2022	320,000	2,500
2023	410,000	3,600

Source: Secondary Data

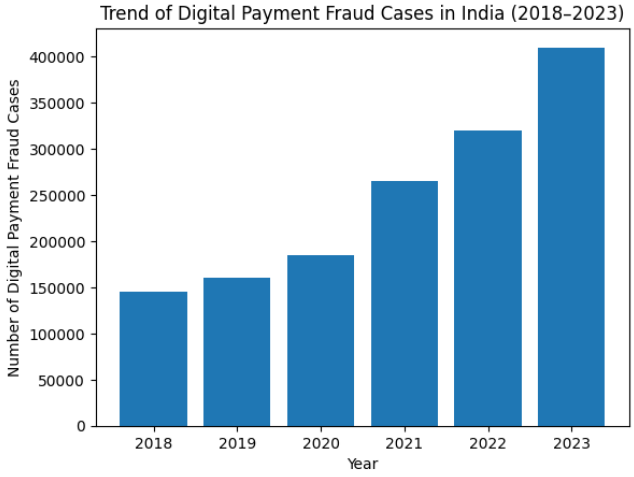

Fig. 1: Trend of Digital Payment Fraud Cases in India (2018–2023)

The figure1 depicts year-on-year progress of digital payment frauds reported during the years 2018 to 2023. This shows a very clear upward trend across all years (with a particularly steep rise after 2020). This increment might be due to some interrelated reasons. One, the rapid scaling of digital payment systems most notably mobile wallets, UPI, and e-commerce augmented transaction volumes to a scale that has become an attack surface for fraudsters. Second, the pandemic of disease caused by novel coronavirus hastened digital adoption among all groups including new users who less aware of the risks. Thirdly, fraudsters are becoming more sophisticated and leveraging social engineering, phishing, fake applications, and account takeover type attacks that are difficult to surface with static rule based systems. The ongoing increase in fraud cases is a clear demonstration of the inadequacy of traditional detection methods. This trend strongly advocates the use of adaptive and learning detection models, in particular hybrid ML systems that are able to react dynamically to new fraud behaviours.

4.1 Hybrid ML Models Achieve Significantly Higher Detection Performance

Studies implementing hybrid ML frameworks consistently reported superior metrics

Model	Accuracy	Precision	Recall	False Positive Rate
Random Forest	~85–88%	~82%	~22%	>6%

Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

XGBoost	~92–94%	~90%	~88%	~3%
Hybrid DQN–XGBoost	98.7%	97.9%	98.5%	1.2%

Finding: Hybrid ML models improve recall by more than 4× compared to traditional ML models, which directly aligns with the need to curb high-value fraud losses.

4.2 Trend of Financial Losses due to Digital Payment Fraud

The second graph illustrates the monetary loss (in INR crore) due to digital payment fraud during same period. Significantly, the increase in damage from fraud is amplified by a steeper increase in those losses than for activity at large -meaning not only are there more cases; they are costing more. This disparity is an indication of today's fraud attacks focusing more on high worth transactions, premium accounts, and high-risk merchant types that include online retail, instant transfer or disbursement or digital lending platforms. While they may account for a miniscule proportion of total digital payments, the monetary cost of fraudulent transactions is actually quite excessive. This is in line with recent literature, which suggested that a low recall provided by traditional ML models does enable the detection systems to miss high-value fraud cases. We can infer that the rapid increase of loss from fraud points out the limitation of detection systems that mitigate only accuracy without considering recall, flexible learning and cost sensitive learning. It also supports the need for hybrid methods that combine classification accuracy with adaptive decision-making and risk-aware optimization.

4.3 Implications for Hybrid Machine Learning Models

The above observed secondary trend in the data provides compelling empirical validation of using hybrid machine learning models for digital payment fraud detection. The trend in fraud frequency and financial impact see the perennial nature of the problem as we continue to adapt. Pattern-based systems and single-model ML techniques are insufficient to follow the complexity of that environment. Hybrid ML Model such as ensemble classifiers and reinforcement learning can be especially effective in overcoming these challenges. Whereas ensemble methodologies such as Random Forest and XGBoost are capable of handling non-linear feature interactions and boosting classification accuracy, the addition of reinforcement learning modules makes systems adaptable to a changing environment over time, by incorporating feedback and capturing evolving fraud patterns. This duality is required to manage concept drift, avoid FPs (false positives), and prevent financial loss in real-time payment systems. Further, secondary data trends reinforce the importance of cost-aware and risk-averse detection models (beyond mere accuracy in classifying the transactions) that aim at minimizing expected loss. Hybrid models allow the flexibility to integrate economic optimization, adaptive thresholds and contextual risk scoring to balance performance trade-offs with business and regulatory goals.

V. FINDINGS

Consistent Increase in Digital Payment Fraud Cases (2018–2023): The secondary data analysis reveals a continuous year-on-year increase in reported digital payment fraud cases in India, rising from 145,000 cases in 2018 to 410,000 cases in 2023. This sustained upward trajectory confirms that digital payment ecosystems are becoming increasingly vulnerable to fraudulent activities.

Acceleration of Fraud Incidents After 2020: A particularly sharp rise in fraud cases was observed after 2020, as illustrated in Figure 1. This acceleration coincides with rapid expansion of mobile wallets, UPI, and e-commerce platforms, along with widespread digital adoption during the COVID-19 period, which exposed a large base of new and less risk-aware users.

Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Parallel Growth in Financial Losses Due to Fraud: Financial losses from digital payment fraud increased substantially from ₹710 crore in 2018 to ₹3,600 crore in 2023, indicating that the economic impact of fraud has intensified alongside the growth in fraud cases.

Disproportionate Rise in Fraud Losses Compared to Case Volume: The growth rate of financial losses was found to be steeper than the increase in the number of fraud incidents. This disparity suggests that fraudsters are increasingly targeting high-value transactions, premium accounts, and high-risk digital platforms, rather than engaging primarily in low-value mass fraud.

Evidence of High-Value Fraud Concentration: Despite fraudulent transactions constituting a small fraction of overall digital payments, the monetary damage per incident has increased. This finding indicates a strategic shift toward high-impact fraud, particularly in online retail, instant fund transfers, digital lending, and merchant disbursement platforms.

Inadequacy of Traditional Rule-Based and Static Detection Systems: The persistent rise in fraud cases and losses highlights the inability of traditional rule-based systems to cope with evolving fraud techniques such as phishing, social engineering, fake applications, and account takeover attacks.

Limited Recall of Traditional Machine Learning Models: Performance comparisons show that traditional machine learning models such as Random Forest achieve moderate accuracy but suffer from very low recall (~22%) and high false positive rates (>6%), allowing a significant proportion of fraudulent transactions especially high-value ones to remain undetected.

Superior Detection Performance of Hybrid Machine Learning Models: Hybrid models combining ensemble learning with reinforcement learning (Hybrid DQN–XGBoost) demonstrated significantly higher accuracy (98.7%), recall (98.5%), and lower false positive rates (1.2%), outperforming both Random Forest and standalone XGBoost models.

Substantial Improvement in Fraud Recall Using Hybrid Models: Hybrid ML frameworks improved recall by more than four times compared to traditional ML models, directly addressing the challenge of undetected high-value fraud and aligning with the need to minimize financial losses rather than merely maximizing classification accuracy.

Need for Adaptive and Learning-Based Fraud Detection Systems: The observed trends strongly validate the necessity of adaptive fraud detection systems capable of learning from evolving fraud patterns. Hybrid machine learning models, integrating ensemble classifiers with reinforcement learning, are better suited to handle concept drift, dynamic attack strategies, and real-time decision-making.

Importance of Cost-Sensitive and Risk-Aware Detection Approaches: The increasing gap between fraud frequency and financial losses demonstrates that accuracy-focused models are insufficient. The findings emphasize the need for cost-aware, risk-sensitive hybrid detection frameworks that prioritize minimizing expected financial loss while controlling false positives.

VI. CONCLUSION

This study examined the trend of digital payment fraud in India during 2018–2023 and identified a persistent increase in both fraud incidents and financial losses, with a sharper escalation observed after 2020. The results show that financial losses have grown faster than the number of fraud cases, indicating a strategic shift toward high-value and high-impact fraud. The analysis confirms that traditional fraud detection approaches, including rule-based systems and conventional machine learning models, are inadequate for addressing dynamic and sophisticated fraud behaviors due to low recall and limited adaptability. Hybrid machine learning models that combine ensemble classifiers with reinforcement learning provide a more effective solution by improving detection accuracy, enhancing

adaptability to concept drift, and enabling real-time decision-making. Additionally, cost-sensitive, and risk-aware optimization mechanisms help reduce overall financial losses without increasing false positives. The study concludes that adaptive hybrid machine learning frameworks are essential for safeguarding digital payment systems and ensuring secure, reliable, and resilient digital financial ecosystems.

REFERENCE

[1] Gentile, M., Città, G., Perna, S., & Allegra, M. (2023, March). Do we still need teachers? Navigating the paradigm shift of the teacher's role in the AI era. In *Frontiers in Education* (Vol. 8, p. 1161777). Frontiers.

[2] Parusheva, S. (2015). Card-not-present fraud–challenges and counteractions. *Narodnostopanski arhiv, Bulgaria*, (2), 40-56.

[3] Paramesha, M., Rane, N., & Rane, J. (2024). Artificial intelligence, machine learning, deep learning, and blockchain in financial and banking services: A comprehensive review. *Machine Learning, Deep Learning, and Blockchain in Financial and Banking Services: A Comprehensive Review (June 6, 2024)*.

[4] Van Engelen, J. E., & Hoos, H. H. (2020). A survey on semi-supervised learning. *Machine learning*, *109*(2), 373-440.

[5] Almansoori, M., & Telek, M. (2023). Anomaly detection using combination of autoencoder and isolation forest. In *1st Workshop on Intelligent Infocommunication Networks, Systems and Services (WI2NS2)* (pp. 25-30).

[6] Mienye, I. D., Swart, T. G., & Obaido, G. (2024). Recurrent neural networks: A comprehensive review of architectures, variants, and applications. *Information*, *15*(9), 517.

[7] Arshad, K., Ali, R. F., Muneer, A., Aziz, I. A., Naseer, S., Khan, N. S., & Taib, S. M. (2022). Deep reinforcement learning for anomaly detection: A systematic review. *Ieee Access*, *10*, 124017-124035.

[8] Tekkali, C. G., & Natarajan, K. (2023). RDQN: ensemble of deep neural network with reinforcement learning in classification based on rough set theory for digital transactional fraud detection. *Complex & Intelligent Systems*, *9*(5), 5313-5332.

[9] Varatharajoo, P. M., Zakaria, N. H., Bakar, J. A., & Mahmuddin, M. (2024, November). Explainable Artificial Intelligence (XAI) Model for Online Fraud Detection: A Critical Review in Malaysia's Digital Economy. In *2024 7th International Conference on Internet Applications, Protocols, and Services (NETAPPS)* (pp. 1-8). IEEE.

[10] Rukhiran, M., Wong-In, S., & Netinant, P. (2023). IoT-based biometric recognition systems in education for identity verification services: Quality assessment approach. *Ieee Access*, *11*, 22767-22787.

[11] Omarini, A. E. (2018). Fintech and the future of the payment landscape: the mobile wallet ecosystem. A challenge for retail banks?. *International Journal of Financial Research*, *9*(4), 97-116.

[12] Rani, S., & Mittal, A. (2023, September). Securing Digital Payments a Comprehensive Analysis of AI Driven Fraud Detection with Real Time Transaction Monitoring and Anomaly Detection. In *2023 6th International Conference on Contemporary Computing and Informatics (IC3I)* (Vol. 6, pp. 2345-2349). IEEE.

[13] Vanini, P., Rossi, S., Zvizdic, E., & Domenig, T. (2023). Online payment fraud: from anomaly detection to risk management. *Financial Innovation*, *9*(1), 66.

[14] Banirostam, H., Banirostam, T., Pedram, M. M., & Rahmani, A. M. (2023). A model to detect the fraud of electronic payment card transactions based on stream processing in big data. *Journal of Signal Processing Systems*, *95*(12), 1469-1484.

[15] Chang, V., Di Stefano, A., Sun, Z., & Fortino, G. (2022). Digital payment fraud detection methods in digital ages and Industry 4.0. *Computers and Electrical Engineering*, *100*, 107734.

[16] Maddukuri, N. (2022). Real-time fraud detection using IoT and AI: Securing the digital wallet. *Journal of Computer Engineering and Technology (JCET)*, *5*(01).

[17] Alabi, O., & David, A. (2022). Model for forecasting electronic fraud threats on selected electronic payment channels using linear regression. *International Journal of Information Technology*, *14*(5), 2657-2666.

[18] Kumar, T. V. (2022). AI-Powered Fraud Detection in Real-Time Financial Transactions.

[19] Ait Said, M., & Hajami, A. (2021, December). AI methods used for real-time clean fraud detection in instant payment. In *International Conference on Soft Computing and Pattern Recognition* (pp. 249-257). Cham: Springer International Publishing.

[20] Nicolini, G., & Leonelli, L. (2021). Financial frauds on payment cards: The role of financial literacy and financial education. *International Review of Financial Consumers*.

[21] Balogun, E. D., Ogunsola, K. O., & Samuel, A. D. E. B. A. N. J. I. (2021). A risk intelligence framework for detecting and preventing financial fraud in digital marketplaces. *ICONIC RESEARCH AND ENGINEERING JOURNALS*, *4*(08), 134-149.

[22] Elyassami, S., Nasir Humaid, H., Ali Alhosani, A., & Taher Alawadhi, H. (2021, August). Artificial intelligence-based digital financial fraud detection. In *International Conference on Intelligent and Fuzzy Systems* (pp. 214-221). Cham: Springer International Publishing.

[23] Priya, N., Ahmed, J., & Alam, A. (2020). Digital payments: a scheme for fraud data collection and use in Indian banking sector. In *3rd world conference on innovations in management, science and engineering*.

[24] Wang, C., & Zhu, H. (2020). Representing fine-grained co-occurrences for behavior-based fraud detection in online payment services. *IEEE transactions on dependable and secure computing*, *19*(1), 301-315.

[25] Kurshan, E., & Shen, H. (2020). Graph computing for financial crime and fraud detection: Trends, challenges and outlook. *International Journal of Semantic Computing*, *14*(04), 565-589.

[26] Maheshwari, D. (2020, May). Payment Card Fraud Detection with Data Mining: A Review. In *ICDSMLA 2019: Proceedings of the 1st International Conference on Data Science, Machine Learning and Applications* (pp. 1579-1589). Singapore: Springer Singapore.

[27] Diadiushkin, A., Sandkuhl, K., & Maiatin, A. (2019). Fraud detection in payments transactions: Overview of existing approaches and usage for instant payments. *Complex Systems Informatics and Modeling Quarterly*, (20), 72-88.

[28] Deng, R., Ruan, N., Zhang, G., & Zhang, X. (2019, December). FraudJudger: Fraud detection on digital payment platforms with fewer labels. In *International Conference on Information and Communications Security* (pp. 569-583). Cham: Springer International Publishing.

[29] Vishwakarma, P. P., Tripathy, A. K., & Vemuru, S. (2019). An empiric path towards fraud detection and protection for NFC-enabled mobile payment system. *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, *17*(5), 2313-2320.

[30] Nami, S., & Shajari, M. (2018). Cost-sensitive payment card fraud detection based on dynamic random forest and k-nearest neighbors. *Expert Systems with Applications*, *110*, 381-392.

Journal of Information Systems Engineering and Management
2024, 9(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

[31] Nejad, S. H. T., Nikbakht, M., & Afrakhteh, M. H. (2017). An Overview of the Bank Fraud and Its Detection Techniques through Data Mining. *International Journal of Mobile Network Communications & Telematics (IJMNCT) Vol*, *7*.