International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

FINANCIAL TECHNOLOGY AND AI-DRIVEN FRAUD DETECTION IN REAL-TIME TRANSACTIONS

[1]Ashutosh Chandra Jha, [2]Ganpati Goel

[1]Network Security Engineer, NewYork, USA

ORCID: 0009-0006-4713-0541

ashutoshjhany@gmail.com

[2]Zero Motorcycles Inc., Scotts Valley, California, USA

Email: ganpati6341@gmail.com

Abstract

Financial Technology (FinTech) has rapidly transformed the financial industry, particularly by enabling real-time payments, which streamline financial services. However, the speed of these transactions has significantly increased the risk of fraud, posing a major challenge to financial institutions. AI-driven fraud detection systems leveraging machine learning algorithms have emerged as powerful tools to combat this issue. These systems utilize predictive analytics, anomaly detection, and behavioral analysis to identify and block fraudulent transactions in real time. However, the effectiveness of these systems is heavily dependent on network infrastructure, particularly ultra-low-latency networks, which are crucial for timely fraud detection. This paper examines the integration of AI technologies with ultra-low-latency networks to secure real-time financial transactions and highlights case studies where financial institutions have successfully adopted these solutions. As AI and network infrastructure continue to evolve, their combined potential for proactive fraud detection is expected to grow, offering enhanced protection for real-time transactions in the future.

Keywords: *AI-Driven Fraud Detection, Anomaly Detection, Financial Technology (FinTech), Machine Learning, Real-Time Payments (RTP), Ultra-Low-Latency Networks*

1. Introduction

Over the past few years, the world financial environment has been evolving rapidly, which is mostly facilitated by the development of financial technology (FinTech). This change has broken down the conventional banking systems, and has created a new inception of bank services that are digital first. Leveraging through mobile payments and blockchain, FinTech has converted the gap between consumers and financial institutions serving them in a faster, less expensive, and efficient way. Historically, banking was mostly a physical operation that demanded the customer to transact with the tellers. Yet, the banking industry has become more digitized now due to the advent of the internet and mobile technology, where mobile wallets, peer-to-peer lending, robo-advisor, and digital insurance platforms are provided. The FinTech market is expanding at a considerable rate, and currently, it is worth more than 100 billion

Received: August 12, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

dollars, with a lot of investments that promote the development of digital payments, online banking, and other financial services.

One of the main innovations in FinTech is the establishment of real time payments (RTP) that provide immediate transfers of money among individuals and companies within seconds rather than have to wait a long time due to the utilization of wire transfer or checks like has been experienced in conventional bank systems. Swift Systems such as SWIFT GPI, Faster Payments, Zelle, and SEPA Instant Credit Transfer have been helpful in providing real-time payment systems in the entire world. With the growing popularity of RTP systems, substantial advantages will be offered, such as improvement in cash flows of businesses, more timely availability of funds among consumers, and minimization of the risks associated with slowness of transactions. Nevertheless, the emergence of RTP also comes with a number of challenges especially in the area of fraud detection.

In the traditional payment systems, the time taken between a transaction and its settlement gave time to stop a transaction due to fraud being identified. Contrary to this, real-time payments have no such cooling-off period, and the advantage of these transactions is given to the fraudsters, who have a chance to realize that transactions are fast and irrevocable. With the increase in the use of real-time transactions, cybercriminals have not been left behind as they have evolved more advanced tricks such as account takeovers, identity thefts, and the manipulation of transactions to defeat security measures. The international payment card fraud market in 2019 was estimated to be 28.65 billion, which demonstrates the extent of the issue. Moreover, the urge to combat fraud in real-time payment system is even more urgent as the volume of the real-time payments in the world continuously increases, reaching 28 in 2019 and predicted at 45 in 2024.

The battle against real-time fraud is in artificial Intelligence (AI) and Machine Learning (ML) frontiers. The AI-based fraud detection is an innovative system that employs sophisticated algorithms to transform transaction data on behavior, anomalies, and patterns of fraud in real time. The most important aspect of AI fraud detection is predictive analytics, which, as its name suggests, is used to predict a possible fraud based on previous transactions. These systems are dynamic in nature and have been enhanced through machine learning thus this makes them adapt to the emerging fraud detection challenges. Another way AI is applied is that the systems can detect anomalies and analyze behaviour to evaluate user activity. Having a benchmark of normal operations, these systems are able to indicate suspicious transactions, like abnormal amount or an abrupt increase in the speed of transactions, which could be as a result of fraudulent activity.

The effectiveness of the AI in fraud detection directly depends on the quality of the underlying network infrastructure. Ultra-low-latency networks are also needed to support the real-time implementation of the AI-based fraud detection systems. With these networks, financial institutions are able to handle transactions in an adequate speed capable of detecting and preventing fraudulent transactions at the point of transfer of money between two or more parties. In this paper, the author explains how AI technologies can be used together with ultra-low-latency networks to make real-time financial transactions safer. It also analyzes case

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

studies of successfully implemented AI-driven fraud detection systems by financial institutions in response to the increasing risk of fraud in FinTech.

This paper also compares standard industry-standard fraud detection models, including rule-based systems, credit scoring models, and traditional statistical fraud detection, to help show how AI-based fraud detection models serve as a more proactive means of preventing fraud. This paper brings to light the practical insights into the future of safe and reliable real-time financial transactions by analyzing and examining AI technologies, machine learning models, and network infrastructure.

2. Literature Review

2.1 Fraud in Financial Transactions

Financial fraud has also developed over the years, not to mention that it has never been restricted to the conventional forms such as check frauds and cash thefts but has evolved into a more sophisticated form of online fraud [1]. Historically, fraudsters could easily misuse any physical system and tamper with paper records to make unauthorized transactions by interfering with it. Nonetheless, due to the development of digital technology and the emergence of online banking, the fraud that once was a comparatively easy process has become more sophisticated and now includes such cybercrimes as phishing, account takeovers, and identity theft. Digitization of processes, including Enterprise Resource Planning (ERP) and online financial solutions, has resulted in large interconnected data spaces that, although beneficial by increasing operational efficiency, has increased the attack space of potential legal fraud [2]. Besides, the growing trend of using artificial intelligence (AI) and machine learning to automate financial processes has brought both opportunities and threats. The same technologies have been used by the same fraudsters to outwit security systems and establish vulnerabilities in the digital infrastructures [3]. Therefore, organizations should not solely work on digital transformation but also invest their efforts in transparency, data stewardship, and sound AI-based governance to create resilient mechanisms against emerging fraud trends.

Financial transactions have continued to rise and so is the cost of fraud all over the globe. In 2019, the payment card fraud in the world amounted to billions of dollars, which is not likely to slow down in the future. With the current trend of moving financial services to online stores the chances of committing a fraud are increasing. This has especially occurred in real-time payments systems which, although granting the advantage of finality of a transaction in real-time, also expose the financial institution to fraudulent activity. In conventional ways of payment, time usually existed between the establishment and payment of a transaction where checks and verification could be conducted before money is sent. But in fact, real-time payments, due to their nature, are final and non-reversible when applied, providing few chances of post-payment intervention or fraud detection. This non-delay causes a very big problem with regard to the real-time transaction security.

With increased use of real time payments, fraudsters have also adjusted their strategies and take advantage of the fact that real time payments are instantaneous. According to data published in 2019, around 28 percent of global payments were real-time in 2019 and they are

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

estimated to rise to 45 percent by 2024. Such surge of real time transactions highlights the importance of having well-developed, fast fraud detection systems capable of running as real time to ensure that fraudulent transactions do not occur before the transaction is executed.

Figure 1 shows, financial fraud has evolved, encompassing various types such as bribery, corruption, procurement fraud, and misuse of accounts. These complex fraud schemes require fast and efficient real-time fraud detection systems, especially in the era of increasing real-time payments.

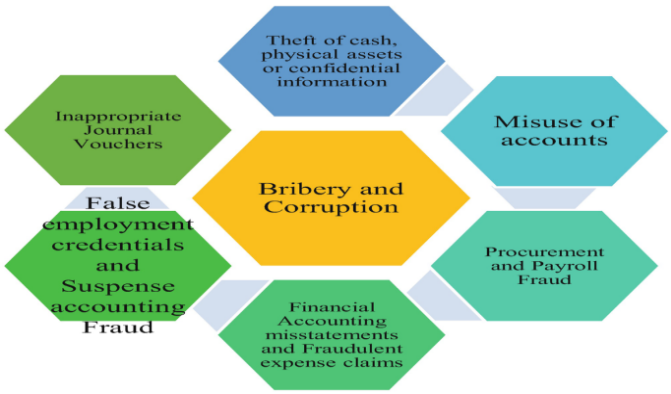

Figure 1: ***Financial and Systematic Fraud***

2.2 AI and Machine Learning Fraud Detection.

Machine learning (ML) and artificial intelligence (AI) technologies have become unavoidable in modern fraud detection systems [4]. By leveraging these technologies, financial institutions can identify fraud patterns and forecast potential fraudulent activities through the real-time analysis of vast transaction datasets. Currently, about 60 percent of financial institutions are utilizing AI in their fraud detection processes due to its superior ability to detect anomalies and suspicious behaviors more effectively than conventional methods. Trained on historical data, AI models can recognize both known fraud patterns and adapt to new, emerging tactics used by fraudsters. However, as these intelligent systems increasingly access sensitive financial data, ensuring secure and trustworthy data environments becomes crucial. Implementing frameworks such as zero-trust data architectures, which emphasize continuous verification and strict access control, can safeguard sensitive datasets against unauthorized manipulation and misuse [5]. This integration of AI-driven analytics with robust data security frameworks ensures that fraud detection systems remain both intelligent and resilient in the face of evolving digital threats.

Supervised learning, unsupervised learning, and reinforcement learning are the most common among all the methods of detecting fraud that AI systems utilize. The learning algorithms under supervision are trained using labelled data, i.e. known fraudulent or legitimate transaction. These models are next used to group new transactions by their similarity to the described data. Scrutinized learning, in its turn, allows AI to detect fraud without labels and evolve in accordance with emergent patterns of fraud by detecting suspicious activity in transactional data. A further advanced form of AI is the reinforcement learning wherein the models are built upon continuous feedback and the models increase their detection skills continuously as they

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

experience new instances of fraud running in real time. The dynamic learning process would be applicable particularly in catching up fraud methods which may not ever have been identified before.

Intelligence real-time monitoring systems would utilize AI to examine transactions in milliseconds and provide immediate alerts in the event of any suspicious activity detected. These systems do not merely operate to identify a single instance of fraud but also they are employed to provide an insight into the future occurrence of frauds based on the trend and pattern in the information. The MasterCard Decision Intelligence platform, featuring AI running billions of transactions every year, is one example of an application of this technology in practice to identify systematically and preempt fraud on a global payment network.

2.3 Real-Time Transactions with Ultra-Low-Latency Networks.

AI-based fraud detection systems should work effectively whereby the network infrastructure should be able to support transactions within a very short time [6]. Ultra-low-latency networks This type of network must support large amounts of traffic and latency less than 10 milliseconds. Such rate of fastening is very important in the light of making sure that the fraud detection systems can process transactions prior to their completion and transfer of funds. Slack processing times can be a loss of chances of fraud prevention and therefore the fraud acts may go through without detection.

The possibility of ultra-low-latency in real-time transactions has been transformed through the launch of high-speed 5G networks that are much faster in transmitting data and lower latency than the other generations of mobile networks, which are ideal in real-time processing applications, including financial transactions. Furthermore, fiber-optic technology is essential in the context of providing rapid data transfer over financial networks that offers the platform on which transactions may be conducted safely and efficiently. An example is VisaNet which handles up to 65,000 transaction messages each second with an average transaction latency of less than 5 milliseconds. This is a good performance level that will push the fraud detection systems to perform at the required speed to avoid the fraud activities on real time transactions.

2.4 Fraud Detection with Blockchain.

The ability of blockchain technology to provide transparent and irreversible records on transactions and secure storage has made it very popular. Blockchain keeps a record of each and every transaction on a decentralized registry, which makes the data of the transaction non-modifiable and impossible to tamper with, further safeguarding against fraudulent operations. In this non-repudiable and invariable database of transactions, it is very hard to modify or forge the records of transactions and this weakness is very likely to occur with the traditional, centralized system of finance. Additionally, also as the organizations shift monolithic financial systems to more distributed digital systems, clear context delimitation and creation is necessary in order to allow secure and efficient integration of a blockchain with the rest of the systems [7]. Also, fault-tolerant and event-driven architectures promote the stability of blockchain-based financial solutions, reducing risks of data hijacking and guaranteeing system availability even in the presence of cyber threats [8]. In this way, the collaboration of blockchain with

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

resilient system architectures, in addition to improving transparency and trust, also strengthens financial systems against new types of digital fraud.

Blockchain can be employed in conjunction with AI to enhance fraud detection as it will make the processes more transparent and traceable. Fraud detection AI systems will be able to process blockchain transaction data and identify patterns of fraud activities and the blockchain record ensures that transaction data remains safe and difficult to change. The AI and blockchain have already been shown to be efficient in practice. To name a few examples, the Deutsche bank has been in a position to integrate AI with blockchain technology to ensure the use of AI to increase the security of cross-border payment that has reduced fraud by up to 30 percent in two years. This integration makes the financial institutions to have a healthy and dynamic real time assurance that financial transactions have been secured and risks of frauds reduced [9]. The combination of AI and blockchain technologies is a powerful force that assists in enhancing fraud by the way of real time pay system as well as delivering the power and safety that must be acquired in the contemporary financial setting that remains immensely dynamic.

Figure 2 shows, blockchain's key features, such as decentralization, immutability, transparency, and security, are essential in ensuring secure and transparent transactions. When integrated with AI, blockchain enhances fraud detection by providing tamper-proof transaction records, improving security in real-time financial systems.

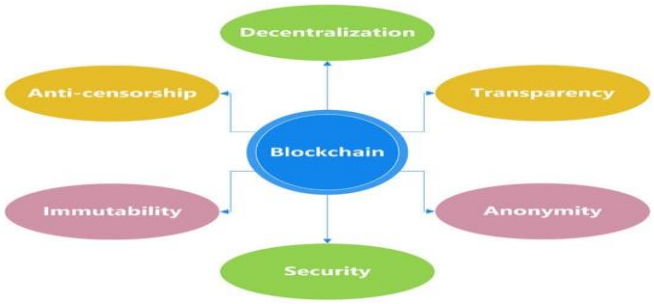

Figure 2: ***Convergence of Artificial Intelligence***

3. AI-Driven Fraud Detection in Real-Time Transactions

3.1 Overview of AI Techniques in Fraud Detection

Artificial intelligence (AI) is now used in combating fraud in the financial system, but this technology is necessary particularly in dealing with real-time transactions. Fraud detection and prevention is supported with the help of machine learning algorithms based on AI techniques that are implemented in handling communication of transaction data in real-time manner. The algorithms can identify suspicious patterns and abnormalities that otherwise could go unidentified and the response time of fraud prevention is fast.

One of the most common forms of AI in the fraud detection is supervised learning. The models in this method are designed by training them on labeled data sets where legitimate and fraud transactions are represented. Based on this training data, the algorithms that can be used to paint a picture of new transactions being fraudulent or legitimate include decision trees, random

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

forests, and logistic regression. Decision trees are useful since they (trees) subdivide data into branches according to decision-making rules, whereby the model can distinguish the most important variables or features that can confirm possible fraud. The technique of ensemble learning known as random forests is a combination of a number of decision trees to enhance the accuracy of predictions and decrease overfitting. Instead, a statistical model, logistic regression predicts the likelihood of an ongoing transaction to be a fraud, given some specified set of input features. With the amount of financial data and speed growing by the day, it is necessary to effectively organize and process such large volumes of data to retain the real-time abilities of fraud detection. By using scalable data store like MongoDB, AI models can process big data streams more efficiently to deliver timely and correct detection of big transaction network[10].

Unsupervised learning is another technology needed to detect fraud that does not require labeled data. Such algorithms as k-means clustering and autoencoders can be used. K-means clustering data points, groups them into clusters and cluster them based on similarity, which allows detecting unusual patterns or outliers that may point to a fraud. Neural networks that use autoencoders are designed to encode and decode information, which is why they tend to be handy at detecting anomaly in transaction data. Such unmonitored models are particularly useful to identify new types of fraud which have not been encountered in the past datasets. Reinforcement learning involves an AI process of refining its decision-making process in response to feedbacks. Appropriate in the context of fraud detection, reinforced learning models are able to evolve in real time as they learn through every interaction and feedback and improve their capacity to detect fraud. These models are especially useful in turbulent situations in which fraud schemes are changing at a fast pace.

3.2 Fraud detection in Real-Time Systems.

Real-time fraud detection is one of the most important elements of the contemporary financial system, as it guarantees that fraudulent transactions are detected and prevented in real time, prior to funds transfer. The fraud detection systems run with the help of AI analyze real-time transaction data and compare it to the historical data to identify suspicious behavior. One of the important tools in the AI systems is predictive fraud detection, where the information in the history of transactions is analyzed to forecast the possibility of the transaction happening to be fraudulent. With the aid of data comparing the peculiarities of a new transaction, i.e. the amount, the location and the frequency, the system can determine whether the ordeal transaction is abnormal. This prediction ability enables this to be detected before the transaction is processed and the loss of finance is avoided and as much as possible the disturbance of the legitimate user is minimal. As an example, the Decision Intelligence system by MasterCard utilizes AI to process millions of transactions in real time, and it calculates the risk of fraud using a combination of factors, including transaction history of the cardholder, geographic location, and type of merchant. With a combination of this data point, the platform is able to make decisions instantly, which can either approve or flag transactions to be reviewed again. Through this, real-time fraud prevention is just possible and this means there is a high chance of preventing fraud to be executed.

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Figure 3 shows the fraud detection process involves several key steps, including customer authentication, identifying relationships, creating association rules, and analyzing transaction patterns. These steps work in tandem to ensure that fraudulent activities are flagged and prevented in real-time, enhancing the security of financial transactions.

Figure 3: ***Fraud detection***

3.3 Secure Transactions with blockchain.

The blockchain technology presents an exclusive benefit in the process of financial transactions security. Whereas in the past, transaction data could be altered or distorted as it was recorded by a central repository, blockchain establishes a decentralized and unalterable registry capturing every transaction transparently. A transaction cannot be edited or deleted once it is being added to blockchain, which, at the same time, serves as a secure basis of financial transactions.

AI used together with blockchain will further speed up the detection of fraud in that they will offer a secure and tamper-free record of all transaction histories. AI systems have the capability to scan blockchain records in real-time, and this is what can detect abnormal activities or behaviors that can be a sign of fraudulent behavior. Blockchain is the reason behind the transparency and immutability of transactions, which is essential in providing tracing of all transactions that can be used in auditing and confirming authenticity of financial transactions. One application of blockchain in fraud detection is Ripple, a live cross-border payment network that is based on blockchain technology in order to trace international payments. The system offered by Ripple ensures that every transaction is documented in the blockchain to offer an inalienable record and can be accessed by all the involved parties. Such transparency along with the fraud detection provided by AI makes sure that the fraud cases may be eliminated and prevented even prior to impacting the transaction process [11].

3.4 Case Study: HSBC Fraud Detection by AI.

The case of HSBC as one of the largest banks globally represents a good example on how AI can be applied to detect fraud in real-time transactions. The bank handles transactions to the tune of more than one billion each month and as such, real time fraud detection is vital to the operations. In an effort to fight the increasing challenge of financial fraud, HSBC has adopted highly technological AIs in its fraud detection systems. Such artificial intelligent programs process large amounts of transaction data and identify suspicious acts on a historic basis of

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

behavioral patterns. Just as adaptive AI feedback software applied to measure and react to user activity in other applications like individualized learning and career advice, the fraud detection models also constantly improve their precision by learning new trends and consequences [12]. The dynamism in learning processes as exhibited by personalized recommendation systems through AI systems are able to adapt the responses according to requirements, and subsequently, refine prediction accuracy over time, proving that the enhancement of the idea of reliability in decision making in tons of complex situations, such as in banking fraud prevention [13]. Using adaptive intelligence in this way, the AI infrastructure provided by HSBC could serve as a model of how situational-aware algorithms could enhance resilience in the face of adaptable fraud schemes without impacting operational performance. With the help of AI, HSBC would be able to identify suspicious transactions on time and correctly. The AI models will take into account various aspects, including the number of transactions, address and frequency of the activity to detect abnormalities that are not part of the normal behaviour of a customer. In case of any transaction that is believed to be suspicious, it is questioned by default and in the event there is an urgency the transaction can be left pending until transfer of funds.

The HSBC man-made fraud detection system, which has been enhanced with AI, has ensured that the number of fraud cases in the firm has significantly been reduced and has saved the firm millions of dollars that could have been realized in terms of the fraudulent transactions [14]. The system is also dynamic and adaptive making sure that the system is practical in unraveling new patterns of fraud, as it acquires new tasks with time thus it provides HSBC with a dynamic and resolute approach to real-time fraud detection. These additions to the AI-powered scams-detection algorithms, as well as the capabilities of blockchain and the option of real-time surveillance, show how AI is gradually becoming handy in guaranteeing financial transactions. The additional specialization and integration of these technologies will be very important in addressing the ever evolving challenges of fraud in financial institution.

4. High-Performance Network Infrastructure for Real-Time Transactions

4.1 Designing Ultra-Low-Latency Networks

The demand to have ultra-low-latency networks cannot be quantified when dealing with real-time financial transactions. Latency is an important aspect of securing the safety and effectiveness of transactions processing because it is the time that the data requires to travel between points. A latency lower than 10 milliseconds (<10 ms) is prone to be required in a modern financial system to achieve fast and secure transactions, especially in AI-driven fraud detection systems. Even minimal delays in making transactions can mean that chances of identifying fraudulent activity have been missed since transactions in the system have to be processed, analyzed and grouped in real time before they can be completed. In order to accomplish this level of speed without undermining the security of the system, it is necessary to include more sophisticated security mechanisms directly into continuous integration and deployment (CI/CD) pipelines, so that the systems of AI-based fraud detection could be continuously tested, updated, and protected against any new vulnerabilities [15]. This DevSecOps-oriented approach allows organizations to maintain both the responsiveness and

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

robustness of their real-time fraud detection infrastructures, effectively balancing performance with security.

Financial transactions are time-sensitive and may cause a big loss in finance, customer dissatisfaction, or even non-compliance of the regulation. Reducing the risks related to it has led to the creation of ultra-low-latency networks, which has become a priority among financial institutions and payment platforms. 5G networks are one of the technologies that allow reducing transaction latency. The advent of the 5G technology has greatly decreased the time in which the data is being given to the recipient consequently, the network speeds and response times are greatly improved compared to the previous generations of mobile radio [16]. The 5G network allows the transmission of high bandwidth and the possibility to send data at the speed of up to 10 Gbps and significantly reduce the time lag down to 1 millisecond. This render 5G a perfect solution to real time financial transactions, given the fact that it can handle fast data processing and that fraud detection algorithms in place can process transactions real time without a lag. High efficiency of 5G also amplifies the capability to accommodate high amounts of transactions at once, which is significant when considering global financial systems at the size of global geographic coverage.

4.2 Network Performance Metrics.

Key measurements can be used to assess the performance of network infrastructure addressing financial transactions, e.g., transaction throughput and latency. VisaNet is such example, one of the largest and the most recognized payment networks in the world with an amazing processing capacity of 65,000 transactions/sec. The fact that VisaNet has been able to process this huge number of transactions with a high level of speed is an indication of the efficiency of the high-performance network infrastructure. An important aspect of VisaNet infrastructure is that it is capable of sustaining below 5 milliseconds (less than 5ms) of latency per transaction. This is to be achieved with the lowest possible latency which is very critical in making sure that the fraud detection system is able to analyze each transaction as it happens and immediate action is taken. The high speed response enables to identify fraud instantly, it means that VisaNet will be able to detect suspicious transactions and prevent fraudulent transactions until they are completed. VisaNet offers low latency and high throughput to make sure that the financial transactions are completed worldwide in a safe and efficient way. In the case of financial institutions and payment systems, it is essential to have networks that can withstand large volumes of transactions to be made and very low latency. This will help to ensure that AI-based fraud detection systems are not troublemakers and consequently ensure that potential threats which may have resulted in a fraud are prevented.

As depicted in the figure below, network performance metrics such as throughput, packet delivery ratio (PDR), and end-to-end (E2E) delay are essential for assessing the efficiency of financial transaction networks. VisaNet, for example, achieves impressive transaction throughput and maintains latency below 5 milliseconds, ensuring rapid fraud detection and secure financial processing.

Received: August 12, 2025

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

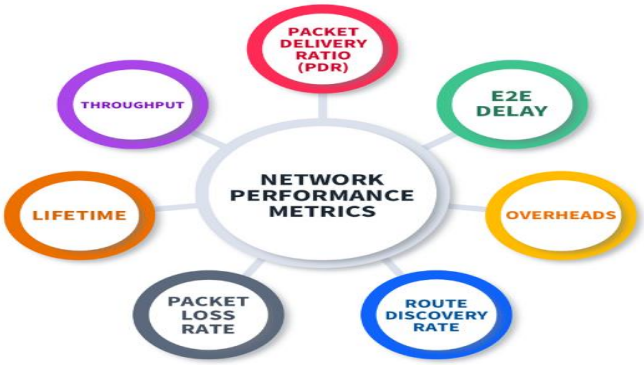

Figure 4: ***How to Leverage Performance Metrics and Sensors for Network Efficiency***

4.3 Case Study: Network Infrastructure of PayPal.

Another example of businesses that have utilized its network infrastructure to the fullest extends to PayPal, since it provides ultra-low-latency processing of transactions. Being one of the largest online payment system in the world, PayPal does millions of transactions in a single day and this means that a high-performance network is required to facilitate such transactions in the fastest time possible. In a bid to do this, PayPal uses Content Delivery Networks (CDNs) and fiber-optic lines to make sure that information is sent fast and efficiently through its network. CDNs are essential to enhance the performance of a network, through distributing data about various geographically distributed servers and thereby reducing the distance that the data would travel to a destination, thereby reducing latency. The implementation of CDNs by PayPal also guarantees it operates transactions with no unnecessary delays, even when the traffic peaks. Also, special fiber-optic lines of PayPal provide a furthering speed of transaction because of the direct and high-bandwidth channel of communication between the data centers and payment processors at PayPal. With this mix of CDNs and fiber-optic technology, PayPal can afford transaction latency of less than 3 milliseconds, which guarantees high processing speed and fraud detection.

PayPal's exceptional performance in secure and efficient payment processing can largely be attributed to its investment in low-latency, robust network infrastructure. By minimizing latency, PayPal ensures that its AI-powered fraud detection mechanisms can operate in real time, allowing the system to identify and block fraudulent transactions before they are finalized. This proactive approach not only enhances transaction security but also maintains a seamless customer experience by processing high volumes of payments without compromising speed or analytical accuracy. Underpinning this capability is the convergence of predictive analytics and DevOps efficiency, which enables PayPal to integrate continuous monitoring, model optimization, and automated deployment within its operational framework [17]. Through this synergy, PayPal's infrastructure combines the agility of DevOps with the foresight of predictive analytics, ensuring that fraud detection models remain adaptive, responsive, and effective in mitigating emerging digital threats across its global transaction ecosystem.

Received: August 12, 2025

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

With those, PayPal has proved how network infrastructure is of the utmost importance to facilitate the real-time processing of transactions and detecting fraud. With the ever-changing financial services shifting towards instant payment, the position of high-performance networks will only gain prominence in maintaining the security and integrity of financial transactions through the globe.

5. AI and Blockchain Integration for Fraud Detection

5.1 AI's Role in Blockchain for Financial Transactions

Artificial intelligence (AI) has served as a powerful means to fight fraud in the financial transaction, which has led to the integration of AI and blockchain technology. Blockchain make sure that a fast and secure, transparent, unaltered registry of the records of the transactions, AI, in its turn, enables to detect and prevent instances of fraud more efficiently by analysing the massive amounts of data on transactions in real time. These technologies are combined in a holistic manner to add up to enhance safeguard of financial systems. The potential of smart contracts is one of the most important opportunities of blockchain in fraud detection. Smart contracts refers to self-executing contracts containing rules and conditions coded in on the blockchain. When these conditions are fulfilled, the agreements automatically enforce and control the terms of the transaction automatically without the intervention of man. With the integration of AI and smart contracts, financial institutions will be able to automatize the fraud detection and fraud prevention process. There is continuous real-time detection of transaction indicators by AI systems, to detect possible fraudulent activity, and smart contracts promptly ensure the prevention of suspicious transactions or other protective actions. This resembles other areas of AI automation plans, like those driven by CI/CD enabled retail systems, where smart systems are both handling security vulnerabilities and operational controls to maximize performance and reduce risks [18]. In the financial sphere, it guarantees quick, automatic, and trustworthy reaction to the new threats, which would contribute greatly to the stability and reliability of the transaction systems.

Allowing smart contracts enables quicker and more competent detection of fraud, which should not have been detected manually. In case a transaction has been identified as a possible fraud, the smart contract may come to a halt, label the transaction as inspected, or even undo the transaction on the basis of predetermined security measures. The combination of AI and blockchain will increase the performance and scalability of fraud prevention systems so that the verification of financial transactions and validation are carried out in time.

One more important advantage of blockchain in fraud detection is the fact that records cannot be changed [19]. When a transaction is entered into a blockchain, it is not possible to modify or remove it, and as a result, it creates an indisputable and impeccable history of the transaction. This unchangeable history makes the financial system clean and practically unattainable by cheaters to tamper with transaction history. With the transparent ledger provided by blockchain and the analysis facilitated by Videosense, the institutions will be able to track their transactions in real-time, confirm their authenticity, and identify discrepancies that can be viewed as fraud

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

signs. This is further enhanced by the security guaranteed by the decentralized characteristics of blockchain, as such a risk of centralized points of failure does not exist. Since there is a multiplicity of copies of the ledger which are stored in a distributed network, and therefore, the copying of transaction records by a singled malicious actor is much more difficult to exploit without being detected. This transparency will make it hard to commit fraud undetected as well, and AI can analyze the data in a quick and precise manner.

5.2 Case Study of Fraud Detection at Deutsche Bank.

The Deutsche Bank, one of the most successful banking and financial institutions globally, is one of the brightest examples of successful implementation of AI and blockchain to address fraud issues. Deutsche Bank has pursued a parallel approach of leveraging AI and blockchain technology to increase the security and efficiency of the cross-border payment system, which, over the years has been a source of fraud in the financial institution due to the complexity of cross-border transfers as well as the financial institutions involved. Because many middle men are involved in the process of cross-border payment, costs are usually very high since each of them has their own records and systems of transactions [20]. This sophistication is further exposing the possibility of fraud because, one might not be in a position to track and authenticate every action during payment processing. To counter such a weakness, Deutsche Bank has adopted a system which combines AI and blockchain to develop a risk-free and more open structure of cross-border transactions. Blockchain offers an effluvial and real-time system of all the transaction in a blockchain that enables every member of the payment network to audit and verify the history of transactions in real-time. Similarly to the advancements in telematics to manage the fleet, the cross-border payment is not only cheap and more secure, but also much more resilient to fraud the implementation of AI and blockchain guarantees [21].

However, AI is an extension of machine learning to examine the volume of transaction data available in large quantities to determine the trends and abnormalities that could be indicative of fraud. The machine learning algorithms will continuously refresh themselves with new information and the system continues to evolve and keep pace with the emerging techniques of fraud. The prediction of suspicious behavior by artificial intelligence is possible, and it is combined with blockchain transparency that lets Deutsche bank prevent swindled transactions before they take effect.

The results of this integration have been magnificent. Deutsche Bank has the opportunity to reduce cross-border fraud by 30 per cent in two years, showing that the implementation of a mixture of blockchain and AI was effective in fraud prevention. Not only did the speed at which fraudulent transactions could be identified increase due to the application of AI in this system, but it also gave the bank a chance to simplify the mechanisms of issuing and receiving cross-border payments. Blockchain non-modifiable record provided a clear and auditable trail of all transactions, reducing the effect of errors and fraud and making the system more transparent on a general basis. As it is reported in this case study, AI in combination with blockchain could be useful in the detection of fraud within the financial systems. With both technologies, DuBoise Bank has come up with a safer and more effective cross border payment infrastructure that has reduced gains of the scam which is a positive contribution to the overall purity of the

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

payment. The growth of AI and blockchain by financial institutions can make this trend even more popular, and the tendency provides a viable solution to the growing issue of financial-related fraud.

Figure illustrates the conceptual framework for AI adoption in fraud detection, with transparency, algorithmic bias, and fairness perception influencing trust and regulatory compliance, which in turn drive AI adoption.

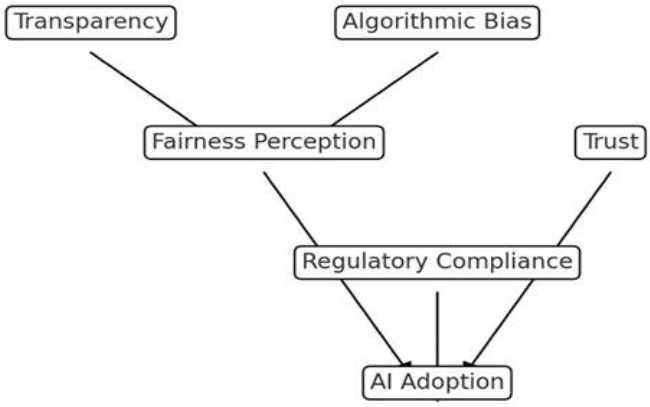

Figure 5: Conceptual framework diagram.

6. Methodology

6.1 Data Collection

The growth of the successful models of detecting fraud used in real-time fiscal operations relies heavily on gathering of big and varied data sets. Such datasets are necessary in order to train the model that is capable of detecting fraudulent activity. In order to make sure that the models reflect the large variety of users of variations of a real-life transactions, a heterogeneous and extensive dataset is to be assembled. Startups that have been tested to be reliable sources of data are recognized financial institutions and payment processors like Stripe, Visa, and Mastercard that provide service to a massive number of transactions across the world. These channels are rich in data with important elements of transactions including transaction values, geographical location, time, type of merchant, user data, and device data. Such variety of data plays a vital role in teaching fraud detection models to learn a normal pattern of transactions and identify abnormal to detect a fraud [22;23].

In the case of supervised learning processes, labeled data is essential, both transaction data is labeled as either an outlier or as a legitimate transaction. The detection of the fraudulent transactions is done manually, in accordance with the existing fraud detection schemes, which forms a labeled dataset to train the models. Such datasets integrate both authentic and fraudulent records and this enables such a model to generalize well and to identify fraud in the subsequent transactions. The data will be reliable and obtained to secure the reliability of the information since it will be obtained with the help of reputable financial organizations, and payment processors that are familiar with operating safe and high-volume transactions. This makes sure that the data sets are correct, full and reflect the actual behavior of transactions in

Received: August 12, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

the real world. This labeling is strictly carried out to prevent any mistake during model training to increase the performance of the fraud detection models that are obtained.

6.2 Fraud Detection Models

The fraud detection models utilize machine learning algorithms that identify trends and patterns associated with fraudulent transactions. These algorithms are optimized using performance metrics, such as precision, recall, F1-score, and Area Under the Curve (AUC), to evaluate the model's ability to detect fraud while minimizing false positives and false negatives.

One widely used algorithm is Random Forests, an ensemble learning technique that operates by generating multiple decision trees using random subsets of the data. The outputs of these trees are aggregated to produce a final decision. This method is particularly effective when dealing with large, complex datasets, as it reduces overfitting, especially when data is noisy or incomplete. In fraud detection, key features such as transaction volume, frequency, and geographic location are used to differentiate between legitimate and fraudulent transactions. The model's performance is further enhanced by operating in secure, high-integrity environments, similar to protection mechanisms found in enterprise systems, ensuring that the predictions remain accurate and trustworthy [24].

Another effective fraud detection technique is Deep Neural Networks (DNNs), which are adept at identifying complex, high-dimensional patterns in data. DNNs utilize multiple layers of synthetic neurons to learn intricate patterns in transaction data, making them especially useful for detecting new or previously unseen forms of fraud. While training DNNs requires substantial labeled data and high computational power, they are highly effective in adapting to evolving fraud tactics [25].

To evaluate the effectiveness of these models, various performance metrics are used. Precision measures the proportion of predicted fraudulent transactions that are truly fraudulent, minimizing false positives (legitimate transactions flagged as fraud). Recall, or sensitivity, represents the percentage of actual fraudulent transactions detected by the model, reducing false negatives (fraudulent transactions that go undetected). F1-score is a balanced metric combining precision and recall, providing a single evaluation of model performance. AUC measures the model's ability to distinguish between legitimate and fraudulent transactions, with higher AUC values indicating better overall performance, especially in cases where fraud is rare.

As shown in the figure above, AI and machine learning techniques, such as ensemble learning, predictive analysis, and anomaly detection, significantly enhance fraud detection accuracy by identifying complex patterns and anomalies, enabling faster, more reliable identification of fraudulent activities.

Received: August 12, 2025

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

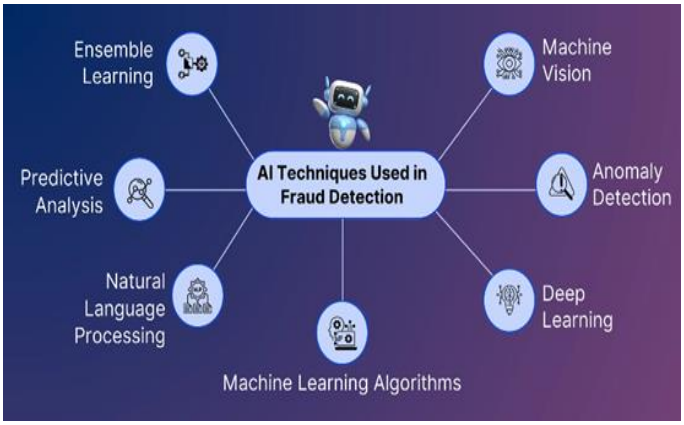

Figure 6: ***How Does AI/ML Improve Fraud Detection Accuracy***

6.3 Network Infrastructure installation.

After development and training of the fraud detection models, they need to be put into test in a live operational environment where the infrastructure should be high performance network infrastructure that would be able to handle real-time transaction data. The effectiveness of AI-driven fraud detection systems may be compromised by any type of delay with the response time. Hence, a network environment that facilitates ultra-low-latency processing must be in place to make sure that fraudulent activities remain detected and addressed at the earliest opportunity [26].

A testbed environment is established, which approximates a real-life financial network of transactions. It is an architecture where high-performance servers, well-configured network links, and low-latency communication patterns are used to enable fraud detection models to be deployed and refined using real-time conditions. The network infrastructure connects as well with high-speed internet connections i.e., fiber-optic networks or more recent 5G technology, which deliver low-latency and high-throughput connections, which means fast data transfer and delays in fraud detection are avoided.

Several types of financial transactions are carried out such as credit card purchases, bank transfers, and even cross-border transactions in order to approximate real-world conditions. The models of fraud detection are tested in terms of their effectiveness to detect fraud within the context of real life situations. With the help of such testing process, the fraud detection algorithms can be optimized as well as the network infrastructure in order to guarantee minimal delays as well as high effectiveness. The internalization and feedback of the continuous simulation can help the system to evolve to the new pattern of fraud, making the fraud detection system in line with the latest and updated threats [27].

7. Experiments and Results

7.1 Fraud Detection Performance

It is through this that the performance of fraud detection models is measured in terms of identifying the right transactions (fraud transaction) without causing errors, whether false gains

Received: August 12, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

(legitimate transactions being classified as fraud) or false losses (fraudulent transactions that are not picked up). In the given research, a group of AI models were experimented on in order to determine their ability to recognize fraud in real-time transactions in the financial sector. The accuracy rate was at 94 percent with the Random Forest model which is an ensemble technique. In this algorithm, numerous decision trees are created and the results are used to make an average to minimize overfitting and also enables better prediction efficiency. Although the Random Forest model was good it still had moderate false positive results particularly in situations where the transactions vary quickly and this is complex. Stability and speed are the positive aspects of the model, thus it can fit environments where there are only a few computational resources [28].

Deep Neural Networks (DNNs), conversely, were a type of deep learning which scored higher at 97 percent accuracy in detecting fraudulent transactions. High-level patterns and associations in the data can be detected by the DNNs using more than one processing layer, and thus, they can be highly useful in detecting complex fraud schemes and handling unstructured data with many interacting variables. DNNs were also more accurate in comparison to Random Forests due to their ability to identify more nuanced and dynamic indicators of fraud compared to traditional models. Nevertheless, large datasets and computational resources are needed to train the DNNs making them inefficient in some cases. The performance of these models is similar to the role of dynamic notification systems in healthcare, where real-time data processing and immediate response are necessary to successfully detect fraud [29]. The major conclusion of these experiments is the trade-off between the complexity and the computation requirement of the model. Random Forests are less accurate, however, much more stable and therefore faster, whereas DNNs are more accurate, yet more work-intensive and time-consuming.

Figure 7 illustrates a comparison between Random Forest and Deep Neural Networks (DNNs) in fraud detection. It highlights the differences in accuracy, false positives, and processing time, showcasing the trade-offs between model complexity, speed, and detection performance.

Received: August 12, 2025

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

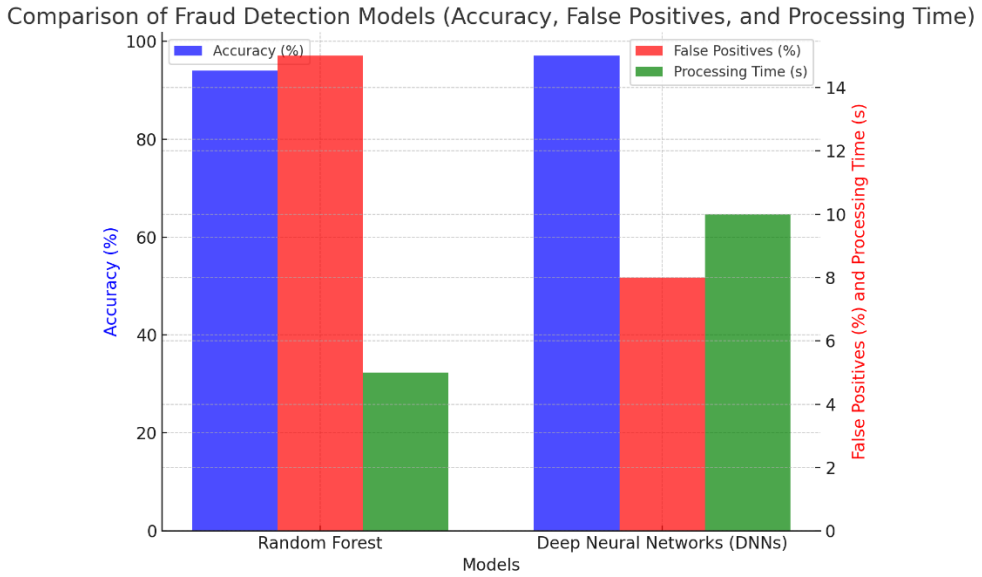

Figure 7: performance of the Random Forest and Deep Neural Networks (DNNs) models in fraud detection.

7.2 Network Performance

The defrauding systems performance is also very dependent on the networked infrastructure employed to conduct transactions. Still-up-to-date detecting fraud needs ultra-low-latency networks that can act within milliseconds in order to implement a timely reaction [30]. This part compares fiber-optic network and 5G network with the functioning of transactions.

Fiber-optic is still considered to be the standard of the high-speed and low-latency data transmission, though it has a significant bandwidth and small latency. It was experimentally demonstrated that fiber-optic networks minimized latency to less than 5ms, necessary to detect and block fraudulent transactions in fraud detection models. Nevertheless, the 5G technology with its ultra-low latency and high throughput enhanced speed and reliability of fraud detection as 5G networks enabled the financial institutions to conduct transactions in a substantially higher rate than in any traditional configuration of a network. This allows fraud detection algorithms to interact with transactions on-the-fly, immediately, and therefore avoid any misbehavior on its trail.

A good example of the performance network infrastructure is the VisaNet, which handles up to 65000 transactions a second and had a 99.99 uptime. VisaNet has less than 2ms average transaction time so that the fraud detection systems can work at a high speed, which detects and prevents fraud at minimum delay. One of the experiments proved that fiber-optic and 5G networks are both suitable when it comes to detecting fraud in real-time, with the latter having a clear edge in speed and reliability of making transactions. These findings support the significance of high-performance network infrastructure towards supporting real-time fraud detection systems. Fraud detection algorithms can run more effectively with the development of network technologies such as fiber-optics and the 5G, whereby financial transactions are processed faster and more secure.

Received: August 12, 2025

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

As illustrated in the figure below, effective fraud detection systems are crucial in ensuring that networks are both scalable and reliable, while minimizing risks. Systems must be regulatory-friendly, ready for the future, and customer and manager-friendly to succeed.

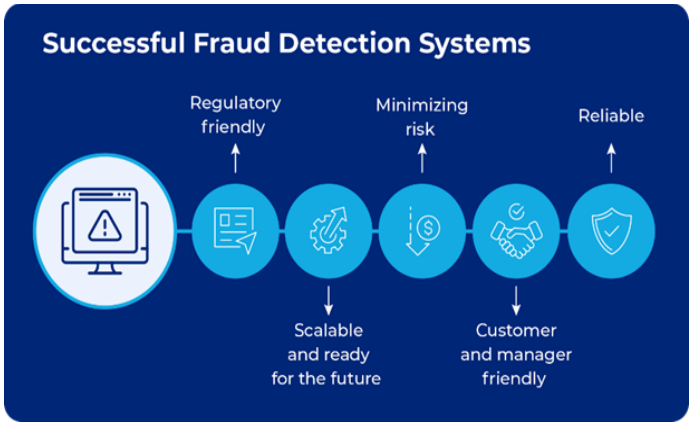

Figure 8: ***How AI Fights Banking Fraud in Real Time***

8. Discussion

8.1 Challenges and Limitations

The trade-off between false positives and false negatives is one of the main problems of fraud detection systems, and those that operate with AI, in particular, are false positives [31]. The legitimate transactions are wrongly identified as being fraudulent, which can result in customers and merchants suffering unnecessary friction. False negatives, however, are even worse as they imply fraudulent transactions are processed and finalized unnoticed and unimpeded.

One of the most challenging problems that need to be solved in the fraud detention systems design is to strike the right balance between false negatives and false positive. Although, the higher the sensitivity with a model, the greater the probability of detecting a fraudulent activity (improving recall), this can lead to more false positives. On the other hand, the reduction of false positives can cause the system to ignore the real cases of fraud. This is why it is necessary to fine-tune the model to find a plausible compromise where both of these types of errors do not severely disrupt the performance of the system. Like generative AI models of medical diagnosis, where synthetic data are applied to learn algorithms to achieve more accurate, but not overfitted detection, and transformer-based and other neural network designs in visual question answering, which trade-off sensitivity and specificity to achieve reliable performance, fraud detection models should strike a sensitive and specificity balance on complex, dynamic data [32;33].

8.2 AI Model Limitations

Although AI has already shown a very positive response in fraud detection, it is not completely devoid of drawbacks [34]. The reliance on the past is one of the critical shortcomings. Supervised learning models heavily depend on historical transaction information in order to predict and train AI models to commit fraud. Nonetheless, it may be harmful when fraudsters come up with innovative strategies that do not follow the previous trends. The development of

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

AI models might be less effective in detecting new ways of attack due to the development of fraud. This emphasizes the need to constantly revise models using new information and make sure that they can address new threats. The other weakness of AI in fraud detection is that it is mostly black-box with the practices of complex models, including deep neural networks, not necessarily transparent. Such unaccountability may be an inconvenience in regulated markets, where financial institutions are required to explain their decisions to detect fraud to the regulators and to provide explanations to the customers. The fact that it is impossible to completely understand the way AI systems can reach their conclusions may restrain the use of these technologies in some sectors.

8.3 Future of AI in Fraud Detection.

The AI future regarding fraud detection is full of promise particularly in the area of AI explainability and quantum computers. The interpretability of AI is becoming an important criterion, especially in highly regulated industries, especially in finance. Continued studies are undertaken to come up with algorithms that will enable AI models to be more interpretable so that bankers can know exactly how and why this or that transaction is being considered as fraudulent. This level of transparency not only helps address regulatory compliance but it assists in building trust with clients, who will tend to be more accommodative of AI-based judgments once they can determine the logic behind the scoring. Similarly to the integration of AI in customer relationship management (CRM) and sales operations of enterprises, where explainable AI promotes better decision making, customer retention, and governance of scalable systems, interpretability of model fraud detection is associated with the effectiveness of the operations of these systems and the trust of stakeholders [35;36].

Going even deeper into the future, the role that quantum computing can have in AI-enabled fraud detection cannot be overlooked [37]. However, quantum computing can compute very large volumes of data much faster than classical computers are able to. With AI models, quantum computing would be able to detect fraud considerably quicker, allowing millions of transactions to be analyzed in real-time and with even higher accuracy. Quantum algorithms would allow tackling optimization issues and analyzing data in previously unachievable ways using quantum algorithms would be offering financial institutions an unmatched power to fight fraud on-the-fly.

Chart below illustrates the network performance for fraud detection across different types of networks. As shown in the figure, fiber-optic networks have a latency of less than 5ms, while 5G networks reduce latency to less than 2ms, significantly enhancing real-time fraud detection.

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

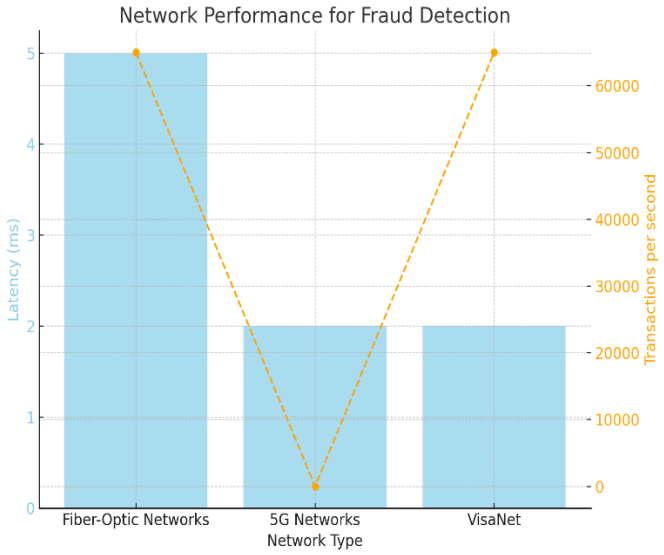

Figure 9: network performance for fraud detection

8.4 Case Study of Future Potential of AI JPMorgan Chase.

JPMorgan Chase has been among the pioneers to consider integrating quantum computing in its fraud detection machines, specifically in high-frequency trading [38]. Thousands of transactions are carried out in such markets in a second, and the possibility of fraud is high. JPMorgan is beginning to trial quantum computing in order to expedite real-time fraud detection and boost the security of its trading systems [39]. Through quantum computing, JPMorgan has the potential to significantly enhance both the efficiency and effectiveness of its fraud detection processes. Quantum systems can process vast volumes of trading data at unprecedented speeds, enabling the bank to identify and respond to malicious activities far more quickly than conventional computing methods allow. The advancement of quantum technology opens up substantial opportunities to transform real-time fraud detection, particularly in high-frequency trading systems, resulting in financial markets that are not only faster but also more secure. Similar to the improvements seen in advanced computational techniques for tasks like image captioning—where innovative algorithms dramatically increase processing efficiency and accuracy—quantum computing in finance can optimize the detection of complex fraud patterns and support robust, real-time decision-making in large-scale transactional environments [40].

Table below shows AI explainability is crucial for regulatory compliance and building trust with clients, while quantum computing in AI helps process vast amounts of data in real-time, enhancing fraud detection accuracy.

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Table 1: ***future of AI in fraud detection***

Future Aspect	Description	Benefits	Examples / Applications
AI Explainability	Making AI models interpretable so that institutions understand how and why transactions are flagged as fraudulent.	- Regulatory compliance- Builds trust with clients- Enhances decision-making	- Integration in CRM systems- Enterprise sales operations- Fraud detection model transparency
Quantum Computing in AI Fraud Detection	Using quantum computing to process massive volumes of data faster than classical computers, enabling AI models to detect fraud in real time.	- Real-time analysis of millions of transactions- Higher accuracy in fraud detection- Tackling complex optimization problems	- High-frequency trading fraud detection- Large-scale transaction monitoring in banks- AI-powered financial market security

9. Conclusion

The application of artificial intelligence (AI) in real-time to detect fraud has today become one of the unquestionable assets in the realm of the financial sector and payment systems that alter the way the operations of financial institutions are secured. Due to advanced machine learning, AI systems can analyze the massive amount of data on the transactions in real time and attend to patterns of fraud and anomalies with remarkable speed and accuracy. The AI systems that will simplify identification of fraud will be essential in ensuring that fraud is prevented by identifying it early enough before occurrence before affecting the financial institutions and clients. These systems have evolved to become highly effective in identifying and complying to the new trends of frauds and can contribute to the enhanced security of the financial transaction in the dynamic environment.

Received: August 12, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Smart algorithms are only one of the aspects of conversation on AI efficiency in detecting fraud. In the defense of modern financial systems, it is important to combine the forces of ultra-low-latency networks and AI. Live financial transactions are also quite challenging regarding the advanced methods of those frauds detection and devices required to implement it in time. The application of the use of fiber-optic networks and 5G technologies is necessary in the scenario in which it is necessary to ensure that the transactions are processed within the shortest time possible and the systems of AI can promptly analyze the transactions and make immediate decisions. However, having AI predictive capabilities integrated with low-latency networks and record speeds will offer a potent framework that can help prevent fraud within seconds and ensure the continued safety of financial institutions by countering threats. Regarding the future perspective, AI in fraud detection has a bright future. The further development of AI technologies, including deep learning, natural language processing, and reinforcement learning, will help improve the scheme for detecting suspicious fraud with even greater precision. The new technologies will likely transform the process of fraud detection into an active rather than a reactive one, and AI systems will anticipate and prevent fraud even before it occurs. The next generation of network infrastructures, namely 5G, will be further developed, enabling real-time operations to be performed much faster and more reliably, thereby enhancing the real-time performance of AI systems.

Quantum computing is also expected to incorporate AI-based fraud detection in the near future, likely revolutionizing the field. Quantum computing can perform significantly more data processing and far faster than can currently be done, which may enhance the detection and prevention of fraud many times over, particularly in high-frequency trading and cross-border transactions. AI and ultra-low-latency networks play a crucial role in ensuring the safety of financial transactions worldwide, as the world becomes increasingly digital. Financial institutions will be more convinced of the need to protect their customers, prevent fraud, and maintain the integrity of the economic system as technology continues to evolve through innovations. The AI in fraud detection can be taken to even greater levels in the future, and the actual research and development point to the future of making the fraud prevention mechanisms more efficient and effective.

References;

[1] Ambashtha, K. L., & Kumar, P. (2023). Online fraud. In *Financial crimes: A guide to financial exploitation in a digital age* (pp. 97-108). Cham: Springer International Publishing. https://link.springer.com/chapter/10.1007/978-3-031-29090-9_7

[2] Bonthu, C. (2025). Unifying multiple ERP systems: A case study on data migration and integration. *Utilitas Mathematica.* https://utilitasmathematica.com/index.php/Index/article/view/2785

[3] Bonthu, C., & Goel, G. (2025). Autonomous supplier evaluation and data stewardship with AI: Building transparent and resilient supply chains. *International Journal of*

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Computational and Experimental Science and Engineering. https://ijcesen.com/index.php/ijcesen/article/view/3854/1154

[4] Gupta, P. (2023). Leveraging machine learning and artificial intelligence for fraud prevention. *SSRG International Journal of Computer Science and Engineering*, *10*(5), 47-52. https://validit.ai/wp-content/uploads/2023/09/0c6d0a_793e0cb0b0b845fc8f9b493ceefc8ce3-1.pdf

[5] Chadha, K. S. (2025). Zero-trust data architecture for multi-hospital research: HIPAA-compliant unification of EHRs, wearable streams, and clinical trial analytics. *International Journal of Computational and Experimental Science and Engineering*, *12*(3), 1–11. https://ijcesen.com/index.php/ijcesen/article/view/3477/987

[6] Rehan, H. (2021). Leveraging AI and cloud computing for Real-Time fraud detection in financial systems. *Journal of Science & Technology*, *2*(5), 127. https://orcid.org/0009-0003-0774-5777

[7] Chavan, A. (2022). Importance of identifying and establishing context boundaries while migrating from monolith to microservices. Journal of Engineering and Applied Sciences Technology, 4, E168. http://doi.org/10.47363/JEAST/2022(4)E168

[8] Chavan, A. (2024). Fault-tolerant event-driven systems: Techniques and best practices. Journal of Engineering and Applied Sciences Technology, 6, E167. http://doi.org/10.47363/JEAST/2024(6)E167

[9] Rane, N., Choudhary, S., & Rane, J. (2023). Blockchain and Artificial Intelligence (AI) integration for revolutionizing security and transparency in finance. *Available at SSRN 4644253*. https://dx.doi.org/10.2139/ssrn.4644253

[10] Dhanagari, M. R. (2024). Scaling with MongoDB: Solutions for handling big data in real-time. *Journal of Computer Science and Technology Studies, 6*(5), 246-264. https://doi.org/10.32996/jcsts.2024.6.5.20

[11] Turksen, U., Benson, V., & Adamyk, B. (2024). Legal implications of automated suspicious transaction monitoring: enhancing integrity of AI. *Journal of Banking Regulation*, *25*(4), 359-377. https://link.springer.com/article/10.1057/s41261-024-00233-2

[12] Karwa, K. (2023). AI-powered career coaching: Evaluating feedback tools for design students. Indian Journal of Economics & Business. https://www.ashwinanokha.com/ijeb-v22-4-2023.php

[13] Karwa, K. (2024). Navigating the job market: Tailored career advice for design students. *International Journal of Emerging Business*, *23*(2). https://www.ashwinanokha.com/ijeb-v23-2-2024.php

[14] von Struensee, S. (2021). Analyzing Dilemmas Posed by Artificial Intelligence and 4IR Technologies Requires using all Available Models, Including the Existing International Human Rights Framework and Principles of AI Ethics. *Including the*

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Existing International Human Rights Framework and Principles of AI Ethics (June 25, 2021). https://dx.doi.org/10.2139/ssrn.3874279

[15] Konneru, N. M. K. (2021). Integrating security into CI/CD pipelines: A DevSecOps approach with SAST, DAST, and SCA tools. *International Journal of Science and Research Archive*. Retrieved from https://ijsra.net/content/role-notification-scheduling-improving-patient

[16] Cheng, X., Fang, L., Yang, L., & Cui, S. (2017). Mobile big data: The fuel for data-driven wireless. *IEEE Internet of things Journal*, *4*(5), 1489-1516. https://doi.org/10.1109/JIOT.2017.2714189

[17] Kumar, A. (2019). The convergence of predictive analytics in driving business intelligence and enhancing DevOps efficiency. International Journal of Computational Engineering and Management, 6(6), 118-142. Retrieved from https://ijcem.in/wp-content/uploads/THE-CONVERGENCE-OF-PREDICTIVE-ANALYTICS-IN-DRIVING-BUSINESS-INTELLIGENCE-AND-ENHANCING-DEVOPS-EFFICIENCY.pdf

[18] Malik, G., Brahmbhatt, R., & Prashasti. (2025). AI-driven security and inventory optimization: Automating vulnerability management and demand forecasting in CI/CD-powered retail systems. *International Journal of Computational and Experimental Science and Engineering.* https://ijcesen.com/index.php/ijcesen/article/view/3855/1153

[19] Ashfaq, T., Khalid, R., Yahaya, A. S., Aslam, S., Azar, A. T., Alsafari, S., & Hameed, I. A. (2022). A machine learning and blockchain based efficient fraud detection mechanism. *Sensors*, *22*(19), 7162. https://doi.org/10.3390/s22197162

[20] Sule, A. K., Eyo-Udo, N. L., Onukwulu, E. C., Agho, M. O., & Azubuike, C. (2024). Implementing blockchain for secure and efficient cross-border payment systems. *International Journal of Research and Innovation in Applied Science*, *9*(12), 508-535. https://doi.org/10.51584/IJRIAS.2024.912047

[21] Nyati, S. (2018). Transforming telematics in fleet management: Innovations in asset tracking, efficiency, and communication. International Journal of Science and Research (IJSR), 7(10), 1804-1810. Retrieved from https://www.ijsr.net/getabstract.php?paperid=SR24203184230

[22] Pinnapareddy, N. R. (2025). Carbon conscious scheduling in Kubernetes to cut energy use and emissions. *International Journal of Computational and Experimental Science and Engineering.* https://ijcesen.com/index.php/ijcesen/article/view/3785

[23] Pinnapareddy, N. R. (2025). Cloud cost optimization and sustainability in Kubernetes. *Journal of Information Systems Engineering and Management.* https://www.jisem-journal.com/index.php/journal/article/view/8895

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[24] Rajgopal, P. R. (2025, August). Secure enterprise browser – A strategic imperative for modern enterprises. *International Journal of Computer Applications, 187*(33), 53–66. https://doi.org/10.5120/ijca2025925611

[25] Rajgopal, P. R. (2025, October). SOC talent multiplication: AI copilots as force multipliers in short-staffed teams. *International Journal of Computer Applications, 187*(48), 46–62. https://doi.org/10.5120/ijca2025925820

[26] Bello, O. A., Ogundipe, A., Mohammed, D., Adebola, F., & Alonge, O. A. (2023). AI-driven approaches for real-time fraud detection in US financial transactions: Challenges and opportunities. *European Journal of Computer Science and Information Technology*, *11*(6), 84-102. https://www.eajournals.org/

[27] Alimi, I. A., Patel, R. K., Muga, N. J., Pinto, A. N., Teixeira, A. L., & Monteiro, P. P. (2021). Towards enhanced mobile broadband communications: A tutorial on enabling technologies, design considerations, and prospects of 5G and beyond fixed wireless access networks. *Applied Sciences*, *11*(21), 10427. https://doi.org/10.3390/app112110427

[28] Raju, R. K. (2017). Dynamic memory inference network for natural language inference. International Journal of Science and Research (IJSR), 6(2). https://www.ijsr.net/archive/v6i2/SR24926091431.pdf

[29] Sardana, J. (2022). The role of notification scheduling in improving patient outcomes. *International Journal of Science and Research Archive*. Retrieved from https://ijsra.net/content/role-notification-scheduling-improving-patient

[30] Ji, Y., Zhang, J., Xiao, Y., & Liu, Z. (2019). 5G flexible optical transport networks with large-capacity, low-latency and high-efficiency. *China Communications*, *16*(5), 19-32. https://doi.org/10.23919/j.cc.2019.05.002

[31] Olushola, A., & Mart, J. (2024). Fraud detection using machine learning. *ScienceOpen Preprints*. https://www.scienceopen.com/hosted-document?doi=10.14293/PR2199.000647.v1

[32] Singh, V. (2021). Generative AI in medical diagnostics: Utilizing generative models to create synthetic medical data for training diagnostic algorithms. International Journal of Computer Engineering and Medical Technologies. https://ijcem.in/wp-content/uploads/GENERATIVE-AI-IN-MEDICAL-DIAGNOSTICS-UTILIZING-GENERATIVE-MODELS-TO-CREATE-SYNTHETIC-MEDICAL-DATA-FOR-TRAINING-DIAGNOSTIC-ALGORITHMS.pdf

[33] Singh, V. (2022). Visual question answering using transformer architectures: Applying transformer models to improve performance in VQA tasks. Journal of Artificial Intelligence and Cognitive Computing, 1(E228). https://doi.org/10.47363/JAICC/2022(1)E228

[34] Kamuangu, P. (2024). A review on financial fraud detection using ai and machine learning. *Journal of Economics, Finance, and Accounting Studies*, *6*(1), 67.

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

https://www.researchgate.net/profile/Paulin-Kamuangu-2/publication/378142600_A_Review_on_Financial_Fraud_Detection_using_AI_and_Machine_Learning/links/65c9981679007454977d9541/A-Review-on-Financial-Fraud-Detection-using-AI-and-Machine-Learning.pdf

[35] Subham, K. (2025). Integrating AI into CRM systems for enhanced customer retention. *Journal of Information Systems Engineering and Management.* https://www.jisem-journal.com/index.php/journal/article/view/8892

[36] Subham, K. (2025). Scalable SaaS implementation governance for enterprise sales operations. *International Journal of Computational and Experimental Science and Engineering.* https://ijcesen.com/index.php/ijcesen/article/view/3782

[37] Kaal, W. A. (2024). Quantum Economy and the Future of Work. *Available at SSRN 4900880*. https://dx.doi.org/10.2139/ssrn.4900880

[38] Fatunmbi, T. O. (2024). Advanced frameworks for fraud detection leveraging quantum machine learning and data science in fintech ecosystems. https://www.researchgate.net/publication/390667808_Advanced_frameworks_for_fraud_detection_leveraging_quantum_machine_learning_and_data_science_in_fintech_ecosystems

[39] Ganapathy, A. (2021). Quantum computing in high frequency trading and fraud detection. *Engineering International*, *9*(2), 61-72. https://pdfs.semanticscholar.org/5c94/78db47395fa8b5ddf758f06bb3a9070c86de.pdf

[40] Sukhadiya, J., Pandya, H., & Singh, V. (2018). Comparison of Image Captioning Methods. *INTERNATIONAL JOURNAL OF ENGINEERING DEVELOPMENT AND RESEARCH*, *6*(4), 43-48. https://rjwave.org/ijedr/papers/IJEDR1804011.pdf

Received: August 12, 2025