Online Transaction Fraud Detection and Prevention Using Hmm and Behavior Analysis

Mr. Abjijeet More[*1], Dnyaneshwari Khane[2], Mansi Nagane[3] & Tanuja Bhoir[4]

[*1]Assistant Professor, Pillai HOC College of Engineering and Technology, Rasayani, Maharashtra

[2,3,&4]Student, Pillai HOC College of Engineering and Technology, Rasayani, Maharashtra

Abstract:

The objective of this project is to both prevent and detect fraudulent transactions. As the use of online transactions, such as NEFT and RTGS, has grown with the rapid advancement of internet technology, credit card payments have become a popular method of payment for both offline and online purchases. However, this has also led to an increase in online transaction fraud. Criminals have taken advantage of the popularity of network transactions to commit crimes, causing banks to suffer significant losses. The current fraud detection system only identifies fraudulent transactions after they have been completed. To address this issue, we will use the Hidden Markov Model (HMM). This will allow for fraud to be detected during the transaction and immediately blocked by sending a verification code to the user's email address. To improve the system's effectiveness, we have incorporated a real-time payment gateway method. Furthermore, we will utilize behavior analysis to comprehend the user's spending habits. This combination of HMM and behavior analysis will facilitate advanced fraud analysis with a low false alarm ratio.

Keywords: Fraud Detection System (FDS), Card Holder, Transaction, Hidden Markov Model (HMM), Behavior Analysis (BA).

DOI: 10.24297/j.cims.20235.16

1. Introduction

Machine learning: A subset of artificial intelligence called machine learning involves making machines imitate intelligent human behavior. Systems using artificial intelligence are created to solve complicated issues similarly to humans. The application of machine learning in fraud detection is based on the notion that fraudulent transactions exhibit particular patterns that differentiate them from legitimate ones. Using ML enables the creation of algorithms that can automatically process large datasets, without the need for manual intervention to identify potentially fraudulent activities. Consequently, machine learning-based systems can reveal hidden and implicit correlations, making them highly effective in detecting fraud in real-time data, surpassing traditional methods.[1]

Fraud Detection: The detection of fraud entails monitoring the transaction behavior of a cardholder to differentiate between transactions initiated by the cardholder and those initiated by a third party. There are two primary methods for fraud detection: corrupted detection and unexpected detection. Misuse detection involves using classification methods to determine whether an incoming transaction is fallacious or not.[9] On the other hand, anomaly detection focuses on identifying abnormal behavior. Supervised learning is a machine learning technique that involves training an algorithm using labeled historical data to predict target variables in future data. In contrast, unsupervised learning involves processing unlabeled data and clustering it into different categories to uncover hidden relationships between variables in data items.[10]

Behavior Analysis: The Fraud Detection System (FDS) of a credit card issuing bank utilizes a Behavior Analysis (BA) approach, which studies the behavior of both human and non-human organisms. The FDS processes every incoming transaction, verifying the card information and transaction amount to ascertain whether it is legitimate or fraudulent. However, the FDS lacks knowledge of the specific items being purchased in the transaction. When the FDS detects a fraudulent transaction, the bank declines it. [1]

2. Literature Survey

Online Transaction fraud Detection the use of HMM & Behavior Analysis" the detection of fraud transaction after the transaction is completed. It makes use of HMM which statistical stochastic mannequin is used to mannequin randomly altering system. Fraudulent transactions are identified in real-time, and if there are three failed attempts to verify the transaction, the card is blocked. Machine-based fraud detection primarily relies on analyzing the spending patterns of the cardholder to detect potentially fraudulent activities. The spending habits.

Algorithm used: 1) Training set is based totally on clustering scheme.2) Detecting take region by using analyzing the distinction in the likelihood and trying outthe effect with education phase [1].

Xiaoguo Wang and his colleagues have presented a method for detecting fraud in banks using the Hidden Markov model. Their approach involves using a potential algorithm to analyze the transaction frequency and volume sequence of bank accounts, which is then used to build and test the model. The researchers conducted scan and bank data verification experiments, which demonstrated that their method can effectively detect fraudulent activities in low and medium frequency and volume consumer organizations. The proposed model analyzes the spending patterns of individual users based on their historical transaction data, and generates unique consumption parameters for each user. These parameters are then used as a reference to select appropriate Hidden Markov models, which ultimately determine the probability of fraudulent transactions. Overall, the model provides a promising solution to the problem of bank fraud.[2]

Fraud loses in the card payment industries have been steady for several years as fraud fighting capabilities deployed by issues merchants and ATM and merchant acquires made the challenges of criminal who deployedever more sophisticated needs to comprise the system [3].

The paper discusses the application of the Hidden Markov model algorithm in detecting and preventing fraud in web banking, while ensuring that legitimate transactions are not declined by implementing a one- time password generated by the bank. To create the proposed system, the researchers developed a mock bank account database for various users and created an internet carrier based on Tomcat Apache that allows customers to use online banking. They also developed a customer software that enables users to make online payments based on their transaction history. Using this database, they created a transaction pattern analysis algorithm based on HMM that can detect ongoing fraudulent transactions. To implement the HMM algorithm, the researchers utilized Java series API. Once a fraudulent transaction is identified, the system dispatches an OTP to the customer to confirm their identity and proceed with the transaction. Overall, the proposed system provides a comprehensive solution for detecting and preventing fraudulent activities in web banking while ensuring secure transactions.[4]

In this research paper, the authors explore the use of machine learning algorithms to detect fraud in savings cards. They compare the performance of several popular models, such as NB, SVM, and DL, on a publicly available credit card dataset, both individually and in hybrid models using AdaBoost and majority voting. To measure performance, the authors use the MCC metric, which takes into account true and false positives and negatives. The results show that the majority voting method achieves the highest MCC score of 0.823. Additionally, the authors evaluate the models on a real deposit card dataset and introduce noise ranging from above 10% and below 30% into the data samples. They find that the majority voting method performs the best, achieving an MCC score of 0.942 with approximate 30% noise.These findings suggest that the majority voting method is robust and effective in detecting fraud, even in the presence of noise in the dataset.[5]

The objective of this study is to prevent online credit card fraud through the use of a hidden Markov model. The proposed system handles a vast number of credit card transactions by simplifying the process and eliminating complexity using HMM. Transactions are classified into low, medium, and high groups, which serve as symbols or states in the HMM. It is suggested to adopt a technique for identifying spending patterns of cardholders, which will determine the value of observation symbols and the initial estimation of the model parameters. By checking the incoming transaction, the system can determine if it is fraudulent or not and proceed accordingly. [6].

3. Problem Statement

According to the nilson report [3], card-based payment systems experienced a loss of $28.65 billion worldwide in 2019. the report presents a graph forecasting the trend of these losses until 2027.

Among global brand cards such as american, diners club/discover, jcb, mastercard, visa, and unionpay, fraud accounted for $25.53 billion in losses in 2019, which is a 2.7% increase from the previous year. this amount represents 89.11% of the total global fraud losses in 2019.

4. Methodology

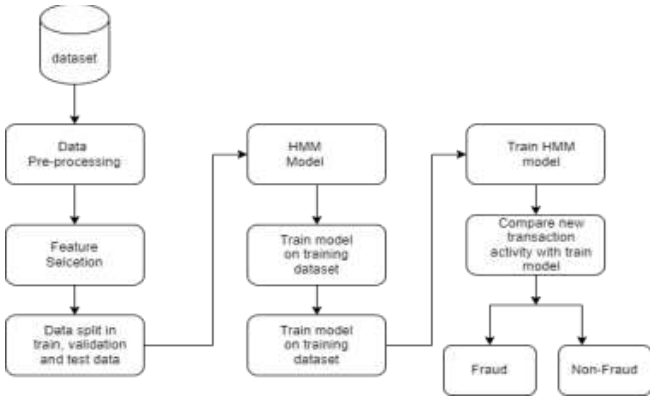

Figure 4.1: System Architecture

The widespread adoption of online transactions and various payment tools, along with the rapid growth of internet finance, have become an integral part of people's daily activities. However, this convenience has also led to an increase in online trading fraud [2]. According to Nielson's learn about on net usage, a hundred percent of the globe's populace makes use of the internet, with a boom charge of 13,941% from 2000 to 2020.

E-commerce transactions have increased by a staggering 600% globally since 2010 [3]. To combat fraud, aHidden Markov Model (HMM) can be employed. An HMM models a probability distribution over sequences of compliances, where the system being modeled is assumed to be a Markov process with an unobserved state [4].

We will augment a fictitious database of financial institution accounts for numerous customers. A network provider entirely based on a Python Flask server is created and implemented to enable customers to use online banking. Wehave built the shopping website which provides the services to the user and allows user to make the online payment usingthe stripe API. We will use HTML pages for consumer-servercommunication. We can even design a consumer-facing utility and a server-facing utility for use with Python and Flask. The consumer needs to talk to the server about using the Flask server. can also be maintained through the use of serialized objects. The online shopping websites provides theservices to the user. Users who are already registered can login to the site, while those who are not registered must first complete the registration process. During registration, the system will prompt users to provide some personal details that will be used for authentication purposes. Once logged in, users can browse the available products and add items to their cart for further transactions.

When making a payment, the payment system prompts the user to input their card details, including the card number, CVV, and expiration date. The system then cross-checks this information with past transactions stored in its database. If any discrepancies or anomalies are detected between the current and past transactions, the system flags the transaction as potentially fraudulent. Details of the user's orders and transaction amounts are stored in SQL database tables and compared to each new transaction to identify any irregularities. [1]

The current system for detecting fraudulent transactions relies on analyzing a user's transaction history to establish their spending behavior. A Hidden Markov Model is used to represent this behavior in a simple and easily manageable sequential model consisting of two levels. If a potentially fraudulent transaction is detected, a one-time password is sent to the consumer to confirm their identity and prevent the transaction from being completed if it is indeed fraudulent. Transaction amounts are used as observations in this model. Our proposed system is highly reliable and significantly less complex than existing systems, and although our simulation analysis was performed on a small dataset, we believe our system has the potential to handle a wide range of transactions encountered in real-life scenarios.

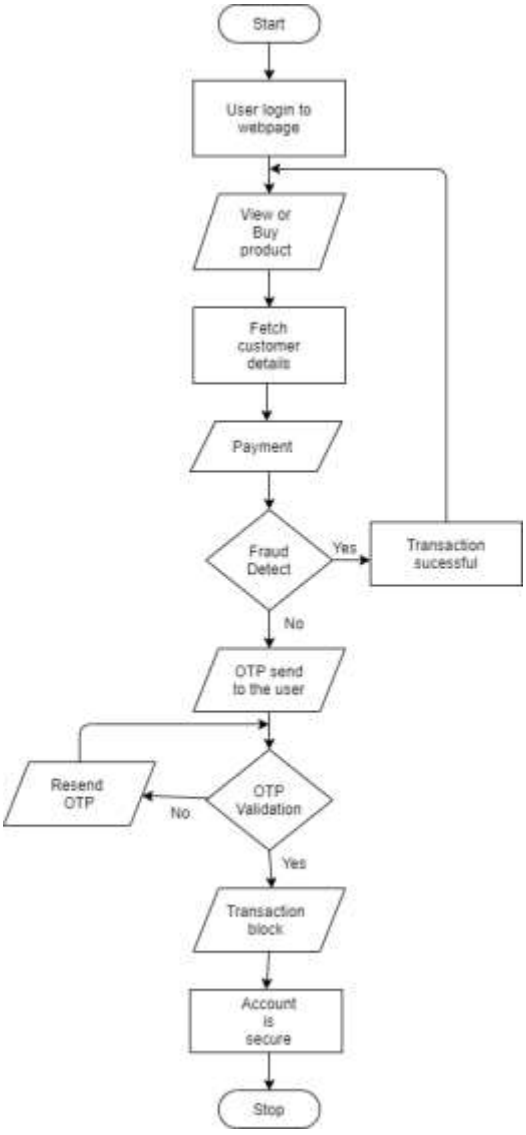

Figure 4.2 Flowchart

5. Conclusion

The methodology proposed in this study is centered around detecting and preventing fraudulent activity in internet banking. the bank employs a fraud detection system integrated with a prediction mechanism that takes into account user behavior. the attack strategy for signature-based online banking processes involves manipulating the software to display correct transactions on the screen while executing fraudulent transactions in the background. to address this, the hidden markov model is utilized to track user behavior, which is recorded and analyzed for any new transactions. the legitimacy of incoming transactions is evaluated based on the user's spending patterns, and fraudulent activity is detected and prevented by sending a verification code to the user's email address. this system is capable of distinguishing between legitimate and fraudulent users, enabling more effective fraud prevention in internet banking.

References

1. Online transaction fraud detection using hidden Markov model and behavior analysis, Niki Patel, Yanyan Li and Ahmad Hadaegh, Published in: International Journal of Computer Science and Security (IJCSS), year 2021.
2. Research on Bank Anti-Fraud Model Based on K-Means and Hidden Markov Model, Xiaoguo Wang, Hao Wu, Zhichao Yi, Published in: IEEE 3rd International Conference on Image, Vision and Computing (ICIVC), year 2018.
3. Nilson Report, Year December 2021.
4. Internet banking fraud detection using HMM, Mr. Sunil S Mhamane, Mr. L.M. RJ Lobo, Published in: Third International Conference on Computing, Communication and Networking Technologies (ICCCNT'12), Year 2012.
5. Credit Card Fraud Detection Using Adaboost and majority voting, Kuldeep Randhawa, chu kiong loo manjeevan seera chee peng lim and asoke k. nandi, year February 15, 2018.
6. Card Fraud Detection System in Payment Gateway by HMM, Dhanashree Devendra Surve and Prof. Chaitanya Mankar, Year 2020.
7. Fraudulent Internet Banking Payments Prevention using Dynamic Key, Osama Dandash, Osama Dandash, Phu Dung Leand Bala Srinivasan. Year 2008.
8. Random Forest for Credit Card Fraud Detection S. Xuan, G. Liu, Z. Li, L. Zheng, S. Wang and C. Jiang, Published In: IEEE 15th International Conference on Networking, Sensing and Control (ICNSC), Year 2018
9. Credit card fraud detection using Machine Learning Techniques: A Comparative Analysis, John O. Awoyemi, Adebayo O. Adetunmbi, Samuel A. Oluwadare, Published In: International Conference on Computing Networking and Informatics (ICCNI), Year 2017.
10. Fraud Detection: How Machine Learning Systems Help Reveal Scams in Fintech, Healthcare, and eCommerce Published by Altexsoft, Year 2017.
11. Credit Card Fraud Detection and Concept-Drift Adaptation with Delayed Supervised Information, Andrea Dal Pozzolo, Giacomo Boracchi, Olivi Caelen, Cesare Alippi, and Gianluca Bontempi, Published In: International Joint Conference on Neural Networks, Year 2015.