International Journal on Science and Technology (IJSAT)
E-ISSN: 2229-7677 ● Website: www.ijsat.org ● Email: editor@ijsat.org

Machine Learning for Fraud Detection in Financial Transactions

Srinivasa Kalyan Vangibhurathachhi

Srinivasa.Kalyan2627@gmail.com

Abstract

As the global financial systems become more globalized and digitized, the threats of financial fraud are becoming massive accounting over $5 trillion annually, and sophisticated as cyber criminals ever-changing tactics. The traditional rule-based fraud detection systems that institutions have relied on are unable to meet this escalating challenge due to their inflexibility, high false-positive rates, and inability to process large-scale data in real-time. Machine learning offers an impressive alternative with transformative solutions that leverage predictive analytics models, anomaly detection, and adaptive learning to boost systems' accuracy, scalability, and responsiveness in fraud detection.

This article investigates the application of supervised, unsupervised, and deep learning machine learning techniques in detecting credit card fraud, identity theft, and cryptocurrency scams, highlighting their advantages over conventional methods. The article also highlights the challenges that machine learning techniques need to grapple with through more research and investment to be more efficient, such challenges include data imbalance, regulatory constraints, computational costs, and model interpretability.

Keywords: Machine Learning, Fraud Detection, Financial Transactions, Anomaly Detection, Cybersecurity, Deep Learning, Regulatory Challenges

1. INTRODUCTION

Globally, the threat of financial fraud is rising steadily. According to the Association of Certified Fraud Examiners (ACFE), fraud-related financial losses amounted to $5 trillion as of 2024, with the financial sector being the most affected (Veno, 2024). With digital payment space alone, credit card fraud alone accounted for $33.83 billion in losses in 2023, with projections suggesting that this figure could rise to over $43 billion by 2026 (Nilson Report, 2024; Rej, 2023). The challenge is further highlighted by the fact that there were 416,582 cases of credit card fraud in 2024 (Castillo, 2024). In recent years, the rapid growth of online banking, mobile payments, and cryptocurrency exchanges has created new opportunities for cybercriminals, making fraud detection both more complex and critically urgent.

The dynamics of financial fraud are continuously evolving, with cyber criminals deploying progressively sophisticated techniques and capabilities to exploit vulnerabilities in financial systems and transaction systems. The most common form of financial fraud is credit card fraud, where stolen details are used for unauthorized purchases as well as identity theft whereby fraudsters develop synthetic identities to open fake accounts, there were 1,135,291 cases in 2024 (Caporal, 2025). Another major

financial concern is money laundering, with the criminals using multiple transactions and techniques to obscure the origin of illicit funds. UN estimates that 2–5% of global GDP (800B–2 trillion annually) is laundered through layered transactions (United Nations, 2024). With the rapid adoption of cryptocurrency, there are new forms of fraud such as 'rug pulls', where crypto developers create fraudulent projects to attract speculative investment before disappearing with the funds (Gerken (2025).

As cyberattacks within the financial systems have become more sophisticated, the existing methods and systems, which usually rely on rule-based approaches, of fraud detection and mitigation have struggled to adapt to emerging fraud tactics. They also generate high numbers of false positives, transactions incorrectly classified as fraudulent, making them ineffective, particularly when dealing with massive volumes of transactions. To mitigate these shortcomings, financial institutions globally are rapidly integrating machine learning algorithms in their systems, to enable large-scale analysis of large transaction datasets in real-time to effectively and efficiently identify complex fraud patterns that traditional methods often miss. Machine learning-powered fraud detection systems have been shown to reduce fraud losses by up to 30% by improving detection accuracy and minimizing disruptions for legitimate customers by eliminating false positives and negatives (Finextra Research, 2025). The effectiveness of Machine learning-based fraud detection depends on the quality and diversity of data sources. Financial institutions use a combination of transaction history, geolocation data, device fingerprints, behavioural analytics, and external threat intelligence to train their models (Ashraf and Schaffer, 2024). For example, banks analyze customer spending behaviour to create a profile of deviations that could indicate fraud, including sudden large transaction in a foreign country when a user has never traveled abroad. Furthermore, companies like Mastercard AI-powered fraud scoring systems to assess transaction risk based on patterns across millions of merchants and cardholders worldwide (Browne, 2024).

Despite its advantages in enhancing fraud detection, Machine learning-driven fraud detection faces several challenges. One of the biggest hurdles is data imbalance, where fraudulent transactions constitute only a tiny fraction (typically 0.1% - 1%) of total transactions, making it difficult for models to learn effectively and requiring massive computational resources to detect the fraud (Buehler, 2024). Additionally, fraudsters continuously evolve their tactics, using techniques like adversarial attacks to bypass detection algorithms, implying that these techniques also need to continue to evolve to offer utility to financial firms. Moreover, regulatory and compliance constraints, such as the General Data Protection Regulation (GDPR) in Europe and data other data privacy rules in the US, further impose strict requirements on how financial institutions handle and process customer data. Ensuring that fraud detection models comply with these regulations while maintaining efficiency is an ongoing challenge.

Against the backdrop of accelerated adoption of machine learning to combat increasingly sophisticated financial fraud, this research highlights the limitations of traditional fraud detection systems, investigates machine learning solutions and use cases, and examines the challenges of machine learning implementation. The key specific objectives are:

i) Analyzing the role of machine learning in enhancing fraud detection accuracy, scalability, and adaptability.
ii) Comparing the performance of Machine learning-based fraud detection models with traditional rule-based approaches.
iii) Examining challenges in Machine learning-driven fraud detection, including data imbalance, adversarial attacks, and regulatory constraints.

iv) Exploring emerging AI-driven fraud prevention techniques such as deep learning, federated learning, and anomaly detection.

2 PROBLEM STATEMENT

As financial fraud continues to escalate globally, traditional fraud detection systems, which are primarily rule-based and threshold-driven, remain inadequate in addressing increasingly sophisticated fraud tactics. These conventional methods suffer from three critical limitations: first, they are inflexible which inhibits their ability to detect Novel Fraud Patterns. The rule-based systems depend on predefined criteria for detecting and mitigating anomalies (fraud) in the systems, this makes them ineffective against emerging fraud schemes such as synthetic identity fraud (1.1 million cases in 2024, Caporal 2025). Their static nature prevents real-time adaptation to new attack vectors (Haider et al. 2024). Second, rule-based methods have high prevalence of false-positive rates resulting in operational Inefficiencies. This is because these traditional methods flag an excessive number of legitimate transactions as fraudulent, causing customer friction and increased manual review costs (Finextra Research, 2025). This inefficiency undermines trust and increases compliance burdens. Finally, traditional fraud detection methods are unable to process large-scale, real-time transaction data, without significant errors. This implies that with financial institutions processing millions of transactions per second, traditional systems lack the computational scalability to analyze behavioral anomalies effectively (Abakarim et al. 2018).

Machine learning presents a capable alternative by leveraging predictive analytics, anomaly detection, and adaptive learning to improve fraud detection accuracy and address the issues of scalability that limits the efficacy of traditional methods. This study investigates how machine learning can overcome the shortcomings of traditional fraud detection, evaluates its comparative performance, and identifies key implementation challenges. The findings will inform financial institutions on optimizing fraud prevention strategies in an evolving threat landscape.

3.0 PROPOSED SOLUTION: MACHINE LEARNING FOR FRAUD DETECTION IN FINANCIAL TRANSACTIONS

By having predictive analytics, anomaly detection, and adaptive learning capabilities, machine learning offers a robust solution to financial fraud detection boosting the overall accuracy, efficiency, and adaptability of fraud detection systems. In contrast to traditional rule-based methods that rely on static fraud patterns, machine learning models dynamically analyze large-scale financial transactions in real-time, identifying fraudulent behaviors that are usually missed by conventional techniques (Ali et al., 2022). Below are machine learning techniques that bolsters fraud detection:

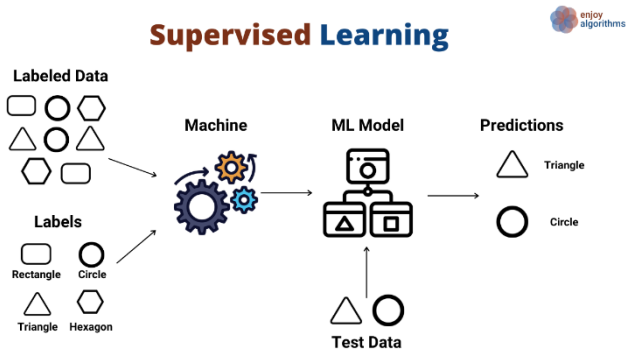
3.1 Supervised Learning Techniques

Supervised learning techniques entails training labeled datasets with fraudulent and legitimate transactions, enabling the system to learn intricate patterns, correlations, and anomalies in transactional data (Nerurkar et al. 2021). After training, the models are able to effectively detect fraudulent activity in real time by applying the learned decision boundaries to new, unseen transactions. Among the most widely deployed supervised learning techniques are Logistic Regression, which estimates the probability of fraud by analyzing historical transaction patterns (Sadgali et al., 2019); Decision Trees and Random

Forests, which uses hierarchical decision paths based on transaction features to classify fraud (Vuppula, 2021); and Support Vector Machines, which identify an optimal hyperplane to separate fraudulent from non-fraudulent transactions (Bello et al., 2023). These models are highly interpretable, scalable, and adaptable to evolving fraud patterns, which makes them appealing

The ability to generalize from history data while maintaining high precision in task classification makes supervised learning technique highly effective (Sadgali et al., 2019). Logistic Regression offers a probabilistic framework that is critically useful for risk scoring, while Decision Trees and Random forests are massively useful in handling non-linear relationships and feature interactions. Conversely, Support Vector Machines are valuable in high-dimensional spaces, making them suitable for datasets with numerous transaction attributes.

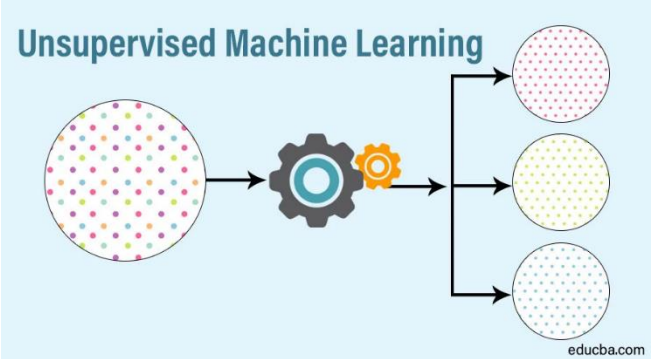
Figure 1: Supervised Learning model framework



3.2 Unsupervised Learning Techniques

Unlike supervised models, unsupervised learning techniques do not rely on labeled databases examples, rather they identify unusual patterns or deviations from typical transaction behavior which are flagged as anomalies and possible fraud (Cholevas et al. 2024). Clustering algorithms, including K-Means and DBSCAN, classify similar transactions together and flag outliers as potential fraud by detecting unusual patterns that do not conform to established clusters (Sadgali et al., 2019). Autoencoders are also advanced unsupervised technique for anomaly detection. These are a type of neural network trained to reconstruct normal transactional data with minimal error; when presented with fraudulent transactions, the reconstruction error increases significantly, allowing the model to flag these instances as suspicious (Dornadula& Sa, 2019). Combined, these unsupervised learning techniques are valuable in detecting previously unseen fraud schemes given they do not depend on historical labels.

Figure 2: Unsupervised Learning model framework



3.3 Semi-Supervised and Hybrid Models

Semi-supervised and hybrid models enhance fraud detection by leveraging both labeled and unlabeled data, combining the strengths of supervised and unsupervised learning to improve accuracy and adaptability. Self-Organizing Maps (SOMs), a type of neural network, reduce high-dimensional transaction data into a lower-dimensional representation, enabling the identification of anomalous patterns that usually indicate fraud (Bello et al., 2023). Federated learning further bolsters the effectiveness by using a decentralized approach and enabling multiple financial institutions to collaboratively train fraud detection models without the need to directly share sensitive customer data, thereby preserving privacy while improving model robustness (Vuppula, 2021). These approaches are particularly effective in scenarios where labeled fraud data is scarce or where data privacy regulations restrict centralized model training, like EU while data needs to be localized.

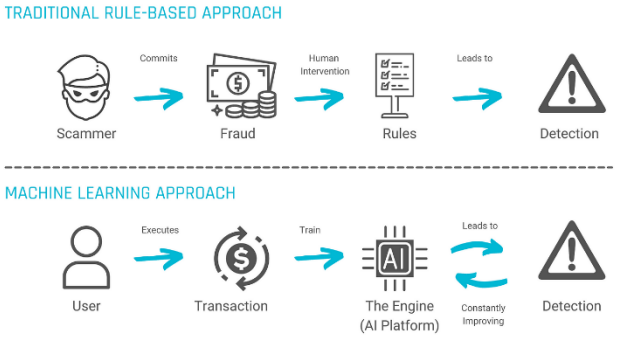
3.4 Deep Learning for Fraud Detection

Deep learning models attains fraud detection by capturing complex, non-linear patterns in transaction data. For instance, Convolutional Neural Networks (CNNs) analyze sequential transaction data to identify suspicious activities (Sadgali et al., 2019), while Long Short-Term Memory (LSTM) networks process time-series data to detect fraudulent behavior over time (Bello et al., 2023). On the other hand, Graph Neural Networks (GNNs) enhance detection by modeling relationships between transactions, customers, and merchants to uncover coordinated fraud schemes (Dornadula& Sa, 2019). These advanced techniques significantly improve accuracy in identifying sophisticated fraud

3.5 Real-Time and Adaptive Fraud Detection

Real-time fraud detection is critical for financial institutions to mitigate losses as well as to avoid downtime that often occur after cyber-attacks. This is facilitated by models employing adaptive learning to dynamically update based on emerging fraud patterns (Almazroi& Ayub, 2023). Advanced techniques like ResNeXt-embedded Gated Recurrent Units (GRU) enable high-speed (Alsubaei et al. 2024), accurate analysis of transaction data, while Autoencoders with ResNet (EARN) enhance fraud detection through efficient dimensionality reduction and improved feature representation (Tekkali and Natarajan, 2024). These methods ensure rapid, scalable detection of fraudulent activities in dynamic financial environments.

Figure 3: Traditional rule-based approach Vs Machine Learning for Fraud Detection



4.0 USE CASES MACHINE LEARNING IN FRAUD DETECTION

4.1 Credit Card Fraud Detection

Machine learning models help detect fraudulent credit card transactions by analyzing spending behavior, transaction locations, and historical data patterns. By leveraging anomaly detection techniques, machine learning algorithms can identify card-not-present (CNP) fraud and unauthorized transactions in real time (Chatterjee et al. 2024). The systems use behavioral profiling to compare current transactions against past spending habits, flagging suspicious deviations. Additionally, banks utilize deep learning models to assess risk scores before approving transactions, reducing false positives and improving security (Dornadula& Sa, 2019).

4.2 Identity Theft Prevention

Fraudsters leverage stolen personal data to create fraudulent accounts, obtain credit, or execute unauthorized transactions. There were 416,582 cases of credit card fraud in 2024 (Castillo, 2024). Machine learning models combat these threats by analyzing discrepancies in user-submitted information, geolocation patterns, and behavioral anomalies to flag potential identity theft (Zilberman et al., 2024). These systems continuously adapt to emerging fraud tactics, improving detection of synthetic identities and unauthorized access attempts. Additionally, financial institutions enhance security by integrating machine learning with biometric authentication—such as facial recognition and fingerprint scanning—to further mitigate identity fraud risks (Sadgali et al., 2019)

4.3 Cryptocurrency Fraud Prevention

Cryptocurrency fraud schemes, such as rug pulls, exploit the anonymity of digital assets. machine learning models analyze blockchain transaction data to detect fraudulent activities by identifying irregular wallet behavior and suspicious fund movements. Fraud detection systems use clustering algorithms to flag accounts involved in high-risk transactions, helping crypto exchanges prevent illicit activities. Additionally, AI-driven risk assessment tools provide real-time alerts on potential threats, safeguarding investors from financial scams (Dornadula& Sa, 2019).

5.0 CHALLENGES

Although machine learning significantly outperforms traditional rule-based systems in fraud detection, critical challenges persist—most notably severe class imbalance. In financial datasets, fraudulent transactions typically represent just 0.1%–1% of total transactions, creating a skewed distribution (Buehler, 2024). This imbalance biases machine learning models toward the majority class (legitimate transactions), degrading their ability to recognize fraud. Oversampling techniques like Synthetic Minority Over-sampling Technique (SMOTE) and undersampling methods help, but they can introduce biases and reduce model generalization (Elreedy et al. 2024).

Regulatory and privacy constraints also limit the implementation of Machine learning-driven fraud detection. Compliance with regulations like the General Data Protection Regulation (GDPR) restricts access to customer transaction data, which is crucial for training effective models. Financial institutions must balance fraud prevention with privacy protection, often leading to reduced dataset diversity and lower detection accuracy. Federated learning is an emerging solution that enables

collaborative fraud detection without direct data sharing, but its adoption is still in its early stages (Almazroi& Ayub, 2023). High computational cost of machine learning models is also a major challenge, especially deep learning-based fraud detection systems. Such models require massive amounts of data and computational power to analyze transactions in real-time. Small financial institutions with limited resources may struggle to implement and maintain these systems, making fraud detection less accessible outside large enterprises (Sadgali et al., 2019).

Finally, model interpretability is also a significant concern. Machine learning models, particularly deep learning techniques, function as black boxes, making it difficult to explain their decision-making processes. Regulatory agencies and financial institutions require transparency in fraud detection systems to justify flagged transactions. Techniques such as SHAP (SHapley Additive exPlanations) and LIME (Local Interpretable Model-agnostic Explanations) are being explored to improve model interpretability, but they are not yet widely adopted in financial fraud detection (Ali et al., 2022). Addressing these challenges requires ongoing advancements in machine learning model robustness, privacy-preserving techniques, and regulatory-compliant solutions to ensure fraud detection remains effective in an evolving digital landscape.

6.0 CONCLUSION

The rise of financial fraud in an increasingly digital world underscores the urgent need for advanced detection systems capable of combating sophisticated and evolving threats. Traditional rule-based methods are unable to keep up with current sophisticated challenges, due to lack of inflexibility, high false-positive rates, and inability to process large-scale real-time data efficiently. To address the shortcoming, organisations are increasing adopting machine learning as a powerful alternative, offering predictive analytics, anomaly detection, and adaptive learning capabilities that significantly enhance fraud detection accuracy, scalability, and adaptability.

The key machine learning techniques being utilized are supervised and unsupervised learning techniques, hybrid models, and deep learning architectures. These machine learning techniques offer a diverse toolkit for identifying fraudulent activities across credit card transactions, identity theft, and cryptocurrency scams. The techniques boost detection rates while also reducing operational inefficiencies by minimizing false positives and enabling real-time analysis. Nonetheless, the are key challenges such as data imbalance, regulatory constraints, computational costs, and model interpretability that restrain machine learning techniques' potential to identifying and mitigating all unauthorized entry to financial systems.

Leveraging machine learning techniques fully for fraud detection requires financial institutions to invest in robust data infrastructure, adopt privacy-preserving techniques like federated learning, and prioritize transparency through emerging AI methods. Collaboration between industry stakeholders, regulators, and technology developers is also essential for addressing these challenges and create a secure, adaptive framework for fraud prevention. Cybercrimes will continue improve their tactics, as such the financial sector must remain proactive in leveraging cutting-edge machine learning solutions.

REFERENCES

[1] Abakarim, Y., Lahby, M., & Attioui, A. (2018, October). An efficient real time model for credit card fraud detection based on deep learning. In Proceedings of the 12th international conference on intelligent systems: theories and applications (pp. 1-7).

[2] Ali, A., Abd Razak, S., Othman, S. H., Eisa, T. A. E., Al-Dhaqm, A., Nasser, M., Elhassan, T., Elshafie, H., & Saif, A. (2022). *Financial fraud detection based on machine learning: A systematic literature review.* Applied Sciences, 12(9637). https://doi.org/10.3390/app12199637

[3] Alsubaei, F. S., Almazroi, A. A., & Ayub, N. (2024). Enhancing phishing detection: A novel hybrid deep learning framework for cybercrime forensics. IEEE Access, 12, 8373-8389.

[4] Ashraf, F. and Schaffer, A. (2024). *Combating Financial Crime: AI and Machine Learning in Anomaly Detection and Risk Management*. [online] doi:https://doi.org/10.13140/RG.2.2.22450.41927.

[5] Bello, O. A., Folorunso, A., Ejiofor, O. E., Budale, F. Z., Adebayo, K., & Babatunde, O. A. (2023). *Machine learning approaches for enhancing fraud prevention in financial transactions.* International Journal of Management Technology, 10(1), 85–109.

[6] Browne, R. (2024). *Mastercard jumps into generative AI race with model it says can boost fraud detection by up to 300%*. [online] CNBC. Available at: https://www.cnbc.com/2024/02/01/mastercard-launches-gpt-like-ai-model-to-help-banks-detect-fraud.html.

[7] Buehler, J. (2024). Investigating Fraudulent E-Commerce Transactions: A Data-driven Approach Using Machine Learning.

[8] Caporal, J. (2025). Identity Theft and Credit Card Fraud Statistics for 2024. [online] The Motley Fool. Available at: https://www.fool.com/money/research/identity-theft-credit-card-fraud-statistics/.

[9] Castillo, M. (2024). Why credit card fraud alerts are rising, and how worried you should be about them. [online] CNBC. Available at: https://www.cnbc.com/2024/09/12/why-credit-card-fraud-alerts-are-rising.html.

[10] Chatterjee, P., Das, D., & Rawat, D. B. (2024). Digital twin for credit card fraud detection: Opportunities, challenges, and fraud detection advancements. Future Generation Computer Systems.

[11] Cholevas, C., Angeli, E., Sereti, Z., Mavrikos, E., & Tsekouras, G. E. (2024). Anomaly detection in blockchain networks using unsupervised learning: A survey. Algorithms, 17(5), 201.

[12] Dornadula, V. N., & Sa, G. (2019). Credit card fraud detection using machine learning algorithms. Procedia Computer Science. https://www.sciencedirect.com/science/article/pii/S1877050919300079

[13] Elreedy, D., Atiya, A. F., & Kamalov, F. (2024). A theoretical distribution analysis of synthetic minority oversampling technique (SMOTE) for imbalanced learning. Machine Learning, 113(7), 4903-4923.

[14] Finextra Research (2025). How AI is Fighting Financial Fraud: Strategies Banks Use: By Shailendra Prajapati. [online] Finextra Research. Available at: https://www.finextra.com/blogposting/27806/how-ai-is-fighting-financial-fraud-strategies-banks-use.

[15] Gerken, T. (2025). Argentina president accused of fraud over crypto crash. [online] 17 Feb. Available at: https://www.bbc.com/news/articles/cp9x9j89evxo.

[16] Haider, Z. A., Khan, F. M., Zafar, A., & Khan, I. U. (2024). Optimizing Machine Learning Classifiers for Credit Card Fraud Detection on Highly Imbalanced Datasets Using PCA and SMOTE Techniques. VAWKUM Transactions on Computer Sciences, 12(2), 28-49.

[17] Nerurkar, P., Bhirud, S., Patel, D., Ludinard, R., Busnel, Y., & Kumari, S. (2021). Supervised learning model for identifying illegal activities in Bitcoin. Applied Intelligence, 51, 3824-3843.

[18] Nilson Report. (2024). Card industry's fraud-fighting efforts pay off: Nilson Report. [online] Payments Dive. Available at: https://www.paymentsdive.com/news/card-industry-fraud-fighting-efforts-pay-off-nilson-report-credit-debit/639675/.

[19] Rej, M. (2023). Credit Card Fraud Statistics (2023) Merchant Cost Consulting. [online] merchantcostconsulting.com. Available at: https://merchantcostconsulting.com/lower-credit-card-processing-fees/credit-card-fraud-statistics/.

[20] Sadgali, I., Sael, N., & Benabbou, F. (2019). Performance of machine learning techniques in the detection of financial frauds. Procedia Computer Science. https://www.sciencedirect.com/science/article/pii/S187705092030065XMedium. "Decentralized AI vs. Centralized AI: Key Differences and Advantages." https://medium.com/coinmonks/decentralized-ai-vs-centralized-ai-key-differences-and-advantages-3bff25589782 (Accessed: 11th March 2025)

[21] Tekkali, C. G., & Natarajan, K. (2024). Transfer learning of pre-trained CNNs on digital transaction fraud detection. International Journal of Knowledge-Based and Intelligent Engineering Systems, 28(3), 571-580.

[22] United Nations (2024). Improving regional investigations on money laundering and asset recovery. [online] United Nations: UNODC Regional Office for. Available at: https://www.unodc.org/roca/en/NEWS/news_2024/november/improving-regional-investigations-on-money-laundering-and-asset-recovery.html.

[23] Veno, J. (2024). Preventing and Detecting Occupational Fraud. [online] Njcpa.org. Available at: https://www.njcpa.org/article/2024/09/20/preventing-and-detecting-occupational-fraud.

[24] Vuppula, K. (2021). An advanced machine learning algorithm for fraud financial transaction detection. Procedia Computer Science. https://www.sciencedirect.com/science/article/pii/S187705092030065X

[25] Zilberman, A., Offer, A., Pincu, B., Glickshtein, Y., Kant, R., Brodt, O., ... & Elovici, Y. (2024). A Survey on Geolocation on the Internet. IEEE Communications Surveys & Tutorials.M. Kolhar, F. Al-Turjman, A. Alameen andM.M. Abualhaj, "A three layered decentralized IoT biometric architecture for city lockdown during COVID-19 outbreak", *Ieee Access*, vol. *8*, pp. 163608-163617, 2020.