International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) e-ISSN: 2395-5325
Volume 8, Issue 1 (April '2025)

A STUDY ON DIGITAL TRANSACTIONS FRAUD DETECTION SYSTEM

L. Haripriya,
PG Student,
Department of Computer Applications,
Vellalar College for Women, Erode,India.

S. Kavipriya,
PG Student,
Department of Computer Applications,
Vellalar College for Women, Erode, India.

N. Geetha,
Assistant Professor,
Department of Computer Applications,
Vellalar College for Women, Erode, India.

Abstract: Digital transactions have grown exponentially with the rise of online banking, e-commerce and financial technology. However, this growth has also led to an increase in fraudulent activities such as credit card fraud, phishing, account takeovers and cryptocurrency scams. Traditional rule-based fraud detection methods struggle to keep up with evolving fraud tactics, making advanced artificial intelligence (AI) and machine learning-based models essential for fraud prevention. This survey explores various types of digital transactions, common fraud detection techniques using data mining and recent research contributions in the field. The study on supervised, unsupervised and hybrid machine learning approaches discussing their advantages and limitations. Additionally, we highlight the key challenges in implementing effective fraud detection systems and examine future trends, including real-time analytics, blockchain integration, behavioural biometrics and explainable AI, to enhance the security of digital transactions. This will be helpful to the researchers for their future research direction in this area.

Keywords: Digital transactions, fraud detection, credit card fraud, cryptocurrency scams, machine learning, data mining, supervised learning and unsupervised learning.

I. INTRODUCTION

Digital transactions have revolutionized financial services by providing fast, secure and convenient payment methods. However, as transaction volumes grow, so does the risk of fraudulent activities. Fraudulent digital transactions result in financial losses, damage consumer trust and pose security risks to financial institutions.

Fraud detection involves identifying suspicious transactions using advanced analytics and machine learning techniques. Traditional fraud detection methods rely on predefined rules and manual review, which are ineffective in detecting new fraud patterns. Data mining techniques offer a more adaptive and efficient approach by analysing large datasets and identifying anomalies or fraudulent behaviours. This survey explores different types of digital transactions, fraud detection techniques using data mining, recent advancements and future research directions in combating digital transaction fraud. Section I contains the introduction of the impact of fraud detection in digital transactions. Section II covers the different payment mode of digital transactions. Section III discusses the different fraud detection methods are used in digital transactions. Section IV covers the literature survey of emerging techniques for fraud detection system as well as several extended work in these areas. Section V concludes the fraud detection techniques and identifies the future directions in this field.

II. DIGITAL TRANSACTION VARIANTS

Digital transactions can be classified into several categories based on the mode of payment and platform used. The most common variants include:

Payment Card Fraud - Payment card fraud occurs when criminals use stolen or counterfeit credit/debit card details to make unauthorized transactions. One of the most common forms is Card-Not-Present (CNP) fraud, where stolen card details are used for online purchases without requiring the physical card. Another variant is card skimming, where criminals install skimming devices on ATMs or point-of-sale (POS) terminals to capture card information. Chargeback fraud, also known as friendly fraud, happens when a customer makes a legitimate purchase but later disputes the transaction falsely to receive a refund while keeping the product.

Account Takeover Fraud (ATO) - Account takeover fraud occurs when cybercriminals gain unauthorized access to a user's banking, e-commerce or payment account. This is often achieved through phishing attacks, credential stuffing (using

stolen usernames and passwords from data breaches) or malware infections. Once inside the account, fraudsters can transfer funds, make unauthorized purchases or change account details to lock out the legitimate owner. The rise of digital wallets and online banking has made ATO a growing concern for financial institutions.

Phishing and Social Engineering Fraud - Phishing is one of the most prevalent methods used by fraudsters to steal sensitive information. In a phishing attack, scammers send fraudulent emails, messages or fake websites that appear to be from legitimate financial institutions, tricking users into entering their login credentials or card details. Business Email Compromise (BEC) scams involve impersonating company executives or suppliers via email to trick employees into transferring funds to fraudulent accounts. Another emerging threat is SIM swap fraud, where criminals hijack a victim's phone number by transferring it to a new SIM card, bypassing SMS-based two-factor authentication to gain access to banking accounts.

Mobile Payment Fraud - With the growing popularity of mobile wallets and contactless payments, fraudsters have developed new tactics to exploit mobile transactions. Fake payment apps trick users into entering their banking credentials, which are then stolen by criminals. Malware and keyloggers installed on smartphones can capture transaction details and passwords. Additionally, QR code fraud occurs when scammers replace genuine QR codes with fraudulent ones, redirecting payments to their accounts instead of the intended recipient.

Cryptocurrency and Blockchain Fraud - Cryptocurrency transactions, while secure, has become a target for fraudsters due to their decentralized and irreversible nature. Crypto scams and Ponzi schemes promise high returns to investors but ultimately collapse, leaving victims with significant losses. Cryptojacking is another form of fraud where hackers secretly use victims' computers or mobile devices to mine cryptocurrency without their knowledge. Additionally, exchange hacking and wallet theft involve cybercriminals attacking cryptocurrency exchanges or exploiting security vulnerabilities to steal digital assets.

E-commerce Fraud - E-commerce platforms face various fraud risks, including fake online stores, where fraudsters create websites that appear legitimate but never deliver products after receiving payments. Triangulation fraud involves a scammer using stolen card details to buy products from a legitimate retailer and reselling them to unsuspecting buyers. Refund and return fraud occurs when customers exploit return policies by sending back fake or damaged items while requesting refunds.

Money Laundering and Financial Crimes - Fraudsters often use digital transactions to launder illicit funds and hide the origins of criminal earnings. Money mule fraud involves criminals recruiting individuals to receive and transfer stolen money, making it harder to trace the source of fraudulent transactions. Synthetic identity fraud is another tactic where fraudsters combine real and fake identity details to create new identities, which they use to open bank accounts, apply for loans or commit other financial crimes.

ATM and Point-of-Sale (POS) Fraud - ATMs and POS terminals are also targeted by fraudsters. ATM jackpotting is a technique where hackers install malware or use hardware devices to take control of ATMs, forcing them to dispense large sums of cash. POS terminal tampering occurs when fraudsters manipulate POS machines to steal card data or alter transaction details, leading to unauthorized fund withdrawals or purchases.

Deepfake and AI-Driven Fraud - Advancements in artificial intelligence have introduced new fraud risks, such as deepfake impersonation, where AI-generated voices or videos are used to mimic company executives and trick employees into making unauthorized payments. Automated bot attacks are another threat, where fraudsters deploy bots to conduct rapid fraudulent transactions or test stolen credentials on banking and payment platforms.

Fake Investment and Romance Scams - Scammers often use emotional manipulation and financial deception to defraud victims. Romance scams involve fraudsters developing online relationships with victims and convincing them to send money for fake emergencies. Similarly, fake loan and investment scams promise high returns on financial investments but ultimately disappear with the victims' funds. These scams have become more prevalent with the rise of social media and online investment platforms.

III. DIGITAL TRANSACTION FRAUD DETECTION METHODS

Identifying digital transaction fraud requires a blend of machine learning, rule-based analysis and behavioral analytics. Various methods help to identify and prevent fraudulent activities by analysing transaction patterns, user behaviour and device characteristics.

Machine Learning-Based Detection - Machine learning models play a crucial role in fraud detection. Supervised learning uses labelled fraud and non-fraud data to train models like decision trees, neural networks, and random forests. Unsupervised learning detects anomalies without labelled data using clustering techniques such as K-means or autoencoders. Deep learning models, such as LSTMs, analyse transaction sequences over time to identify suspicious behaviour.

Rule-Based Systems - Rule-based detection relies on predefined rules to flag suspicious transactions. These rules may include setting thresholds for transaction amounts, monitoring rapid multiple transactions, or blocking payments from high-risk locations or unrecognized devices.

Anomaly Detection - Anomaly detection identifies deviations from a user's normal transaction behaviour using statistical models and AI. For example, if a user suddenly makes a high-value transaction from a different country, the system may trigger an alert or require additional verification.

Behavioural Biometrics - This method tracks user interactions, such as typing speed, mouse movements, and login patterns, to detect unusual behaviour. Any deviation from a user's normal activity may indicate fraudulent access.

Device Fingerprinting - Device fingerprinting identifies a user's device based on IP address, browser type, and system configuration. If an unrecognized device is used, the system may block the transaction or require multi-factor authentication.

Geolocation & IP Tracking - This method verifies whether a transaction's IP address and location match previous behaviour. If a transaction originates from a blacklisted or suspicious IP, it can be flagged or blocked.

Velocity Checks - Velocity checks detect high-frequency transactions within a short period. For example, if a credit card is used in multiple locations within minutes, the system may suspect fraud and restrict further transactions.

Blockchain & AI-Based Security - Blockchain technology ensures transaction integrity and prevents data tampering, while AI continuously learns new fraud tactics and adapts to emerging threats, improving security over time.

Multi-Factor Authentication (MFA) - MFA adds an extra layer of security by requiring users to verify their identity through OTPs, biometrics, or security questions, reducing the risk of unauthorized access.

Consortium Data Sharing - Banks and payment processors share fraud data across institutions, helping detect known fraud patterns and preventing fraudsters from exploiting different platforms.

By combining these advanced fraud detection techniques, financial institutions and businesses can enhance security, reduce fraud risks, and protect digital transactions from malicious activities.

IV. LITERATURE REVIEW

To better understanding of fraud detection in digital transaction systems, it is helpful to review and analyze existing research in the literature. Consequently, recent approaches and methodologies for detecting fraud in digital transactions are discussed.

Zhang L. and Li H. (2019) proposed an autoencoder-based approach for detecting anomalies in mobile payment transactions. The model uses an unsupervised deep learning technique to learn normal transaction patterns and identify deviations that may indicate fraud. By minimizing reconstruction errors, the autoencoder effectively detects suspicious activities. Experimental results show the model's high accuracy and efficiency in mobile payment fraud detection.

Chen J. et al. (2020) presented a deep learning approach for detecting fraudulent activities in online banking. The authors develop a neural network model that analyzes large-scale transactional data to identify suspicious patterns. By leveraging advanced feature extraction and real-time analysis, the proposed system improves detection accuracy while minimizing false positives. The study demonstrates the model's effectiveness in enhancing cybersecurity for financial institutions.

Kumar A. and Sharma R. (2021) proposed a credit card fraud detection system using a combination of Random Forest and Support Vector Machine (SVM) algorithms. The authors compare the performance of these models in identifying fraudulent transactions from imbalanced datasets. Experimental results show that the Random Forest algorithm achieves higher accuracy and better fraud detection rates, while SVM effectively reduces false positives. The study highlights the importance of using ensemble methods for reliable fraud detection in financial systems.

Nguyen T. and Pham D. (2021) proposed a clustering-based approach for detecting fraudulent activities in cryptocurrency transactions. The authors apply unsupervised learning techniques to group similar transactions and identify anomalies indicative of fraud. By analyzing transaction patterns and network behavior, the model effectively detects suspicious activities. The study highlights the method's efficiency in enhancing security and preventing financial crimes in the cryptocurrency ecosystem.

Gupta S. et al. (2022) presented a graph-based approach to detect fraudulent activities in e-commerce platforms. The authors construct transaction graphs to capture relationships

between users, products and payment methods. By applying graph analysis techniques and anomaly detection algorithms, the model identifies suspicious patterns and collusive behaviors. The proposed method enhances fraud detection accuracy and is effective in identifying complex fraud schemes.

Wang Y. and Zhou L. (2023) presented a hybrid deep learning model designed for adaptive fraud detection in dynamic environments. The model combines CNNs for feature extraction and long short-term memory (LSTM) networks for detecting temporal patterns in transaction data. It continuously updates itself to adapt to evolving fraud tactics. Experimental results demonstrate the model's high accuracy, reduced false positives and effectiveness in real-time fraud detection.

Y. Chen et al. (2023) proposed a hybrid machine learning model to improve the accuracy of transaction fraud detection. The model combines supervised and unsupervised learning techniques to detect both known and emerging fraud patterns. By leveraging feature engineering and ensemble methods, it enhances detection performance while minimizing false positives. Experimental results demonstrate the model's effectiveness in identifying fraudulent transactions in real-world financial datasets.

D. Johnson and E. Brown (2024) proposed a hybrid approach combining deep learning and Random Forest algorithms for financial fraud detection. The deep learning model extracts complex patterns from transaction data, while the Random Forest algorithm enhances classification accuracy. The hybrid system demonstrates improved fraud detection rates and reduced false positives, making it a robust solution for financial institutions.

M. Lee et al. (2024) presented a hybrid ensemble model combining multiple deep learning architectures to detect credit card fraud. The model integrates convolutional neural networks (CNNs) and recurrent neural networks (RNNs) to capture both spatial and temporal patterns in transaction data. By employing an ensemble approach, the system enhances detection accuracy and reduces false positives. The study demonstrates the model's effectiveness in improving fraud detection for financial institutions.

A. Kumar et al. (2025) presented a hybrid approach combining Machine Learning (ML) and Deep Learning (DL) techniques to enhance cyber fraud detection. The authors propose an integrated model that leverages the strengths of both ML algorithms for feature extraction and DL models for pattern recognition. Experimental results demonstrate significant improvements in detection accuracy and reduced false positives compared to traditional methods. The study highlights the model's applicability in real-time fraud prevention for financial institutions.

V. CONCLUSION

Digital transaction fraud detection is crucial in preventing financial losses and maintaining trust in online financial services. Data mining techniques, including supervised, unsupervised and hybrid learning, play a significant role in identifying fraudulent transactions. While machine learning models improve accuracy, challenges like imbalanced data, real-time fraud detection and evolving fraud patterns remain. Future advancements in explainable AI, blockchain and federated learning will enhance fraud detection capabilities. Continued research in adaptive fraud prevention models is necessary to combat emerging cyber threats.

VI. REFERENCES

[1] A. Kumar, B. Singh, and C. Patel., "Achieving Excellence in Cyber Fraud Detection: A Hybrid ML+DL Approach", Applied Sciences, 2025.

[2] Chen J., Zhang P., & Wang X., "Deep Learning-Based Online Banking Fraud Detection", IEEE Transactions on Cybersecurity, 25(4), 56-72, 2020.

[3] D. Johnson and E. Brown., "Enhancing Financial Fraud Detection with Hybrid Deep Learning and Random Forest Algorithms", International Journal of Artificial Intelligence and Machine Learning, 2024.

[4] Gupta S., Patel K., & Roy M., "Graph-Based Analysis for E-commerce Fraud Detection", Computational Intelligence Review, 29(5), 142-158, 2022.

[5] Kumar A., & Sharma R., "Credit Card Fraud Detection Using Random Forest and SVM", International Journal of Data Science, 18(3), 112-126, 2021.

[6] M. Lee, J. Kim, and H. Park., "A Hybrid Deep Learning Ensemble Model for Credit Card Fraud Detection", IEEE Transactions on Neural Networks and Learning Systems, 2024.

[7] Nguyen T., & Pham D., "Clustering-Based Cryptocurrency Fraud Detection", Blockchain Security Journal, 6(1), 33-48, 2021.

[8] Wang Y., & Zhou L., "A Hybrid Deep Learning Model for Adaptive Fraud Detection", Neural Networks in Cybersecurity, 35(1), 77-91, 2023.

[9] Y. Chen, M. Liu, and S. Zhang,"Enhancing Transaction Fraud Detection with a Hybrid Machine Learning Model", IEEE Conference on Cybersecurity, 2023.

[10] Zhang L., & Li H., "Autoencoder-Based Anomaly Detection in Mobile Payment Transactions", Journal of Machine Learning Applications, 14(2), 89-104, 2019.

