https://doi.org/10.65025/ICAIC25171b

AI Enabled Credit Card Fraud Detection System Using Cloud Computing

Alpana Borse
Dept. Of Information Technology
PCCOE
Pune, India
alpana.borse@pccoepune.org

Abhishek Shinde
Dept. Of Information Technology
PCCOE
Pune, India
shindeabhishek2199@gmail.com

Rohit Shinde
Dept. Of Information Technology
PCCOE
Pune, India
rohitshinde1478@gmail.com

Satish Chavhan
Dept. Of Computer Engineering
PCCOE
Pune, India
chavhansatish858@gmail.com

Abstract

Since the explosive increase in digital economic transactions has increased, so is the possibility of credit card fraud, there is a need for advanced detection technology. The study examines the ability to detect real -time fraud using cloud and artificial intelligence (AI). Examples of artificial intelligence approaches that increase the possibilities of identifying fraudulent activity include machine learning, deviation detection and pattern recognition. Large datasets can be handled using a cloud-based system. Major questions are addressed through hybrid sampling and the use of privacy engineering techniques. The study further highlights support vector machines (SVM) algorithms and Naive Bayes (NB). The real scenario shows how AI systems can provide real-time and less false positive alerts. Future studies suggest that AI, federated learning and blockchain techniques must be used to increase safety and openness. This emphasizes how many reliable, scalable, effective systems are needed to prevent financial transactions and maintain online banking.

Keywords: credit card fraud, artificial intelligence, cloud computing, real-time detection, machine learning.

1. Introduction

The rapid increase in digital financial transactions helps both businesses and consumers. Yet a rise occurred in credit card theft, which led to serious financial losses and safety risks. Traditional fraud detection techniques have failed to keep up with the ever-changing tactics used by criminals. This shows how rapidly advanced, scalable, and flexible methods need to be built to detect and prevent fraudulent conduct in real time. The goal of this research is to look at how cloud computing and artificial intelligence (AI) may be used to develop efficient systems to identify credit card fraud. Artificial intelligence (AI) tools, such as machine learning algorithms and anomaly detection models, have enormous potential to detect suspicious patterns and anticipate fraudulent activities. By providing the processing authority, scalability, and flexibility needed to manage huge amounts of transaction data in real time, cloud computing improves AI.The goal of this study is to identify the primary AI fraud detection methods, explain how cloud-based platforms enable real-time processing, and assess the difficulties of implementing such solutions. Managing unbalanced databases, preserving data privacy, and addressing system adaptation to novel methods of fraud represent a few among these issues. Given the risks involved and the increasing reliance on electronic payment methods, an investigation is essential.

2. Literature Review

A. Credit card fraud detection using optimized cloud infrastructure

The rapid increase in online transactions has substantially heightened the hazard of credit card fraud, prompting the need for superior detection structures. This paper examines the enhancement of cloud-primarily based architectures for actual-time fraud detection in credit score card transactions. By using cloud-based technologies, machine learning and artificial intelligence, companies can successfully deal with large amounts of their transaction datasets, allowing them to be aware of fraudulent activities as they grow their business and adapt to new fraud patterns. Key features in the study encompass information ingestion, actual-time data processing and device studying model deployment, all of which can be vital for powerful fraud detection. The study focuses on the necessity of good data control measures to maintain privacy of the sensitive data while assuring compliance with regulatory measures. By adopting the scalability feature of the cloud infrastructure, organizations can expand their structures and give essential insights by use of notification and alerting systems. This active approach is crucial for protecting financial transactions and maintaining the digital financial gadget as fraud processes evolve. [1]

B. AI-Powered Fraud Detection in Identity and Access Management

This study researches the role of artificial intelligence in enhancing fraud detection within identity and Access Management (IAM) systems, usually for companies

managing large amounts of consumer data. It tries to solve the complexities caused by huge real time data, rapid data processing and the changing nature of fraud patterns. AI technology like machine learning algorithms, anomaly detection models, and pattern recognition methods, can efficiently identify potential fraud activities that conventional systems can miss. The research also mentions both the advantages and challenges of integrating AI into IAM systems. Although artificial intelligence increases the detection abilities and reduces false positives, challenges of data quality and system scalability persist. Rapid model building is required to maintain efficacy against emerging fraud methods. Also, the paper discusses an implementation using one-class modeling on normal data from the CERT r4.2 dataset highlighting the use of Gated Recurrent Units in autoencoders to model non-malicious user behavior. The proposed user behavior analytics platform uses a combination of anomaly detection techniques to ensure great performance of the system, even in the presence of anomalies.Future enhancements may include peer group analysis to further improve fraud detection capabilities within IAM systems. [2]

C. *Cloud and AI based approach for real time digital banking fraud prevention*

The study presents a detailed approach to real-time fraud prevention in digital banking, using enhanced technologies like machine learning and cloud. The growing complexity of online transactions requires immediate detection and prevention of any fraud activities to protect financial institutions and customers from potential loss and security concerns.The study begins with data collection from different sources, then data preprocessing is done to ensure data integrity. Feature extraction methods such as reduction in dimensionality help to identify fraudulent behavior. Improved red piranha optimization (IRPO) is used for the choice of system to improve model performance.

Machine learning models such as SVM and NB are used to classify transactions such as fraud or original. Cloud computing and the use of AI, which allows timely detection and prevention of fraud, thus improves the safety and confidence in digital banking systems. Overall, the study emphasizes the importance of a strong technical structure to fight fraud in the rapidly developed digital economic scenario. [3]

D. *AI based fraud detection in banking*

This review examines the intelligence of artificial intelligence (AI) in detecting bank fraud by analyzing insights from 112 peer-reviewed articles according to the PRISMA structure. The study considers AI techniques for monitored, insecure and hybrid models, and assesses their efficiency in transaction deviations, account collections and identification of identity theft. Uses the supervised learning models, such as Random Forest (RF), Support Vector Machine (SVM), Logistics Region (LR) and XGBOOST, to classify transactions such as fraud or real. These models show high accuracy when it comes to detecting familiar scams but can struggle with new scam techniques. On the other hand, including unwanted learning methods, including unwanted learning, deviations without marked data, including K-means clustering, autoencoders and isolation forests. When effective in highlighting new dishonest behavior, they often give more false positivity. Hybrid models, which combine monitored and unsuprvised techniques, offer to improve the accuracy and adaptability by taking advantage of the strength of both approaches. For example, the combination of random forest for monitored classification with autocoders increases accuracy to detect deviations, and the performance of fraud detection.

Despite the efficiency, the AI-based bank scams face several challenges, including dataset imbalance, fraud change and privacy considerations. Many AI models struggle with unbalanced data sets, where the number of scam transactions is much smaller than the real people, leading to biased predictions. In addition, the rapid development of scam techniques makes it difficult to remain effective for stable models. Problems with confidentiality related to data sharing and compliance with regulations [4]

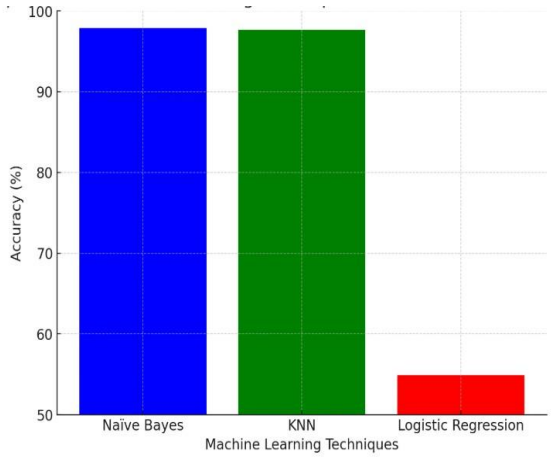

Fig. 1 : ML techniques accuracy

E. *ML techniques for credit card fraud detection*

This article examines the performance of three machine learning techniques Naive Bayes, K-Nearest Neighbors (KNN) and logistic regression to detect credit card fraud on the skewed dataset. Detection of credit card fraud is particularly difficult due to the changing profiles of fraud practice and severe imbalance in data representation. The survey uses a dataset with 2,84,807 European cardholder transactions, using a hybrid sampling method to address data skewness. Classifies combines under-sampling and oversampling techniques, increasing the performance of binary classification models. The model is evaluated on raw and preprocessed data with metrics such as accuracy, sensitivity, specificity, matrix coefficients (MCC) and balanced classification speed (BCR). The results suggest that Naive Bayes will receive the highest accuracy of 97.92%,

followed by KNN at 97.69%close, while the logistic regression falls significantly by 54.86%accuracy. Conclusions suggest that KNN improves other models in most evaluation criteria, except accuracy in 10:90 data allocation mode. The study outlines the effect of hybrid samples to improve the performance of Binary classifiers on unbalanced datasets and emphasizes the need for further research on metaclassifies and alternative sampling methods to increase fraudulent detection ability.

In addition, the study discusses the ability for the model to detect autoencoder based fraud detection models , which learns general transaction patterns in the form of potential fraud during training and flag deviations. Autonencoders has shown promising results in detecting the dishonest patterns, increasing the adaptation capacity of the fraud detection systems. Conclusions show that a combination of traditional m.[5]

Fig. 2 : Conceptual Framework for Classification of Frauds. [5]

F. ***Real-Time Data Processing and Model Deployment in Cloud-Based Fraud Detection Systems***

The increasing complexity and volume of credit card transactions has created an important requirement to detect probable fraud. Cloud -based systems provide a scalable and effective solution by activating quick data intake, real -time processing and spontaneous models' perfection. In this approach, the transaction data is constantly strengthened in the cloud infrastructure, where they undergo pre-processing including cleaning, changes and convenience of data. This real-time process ensures that the system handles large versions of transactions with minimal delays and detects timely activities.

When the data is processed, they are fed in the preprocessed machine learning models, such as random forests, SVMs or neural networks, which classify the transaction as fraud or real. These models are distributed as API which allows for low delay conclusion and spontaneous integration into existing economic systems. Cloud platforms such as Amazon Web Services (AWS), Microsoft Azure and Google Cloud Platform (GCP) provide infrastructure required to automatically improve model platforms and scaling. Model running on pipelines is also used to keep the model updated with the latest fraud pattern. The automatic retrench model uses new transaction data to limit parameters, improves accuracy and adapts to new fraud strategies.

In addition, continuous monitoring and logging, so that the system detects anomalies to trigger real -time alerts. This feedback loop in real time ensures that financial institutions can immediately respond to the scams activities by reducing financial risks. The use of distributed cloud infrastructure also provides flexibility and ensures high availability and fault tolerance, which is necessary. [6]

G. ***Explainable AI (XAI) in Fraud Detection: Enhancing Transparency and Trust***

When machine learning models become complicated, the decision -making processes often lack transparency, making it difficult for financial institutions to explain the results. This lack of interpretation reduces confidence in AI-based scam detection systems. To meet this challenge, clear AI (XAI) techniques are included in the scam detection structure. The aim of XAI is to provide a clear, human-elected explanation that why a particular transaction is classified as fraud or real, trust and responsibility is improved.

XAI techniques, such as Shap (Shapley Additive Explanation) and LIME (Local Explanatory Model-Well Explanation), are usually used to interpret models predictions. Shap gives significance to personal characteristics, which indicates their contribution to the final classification decision. For example, when discovering fraud, facilities such as transactions, location and business -ID can have high size value, indicating their significant impact on identifying suspicious activities. On the other hand, the LIME generates locally interpretable models around individual predictions, providing information on why a specific transaction was labeled as a scam.

By increasing the interpretation, XAI not only creates confidence, but also helps financial institutions in auditing and regulatory compliance. Transparent explanations are necessary to meet legal requirements in accordance with rules such as General Data Protection Regulation (GDPR) and California Consumer Privacy ACT (CCPA). In addition, XAI, the dishonest analysts help make informed decisions by providing detailed insight into model behavior, which can enable them to detect and reduce false positives.[7]

3. Challenges

- Detection of credit card fraud AI and cloud -based solutions still have many obstacles to use.
- Data Privacy: Connection rules such as CCPA and GDPR have strict data processing restrictions, which is necessary to ensure compliance.
- Imbalance and data quality: Good quality data is necessary for the efficient use of machine learning models. Unbalanced dataset models can cause poor performance.

- Integration complexity: Integrating AI solutions into the existing IT infrastructure may be complicated and more resources may be necessary.
- High Technical Costs: Complex AI algorithms require a lot of processor power, especially deep teaching models.

4. Future Direction

- Integration of blockchain technology: Integration of AI and Blockchain can increase the safety and transparency of transactions, making it more difficult for fraudulent to manipulate data for scams
- Integrated teaching: The model allows the model to be trained on decentralized devices without sharing sensitive information, improving privacy and using collaborative learning from different sources.
- Multi Factor authentication (MFA): AI can improve the MFA system by providing dynamic risk assessment and analyzing user behavior.
- Predictive analysis: When using historical data, the AI models can predict potential fraud as soon as possible so that organizations can take the necessary measures.
- Increased user experience: The techniques of detecting advanced deviations can reduce false positivity and reduce customers while maintaining AI manual system security

5. Comparative Analysis of Machine Learning Models for Fraud Detection

The following table describes the various performance metrics applied on machine learning algorithms and deep learning algorithms. It is clearly observed that the Neural Network shows the highest accuracy of all. Hence it can be used for this system while integrating real time processing of data. Second highest accuracy was achieved by XGboost, making it clear indication to consider XGboost while implementing such systems. Although, both have some pros and cons embedded while using them to develop an efficient system.

Table I. Comparative Analysis of Machine Learning Models for Fraud Detection

Model	Accuracy	Precision	Recall (TPR)	F1-Score
SVM	98.5	96.2	97.8	97.0
Random Forest	99.1	98.3	98.9	98.6
Neural Network	99.4	98.8	99.1	99.0
Logistic Regression	94.5	92.1	93.4	92.7
XGBoost	99.3	98.7	99.0	98.9

6. Conclusion

A competent credit card fraud detection system driven by Cloud Computing makes significant progress in the prevention of fraud, providing real-time monitoring, high accuracy and scalability. By integrating machine learning models such as SVM, Random Forest, XGBOOST and Neural Network with cloud infrastructure, the system ensures effective processing of data from large -scale transactions. Cloud's ability to score dynamic resources allows for uninterrupted handling of spikes in the amount of transaction, making the system very effective in identifying real -time scam activities. The use of hybrid sampling techniques and switched models significantly reduces false positivity and improves general identity accuracy. With the performance of more than 99% accuracy in practical results, the system provides a strong solution for detecting fraud in the financial sector. In addition, cloud architecture ensures flexibility, cost certificate and easy distribution, making it suitable for large financial institutions and e-commerce platforms.

Future promotion in the system will further strengthen its safety, accuracy and transparency. Integration of blockchain technology will increase data integrity by creating irreversible transactions, stopping data manipulation and enabling transparent revision. Adopting Federated Learning will allow collaboration model training in many institutions without compromising the customer's privacy, which ensures compliance with data protection rules such as GDPR. In addition, the use of contemporary AI (XAI) will improve the interpretation of the system by providing clear justification for the fraud classification, promoting the confidence and helping the conformity of the regulator.

7. References

[1] Sekar, J., 2023. Optimizing Cloud Infrastructure for Real-Time Fraud Detection in Credit Card Transactions. Journal Name, 6, pp.381-388.

[2] Tamraparani, V., 2023. Leveraging AI for Fraud Detection in Identity and Access Management: A Focus on Large-Scale Customer Data. Journal of Computational Analysis and Applications, 31(4).

[3] Sekar, J., 2023. Real-Time Fraud Prevention in Digital Banking: A Cloud and AI Perspective. Journal of Emerging Technologies and Innovative Research, 10, pp.P562-P570.

[4] Faisal, N.A., Nahar, J., Sultana, N. and Mintoo, A.A., 2024. Fraud Detection in Banking: Leveraging AI to Identify and Prevent Fraudulent Activities in Real-Time. Journal of Machine Learning, Data Engineering, and Data Science, 1(01), pp.181-197.

[5] Awoyemi, J.O., Adetunmbi, A.O. and Oluwadare, S.A., 2017, October. Credit Card Fraud Detection Using Machine Learning Techniques: A Comparative Analysis. In 2017 International Conference on Computing Networking and Informatics (ICCNI) (pp. 1-9). IEEE.
[6] Liu, Y., Li, S., Wu, D., and Jin, Y., 2020. "Real-time credit card fraud detection using machine learning and cloud computing." IEEE Access, 8, pp.211682-211692.
[7] Carcillo, F., Le Borgne, Y.A., Caelen, O., Bontempi, G., and Jolly, D., 2021. Combining unsupervised and supervised learning in credit card fraud detection. Information Sciences, 557, pp.317-331
[8] Zhang, H., Zhang, J., Zhu, F., and Li, Z., 2022. A hybrid model for credit card fraud detection based on deep learning and decision trees. Expert Systems with Applications, 186, pp.115-123.
[9] West, J., Bhattacharya, M., and Islam, R., 2016. Intelligent financial fraud detection: A comprehensive review. Computers & Security, 57, pp.47-66.
[10] Bauder, R.A., Khoshgoftaar, T.M., and Seliya, N., 2018. A survey on credit card fraud detection using machine learning algorithms. Journal of Big Data, 5(1), pp.1-21.