IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, May 2025
Impact Factor: 7.67

Cloud Based Credit Card Fraud Detection Using Random Forest Algorithm

Mrs. S. Ponnarasi[1], R. Akash[2], S. Deepak[3], K. Hari Krishna[4]
Associate Professor, Department of Information Technology[1]
Students, B.Tech., FinalYear, Department of Information Technology[2,3,4,5]
Anjalai Ammal Mahalingam Engineering College, Thiruvarur, India

Abstract: *The advent of electronic payment systems has transformed financial transactions between businesses and consumers alike, providing levels of convenience and efficiency hitherto unknown. But with the change has also come an increased incidence of credit card fraud that threatens the existence of financial institutions and consumers equally. The banking industry is left with the twofold responsibility of protecting information while maintaining smooth transaction processes. The goal of this project is to build a scalable cloud-based system to detect credit card fraud based on the powerful Random Forest machine learning algorithm due to its effectiveness in providing very accurate results along with resistance from overfitting. The planned system starts from a thorough assessment of the available status of fraud with credit cards, including their frequent methods as utilized by cheaters and why older detection procedures failed to adequately stop them.Traditional rule-based systems tend to falter when faced with the ever-changing dynamics of fraud, resulting in more false negatives and negatives. The Random Forest algorithm, however, adopts an ensemble method, building several decision trees to examine transactional data and discern patterns revealing fraudulent activity. This approach makes the model better at generalizing across varied datasets and thus well-suited for practical applications. By hosting the fraud detection system in a cloud computing platform, we are able to leverage the scalability and flexibility required to handle large volumes of transaction data in real-time. The cloud infrastructure enables fast deployment and maintenance, allowing the system to respond to new patterns of fraud and sustain high performance under changing loads. In addition, the inclusion of One-Time Password (OTP) authentication provides a critical level of security, prompting users to verify their identity on high-risk transactions. This multi-factor authentication mechanism greatly minimizes the risk of unauthorized access and maximizes overall transaction security. The performance of the proposed system is tested using large-scale testing on benchmark datasets, quantifying critical performance metrics such as detection accuracy, false positive rates, and processing speed.Early findings suggest that the Random Forest-based approach performs better than conventional methods, with increased detection rates and minimal interference with legitimate transactions. This study highlights the need to embrace sophisticated machine learning methods and cloud computing in the war against credit card fraud, offering a scalable and effective solution that not only safeguards consumers but also builds confidence in electronic payment systems.*

Keywords: Credit card fraud detection, Random Forest, Cloud computing, OTP verification

I. INTRODUCTION

The rapid increase in the use of electronic payment systems has seen a considerable growth in credit card transactions globally. With this rise, credit card fraud has also become a major issue, causing huge losses to financial institutions and eroding the confidence of consumers. Successful identification and blocking of fraudulent transactions are necessary for preserving the integrity of financial systems.

Traditional rule-based methods of fraud detection tend to be insufficient in capturing the complexity and changing patterns of contemporary fraudulent activity. Machine learning methods, specifically ensemble methods like the Random Forest algorithm, have shown to have better performance in classification problems through the use of multiple decision trees to enhance accuracy and mitigate overfitting.This project suggests a cloud-based credit card fraud detection system that employs the Random Forest algorithm to effectively detect fraudulent transactions. The system also includes One-Time Password (OTP) verification as an additional layer of authentication to improve security and avoid unauthorized transactions. Deploying the solution on cloud infrastructure provides scalability, real-

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, May 2025
Impact Factor: 7.67

time processing, and accessibility. The system will improve the accuracy of fraud detection while ensuring efficiency in operations, thereby protecting financial transactions and enhancing user confidence in electronic payment systems.

Random Forest Algorithm

The Random Forest Algorithm is a machine learning ensemble algorithm that is commonly applied to classification and regression problems because of its high accuracy and stability. It works by building many decision trees at training time and predicting the class that is the mode of the classes output by individual trees. This helps to avoid overfitting, which is a problem with single decision trees, thus enhancing generalization on new data. In credit card fraud detection, Random Forest algorithm evaluates different transaction features like transaction amount, time and merchant information to detect patterns that are suggestive of fraudulent transactions. Every decision tree in the forest is trained on a random part of the training set and a random part of the features, promoting diversity among the trees and resulting in more trustworthy predictions. The algorithm's capacity to deal with big data and model complicated interactions among features makes it highly appropriate for fraud detection. Further, Random Forest offers feature importance measures, which can be used to comprehend the most significant factors leading to fraud detection. By taking advantage of Random Forest through a cloud system, the project enjoys elastic computational resources that provide real-time processing of huge transaction volumes, thereby improving the reliability and accuracy of credit card fraud detection.

Cloud computing

Cloud computing provides a scalable and adaptive platform that is suitable for hosting data-intensive applications such as credit card fraud detection systems. The massive volume and velocity of transactional data generated in contemporary financial ecosystems demand powerful computing infrastructure that is capable of real-time processing and analytics. With the help of cloud services, organizations can lease scalable computing capacity on an as-needed basis without having to invest in major hardware purchases. In credit card fraud detection, cloud computing allows for integration and implementation of machine learning techniques such as Random Forest to quickly analyze streaming transaction data. The distributed nature of the cloud allows for parallel processing, minimizing latency and continuous tracking of transactions for fraud. Cloud-based deployment also enhances system usability, making it possible for several stakeholders – banks, merchants, payment processors, among others – to securely and efficiently access the detection platform. In addition, cloud computing facilitates convenient updates and system maintenance of the fraud detection models to allow for timely adaptation by the system of new fraud tactics and patterns. Cloud computing, through its scalability and accessibility features, is hence an integral factor for efficient and effective fraud detection in modern-day digital payment platforms.

One-Time Password (OTP) verification

One-Time Password (OTP) authentication is a widely used security measure that enhances user authentication by asking for a one-time, special code during high-risk transactions or login attempts. As an added layer to standard passwords, OTPs assist in reducing risks due to stolen or compromised credentials. Every OTP is generated dynamically and for a short time or a one-time use, so there are no replay attacks and only the intended user can finalize the transaction. Sent usually to the registered mobile phone or email of the user, OTP verification ensures the authentication of the user, providing an essential step in securing against unauthorized use. This approach is readily incorporated into cloud-based systems, with support for multiple delivery channels like SMS, email, or authenticator apps, to provide accessibility and convenience. Real-time generation and verification of OTPs facilitate quick response to suspicious behavior, enabling immediate intervention to block fraudulent transactions. Overall, OTP verification greatly improves the security and trustworthiness of cloud-based credit card fraud detection systems by combining robust user authentication with sophisticated machine learning methods.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, May 2025
Impact Factor: 7.67

II. EXISTING SYSTEM

There have already been several systems and technologies implemented for the detection and prevention of credit card fraud, particularly using cloud computing.They normally integrate cloud computing, and real-time monitoring of transactions in order to enhance the accuracy, velocity, and scale of fraud detection.The excessive level of losses caused by fraud and consciousness of the relationship between loss and the available limit need to decrease.Detection of credit card frauds with the actual data set is a challenging task.The fraud must be deducted in real time and count of false alert.The log, which will be maintained, will also be a proof to the bank for the transaction incurred.We are unable to find the best detection using this method.This will be minimizing the tedious work of an employee at the bank.

Demerits:

- Testing credit card frauds with real data set is a challenging task.
- The high level of losses due to fraud and the awareness of the relation between loss and the available limit must be decreased.
- Fraud must be deducted in real time and the number of false alert.
- Log, which is kept, will also be an evidence for the bank for the transaction done.
- We can find the most accurate detection by this method.
- This will lessen the painstaking task of an employee in the bank.

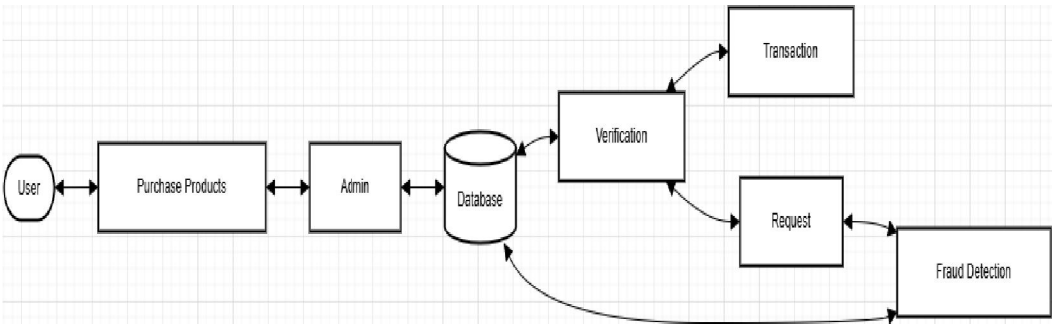
III. PROPOSED SYSTEM

The system under consideration will seek to utilize cloud computing and machine learning to identify credit card fraud in real-time, allowing financial institutions to precisely detect suspicious transactions while reducing false positives. The system will handle high volumes of transaction data, employ sophisticated machine learning algorithms to detect fraud, and dynamically scale to handle heavy traffic during busy periods. Cloud computing ensures that the system is affordable, scalable, and can quickly analyze large sets of data. Fraud detection is much faster than current systems, enabling fast intervention in fraudulent activities. To increase security, the original cardholder is offered OTP verification for each transaction to ensure that only the authorized can make transactions.

Advantage of Proposed System:

- A benefit of using this technique is that the majority of individuals are accustomed to picking up the credit card during other tasks and for this reason will link different moods with particular data set.
- It will provide the precision at the assessment of the data set then it will forecast the data set at the portal.
- The procedure was extremely quick when we applied the random forest segmentation classification to the data set.
- By the ML algorithm will be able to forecast the dataset the log, which is kept, will also serve as a proof for the bank for the transaction done.

IV. SYSTEM ARCHITECTURE DIAGRAM



DOI: 10.48175/IJARSCT-26311

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, May 2025
Impact Factor: 7.67

MODULES

- **Admin Module :** The administrator can manage the system as a whole using this module. The admin can securely log in and carry out tasks like adding or viewing products, tracking user activities, and checking transactions that are marked as fraud. It facilitates smooth backend application management.
- **User Module:** Users can register and securely log in. After authentication, users can search, view, and buy products. While buying, they need to provide their credit card information, which triggers the fraud detection process. The module also manages user sessions and profile information.
- **Transaction Module:** It oversees the process of buying. It records transaction information, including card number, amount, and user activity. It initiates the OTP generation and fraud detection procedure prior to approval of the transaction. This insures that all purchases are both authenticated and secure.
- **Database Module (MySQL):** This module manages data storage and retrieval through a MySQL database. It retains user data, product information, transaction history, OTPs, and fraud detection outcomes. It keeps all data well-organized, secure, and available to other modules for proper functioning.

V. CONCLUSION

This project illustrates how combining cloud computing with the Random Forest machine learning algorithm and OTP verification makes for a strong, scalable, and efficient credit card fraud detection system. With the elastic resources of the cloud, the system can handle large amounts of transaction data in real time, allowing financial institutions to rapidly detect and respond to fraudulent transactions with high accuracy. The Random Forest algorithm's capability to examine intricate patterns in transaction data improves detection efficiency, while OTP verification provides an essential level of user authentication, limiting unauthorized access. Combined, these technologies not only enhance fraud detection rates but also lower false positives, thus ensuring a better experience for genuine users. Additionally, keeping detailed transaction and verification logs offers useful evidence for banks to settle disputes and enhance security policies. Overall, this holistic solution responds to the expanding problem of credit card fraud in an increasingly digital financial environment and encourages safer, more reliable payment systems.

VI. FUTURE WORK

Though the existing system showcases good performance in Random Forest-based credit card fraud detection and OTP verification, there are several potential directions for improvement in future research. The integration of more machine learning algorithms, including deep learning algorithms or gradient boosting methods, might enhance the accuracy of detection and lower false positives even further. Combining real-time behavioral analysis and network-based fraud detection could offer greater insight into user behavior patterns, making the system more robust. Extending multi-factor authentication techniques beyond OTP, e.g., biometric authentication and device fingerprinting, may add to security and minimize dependence on a single authentication method. Additionally, using adaptive learning techniques that refresh fraud detection models with new information on a continuous basis will keep the system ahead of emerging fraud strategies. Lastly, investigation into the use of blockchain technology for secure and tamper-proof transaction logging might enhance transparency and trust between financial institutions and consumers. These improvements would make for a more robust and comprehensive fraud prevention system in future electronic payment systems.

REFERENCES

[1]. Breiman, L. (2001). Random Forests. Machine Learning, 45(1), 5–32.
[2]. Han, J., Kamber, M., & Pei, J. (2011). Data Mining: Concepts and Techniques (3rd ed.). Morgan Kaufmann Publishers.
[3]. Bishop, C. M. (2006). Pattern Recognition and Machine Learning. Springer.
[4]. Murphy, K. P. (2012). Machine Learning: A Probabilistic Perspective. MIT Press.
[5]. Erl, T., Mahmood, Z., & Puttini, R. (2013). Cloud Computing: Concepts, Technology & Architecture. Prentice Hall.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, May 2025
Impact Factor: 7.67

[6]. A. A. A. Alzubaidi, A. A. Alzubaidi, & A. A. Alzubaidi. (2018). Credit Card Fraud Detection Using Machine Learning Techniques: A Review. International Journal of Computer Applications, 181(40), 1–6.

[7]. Jindal, P., & Gupta, T. (2017). A Survey on Credit Card Fraud Detection Techniques. International Journal of Advanced Research in Computer Science and Software Engineering, 7(5), 1–7.

[8]. Chen, L., Ouyang, Y., Zeng, Y. and Li, Y. (2020). Dynamic facial expression recognition model based on BiLSTM-Attention. 15th International Conference on Computer Science & Education (ICCSE), 828-832.

[9]. Li, S. and Deng, W. (2020). Deep facial expression recognition: A survey. IEEE Transactions on Affective Computing, doi:10.1109/TAFFC.2020.2981446.

[10]. Liu, D., Ouyang, X., Xu, S., Zhou, P., He, K. and Wen, S. (2020). SAANet: Siamese action-units attention network for improving dynamic facial expression recognition. Neurocomputing, 413, 145-157.

[11]. Mellouk, W. and Handouzi, W. (2020). Facial emotion recognition using deep learning: review and insights.Procedia Computer Science, 175, 689-694.

[12]. Patel, K., Mehta, D., Mistry, C., Gupta, R., Tanwar, S., Kumar, N., et al. (2020). Facial sentiment analysis using AI techniques: state-of-the-art, taxonomies, and challenges. IEEE Access, 8, 90495-90519.

[13]. Perveen, N., Roy, D. and Chalavadi, K. M. (2020). Facial Expression Recognition in Videos Using Dynamic Kernels. IEEE Transactions on Image Processing. 29, 8316-8325.

[14]. Wu, M., Su, W., Chen, L., Pedrycz, W. and Hirota, K. (2020). Two-stage Fuzzy Fusion Affective Computing, doi: 10.1109/TAFFC.2020.2966440.

[15]. Wen, G., Chang, T., Li, H. and Jiang, L. (2020). Dynamic Objectives Learning for Facial Expression Recognition. IEEE Transactions on Multimedia, 22, 2914-2925.

[16]. Zhi, R., Zhou, C., Li, T., Liu, S. and Jin, Y. (2020). Action Unit Analysis Enhanced Facial Expression Recognition by Deep Neural Network Evolution. Neurocomputing. 425, 135-148