A Study: A Role of AI in Detecting Fraudulent Credit Card Transactions

Yogesh Sonvane; Gaurav Buradkar; Atish Musale
Dept.Master in Computer Application, GHRCEM, Nagpur, India

Abstract

For Banking transactions, credit Card Play a role in Economically growing society it allows a cashless society, credit cards support economic growth by lowering government spending on the production and distribution of currency. Physical theft, phishing, skimming, data breaches, identity theft, chargeback scams, card testing, mail interception, ATM fraud, SIM swapping, and rewards theft are all examples of credit card fraud. In FY24, 29,082 instances of credit/debit card and internet-based fraud were recorded, which represents a 334% rise over the 6,699 cases that occurred in the previous fiscal year. Governments may save billions of moneys by implementing a cashless society, which they could then use on other economic projects. Credit card fraud is an existential threat because it can lead to large financial losses and security risks. Traditional techniques for detecting fraud, including rule-based systems, are frequently unable to keep up with new fraudulent strategies. To increase the security of transactions, improve the accuracy of detection, and reduce false positives, this paper aims to evaluate the credit card fraud detection methods used by banks and the difficulties in implementing the said methods & exploring how artificial intelligence (AI) can be integrated into credit card fraud detection. This study examines various AI methodologies, system architecture, and the deployment of a web-based fraud detection system.

Keywords: Credit Card Fraud, AI, Fraud Detection, Machine Learning, Deep Learning, Anomaly Detection, Transaction Security, Real-Time Monitoring.

1. Introduction

For Banking transactions, credit card fraud is an existential threat because it can lead to large financial losses and security threats. Physical theft, phishing, skimming, data breaches, identity theft, chargeback scams, card testing, mail interception, ATM fraud, SIM swapping, and rewards theft are all examples of credit card fraud. Traditional techniques for detecting fraud, including rule-based Systems, frequently unable to keep up with new fraudulent strategies. In order to increase Security of transactions, improve the accuracy of detection, and reduce false positives, this investigation looks at how Artificial Intelligence (AI) can be included into credit card fraud detection. To identify doubtful transaction patterns in real time, this suggested AI-powered solution makes use of anomaly detection methods, deep learning algorithms, and machine learning models. Financial institutions could boost overall security, automate fraud reporting, and detect fraudulent activity more efficiently by applying AI. The use of artificial intelligence (AI) techniques has led to an evolution in fraud detection, a crucial aspect of protecting a variety of sectors. The importance of financial fraud puts the integrity and stability of the entire financial system in jeopardy in addition to posing significant threats to individual

DOI: https://doi.org/10.5281/zenodo.15464683

customers [12]. In order to ensure a reliable and flexible approach to fraud prevention, this study investigates different AI methodologies, system architecture, and the deployment of a web-based fraud detection system. AI is a collection of cutting-edge tools, techniques, and processes that are critical to the present and future growth of our economy and society. Financial services, optical character recognition, autonomous driving in cars, and disease diagnostics are just a few of the industries that heavily rely on artificial intelligence. Both big and small firms are currently using AI technology. Millions of people now use AI on a regular basis. It is said that artificial intelligence has the potential to significantly boost creativity and technological growth [5].

1. Literature Survey

A Various kinds of fraud methods for detection, which include rule-based systems, machine learning algorithms, and blockchain-based solutions, are used in financial security. While its growing popularity, rule-based detection lacks the capacity to adapt to changing fraud actions. By learning from previous transaction data, machine learning models such as Support Vector Machines (SVM), Random Forest, and Decision Trees improve the accuracy of fraud detection. Autoencoders and Long Short-Term Memory (LSTM) networks are both deep learning techniques that effectively detect complex fraud patterns. Abnormal transactions can also be identified with the help of anomaly detection methods like One-Class SVM and Isolation Forest. Blockchain ensures secure records of transactions; however, due to its high implementation costs, its use is still restricted. This paper analyses how these issues are addressed and how AI-powered fraud detection systems provide financial institutions with a scalable solution.

This literature review explores key research advancements in credit card analytics, emphasizing fraud detection, risk assessment, and data analytics.

2. Evolution of Credit Card Analytics:

Traditional statistical techniques used for risk assessment are where credit card analytics first emerged. An interesting viewpoint on applying statistics and machine learning to credit risk assessment was offered by Galindo and Tamayo [11, 13]. Numerous later studies that emphasised the value of a data-driven strategy in the financial sector were made possible by their work.

3. Fraud Detection Techniques:

AI-driven fraud detection for credit card transactions utilizes various techniques to enhance accuracy and efficiency. Machine learning models classify transactions based on historical data, while deep learning leverages neural networks to detect complex fraud patterns. Anomaly detection identifies deviations from normal spending behaviour, and behavioural analysis tracks user habits to flag suspicious activities. Natural language processing (NLP) helps detect fraud in textual data, such as phishing attempts, whereas graph-based detection uncovers fraud networks by analysing transactional relationships. Reinforcement learning adapts to evolving fraud patterns through real-time feedback, and hybrid approaches combine multiple AI techniques for a more robust fraud detection system.

1. Risk Assessment Paradigms:

Another crucial component of credit card analytics, risk assessment, has moved from

DOI: https://doi.org/10.5281/zenodo.15464683

conventional techniques to more dynamic, data-driven strategies [10, 13].

2. Data Analytics in the Credit Card Industry:

Data analytics has become increasingly important to the credit card industry. A thorough analysis of data modelling and analytics from a big data standpoint. Their research brought to light the subtleties of architecture and the difficulties in managing enormous volumes of data [8, 13].

3. Methodology

1. Data Collection:

The work will utilize an information set that includes both created and real debit card transactions, in addition to details regarding the seller, purchase amount, location, time, and specific patterns of behaviour. Information from banking institutions and freely available information sets, such as the credit card fraud detection dataset from Kaggle, is the database utilized for evaluation.

2. Data Preprocessing:

With the goal of correcting the imbalances in classes, addressing the absence of values, incorporating variable types, managing the cost of transactions, and organizing the collected information, these techniques and sampling approaches are used to even out the dataset.

3. Model Selection & AI Techniques:

The detection of fraud is being studied using a variety of artificial intelligence designs, including supervised learning algorithms such as support vector machine models (SVM), decision trees, random forest models, and logistic regression. Unsupervised approaches to learning, such as isolation forest learning or one-class SVM, are utilized for identifying anomalies. Machine learning models employ methodologies like neural network training (AI), long short-term memory (LSTM), and autoencoders to recognize intricate fraud trends.

4. System Design & Implementation:

The online platform's website, which acts as a fraud prevention structure, is created using HTML, CSS, and JavaScript. The back end of the application, which handles payments and executes the structure for scam identification, is developed with Python and Django. PostgreSQL or MySQL is utilized to manage information securely and monitor past transactions and scam notifications. Protective measures such as encrypted SSL connections and two-factor authentication (2FA) are implemented to enhance the system's security.

5. Model Training and Evaluation:

The artificial intelligence models are built using specified trade information sets, and their effectiveness is evaluated using a range of outcome statistics, such as precision, recall, accuracy, the F1 score, and the AUC-ROC curve. These metrics help in determining how well the technology separates illegal from honest transactions.

6. Testing & Deployment:

When trained, the machine learning model has been integrated into the scam detection network. The platform undertakes a variety of assessment steps, comprising API validation to ensure secure and accurate processing of payments, user experience validation to guarantee pleasant user experiences, and real-time evaluation with generated payments to assess fraud detection outcomes.

DOI: https://doi.org/10.5281/zenodo.15464683

7. Future Improvements & Continuous Improvement:

The algorithm is frequently updated by enhancing artificial intelligence to adapt to new fraud behaviours. Potential.

4. AI Methodologies

Many artificial intelligence (AI) techniques, specifically those that use deep learning (DL) and machine learning (ML), have proven to be very effective in recognizing anomalies and patterns that point to fraud. These techniques offer several advantages over traditional rule-based systems, including the capacity to manage huge volumes of data in real time and react to new varieties of fraud. Some the main AI techniques for recognizing fraud are:

4.1 Supervised Learning:

To distinguish between authentic and fraudulent transactions, supervised learning algorithms are trained on labelled datasets. This method has shown impressive results in a number of fraud detection scenarios:

● **Credit Card Fraud:** According to a thorough study by Bhattacharyya et al., supervised learning methods like support vector machines and logistic regression were able to detect fraud in credit card transactions with up to 98.9% accuracy [9].

● **E-commerce Fraud:** A supervised learning model decreased fraudulent transactions by 73% and false positives by 28% over a six-month period in a large-scale application by a major online retailer [9].

● **Insurance Claim Fraud:** A top insurance firm saved $12 million a year by using a supervised learning model that detected 35% more fraudulent claims than conventional techniques [7].

4.2 Unsupervised Learning:

Unsupervised learning algorithms are especially helpful for spotting novel forms of fraud because they can find anomalies in data without the need for prior labelling.

● **Retail Payment System:** up to 95% of fraud tendencies in retail payment systems that had not yet been identified might be detected using unsupervised learning approaches [7].

● **Money Laundering identification:** By implementing an unsupervised learning model, a major multinational bank greatly improved its Anti-Money Laundering (AML) procedures by reducing false positives by 50% and increasing the identification of suspicious transactions by 20%[4].

● **Loyalty Program Fraud:** An airline firm saved an estimated $7 million in potential damages by using unsupervised learning to find anomalous patterns in its loyalty program. This helped them uncover a sophisticated fraud ring that had escaped detection by conventional approaches [4].

4.3 Reinforcement Learning:

Using input from identified fraud incidents, reinforcement learning continuously improves model performance. This strategy has shown promise in adjusting to changing fraud trends:

● **Adaptive Fraud Detection:** Within three months of deployment, a fintech company's reinforcement learning model demonstrated a 20% increase in fraud detection rates compared to static algorithms [4].

5. Fraud Detection In Banking

DOI: https://doi.org/10.5281/zenodo.15464683

In the banking industry, fraud is defined as intentional deception meant to obtain unapproved financial gains, frequently at the expense of financial institutions or their clients. The two main categories of fraudulent activity are internal and external fraud (Fang et al., 2021). Attacks from outside sources, including phishing, identity theft, and payment fraud, are examples of external fraud (Nicholls et al., 2021). For example, cybercriminals frequently use flaws in online banking systems to carry out illegal transactions or steal private data (Ali et al., 2022) [14].

- **The Transition from Conventional Techniques to AI-Based Strategies**

  Conventional fraud detection techniques, which are mostly rule-based systems, use preset criteria and thresholds to identify questionable activity. These algorithms are useful for identifying simple irregularities, but they are frequently inflexible and unable to adjust to changing fraud trends (Kapadia et al., 2022). Rule-based methods are resource-intensive and prone to high false-positive rates because they need to be updated manually on a regular basis. Furthermore, their capacity to identify new or complex assaults is constrained by their dependence on past fraud trends [14].

- **Types of Credit card fraud**

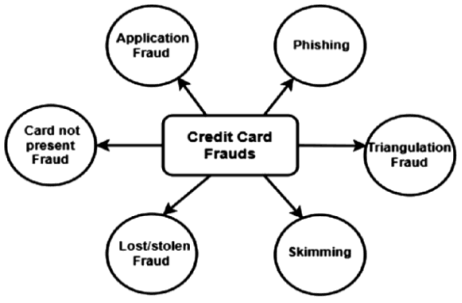

Fig. Types of credit card fraud [6]

- **Using generative AI to improve and supplement fraud detection techniques**

Transformer deep neural networks are the base of generative AI. OpenAI's ChatGPT is one such example of generative AI. Sequential data, such as payment histories and phrases, needs to be utilised for learning generative AI, which aims to generate data sequences as output. It varies from past methods that provide unambiguous categorisation, such fraud or not fraud, using the input and training data delivered to the model in each order. Other method of classification Supply a single output, but generative AI can produce findings repeatedly.

Generative AI has become the ideal instrument necessary to artificially produce data based on real data. Since there are still few viable fraud samples and they are difficult for machine learning to learn from, its development will illustrate crucial applications in fraud detection. In order to improve the fraud signals for essential machine learning tools for fraud detection, a model can employ generative AI and leverage the patterns already present to create new, synthetic samples that mimic real fraud samples. The non-fraudulent information typically comes first in the chain of events and represents the cardholder's real behaviour. In order to train data for fraud detection in machine learning, generative AI may create such payment sequences and mimic a card fraud attack [1].

- **Tools used in OpenAI to effectively detect Fraud in Finance**

  AI-driven fraud detection methods are being used by financial institutions more and more to examine massive transaction records and spot questionable activity.

  1. Logistic regression: Classifies transactions according to cause-and-effect linkages as either fraudulent or non-fraudulent. Functions well with organised

DOI: https://doi.org/10.5281/zenodo.15464683

datasets, but gets complicated when dealing with big data and a lot of variables [1].

2. Decision Trees: Develops a visual model for fraud detection decision-making. identifies important factors linked to fraud and categorises questionable activity. clarifies the reasons for the flagging of specific transactions, improving interpretability.

3. Random Forest: Combines several decision trees to increase precision. improves the accuracy of the fraud detection model and lowers classification mistakes. effectively manages missing and imbalanced data, however it occasionally causes overfitting.

4. Networks of neurones: Uses cognitive processes that are similar to those of humans to examine transaction history. detects new fraud attempts by continuously learning from previous fraud trends. improves detection accuracy by using numerous computing levels.

5. Learning in Depth: Improves fraud protection by learning from large transaction data.
Mastercard uses deep learning models to identify fraudulent transactions and minimise false declines.
By analysing data from billions of transactions per year, it gets better [1].

6. Natural language processing: Detects fraud by examining chat, text, and audio interactions.
utilised to improve standard fraud prevention by financial organisations such as American Express and PayPal. identifies possible fraud by extracting signs from consumer interactions.

- **Benefits of Using AI-Powered Fraud Detection Systems**

AI-powered fraud detection techniques offer an improved method than conventional approaches since they offer real-time analysis and complex fraud pattern detection, and they can be modified to new fraud schemes. By reduce the time, money, and false positives involved, OpenAI will improve the efficiency and accuracy of detecting fraud, and lead to fewer financial losses from cybercrimes. From the perspective of the client, organisations that successfully and precisely detect fraudulent activities protect their clients from becoming individuals of financial fraud, so companies that implement OpenAI benefit from preventing fraud and improving customer loyalty and retention [1].

- **Challenges in AI-Driven Fraud Detection**

Data Privacy and Security: Ensuring compliance with regulations while protecting sensitive financial data.

Imbalanced Datasets: As fraud cases are rare, AI models find difficulties with understanding.

Evolving Fraud Practice: As fraudsters constantly develop new methods, AI models have to change.

False Positives and Negatives: Incorrect fraud detection could result in safety concerns and dissatisfied users.

Explainability and Transparency: Many advanced AI models work as "black boxes," making it harder to figure out their conclusions.

High Computational Costs: AI model setup and training need a large infrastructure and commitment to resources.

6. Key Technologies

Machine learning (ML) and artificial intelligence (AI): These are the tools for

DOI: https://doi.org/10.5281/zenodo.15464683

identifying fraud and examining transaction trends.

Data Processing & Analytics: Preprocessing and statistical analysis are done using Pandas, NumPy, and Scikit-learn.

Backend Development: For safe transaction processing, Python-based frameworks such as Flask and Django were used.

Frontend development: It is the process of creating user interfaces using HTML5, CSS3, JavaScript, React.js.

Database management: PostgreSQL and MySQL are used to store transaction data securely and monitor fraud reports.

Security Measures: SSL encryption, Two-Factor Authentication (2FA), and hashing algorithms (SHA-256, crypt).

Fraud Detection AI: Integration of TensorFlow, IBM Watson, and Azure AI for real-time fraud identification.

System Testing: Selenium for UI testing, Postman for API validation, and Pytest for backend testing.

Cloud Deployment: Hosted on AWS, Google Cloud, or Microsoft Azure for scalability and real-time processing.

7. Future Scope

As technology develops, AI-driven fraud detection is anticipated to change as well. Future studies will concentrate on:

Explainable AI (XAI): Improving the interpretability of models to learn more about fraud detection choices.

Federated Learning: Protecting data privacy while facilitating cooperative fraud detection.

Blockchain Integration: Improving security and stopping fraudulent transactions with blockchain technology.

Automated Feature Engineering: AI-powered techniques for dynamic feature extraction and selection.

Edge Computing: By processing transactions closer to the point of origin, edge computing lowers latency in fraud detection.

8. Conclusion

By providing advanced, real-time solutions to identify fraudulent activity, the incorporation of AI in credit card fraud detection has revolutionised the banking industry. ML and DL, two AI-based fraud detection models, improve security, accuracy, and adaptability while lowering operating expenses. To further optimise AI models, however, issues including data privacy concerns, changing fraud strategies, and computational complexity must be resolved. Financial transactions will become safer and more transparent as a result of future developments in Explainable AI, federated learning, and blockchain integration, which will further improve fraud detection methods. Financial institutions must use cutting-edge AI-driven fraud detection systems to keep ahead of scammers as AI develops further in order to protect both customers and companies.

9. Reference

[1] Ahmadi, S. (2023). Open AI and its impact on fraud detection in the financial industry. Journal of Knowledge Learning and Science Technology, 2(3), 263–281. https://doi.org/10.60087/jklst.vol2.n3.p281

[2] Smith, J. R. (2022). The role of AI in financial fraud detection. Journal of Financial Technology, 12(3), 78–92.

[3] Li, X., Jiang, Y., & Chen, L. (2020). Machine learning techniques for credit card fraud detection: A survey. IEEE

Access, 8, 54517–54530. https://doi.org/10.1109/ACCESS.2020.2989496

[4] Carcillo, F., Le Borgne, Y., Caelen, O., & Bontempi, G. (2018). Streaming active learning strategies for real-life credit card fraud detection: Assessment and visualization. International Journal of Data Science and Analytics, 5(4), 285–300.

[5] Musaab, M. A. (2018). Artificial intelligence in banking industry: A review on fraud detection, credit management, and document processing. Research Reviews: Science and Technology, 2(3), 25–46.

[6] Ounacer, S., Ardchir, S., Rachad, Z., & Azouazi, M. (2018). A proposed architecture for real-time credit card fraud detection. Journal/Conference Name, Volume (Issue),

[7] Cavalcante, R. C., Brasileiro, R. C., Souza, V. L. F., Nobrega, J. P., & Oliveira, A. L. I. (2016). Computational intelligence and financial markets: A survey and future directions. Expert Systems with Applications, 55, 194–211. https://doi.org/10.1016/j.eswa.2016.01.019

[8] Ribeiro, A., Silva, A., & Rodrigues da Silva, A. (2015). Data modeling and data analytics: A survey from a big data perspective. Journal of Software Engineering and Applications, 8(12), 617–634.

[9] Bhattacharyya, S., Jha, S., Tharakunnel, K., & Westland, J. C. (2011). Data mining for credit card fraud: A comparative study. Decision Support Systems, 50(3), 602–613. https://doi.org/10.1016/j.dss.2010.11.002

[10] Khandani, A. E., Kim, A. J., & Lo, A. W. (2010). Consumer credit-risk models via machine-learning algorithms. Journal of Banking and Finance, 34(11), 2767–2787.

[11] Galindo, J., & Tamayo, P. (2000). Credit risk assessment using statistical and machine learning: Basic methodology and risk modelling applications. Computational Economics, 15, 107–143.

[12] Odeyemi, O. (n.d.). Reviewing the role of AI in fraud detection and prevention in financial services.

[13] Patel, K. K. (n.d.). Credit card analytics: A review of fraud detection and risk assessment techniques.

[14] Faisal, N. A., & Nahar, J. (n.d.). Fraud detection in banking: Leveraging AI to identify and prevent fraudulent activities in real-time.

[15] Chunchu, A. (n.d.). Artificial intelligence in retail fraud detection: Enhancing payment security.

[16] Abdulrahman, M. H. A. (n.d.). The impact of artificial intelligence (AI) in detecting fraud.