iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** IV **Month of publication:** April 2024

DOI: https://doi.org/10.22214/ijraset.2024.59557

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue IV Apr 2024- Available at www.ijraset.com

Online Fraud Detection System

Prof. D.C. Dhanwani[1], Aniruddh Tonpewar[2], Devashish Ikhar[3], Komal Ladole[4], Suyog Mahant[5]
P.R. Pote (Patil) Collage of Engineering and Management, Amravati
Department of Computer Science & Engineering, Sant Gadge Baba Amravati University, Amravati, Maharashtra, India

Abstract: ***Financial services are used everywhere and function with high complexity. With the increase in online transacting, frauds too are increasing alarmingly. An automated Fraud Detection System is thus required. With millions of transactions taking place, it is practically impossible to detect frauds manually with good speed and accuracy. We propose a system is that provides a robust, cost effective, efficient yet accurate solution to detect frauds in both online payment transactions and credit card payments. The proposed solution is a Machine Learning model that will serve the purpose of detecting "fraudulent" and all the "genuine" transactions in real time. This is beneficial for all sectors that are even mildly aligned to finance. The solution will help them analyse based on various factors if the ongoing transaction can be harmful and will prevent many unfortunate incidents.***

Keywords: Fraud Classification, Fraud Detection Techniques, Machine learning, Decision tree, Random forest Logistic regression, Fraud detection and prediction.

I. INTRODUCTION

A. *Basic Definition*

Now a days we know that Everyone uses online mode for the money transfer or money usage. All the transaction goes through the UPI phase to ease money transformation of customers. Our UPI ID that is linked to our account is a sensitive information that should be always kept private. Sometimes malware attack such as phishing occur because of that our id may get hacked by hacker and we can loss our money by false transaction.

As the newborn technologies have been developed, we are progressing day by day. But they are not only advantages of this technology, it also leads to some disadvantages also. In this research paper they have used various machine learning algorithms to detect cases related to UPI Frauds. As we do payment through UPI, due to some misuse our id may get hacked which further may result in losing of our money or credential information.

As UPI fraud increasing, machine learning plays important role for developing system to detect the frauds. This research paper uses different mining algorithms that result in low false rate and with high speed. UPI frauds are dangerous to hack our data or to losses money from the account if our id get hacked. At the current state of the world, financial organizations expand the availability of financial facilities by employing of innovative services such as credit cards, Automated Teller Machines (ATM), internet and mobile banking services. Besides, along with the rapid advances of e-commerce, the use of credit card has become a convenience and necessary part of financial life. Credit card is a payment card supplied to customers as a system of payment.

The use of credit cards over the internet was adopted. This has increased rapidly during the past decade and services like e-commerce, online payment systems, working from home, online banking, and social networking have also been introduced and widely used. Due to this, fraudsters have intensified their efforts to target online transactions utilizing various payment systems.

In recent times, improvements in digital technologies, particularly for cash transactions, have changed the way people manage money in their daily activities. Many payment systems have transitioned tremendously from physical pay points to digital platforms. To sustain productivity and competitive advantage, the use of technology in digital transactions has been a game-changer and many economics have resorted to it.

Hence, internet banking and other online transactions have been a convenient avenue for customers to carry out their financial and other banking transactions from the comfort of their homes or offices, particularly using credit cards.

Online Fraud Detection Systems leverage a combination of advanced technologies, including machine learning, artificial intelligence, data analytics, and behavioral analysis, to scrutinize vast amounts of transactional data and identify patterns indicative of fraudulent activity. The effectiveness of OFDS relies on their ability to differentiate between legitimate transactions and fraudulent behavior in real-time, without unduly disrupting the user experience or impeding legitimate business operations.

Achieving this delicate balance requires a multidimensional approach that combines the strengths of various detection techniques while minimizing false positives and false negatives.

As such, Online Fraud Detection Systems must remain adaptive and responsive to emerging threats, continuously updating their detection algorithms and strategies to stay ahead of cybercriminals.

In this review, we explore the state-of-the-art in online fraud detection, examining recent advancements, key challenges, and promising research directions in the field.

Moreover, the landscape of online fraud is constantly evolving, driven by advancements in technology, changes in consumer behavior, and the emergence of new attack vectors.

As such, OFDS must remain agile and adaptive, continuously learning from new data and evolving threat landscapes to stay ahead of cybercriminals.

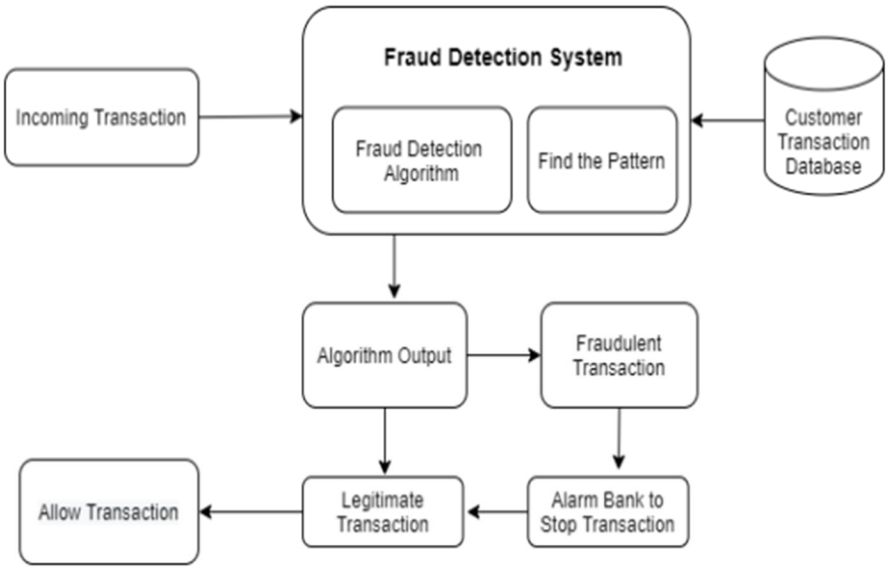
By surveying existing literature and highlighting notable studies, we aim to provide insights into the methodologies, algorithms, and best practices shaping the development and deployment of Online Fraud Detection Systems in today's digital landscape.

Ultimately, our goal is to contribute to the ongoing efforts to enhance the security and resilience of online transactions and protect consumers and businesses from the perils of online fraud.

II. OBJECTIVE

1) To study and analyse the data from the user's database and compare the upcoming data.
2) To study of using machine learning algorithms to detect the UPI frauds.
3) To study and compare the performance of machine learning algorithms such as Bayesian network, Hidden Markov model.
4) To study all the correlate transaction with internet usage time.
5) Investigate the use of machine learning algorithms for fraud detection in financial transactions.
6) Design and develop a real-time monitoring system for continuous fraud detection and prevention.
7) Assessing the performance of the suggested approach in comparison to conventional rule-based systems.
8) Exploring proactive measures for fraud prevention, such as dynamic risk scoring and adaptive thresholds.
9) Analyse scalability and deployment considerations for implementing the proposed system in real – world financial institutions.

III. PROPOSED METHODOLOGY



IV. METHODOLOGY

A. *Data Collection and Preprocessing*

1) Gather transactional data from various sources, including online purchases, financial transactions, login activities, and user interactions.
2) Cleanse and preprocess the data to remove inconsistencies, outliers, and irrelevant information.
3) Transform the data into a suitable format for analysis, considering factors such as data type, scale, and distribution.

B. Feature Engineering

1) Extract relevant features from the preprocessed data, including transaction amounts, timestamps, user demographics, device identifiers, IP addresses, and behavioral attributes
2) .Engineer new features to capture meaningful patterns and relationships in the data, such as transaction frequency, velocity, deviation from typical behavior, and sequence of events.

C. Model Selection and Training

1) Evaluate various machine learning algorithms, such as logistic regression, decision trees, random forests, support vector machines (SVM), neural networks, and ensemble methods, for their suitability in fraud detection tasks.
2) Train multiple models using labeled data, where fraudulent and legitimate transactions are annotated, to learn patterns of fraudulent behavior.
3) Explore both supervised and unsupervised learning approaches, depending on the availability of labeled data and the nature of the fraud detection problem.
4) Consider semi-supervised and active learning techniques to leverage both labeled and unlabeled data for model training.

D. Real-time Monitoring and Detection

1) Deploy trained models to monitor incoming transactions and activities in real-time.
2) Apply anomaly detection techniques to identify deviations from normal behavior, such as unusual transaction amounts, atypical transaction locations, and irregular user behaviors.
3) Set appropriate thresholds and rules to trigger alerts or flag suspicious transactions for further investigation. Implement stream processing techniques to handle high-volume data streams efficiently and enable timely detection of fraudulent activities.

E. Model Evaluation and Validation

1) Assess the performance of the fraud detection models using metrics such as accuracy, precision, recall, F1-score, and area under the receiver operating characteristic curve (AUROC).
2) Conduct cross-validation and holdout validation to evaluate model generalization and robustness on unseen data.
3) Validate model performance using historical data and conduct retrospective analysis to identify missed fraud cases and false positives.

F. Feedback Mechanism and Model Improvement

1) Incorporate feedback loops to continuously update and improve the fraud detection models based on new data and insights.
2) Monitor model performance over time and recalibrate thresholds or update algorithms as fraud patterns evolve.
3) Integrate human expertise and domain knowledge to interpret model outputs, investigate flagged transactions, and provide feedback for model refinement.

G. Integration with Operational Systems

1) Integrate the fraud detection system with operational systems, such as payment gateways, e-commerce platforms, and banking systems, to enable seamless detection and response to fraudulent activities.
2) Implement APIs and webhooks to facilitate communication between the fraud detection system and other business applications. Ensure scalability, reliability, and low latency to support real-time decision-making and transaction processing.

H. Compliance and Reporting

1) Ensure compliance with regulatory requirements and industry standards for data security, privacy, and fraud prevention.
2) Maintain audit trails and documentation of model development, training data, validation processes, and decision rationale.
3) Generate reports and dashboards to provide stakeholders with visibility into fraud detection performance, including detection rates, false positives, and mitigation actions.

V. ADVANTAGES

1) *Real-time Detection:* Online fraud detection systems can detect fraudulent activities in real-time, allowing for immediate intervention and mitigation of potential losses.

2) *Automation:* These systems can automate the process of monitoring transactions, reducing the need for manual intervention and enabling faster response times.
3) *Scalability:* Online fraud detection systems can handle large volumes of transactions efficiently, making them suitable for businesses with high transaction volumes.
4) *Accuracy:* Advanced algorithms and machine learning techniques used in these systems can accurately identify patterns of fraudulent behavior, reducing false positives and negatives.
5) *Cost Savings:* By preventing fraudulent transactions and reducing losses, these systems can save businesses money in the long run.
6) *Reduced Losses:* By identifying and stopping fraudulent transactions early, online fraud detection systems help minimize financial losses for businesses.
7) *Enhanced Security:* Implementing a fraud detection system adds an extra layer of security to online transactions, protecting both businesses and customers from potential fraudsters.
8) *Improved Customer Trust:* When customers feel confident that their transactions are secure, they are more likely to trust the business and continue using its services or purchasing its products.
9) *Customization:* Many fraud detection systems allow businesses to customize rules and parameters to match their specific needs and risk profiles, increasing the accuracy of fraud detection.
10) *Data Analytics:* By analyzing patterns and trends in transaction data, online fraud detection systems can identify potential fraud more effectively than traditional methods.
11) *Regulatory Compliance:* Implementing a fraud detection system helps businesses comply with regulations related to fraud prevention and data security, reducing the risk of fines and penalties.

VI. CONCLUSION

After analyzing various research papers, it has been concluded that Machine Learning can be used effectively to recognize various frauds. Using hidden Markov model, Bayesian network and genetic algorithm we can propose an effective model for the fraud detection. Our goal is to analyse different machine learning techniques in a way that they help us to detect and predict the UPI fraud. Using the data mining technique along with the random forest algorithm, the system's performance rate increases multiple folds and thus addresses the merchant support function. We show that our proposed approaches can detect fraud transactions with very high accuracy and low false positives - especially for TRANSFER transactions. Fraud detection often involves a tradeoff between correctly detecting fraudulent samples and not misclassifying many non-fraud samples.

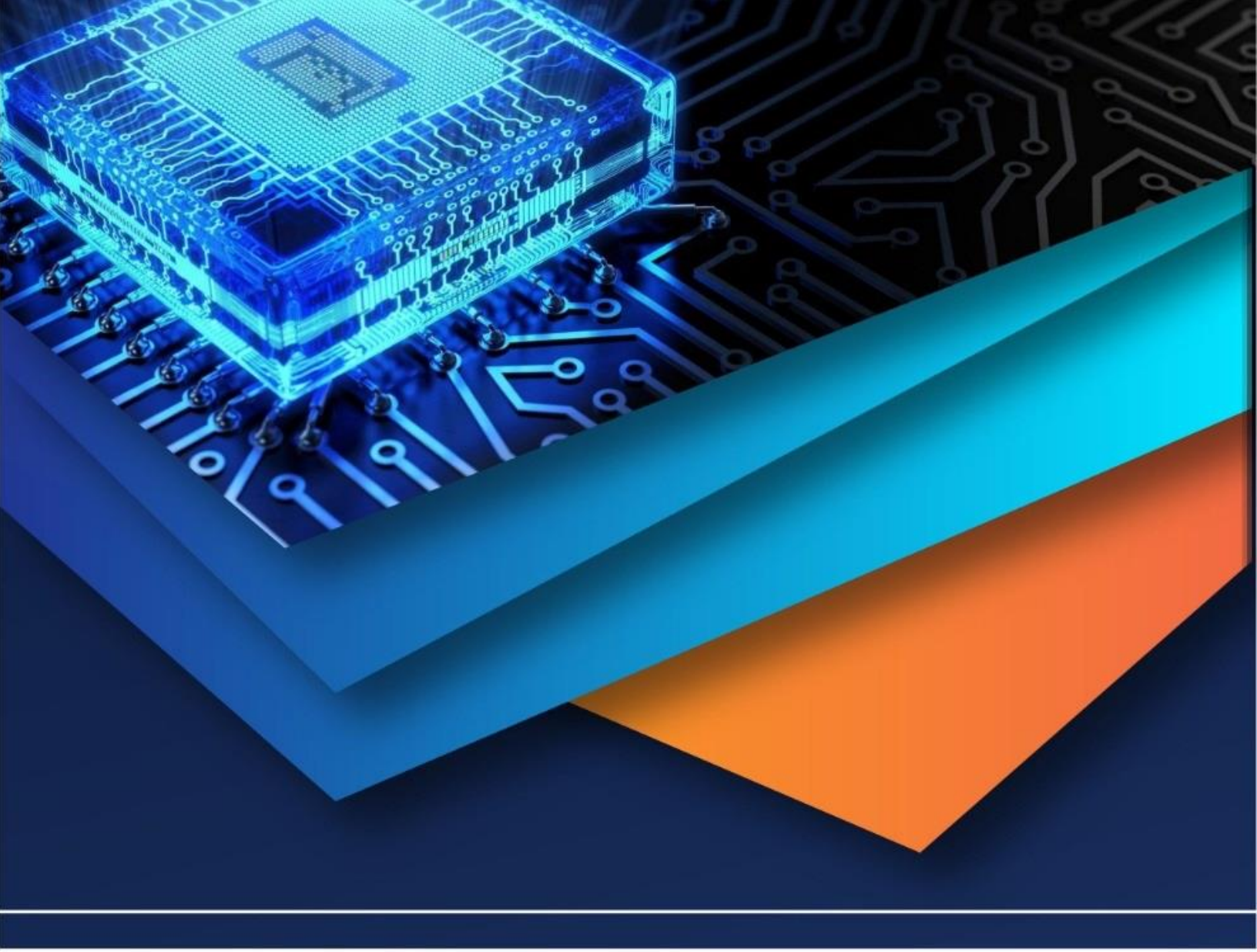
These systems provide real-time detection capabilities, reducing financial losses by swiftly identifying and halting fraudulent activities. By enhancing security measures, they foster trust among customers and stakeholders, thereby safeguarding the reputation and integrity of businesses. Additionally, the scalability and automation of these systems streamline operations, while customizable features enable tailored risk management strategies. Moreover, online fraud detection systems contribute to regulatory compliance, mitigating the risk of penalties and fines.

REFERENCES

[1] Ayushi Agrawal, Shiv Kumar, Amit Kumar Mishra, "A Novel approach for UPI Fraud Detection", 2nd International Conference on Computing for Sustainable Global Development (INDIA.Com), 2018.
[2] N. Sivakumar, R. Balasubramanian, "Cheating identification in Visa Transactions: Classification dangers Also counteractive action Techniques", universal diary for PC science and majority of the data Technologies, vol. 6, no. 2, 2015.
[3] G. T. Costa, A. C. P. L. Carvalho, S. Barbon, "Strict Very Fast Decision Tree: a memory conservative algorithm for data stream mining", May -2018.
[4] Omair B, Alturki, A (2020) A systematic literature review of fraud detection metrics in business processes. IEEE Access 8:26893–26903.
[5] Aye Khine, H. Wint Khine, "A Survey of Decision Tree for Data Streams to Detect UPI Fraud", PROMAC-2019.
[6] KhyatiChaudhary, JyotiYadav, BhawnaMallick, " A review of Fraud Detection Techniques: Credit Card", International Journal of Computer Applications Volume 45– No.1 2022.
[7] Sushmito Ghosh, Douglas L. Reilly, Nestor, "Credit Card Fraud Detection with a NeuralNetwork", Proceedings of 27th Annual Hawaii International Conference on System Sciences, 2022.
[8] J. Zhou, "Negative Selection Algorithms: From the Thymus to V-Detector", PhD Thesis, School of Computer Science, University of Memphis, 2021.
[9] J. Timmis, "Artificial Immune Systems: A Novel Data Analysis Technique Inspired by the Immune Network Theory", PhD. Thesis, School of Computer Science, University of Wales, 2000.
[10] Soltani, N., Akbari, M.K., SargolzaeiJavan, M., "A new user-based model for credit card fraud detection based on artificial immune system," Artificial Intelligence and Signal Processing (AISP), 2012 16th CSI International Symposium on., IEEE, pp. 029-033, 2022.

[11] S. Ghosh and D. L. Reilly, “Credit card fraud detection with a neural-network”, Proceedings of the 27th Annual Conference on System Science, Volume 3: Information Systems: DSS/ Knowledge Based Systems, pages 621-630, 1994. IEEE Computer Society Press.
[12] Masoumeh Zarea poor, Seeja.K.R, M.Afshar.Alam, ”Analysis of Credit Card Fraud Detection Techniques: based on Certain Design Criteria”, International Journal of Computer Applications (0975 – 8887) Volume 52– No.3, 2019
[13] H. Zheng, J. Zhang, “Learning to Detect Objects by Artificial Immune Approaches", Journal of Future Generation Computer Systems, Vol. 20, pp. 1197-1208, 2004.
[14] L. N. de Castro, J. I. Timmis, “Artificial immune systems as a novel soft computing paradigm”, Journal of Soft Computing, Vol. 7, pp 526–544, 2003.
[15] L. N. de Castro, J. Timmis,” Artificial immune systems as a novel soft computing paradigm”, Journal of Soft Computing, PP 526–544, 2023.
[16] J. Zhou, “Negative Selection Algorithms: From the Thymus to V-Detector”, PhD Thesis, School of Computer Science, University of Memphis, 2006.
[17] J. Timmis, "Artificial Immune Systems: A Novel Data Analysis Technique Inspired by the Immune Network Theory", PhD. Thesis, School of Computer Science, University of Wales, 2000.
[18] V. Cutello, G. Narzisi, G. Nicosia, M. Pavone, “Clonal Selection Algorithms: A Comparative Case Study Using Effective Mutation Potentials”, proceeding of International Conference on Artificial Immune Systems (ICARIS), pp. 13-28, 2005.
[19] K.RamaKalyani, D.UmaDevi,” Fraud Detection of Credit Card Payment System by Genetic Algorithm”, International Journal of Scientific & Engineering Research Volume 3, Issue 7, -2012.
[20] Bentley, P., Kim, J., Jung., G. & Choi, J. Fuzzy Darwinian Detection of Credit Card Fraud. Proc. of 14th Annual Fall Symposium of the Korean Information Processing Society. 2000.
[21] Hitoshi Iba, Takashi Sasaki, “Using Genetic Programming to Predict Financial Data”, IEE, 1999.
[22] AbhinavSrivastava, AmlanKundu, ShamikSural, Arun K. Majumdar. “Credit Card Fraud Detection using Hidden Markov Model”, IEEE Transactions on dependable and secure computing, Volume 5; (2008) (37-48).
[23] Anshul Singh, Devesh Narayan “A Survey on Hidden Markov Model for Credit Card Fraud Detection”, International Journal of Engineering and Advanced Technology (IJEAT), (2012). Volume-1, Issue-3; (49-5).

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue IV Apr 2024- Available at www.ijraset.com



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY