IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 3, March 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303050 |

A Review on Credit Card Fraud Detection System Using HMM

Harsha Meghani, Pranjali Dhamale, Tejal Mesharam, Tejas Virkar, Prof. Rutuja Ardak

U. G. Student, Dept. of Computer Science Engineering, PRPCEM, Amravati, Maharashtra, India

U. G. Student, Dept. of Computer Science Engineering, PRPCEM, Amravati, Maharashtra, India

U. G. Student, Dept. of Computer Science Engineering, PRPCEM, Amravati, Maharashtra, India

U. G. Student, Dept. of Computer Science Engineering, PRPCEM, Amravati, Maharashtra, India

Guide & Assistant Professor, Dept. of Computer Science Engineering, PRPCEM, Amravati, Maharashtra, India

ABSTRACT: In response to the escalating prevalence of electronic transactions, the issue of credit card fraud has emerged as a substantial concern for both financial institutions and consumers. This study introduces an innovative methodology for detecting credit card fraud by leveraging Hidden Markov Models (HMMs). Hidden Markov Models are probabilistic models widely employed in the analysis of sequential data.

In our proposed approach, we conceptualize the sequence of transactions conducted by a credit card user as a hidden Markov process. Here, the states within the model signify various transaction patterns, while the observations denote the distinctive characteristics associated with each transaction. Initially, the HMM assimilates knowledge from typical transactions. Subsequently, if a current credit card transaction deviates significantly from the learned patterns, it is flagged as potentially fraudulent. It is imperative to note that while identifying fraudulent activities, the system ensures that legitimate transactions are not mistakenly rejected.

KEYWORDS: Credit card fraud, Hidden Markov Models (HMMs), Hidden Markov process, Transaction patterns, Fraud Detection

I. INTRODUCTION

In today's modern era, our lives have been considerably enriched with conveniences such as online banking, e-cash, online shopping, ticket booking, fee payments, and various other transactional operations conducted over the internet. Among these, credit cards stand out as one of the most popular and conventional means of making online payments. With just a few card details like the security code, expiration date, and card number, individuals can seamlessly engage in online transactions, facilitated mainly through phones or internet platforms.

The increasing prevalence of electronic transactions has undeniably transformed consumer financial behaviour. Within this landscape, credit card transactions play a vital role in driving the global economy forward. However, alongside the convenience they offer, credit cards also present a significant challenge in terms of security and fraud prevention. As financial institutions and merchants' endeavour to safeguard against fraudulent activities, the necessity for robust and efficient fraud detection systems becomes increasingly urgent.

In response to this need, there has been a notable surge in interest surrounding the utilization of sophisticated statistical models for credit card fraud detection. Among these models, the Hidden Markov Model (HMM) has emerged as a promising candidate. HMMs are probabilistic models renowned for their ability to capture temporal dependencies within sequential data, thus making them particularly suitable for analysing the sequential nature of credit card transactions.

II. OBJECTIVE

- Credit card fraud detection systems aim to identify suspicious transactions while allowing legitimate ones to proceed smoothly.
- Machine learning (ML) tools offer advantages over rule-based solutions, providing higher accuracy and precision in fraud detection.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303050 |

- ML systems reduce manual verification workload for analysts and minimize false declines of legitimate transactions.
- ML algorithms can identify new fraud patterns and adapt to changes in the financial environment, enhancing overall effectiveness and efficiency of fraud detection efforts.

III. LITERATURE SURVEY

- In 2019, a research study explored the realm of Credit Card Fraud Detection through Machine Learning and Data Science, uncovering significant challenges. The dynamic nature of both standard and fraudulent transaction profiles, coupled with imbalanced datasets, presented notable obstacles. Evaluation of method performance relied on diverse metrics including accuracy, sensitivity, specificity, precision, Matthew's correlation coefficient, and flat classification rate. Notably, Naïve Bayes, k-nearest neighbour, and logistic regression classifiers showcased optimal accuracy rates of 81.92%, 87.69%, and 54.86%, respectively, with k-nearest Neighbour emerging as the most effective technique.
- In 2021, a fresh perspective on Credit Card Fraud Detection through Machine Learning emerged, emphasizing Fraudulent Detection within Credit Card Systems using SVM & Decision Tree algorithms. The global surge in electronic commerce has heightened fraud occurrences, resulting in considerable financial losses. This innovative system harnesses Support Vector Machine (SVM) & decision tree algorithms, presenting a hybrid solution to effectively combat financial losses.
- In 2022, a new research endeavour unveiled a Behavioural-based credit card fraud detection model employing machine learning algorithms. This model utilized various techniques including Outlier detection, unsupervised outlier detection, Peer group analysis, and breakpoint analysis to forecast fraudulent transactions. While Outlier detection identifies abnormal transactions compared to historical data, it may inadvertently flag legitimate transactions as fraudulent. On the other hand, unsupervised outlier detection discerns customer transaction behavior without preconceptions, while Peer group analysis compares entities with similar traits to identify irregularities, providing an additional layer of fraud detection.

IV. METHODLOGY

Techniques and Algorithms Used: To model the charge card undertaking treat utilizing a Hidden Markov Model (HMM), the following methods and algorithms are working:

A. Hidden Markov Model Representation:

- Transactions are modeled using a Hidden Markov Model (HMM), where states correspond to different price ranges.
- Purchase patterns are categorized into M price ranges (V1, V2, ..., VM), tailored to individual cardholder spending behaviors.
- HMM dynamically determines these price ranges through clustering algorithms, employing K-means clustering on cardholders' transaction records.
- Clustering results in M clusters (Vk) defining distinct price ranges, which are mapped to states in the HMM.
- The model categorizes transactions into three main price ranges: Low (l), Medium (m), and High (h), denoted by V {l, m, h}.
- For example, a $250 transaction falls into the Medium spending category, labeled as M and V(2).

B. Transaction Prediction Process:

- Transaction prediction considers cardholders' purchasing patterns over time, accounting for variations in purchase types and amounts.
- The model analyses changes in purchase amounts within the last 10 transactions to calculate probabilities for categorization.
- During initial stages, when the model lacks recent transaction data, cardholders are prompted to provide basic information such as parental name and place of birth to enrich transaction records and verify spending patterns.

C. Model Description:

- Traditional fraud detection schemes often rely on static data such as CVV numbers and expiration dates, making them vulnerable to phishing attacks and unable to effectively detect fraudulent transactions.
- In the proposed model, transaction analyses are securely conducted on the bank's server, transferring data from one system to another for verification at the user's end.
- Hidden Markov Models are employed to verify transaction authenticity in real-time, enhancing fraud detection throughout the transaction process.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303050 |

- By adapting to cardholder spending patterns and utilizing probabilistic calculations, the model offers a robust approach to identifying fraudulent transactions.
- Security measures such as private labelling and verification questions ensure secure transactions and safeguard against fraudulent activities.

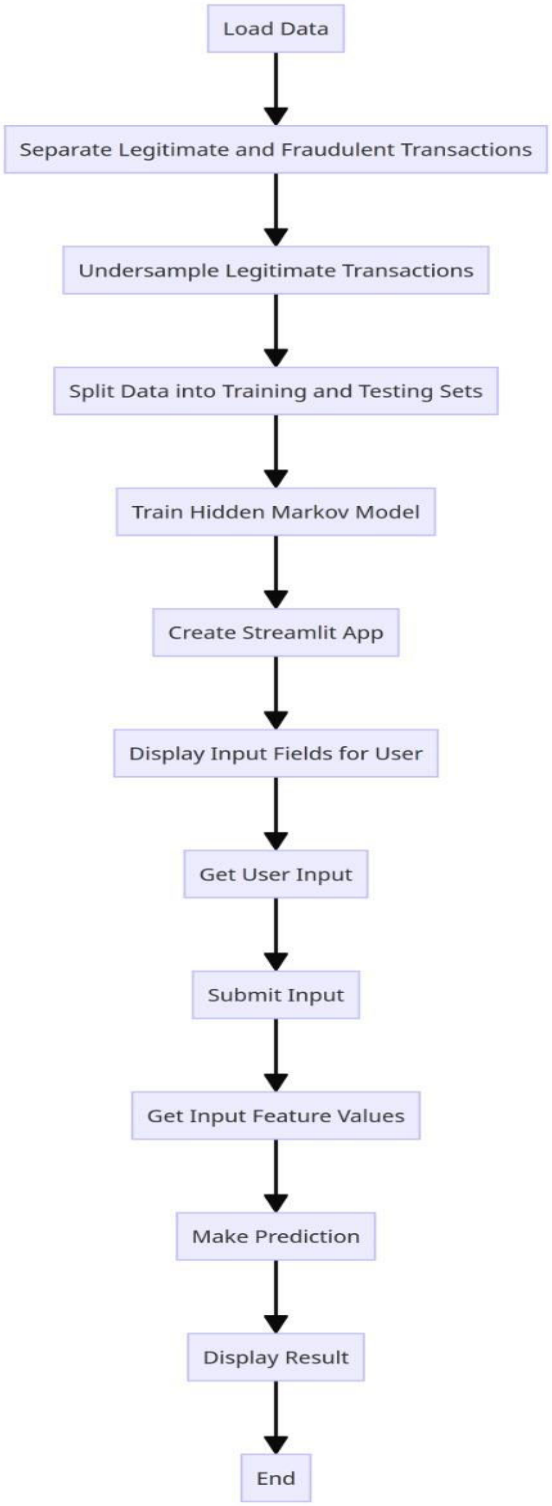

Fig. System Diagram

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303050 |

V. CONCLUSION

The approach leverages Hidden Markov Models (HMMs) to model the underlying stochastic process of credit card transaction processing. Transaction amounts serve as indicators, categorized into different states within the HMM. A method is proposed to comprehend cardholders' spending behaviours, aiding in determining clues' values and initial model configurations. By utilizing HMMs, the system can discern potentially fraudulent transactions based on learned spending habits. Experimental findings demonstrate the efficacy and performance of the system, highlighting the value of learning cardholders' spending profiles.

Evaluation of the method using real-world credit card transaction data has yielded promising outcomes, showcasing its effectiveness in fraud detection and alleviating the workload on analysts through automated processing. Compared to traditional rule-based systems, the adoption of HMMs offers advantages in capturing temporal dependencies and adapting to evolving fraud patterns. This enhances the accuracy and efficiency of fraud detection processes.

REFERENCES

1] V.Bhusari, S.Patil, 2016, “Study of Hidden Markov Model in Credit Card Fraudulent Detection”.
[2] Trends in online shopping, a Global Nelson Consumer Report, (2008).
[3] European payment cards fraud report, Payments, Cards and Mobiles LLP & Author, (2010)
[4] International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, Volume 2, Issue 7, July 2012)511 Credit Card Fraud Detection Using Hidden Markov Model; Vaibhav Gade, Sonal Chaudhari; All Saint College of Technology, Bhopal (M.P.), India.
[5] L.R. Rabiner, “A Tutorial on Hidden Markov Models and Selected Applications in Speech Recognition,” Proc. IEEE, vol. 77, no. 2, pp. 257-286, 1989.
[6] CREDIT CARD FRAUD DETECTION USING HIDDEN MARKOV MODEL by Divya.Iyer, Arti Mohanpurkar, Sneha Janardhan, Dhanashree Rathod, Amruta Sardeshmukh; Department of Computer engineering and Information Technology, MMIT, Pune, India.
[7] Credit Card Fraud Detection Using Hidden Markov Model by Abhinav Srivastava, Amlan Kundu, Shamik Sural, Senior Member, IEEE, and Arun K. Majumdar, Senior Member, IEEE
[8] Ghosh, S., and Reilly, D.L., 1994. Credit Card Fraud Detection with a NeuralNetwork, 27th Hawaii International l Conference on Information Systems, vol. 3 (2003), pp. 621- 630.
[9] Syeda, M., Zhang, Y. Q., and Pan, Y., 2002 Parallel Granular Networks for Fast Credit Card Fraud Detection, Proceedings of IEEE International Conference on Fuzzy Systems, pp. 572-577 (2002).
[10] Stolfo, S. J., Fan, D. W., Lee, W., Prodromidis, A., and Chan, P. K., 2000. CostBased Modeling for Fraud and Intrusion Detaction: Results from the JAM Project, Proceedings of DARPA Information Survivability Conference and Exposition, vol. 2 (2000), pp. 130-144.
[11] Aleskerov, E., Freisleben, B., and Rao, B., 1997. CARD WATCH: A Neural Network Based Database Mining System for Credit Card Fraud Detection, Proceedings of IEEE/IAFE: Computational Intelligence for Financial Eng. (1997), pp. 220-226.
[12] M.J. Kim and T.S. Kim, “A Neural Classifier with Fraud Density Map for Effective Credit Card Fraud Detection,” Proc.Int’l Conf. Intelligent Data Eng. and Automated Learning, pp. 378- 383, 2002

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details