SJIF Impact Factor (2024): 8.675| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 9 | Issue: 4 | April 2024 - Peer Reviewed Journal

FRAUD DETECTION IN UPI TRANSACTIONS USING ML

J. Kavitha[1], G. Indira[2], A. Anil kumar[3], A. Shrinita[4], D. Bappan[5]

Assistant Professor, Dept. of Computer Science and Engineering,
Sanketika Vidya Parishad Engineering College, Visakhapatnam, India [1]
B.Tech (IV/IV) Students, Dept. of Computer Science and Engineering,
Sanketika Vidya Parishad Engineering College, Visakhapatnam, India[2,3,4]

Article DOI: https://doi.org/10.36713/epra16459
DOI No: 10.36713/epra16459

ABSTRACT

Significant obstacles to financial security have arisen as a result of the quick uptake of Unified Payments Interface (UPI) for online transactions and a commensurate rise in fraudulent activity. This paper suggests a novel fraud detection method that makes use of cutting-edge machine learning (ML) algorithms to address this urgent issue. It focuses on integrating a Hidden Markov Model (HMM) into the UPI transaction process. In order to enable the system to identify departures from these learnt behavior's as possibly fraudulent, the HMM is trained to predict the typical transaction patterns for particular cardholders. The suggested system uses a variety of contemporary approaches, such as Kmeans Clustering, Auto Encoder, Local Outlier Factor, and artificial neural networks, to improve algorithmic diversity and flexibility to changing fraud patterns. In addition to addressing issues like test data creation for training and validation, the system emphasizes a heuristic approach to solving high-complexity computational problems, guaranteeing efficacy in a variety of settings. This study, which is positioned as a proactive and adaptable solution, emphasizes how crucial it is to stop UPI fraud and provides a thorough foundation for reliable fraud detection in the ever-changing world of online transactions.

INTRODUCTION

The emergence of online banking has caused a paradigm shift in the current financial transaction landscape, providing individuals and organisations globally with unmatched ease and efficiency. But there are drawbacks to this digital transformation as well, the most significant of which is the growing frequency of fraudulent activity in online transactions. The swift expansion of online banking services has made it easier for bad actors to take advantage of weaknesses, which puts the security and integrity of financial systems at serious risk. Furthermore, the COVID-19 pandemic's start has acted as a trigger, quickening the shift to remote operations and raising the possibility of fraudulent activity in the digital sphere. It is therefore more important than ever to create reliable fraud detection systems in the face of the epidemic highlight how important it is for both customers and financial institutions to strengthen their defences against fraud. The increasing trend of financial transactions occurring on digital platforms underscores the need for advanced security measures and flexible approaches to protect the integrity of online banking systems.

Exiting System

Regarding the field of online banking fraud detection, the systems that are now in place primarily depend on conventional techniques and rule-based methods. In order to identify potentially fraudulent transactions, these systems frequently use static rules and thresholds, usually based on established patterns or anomalies. Although these systems have shown some degree of effectiveness, they have shortcomings in terms of accuracy, scalability, and adaptability, especially when it comes to sophisticated and ever-evolving fraud techniques.

A prevalent obstacle within the current framework is its dependence on static rules, which may not be able to identify subtle or evolving patterns that point to fraudulent activity. Furthermore, the rule-based approach frequently finds it difficult to manage the subtleties and intrinsic complexity of transaction data, particularly given the ever-changing environment of online banking transactions.

The current system's vulnerability to false positives and false negatives is another drawback. Static rules have the potential to unintentionally identify genuine transactions as fraudulent (false positives) or fail to identify actual fraudulent activity (false negatives), which can result in inefficiencies, unhappy customers, and financial losses for financial institutions as well as consumers.

Furthermore, particularly in the context of the Unified Payments Interface (UPI), the current systems would find it difficult to handle the enormous volume and variety of transaction data generated in real-time. The scalability and computing efficiency needed to efficiently process and analyse large-scale transaction datasets may be lacking in traditional methodologies.

SJIF Impact Factor (2024): 8.675| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 9 | Issue: 4 | April 2024 - Peer Reviewed Journal

Overall, even though the current systems have been very helpful in detecting fraud in online banking transactions, they urgently need to be improved in order to handle the new dangers and complexity that come with doing business in the digital sphere. To improve the efficacy, precision, and flexibility of fraud detection systems, sophisticated machine learning and artificial intelligence approaches customised for online banking transactions must be implemented.

Disadvantages

- Limited adaptability
- Scalability challenges
- Limited feature extraction
- Insufficient model interpretability

Proposed System

We present a unique strategy that uses convolutional neural networks (CNNs) for increased fraud detection in online banking transactions in order to overcome the shortcomings of current fraud detection systems. Compared to conventional rule-based approaches, our suggested solution has various advantages, including better accuracy, flexibility, and scalability. We support the use of convolutional neural networks (CNNs) as the primary technology for online banking transaction fraud detection. Especially in image analysis tasks, CNNs have shown impressive skills in feature extraction and pattern detection. We intend to leverage CNNs' capacity to automatically learn hierarchical characteristics and identify complex patterns suggestive of fraudulent activity by applying them to transactional data. Important elements of the system we've suggested include:

Adaptive Learning: Unlike static rule-based systems, our suggested approach makes use of CNN-enabled adaptive learning techniques. With the ability to dynamically modify their internal representations and adjust their parameters in response to incoming data, these neural networks are able to react in real-time to evolving fraud trends and new threats. Its ability to adjust strengthens the system's defences against changing fraud strategies and guarantees steady advancement over time.

Feature extraction and transformation: To extract pertinent characteristics from transactional data and turn them into interpretable representations for fraud detection, our suggested approach makes use of CNNs. CNNs can identify subtle patterns and abnormalities that may escape conventional rule-based methods by automatically learning discriminative features from raw transactional attributes. The method of feature extraction improves the accuracy with which the system can distinguish between authentic and fraudulent transactions.

Real-time Processing: Our suggested solution allows for real-time fraud detection and response in high-volume transaction environments like the Unified Payments Interface (UPI) by utilising the parallel processing powers of CNNs. CNNs streamline the simultaneous processing of massive amounts of transaction data, making it easier to identify fraudulent activity quickly and take prompt action to prevent losses. Despite the inherent complexity of CNNs, we have given priority to interpretability and openness in our suggested solution. We include methods for illustrating and interpreting CNN decision-making processes so that interested parties can comprehend the reasoning behind reported transactions and develop faith in the dependability of the system. Our technology facilitates cooperation between users, regulators, and internal auditors by improving interpretability, which in turn promotes responsibility and adherence to regulatory standards.

Continuous Monitoring and Evaluation: To evaluate the efficacy and performance of our suggested system over time, it is equipped with mechanisms for ongoing monitoring and assessment. We make sure that the fraud detection system is continuously optimised and improved by examining user feedback, comparing model predictions to ground truth labels, and monitoring important performance metrics like precision, recall, and F1-score. The overall effectiveness and dependability of the system are increased by this iterative process, which permits ongoing enhancement and adaptability to changing fraud environments.

Advantages

- Enhanced accuracy
- Adaptability to changing patterns
- Continuous improvement
- Comprehensive fraud detection
- Scalability and efficiency
- Real time detection

SJIF Impact Factor (2024): 8.675| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 9 | Issue: 4 | April 2024 - Peer Reviewed Journal

Block Diagram

Fig1 : System Diagram for UPI fraud Detection using machine learning

RESULTS

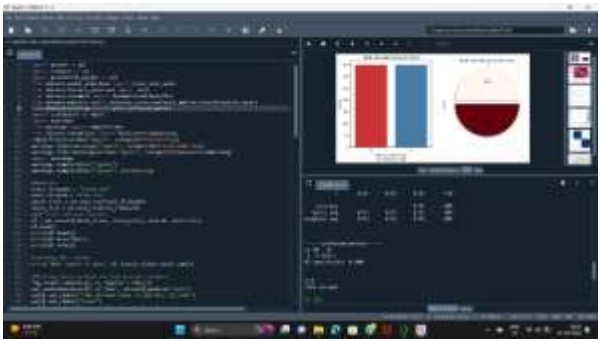

Fig 2: Dataset of Fake Account Count

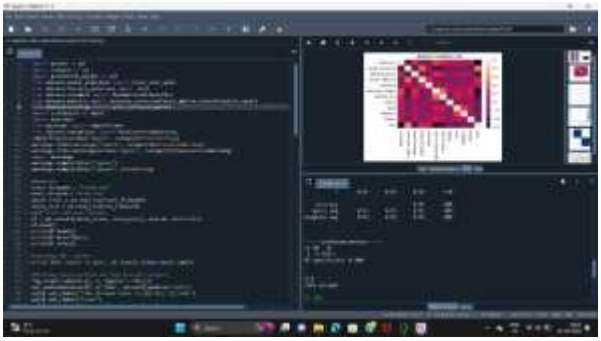

Fig 3: Dataset Correlation Plot

SJIF Impact Factor (2024): 8.675| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 9 | Issue: 4 | April 2024 - Peer Reviewed Journal

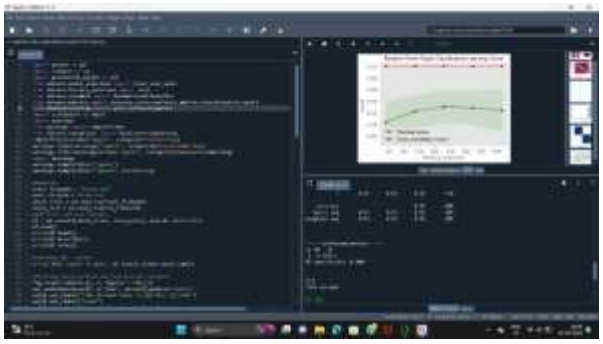

Fig 4 : Regression Forest Digits Classification Learning Curve

CONCLUSION

We have gone through several phases of data collection, pre-processing, algorithm selection, and system implementation in this extensive effort to create a strong fraud detection system. The end result is a solution that has the potential to greatly improve the security and dependability of financial transactions. We started our trip by obtaining a large and comprehensive dataset that included complex transactional information, which served as the foundation for our later investigations.

Setting up a strong basis for later model training required the first stage of data pre-processing. We carefully addressed issues, including the dataset's unequal class distribution, using calculated pre-processing techniques to reduce biases and guarantee the stability of our models. Methods like standardisation-based feature scaling and careful treatment of missing data played a crucial role in getting the dataset ready for efficient model training.

The selection of algorithms was an important factor in guaranteeing the effectiveness of the system in detecting fraudulent actions. We made sure our system could detect a wide range of fraudulent patterns by implementing a diverse ensemble of machine learning algorithms, from more sophisticated techniques like convolutional neural networks to more conventional methods like logistic regression and decision trees. With the contributions of each algorithm, a comprehensive fraud detection system that could handle a variety of fraud scenarios was created.

The system architecture was crucial in guaranteeing scalability, efficiency, and usability during the development and deployment stages. By using technologies like Flask, HTML, CSS, Python, and other programming languages, we were able to smoothly integrate the fraud detection system into the current financial infrastructure, increasing its usability and accessibility for both stakeholders and end users. The seamless deployment and functioning of the system in real-world settings were made possible by this harmonious technology integration.

The fraud detection system is a major improvement in protecting financial transactions from fraudulent activity, as we can see when we consider the results of our work. It is crucial to preserving the integrity and reliability of financial systems because of its capacity to precisely detect fraudulent transactions while reducing false positives. But our adventure doesn't end here. Maintaining protection and security in the ever-changing world of financial transactions will require constant system improvement and refinement to meet changing fraud trends and new security risks. We are prepared to meet upcoming challenges and protect the integrity of financial systems around the globe with a dedication to innovation and vigilance.

REFERANCES

1. *ALESKEROV E, FREISLEBEN, B., and, RAO B (1997) CARDWATCH: A neural network-based database mining system for credit card fraud detection. In Conference (pp. 220–226). IEEE, Piscataway, NJ*
2. *Sahin M (2017) Understanding Telephony Fraud as an Essential Step to Better Fight it [Thesis]. École Doctorale Informatique, Télécommunication et Électronique, Paris*
3. *Abdallah A, Maarof MA, Zainal A (2016) Fraud detection system: A survey. J Netw Comput Appl 68:90–113*
4. *ANDREWS PP, PETERSON MB (eds) (1990) Criminal Intelligence Analysis. Palmer Enterprises, Loomis, CA*
5. *ARTÍS M, AyUSO M, GUILLÉN M (1999) Modeling different types of automobile insurance fraud behavior in the Spanish market. Insurance Math Econ 24:67–81*
6. *BARAO MI, TAWN JA (1999) Extremal analysis of short series with outliers: Sea-levels and athletics records. Appl Stat 48:469–487*
7. *BLUNT G, HAND DJ (2000) The UK credit card market. Technical report, Department of Mathematics, Imperial College, London*
8. *BOLTON RJ, HAND DJ (2001) Unsupervised profiling methods for fraud detection. In Conference on Credit Scoring and Credit Control 7, Edinburgh, UK, 5–7 Sept*
9. *Phua C, Lee V, Smith K, Gayler R (2010) A comprehensive survey of data mining-based fraud detection research. https://doi.org/10.48550/ARXIV.1009.6119*
10. *Summers SL, Sweeney JT (1998) Fraudulently misstated financial statements and insider trading: An empirical analysis. 73(1):131–146https://www.jstor.org/stable/248345*

SJIF Impact Factor (2024): 8.675| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 9 | Issue: 4 | April 2024 - Peer Reviewed Journal

11. *BROCKETT PL, XIA X, DERRIG RA (1998) Using Kohonen's self-organizing feature map to unveil automobile bodily injury claims fraud. J Risk Insur 65:245–274*
12. *Sambra AV, Mansour E, Hawke S, Zereba M, Greco N, Ghanem A, Zagidulin D, Aboulnaga A, Berners-Lee T (2016) Solid:a platform for decentralized social applications based on linked data*
13. *Becker RA, Volinsky C, Wilks AR (2010) Fraud Detect Telecommunications 52(1):20–33*
14. *Dorronsoro JR, Ginel F, Sanchez C, Santa Cruz C (1997) Neural fraud detection in credit card operations. IEEE 8:827–834*
15. *Hand C, Whitrow DJ, Adams C, Juszczak NM, Weston P D (2008) Performance criteria for plastic card fraud detection. JORS 59(7):956–962*
16. *A Survey of Credit Card Fraud Detection Techniques: Data and Technique Oriented Perspective - Samaneh Sorournejad, Zojah, Atani et.al - November 2016*
17. *Support Vector machines and malware detection - T.Singh,F.Di Troia, C.Vissagio, Mark Stamp - San Jose State University - October 2015*
18. *Solving the False positives problem in fraud prediction using automated feature engineering - Wedge, Canter, Rubio et.al - October 2017*
19. *PayPal Inc. Quarterly results https://www.paypal.com/stories/us/paypalreports-third-quarter-2018-results*
20. *A Model for Rule Based Fraud Detection in Telecommunications - Rajani, Padmavathamma - IJERT - 2012*
21. *HTTP Attack detection using n−gram analysis - A. Oza, R.Low, M.Stamp - Computers and Security Journal - September 2014*
22. *Scikit learn - machine learning library http://scikit-learn.org*
23. *Paysim - Synthetic Financial Datasets for Fraud Detection https://www.kaggle.com/ntnu-testimon/paysim1*