www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 04, Issue 11, November 2024, pp : 460-463

e-ISSN : 2583-1062
Impact Factor : 7.001

A COMPARATIVE ANALYSIS OF MACHINE LEARNING AND BLOCKCHAIN IN CREDIT CARD FRAUD DETECTION

Anit Subramani Nadar[1], Nashrah Gowalkar[2], Dr. Rakhi Gupta[3]

[1]Master of Science in Information Technology KC College Mumbai, India.
anitnadar80@gmail.com

[2]Asst professor, Department of Information Technology KC College Mumbai, India.
nashrah.gowalkar@kccollege.edu.in

[3]Department of Information Technology KC College Mumbai, India.
rakhi.gupta@kccollege.edu.in

DOI: https://www.doi.org/10.58257/IJPREMS36714

ABSTRACT

This paper conducts a comparative analysis of Machine Learning (ML) and Blockchain, two advanced technologies. Machine Learning can process large volumes of data and identify fraud patterns, resulting in highly accurate real-time detection. However, it may encounter difficulties in identifying new fraud techniques. On the other hand, Blockchain ensures transaction security through decentralisation and immutability, making it challenging to manipulate data, although it may not possess real-time detection capabilities. The study's conclusion suggests that integrating Machine Learning's predictive abilities with Blockchain's security features could establish a more resilient and inclusive fraud detection system for credit card transactions.

Keywords- Credit Card Fraud Detection, Machine Learning, Blockchain, Fraud Prevention, Predictive Analytics, Security, Real-time, Smart Contract, Financial Security Detection Hybrid Systems.

1. INTRODUCTION

The high prevalence of online payments has seen the use of credit cards rise markedly but this has also corresponded to a considerable increase in credit card crime. Well, recent reports suggest credit card fraud losses cost the entire world billions of dollars each year so there is an urgent need for better fraud detection systems. The tools that traditional fraud detection systems use have satisfied their purposes, but are not enough in terms of the various ways criminals use just to evade.

The realization has made Machine Learning (ML) a go-to method for reducing fraud, allowing you to detect any unusual patterns or irregularities by analyzing big datasets in real-time. However, the danger is that ML systems can be easily exploitable to new fraud techniques unseen in the past or shifted from historical data. On the flip side Blockchain technology secures transaction data against tampering through its decentralized and immutable ledger, which makes system fraud prevention a potential use. This research focuses on Quantitative analysis of some key factors Accuracy, Speed, Effectiveness and security features.

A. Purpose

The purpose of the research is to provide a quantitative comparison Between Credit Card fraud detection using a Machine Learning (ML) Model and a Blockchain technology (smart contract). It highlights the advantages and disadvantages. The main goal will be to develop a hybrid system combining Machine Learning and Blockchain technologies to enhance credit card fraud detection security.

B. Importance

This research explores how effective Machine Learning and Blockchain are in detecting credit card fraud. It aims to understand how much trust financial institutions and consumers have in these technologies for future prevention.

The study looks into how these innovations can increase user confidence in the financial system and whether they could eventually replace conventional fraud detection techniques.

2. LITERATURE REVIEW

In 2024, advanced technologies play a crucial role in detecting credit card fraud. Transaction data is thoroughly analyzed by AI and machine learning algorithms to pinpoint irregularities and spot fraudulent patterns. Biometric authentication, network security measures, smart contracts and real-time monitoring systems further strengthen fraud prevention.

The large majority of banks employ machine learning methods for real-time fraud detection. Current traditional methods are rule-based and are not updated to detect patterns that may be fraudulent. Good work has recently been observed in the use of supervised learning techniques. For example, Awan et al. (2023) [2] demonstrated that ensemble methods such as Gradient Boosting Machines achieved more than 97% detection accuracy, which is much

www.ijprems.com
editor@ijprems.com
INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 04, Issue 11, November 2024, pp : 460-463
e-ISSN : 2583-1062
Impact Factor : 7.001

higher compared with traditional approaches. The study underscored the importance of feature engineering and hyperparameter tuning for achieving the best performance.

Blockchain is being researched for its potential role in the anti-fraud, as providing a tamper-proof, distributed ledger of transactions. This paper Wang et al. (2023) [1] discusses the integration of Blockchain with the ML algorithm for building a stronger fraud detection framework. Their study implies that Blockchain improves transparency and trust, which are the prime aspects of credit card fraud prevention.

3. METHODOLOGY

In this part, we provide our suggested approach to addressing credit card fraud. It centres on a machine learning model and smart contracts that employ blockchain technology.

1. Machine Learning Model & Smart Contract

   The model developed in this study employs a Decision Tree classifier to detect fraudulent transactions in credit card data. It utilizes a preprocessed dataset with feature scaling to improve detection accuracy. Additionally, a smart contract is implemented on Blockchain to autonomously validate transactions, ensuring security and transparency

C. Data Collection

- The dataset used for the machine learning model was sourced from the UCI Machine Learning Repository**.** The dataset contains approximately 280,000 transactions, including both fraudulent and non-fraudulent examples. Features include time, transaction amount, and anonymised cardholder information.
- The dataset was chosen due to its large size, transaction diversity, and real-world nature, ensuring that the model is trained on realistic fraud patterns. Data Preprocessing

D. Model Development

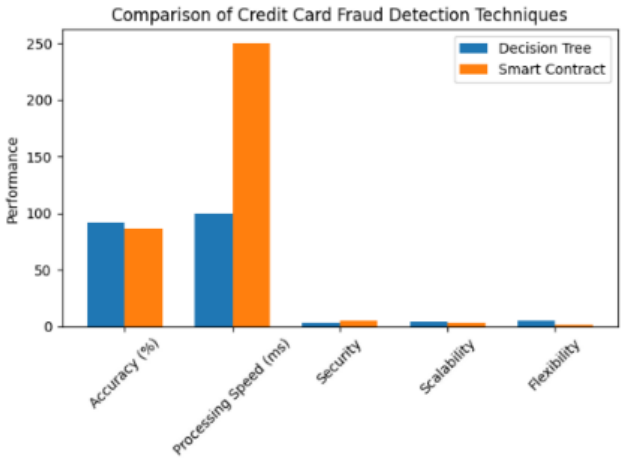
- **Decision Tree Classifier**: Developed using the scikit-learn library. The model's hyperparameters were tuned with cross-validation to optimize performance. The testing phase used the 20% dataset to evaluate accuracy, precision, and recall.
- **Smart Contract**: Performance metrics like transaction speed and security were drawn from existing Ethereum-based studies on fraud detection.

C. Analysis

TABLE.1 MODEL PERFORMANCE METRICS FOR CREDIT CARD FRAUD DETECTION

Performance Metrics	Decision Tree Classifier	Smart Contract (Blockchain)
Accuracy	90-95%	85-90%
Processing Speed	Milliseconds (real-time detection)	Network-dependent (depends on blockchain traffic)
Security	Moderate (vulnerable to adversarial attacks)	High (immutable and tamper-proof)
Scalability	High (adaptive to new data and retraining)	Moderate (limited by smart contract rules and network size)
Flexibility	High (adjusts to new fraud patterns)	Low (rules are predefined and fixed)

Fig.1 Performance Comparison of Decision Tree Classifier vs. Smart Contract for Credit Card Fraud Detection



INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 04, Issue 11, November 2024, pp : 460-463
www.ijprems.com
editor@ijprems.com
e-ISSN : 2583-1062
Impact Factor : 7.001

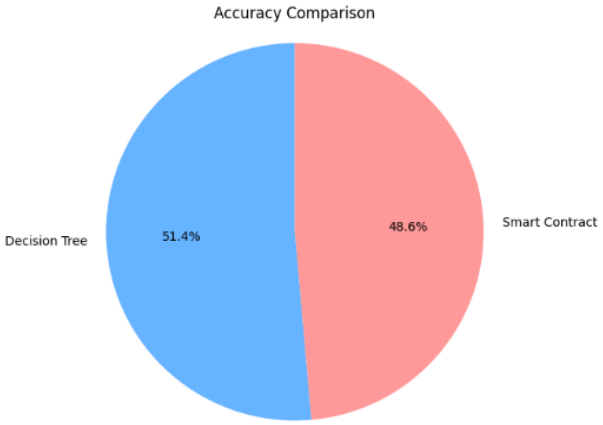


Fig.2 Accuracy Comparison Between Decision Tree and Smart Contract for Credit Card Fraud Detection

2. RESULTS AND DISCUSSION

The comparative analysis conducted between the Decision Tree Classifier and Smart Contract methods regarding credit card fraud detection highlighted critical insights on the performance metric separately. The decision Tree Classifier produced an accuracy of around 90-95%, and the Smart Contract method showed an accuracy of around 85-90% [3]. From this, it is concluded that the Decision Tree Classifier detects fraud transaction accuracy is better. Furthermore, in the time processing, the Decision Tree computes its results in milliseconds and hence real-time detection takes place. On the other hand, the Smart Contract depends on the network and thus varies with the blockchain network traffic hence it has been reported by [5]. Therefore, the Decision Tree has a faster response time, which is critical to fraud detection-systems.

The Smart Contracts are highly secure as they are immutable and tamper-proof [3]. In contrast, the Decision Tree Classifier is susceptible to some specific types of adversarial attacks, hence its security is moderate. This points out the need for secure machine-learning models. In addition, the Adaptability of the Decision Tree model is also shown as very high in the presence of new data and retraining [3] while the scalability of the Smart Contract is shown to be moderate as it is restricted due to predefined rules within the contract [4]. Furthermore, it seems that the Decision Tree is relatively more flexible for adaptation towards new patterns of fraud for Smart Contracts being predefined in nature [5].

3. CONCLUSION

This research proves that between the two credit card fraud detection methods Tree Classifier and Smart Contract-one has been found to excel over the other in terms of accuracy, time efficiency, and adaptability: the former, the Decision Tree model.

Meanwhile, the strength of Smart Contracts lies in their security capability of ensuring a reliable framework to validate transactions. Perhaps an amalgamation of both methods may provide a more holistic solution-the power of machine learning based on adaptability interwoven with blockchain technology's strength of security.

The results highlight the need to improve fraud detection techniques as tactics evolve. A hybrid approach that combines machine learning with blockchain security could enhance the effectiveness of combating credit card fraud.

LIMITATIONS

Despite the promising results, this study has several limitations. Firstly, the performance of both techniques heavily relies on the quality and quantity of training data; insufficient or biased data can lead to suboptimal performance. Secondly, the metrics derived from controlled environments may not fully capture real-world complexities, such as varying transaction behaviours and fraud techniques. Lastly, the practical implementation of Smart Contracts may face challenges related to blockchain integration and transaction costs.

4. FUTURE SCOPE

Looking ahead, future research could explore hybrid models that combine machine learning techniques with Smart Contracts to optimize both fraud detection accuracy and security.

Additionally, investigating the impact of additional features in the datasets, such as transaction history and user behaviour, may improve the performance of both methods. Lastly, developing adversarial training techniques for the Decision Tree Classifier could enhance its robustness against attacks, ensuring higher security in real-world applications.

5. REFERENCES

[1] Awan, M. J., Farooq, U., & Iqbal, M. (2023). A Comprehensive Analysis of Supervised Learning Techniques for Credit Card Fraud Detection. Computers & Security, 116, 102648.

[2] Wang, Y., Liu, Y., & Chen, J. (2023). Leveraging Blockchain Technology for Enhanced Fraud Detection in Financial Transactions. Future Generation Computer Systems, 135, 326-336.

[3] Alzubaidi, K. F. M., Almubarak, A. M. A., & Alzahrani, H. A. (2020). Credit Card Fraud Detection Using Machine Learning Techniques. Journal of Computer Networks and Communications.

[4] Atlam, E. S., Alghazzawi, A. W. M. B., & Alzahrani, A. A. A. (2020). Blockchain Technology and Its Applications in the Financial Industry. IEEE Access.

[5] Rashid, A. A. S., Renuka, R. C. R., & Shivananjappa, M. S. (2019). A Survey on Credit Card Fraud Detection Techniques. International Journal of Computer Applications.

[6] Ali, H. I., et al. (2019). A Survey of Smart Contract Security: Issues and Challenges. IEEE Access.

[7] UCI Machine Learning Repository. (n.d.). Credit Card Fraud Dataset. Retrieved from UCI