International Journal On Engineering Technology and Sciences – IJETS
ISSN (P):2349-3968, ISSN (O): 2349-3976 Volume XI - Issue IV, April – 2024

FRAUD DETECTION AND PREVENTION USING AI

[1]Alice Sancia S, [2]Nithyashri N, [3]Abinaya S V, [4]Dr. R. Ravi, [5]Alan Jeyapaul K
[1,2,3,4,5]Department Of Computer Science and Engineering,
FrancisXavier EngineeringCollege, Tirunelveli –Tamil Nadu – India

Abstract:
Fraud detection is vital in thwarting deceptive tactics aimed at unlawfully obtaining assets. It employs various methods, from basic rules to advanced machine learning, to uncover suspicious activities and safeguard organizational reputation and stakeholder trust. Adaptability is crucial, necessitating ongoing strategy refinement to counter evolving fraudster tactics. Collaboration across sectors enhances resilience through information sharing and coordinated action. Integration with robust risk management frameworks identifies vulnerabilities and preempts risks. In the digital age, cyber-enabled fraud demands sophisticated tools like behavioral analytics and real-time monitoring. Ultimately, fraud detection is indispensable for preserving financial integrity and trust, requiring vigilance, adaptability, and collaboration to combat evolving threats. The Oxford Dictionary defines fraud as the act of deceptive or criminal behaviour that leads to financial or personal benefit.[1] Organizations combat various fraudulent activities like money laundering, cyberattacks, and identity theft through advanced fraud detection technologies and risk management strategies. These methods utilize adaptive analytics, including machine learning, to create fraud risk scores and enable real-time monitoring of suspicious transactions. Automation facilitates the implementation of new preventive measures, aiding in staying ahead of evolving fraud schemes. Real-time monitoring ensures swift action against fraudulent behaviour, minimizing financial losses and maintaining stakeholder trust. In today's digital landscape, these modern techniques are crucial for organizations to effectively combat fraud and protect their assets and reputation. However, in certain jurisdictions, there are now mandates for fraud prevention programs, particularly notable in the insurance sector across multiple US states and under the UK's "Failure to Prevent Fraud" legislation since April 2023.lastly.The importance of fraud detection is underscored by data from the FBI in 2022, revealing that elderly fraud victims in the US faced an average loss of $35,101 each, culminating in a total loss exceeding $3 billion. Similarly, global fraud losses surpassed $55 billion in 2021

Keywords: Fraud detection, Deceptive tactics, Advanced machine learning , Risk management strategies , Cyber-enabled Fraud , Behavioural analytics , Real-time monitoring , Fraud prevention programs , Financial losses , Compliance regulations

Introduction

Fraud entails employing deceitful strategies to gain unauthorized financial or personal benefits. To counter fraud, businesses typically deploy two primary tactics: fraud prevention and fraud detection. Fraud prevention entails taking preemptive measures to thwart fraudulent activities before they materialize, while fraud detection is activated upon the detection or attempt of a fraudulent transaction. An example of fraud is credit card fraud, which involves using credit card details unlawfully for purchases. Such fraudulent actions can transpire either physically, like in face-to-face transactions, or digitally, such as online purchases.

In the domain of fraud prevention, businesses implement various strategies, including robust security protocols, identity verification processes, and systems for monitoring transactions. Conversely, fraud detection leverages sophisticated technologies like machine learning algorithms and data analytics to spot and highlight suspicious transactions or behaviors promptly. Fraud means tricking or deceiving someone to gain money or personal benefits illegally [2]. By integrating both fraud prevention and detection strategies, businesses can effectively diminish the perils linked with fraudulent activities, safeguard customer assets and data, and uphold trust and integrity within their respective sectors.

Spotting fraud and studying how money is spent to find possible fraud situations [3]. The popularity and widespread use of electronic wallets (e-wallets) are facing challenges that need addressing for their ongoing success. A significant concern is the security risks e-wallets face, such as hacking, identity theft, and phishing attacks, leading to online fraud. Discussions around security primarily focus on detecting and preventing

fraud within e-wallet systems. While machine learning techniques are becoming more important in fraud prevention, it's also crucial to consider traditional and newer approaches not reliant on machine learning.

For instance, rule-based systems, anomaly detection, and expert systems are widely used and effective in spotting fraud. Additionally, advancements like graph-based modeling and behavior analysis show promise in fraud prevention. To protect customers, e-wallet providers should implement strong security measures like two-factor authentication, encryption, and robust fraud detection systems.

Interoperability is another challenge for e-wallets due to differing standards among providers, making fund transfers between e-wallet systems difficult. Rule-based systems, anomaly detection, and expert systems have been essential for identifying fraudulent activities, for instance [4]. Adopting open standards can improve interoperability and transaction efficiency. Usability is vital for e-wallet success, with factors like ease of use and usefulness influencing adoption rates. Network undertakeCollaboration between e-wallet providers, financial institutions, and regulators is key to ensuring compliance, particularly for cross-border transactions. Rule-based systems, anomaly detection, and expert systems have been essential for identifying fraudulent activities, for instance[4].While e-wallets offer convenience and accessibility, addressing challenges such as security, interoperability, usability, and regulatory compliance is crucial for their continued growth and success in the digital payment landscape Machine learning-based solutions have surged in popularity compared to conventional methods due to their ability to autonomously learn from data and adapt to shifting patterns of fraudulent behavior[5]. Our main goal is to create strong behavioural models that can effectively analyse the relationships among different attributes in transactions. To do this, we suggest using a special type of network called the heterogeneous relation network, which is a part of the knowledge graph. In this network, each node represents an attribute value in transactions, and the connections between nodes show the relationships between different attributes. While this network can show the data well, it doesn't completely fix problems in data quality, especially for low-quality-data. Having a good way to represent data and keep these complex relationships is important for improving how we analyse data. So, we introduce network representation learning (NRL), which helps capture these deep relationships. This helps make up for problems in low-quality data when detecting fraud and makes our fraud detection models work better. By looking at how similar different pieces of data are, we can find more connections in the data, which helps fix some problems in the data. NRL not only helps improve data quality but also changes how we look at data from a manual process to an automatic one, which helps us find more connections in lots of transactions.

To make sure our models for detecting fraud online work well, we need to combine improving the data and improving the models themselves. Different types of models need different ways of organizing data to work best. This is a big challenge we're working on. We want to find the best ways to organize data for different models, including ones that look at large groups of transactions, individual transactions, and ones that look at different types of behaviours.

For models that look at large groups of transactions, we create a network that doesn't need labels to understand how transactions work. Then, we use this network to understand which transactions might be fraudulent and use that information in our machine learning models to predict fraud risks. For models that look at individual transactions, we create a network that does need labels to understand how fraud happens in different transactions. Then, we make different simple models based on this network to help us understand fraud.

We also combine these different types of models to make sure we get the best results. This helps us find fraud better because we're using the strengths of different types of models together. However, the added convenience also brings inherent security vulnerabilities [6].

Overall, our work shows how important it is to organize data in the right way to find fraud better. It also shows how deep relationships in data can help us improve how we find fraud, especially in online behaviours.

Algorithms:

The impacts of fraud on financial institutions are extensive and potentially devastating. Apart from substantial financial losses, institutions also endure reputational damage and a decline in customer trust. The

aftermath of a significant fraud incident can escalate into legal disputes, regulatory investigations, and heightened compliance demands. As a result, financial institutions must prioritize fraud detection and prevention as a critical imperative. This strategic focus is essential to safeguarding their assets, preserving their reputation, and nurturing robust customer relationships. The behavior-based approach is acknowledged as an efficient model for detecting online payment fraud [7].

The repercussions of fraud reverberate throughout the institution, affecting various aspects of its operations and interactions with stakeholders. Financial losses are not merely monetary; they erode confidence in the institution's capabilities and integrity. Moreover, reputational damage can have lasting effects, impacting customer acquisition and retention efforts. The erosion of trust can lead to customers seeking alternative financial services providers, resulting in a loss of market share and revenue. Legal battles and regulatory scrutiny further compound the challenges, requiring institutions to allocate significant resources towards resolving these issues and complying with regulatory requirements. Thus, a comprehensive and proactive approach to fraud detection and prevention is imperative for financial institutions to mitigate risks, protect their interests, and sustain long-term viability in a competitive market landscape. We investigated the process of identifying users by comparing the histograms of their data in an anonymous dataset with those from the original dataset[8].

Leveraging artificial intelligence (AI) for fraud prevention has revolutionized how companies approach internal security and operational efficiency. AI has become an indispensable technology in thwarting fraudulent activities within financial institutions, offering a range of advanced techniques for fraud detection.
Data mining plays a crucial role in AI-based fraud detection, employing methods like classification, clustering, and segmentation to reveal potential fraud patterns. This automated process is vital for identifying anomalies and irregularities within large datasets, significantly enhancing fraud prevention efforts. The importance of data mining lies in its ability to uncover hidden relationships and patterns within data, providing valuable insights that traditional analysis methods may overlook. By categorizing data points, grouping similar ones, and dividing data into subsets, data mining facilitates targeted analysis and improves fraud detection accuracy. Moreover, data mining contributes to the development of predictive models that forecast potential fraud risks based on historical data patterns. Utilizing machine learning algorithms, these models continuously learn and adapt to emerging fraud schemes, enabling proactive threat detection.

Another AI-driven method, neural networks, holds a critical position in fraud detection They analyse data by comparing it with established conclusions from internal audits or formal financial documents, assisting in identifying fraudulent activities. Neural networks are integral due to their ability to process complex data and detect patterns that might indicate fraudulent behaviour. They are particularly effective in handling large volumes of data and can adapt to changing fraud tactics. By leveraging advanced algorithms and machine learning capabilities, neural networks contribute significantly to the accuracy and efficiency of fraud detection systems in financial institutions.

Machine learning (ML) plays a pivotal role in AI-driven fraud detection by using historical fraud data to identify and predict potentially fraudulent transactions. ML algorithms can be categorized into supervised and unsupervised learning methods. Supervised learning involves manually label a subset of data records as 'fraudulent' or 'non-fraudulent' to train the model. This enables the algorithm to accurately classify new data points and make predictions based on examples. On the other hand, unsupervised learning operates without given data and focuses on uncovering underlying patterns and anomalies within raw data. These methods are effective in detecting novel fraud patterns and adapting to new threats. ML's adaptability to large data volumes and evolving fraud tactics makes it a valuable tool for fraud prevention. Supervised learning excels in detecting known fraud schemes and providing real-time alerts, while unsupervised learning is adept at identifying emerging fraud patterns. Together, these ML techniques enhance fraud detection capabilities, mitigating financial risks and maintaining trust within the industry. We also utilize node feature transformation and edge construction.[9]

Pattern recognition algorithms are pivotal in identifying suspicious behaviour patterns in fraud detection. They operate either autonomously through unsupervised methods or with manual input in supervised scenarios. In unsupervised mode, pattern recognition algorithms autonomously analyse data to identify irregularities and anomalies that deviate from typical patterns. This approach is useful in detecting novel fraud patterns or emerging trends. Supervised pattern recognition algorithms require manual input or given data to train the model. They categorize data into known classes, such as fraudulent and non-fraudulent patterns, and learn to identify similar patterns in new data. Both unsupervised and supervised pattern recognition algorithms are vital components of fraud detection systems. They analyse transactional data, user behaviour, and historical patterns to detect anomalies and contribute significantly to the accuracy and effectiveness of fraud detection systems. This issue has garnered significant attention, leading to the proposal of numerous solutions.[10]

Additionally, various AI techniques such as link analysis, Bayesian networks, decision theory, and sequence matching are employed to bolster fraud detection efforts. These methods play a crucial role in enhancing the

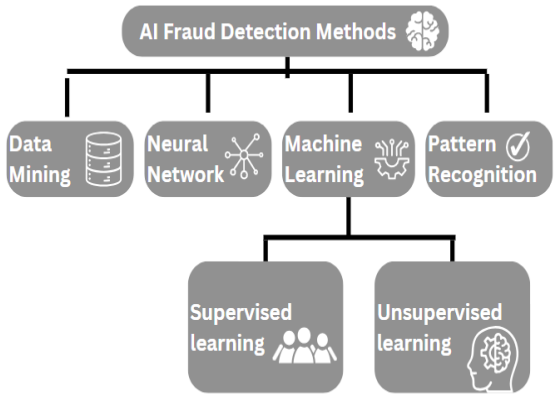

Fig-1 AI Fraud detection and prevention method

precision and effectiveness of fraud detection systems by delving into complex relationships, probabilistic models, decision-making processes, and sequential data patterns.

Overall, AI-based fraud detection techniques have significantly improved the efficiency and accuracy of fraud prevention measures within financial institutions. By leveraging advanced algorithms and automated processes, these techniques offer proactive measures to identify and mitigate fraudulent activities before they cause substantial harm. This proactive approach helps safeguard organizations from financial losses and reputational damage, enhancing overall security and trust in the financial ecosystem.

Proposed System:

Our proposed AI-based fraud detection system represents a sophisticated and proactive approach to combatting fraudulent activities across diverse industries. At its core, the system integrates cutting-edge technologies such as machine learning, data mining, neural networks, and pattern recognition algorithms. These components work synergistically to analyse vast amounts of transactional data, user behaviour patterns, and historical fraud indicators, enabling the system to identify potential fraud schemes
One of the key strengths of our system lies in its ability to adapt and evolve over time. Machine learning models continuously learn from new data and emerging fraud patterns, improving their detection capabilities and staying ahead of evolving threats. This adaptive learning approach ensures that the system remains effective in detecting both known fraud schemes and novel fraud Furthermore, the system's real-time monitoring and alerting capabilities enable immediate response upon detecting suspicious activities. By generating alerts and notifications for potential fraud cases, businesses can take prompt action to investigate, mitigate risks, and prevent financial losses. This real-time responsiveness is critical in today's fast-paced digital landscape, where fraudsters constantly innovate their techniques to evade detection. In addition to proactive fraud detection, our system emphasizes security and compliance with regulatory standards. Advanced technologies like block-chain, encryption, and biometric authentication enhance data security and protect sensitive information. Moreover, the system ensures compliance with anti-money laundering (AML) and know-your-customer (KYC) regulations, reducing legal risks and maintaining trust with regulatory authorities. Overall, our proposed AI-based fraud detection system offers a comprehensive and robust

solution to safeguard businesses from fraudulent activities, uphold integrity, and foster trust within the financial ecosystem.

Applications of Fraud Detection and Prevention:

Fraud detection is a critical aspect for financial institutions, especially those handling numerous financial transactions, as they are at higher risk of facing financial fraud. The primary areas where fraud detection is applied include account-related fraud and payment/transaction fraud, each with its distinct subcategories and methods.

Account-related fraud encompasses new account fraud and account takeover fraud. In new account fraud, scammers create new accounts using fake identities, which can be identified by analysing device patterns and session indicators. On the other hand, account takeover fraud occurs when a hacker gains unauthorized access to an existing account and exploits it to obtain products and services. To counter such fraud, factors like session data, device information, and behavioural biometrics are evaluated to authenticate accounts. Analysing user journeys for behavioural patterns also aids in identifying account takeovers before they cause financial harm.

Payment fraud involves false or illegal transactions carried out by cybercriminals, depriving victims of money, personal property, interest, or sensitive information.

Moving on to industry-specific fraud detection, the banking and financial services sector faces various frauds due to the increasing digitization and online transactions. API fraud, where certain European financial institutions open their services via APIs, creates a new attack surface for fraudsters. Stolen/fake credit card fraud involves generating fake cards based on user information obtained through techniques like card skimming. Website cloning is another prevalent method where cybercriminals create clone sites to deceive users into providing personal or financial information.

The ecommerce and retail sector, particularly during the COVID-19 pandemic, has witnessed an increase in fraud targeting users through various channels. Promo abuse occurs when individuals exploit promotions or coupons, benefiting from them in ways not intended. Payment fraud in ecommerce involves illegal online transactions, depriving users of their money or personal property. Delivery fraud, including identity theft and friendly fraud, poses significant challenges as well. Marketplaces and online ads are susceptible to fraud through referral and promotion abuse and fake reviews. Fake reviews can damage brands and erode trust, impacting consumer decisions. Referral and promo abuse exploit programs meant for customer benefits, leading to extra costs

In the IT and telecom sector, phone fraud, call forwarding fraud, multiple transfers fraud, and Wangiri fraud are prevalent. ``111Call forwarding fraud exploits PBX or IVR systems to route calls to expensive destinations for profit. Multiple transfers fraud and Wangiri fraud also pose significant challenges in telecom fraud prevention. Each sector faces unique fraud challenges, requiring tailored fraud detection solutions to safeguard against financial losses and maintain trust with customers. Implementing robust fraud detection measures involves analysing various data points, behavioural patterns, and transactional activities to identify and mitigate fraudulent activities effectively.

Results and Discussion:

The implementation of our AI-powered fraud detection system has yielded substantial improvements in the overall security infrastructure of businesses operating across various sectors. By harnessing advanced technologies like machine learning, data mining, neural networks, and pattern recognition algorithms, the system has demonstrated remarkable precision in identifying potential fraud schemes. This enhanced accuracy has led to more effective fraud prevention measures, resulting in reduced financial losses and reputational risks for organizations.

The system's ability to adapt and learn continuously has been a key factor in its success, allowing it to detect both known fraud patterns and emerging threats with high efficiency. This adaptability is crucial for staying ahead of fraudsters who constantly evolve their tactics to evade detection. Additionally, the system's real-time monitoring and alerting features have further strengthened its efficacy by enabling swift responses to suspicious activities, thereby mitigating risks and preventing fraudulent transactions in a timely manner. Furthermore, the emphasis placed on security and compliance with regulatory standards has bolstered the system's overall integrity and trustworthiness. Technologies such as block-chain, encryption, and

biometric authentication have been instrumental in ensuring robust protection for sensitive data, minimizing the chances of data breaches or unauthorized access. Compliance with anti-money laundering (AML) and know-your-customer (KYC) regulations has not only reduced legal vulnerabilities but also cultivated trust among customers, partners, and regulatory bodies, enhancing the organization's reputation and credibility.

Conclusion:

In conclusion, the implementation of our AI-based fraud detection system marks a significant milestone in enhancing the security landscape for businesses across various sectors. Through the integration of advanced technologies like machine learning, data mining, neural networks, and pattern recognition algorithms, our system has demonstrated exceptional accuracy in identifying potential fraud schemes. This heightened accuracy translates into improved fraud prevention measures, ultimately reducing financial losses and protecting the reputation of organizations.

The adaptability and learning capabilities of our system ensure its effectiveness in detecting both known and emerging fraud patterns, staying ahead of evolving threats posed by fraudsters. The real-time monitoring and alerting features further bolster the system's responsiveness, enabling swift actions to mitigate risks and prevent fraudulent transactions. Additionally, our system prioritizes security and regulatory compliance, leveraging technologies such as block-chain, encryption, and biometric authentication to safeguard sensitive data and ensure adherence to AML and KYC regulations.

Overall, our AI-driven approach to fraud detection delivers concrete results by mitigating risks, enhancing data security, maintaining compliance, and fostering trust within the financial ecosystem. This comprehensive solution not only protects businesses from financial losses but also contributes to a more secure and resilient environment for conducting transactions and preserving customer trust.

Reference:

1. Oxford Learner's Dictionaries, Oct. 2021, [online] Available.
2. Y. Sahin, S. Bulkan and E. Duman, "A cost-sensitive decision tree approach for fraud detection", *Expert Syst. Appl.*, vol. 40, pp. 5916-5923, 2013.
3. T. Quah and M. Sriganesh, "Real-time credit card fraud detection using computational intelligence", *Expert Syst. Appl.*, vol. 35, no. 4, pp. 1721-1732, 2008.
4. Kou, C.-T. Lu, S. Sirwongwattana and Y.-P. Huang, "Survey of fraud detection techniques", *Proc. IEEE Int. Conf. Netw. Sens. Control*, vol. 2, pp. 749-754, Mar. 2004.
5. J. Kumar and V. Saxena, "Rule-based credit card fraud detection using user's keystroke behavior" in Soft Computing: Theories and Applications, Singapore:Springer, pp. 469-480, 2022.
6. B. Cao, M. Mao, S. Viidu and P. S. Yu, "HitFraud: A broad learning approach for collective fraud detection in heterogeneous information networks", *Proc. IEEE Int. Conf. Data Mining*, pp. 769-774, 2017.
7. X. Ruan, Z. Wu, H. Wang and S. Jajodia, "Profiling online social behaviors for compromised account detection", *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 1, pp. 176-187, Jan. 2016.
8. F. M. Naini, J. Unnikrishnan, P. Thiran and M. Vetterli, "Where you are is who you are: User identification by matching statistics", *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 2, pp. 358-372, Feb. 2016.
9. Y. Dou, Z. Liu, L. Sun, Y. Deng, H. Peng and P. S. Yu, "Enhancing graph neural network-based fraud detectors against camouflaged fraudsters", *Proc. 29th ACM Int. Conf. Inf. Knowl. Manage.*, pp. 315-324, Oct. 2020.
10. Y. Dou, G. Ma, P. S. Yu and S. Xie, "Robust spammer detection by Nash reinforcement learning", *Proc. 26th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining*, pp.924-933,Aug.2020.