A Sequential Pattern Mining Method for the Individualized Detection of Online Banking Fraudulent Transactions

Ghulam Abbas

School of Electrical Engineering, Southeast University,
Nanjing 210096, China
lashariabbas@seu.edu.cn

ABSTRACT

Financial institutions are facing a growing number of challenges as a result of the growth in fraudulent activities in online banking, which calls for the implementation of systems that are more advanced in their identification of fraud. Traditional rule-based techniques have difficulties when it comes to handling rule modifications and do not provide sufficient detail to particular users. This study presents the User-Specific Sequence Pattern Mining Framework for Online Banking Fraud Detection (USPM-FrauD) as a solution to the challenges that have been highlighted. The framework was developed in order to detect fraudulent activity in online banking. This system makes use of sequence pattern mining algorithms in order to examine the transaction logs of every user and find variations that may be indicative of fraudulent conduct. By concentrating on individualized transaction patterns, the USPM-FrauD model provides a method that is both more efficient and more specifically targeted to the identification of fraudulent activity in online banking. When compared to rule-based and Markov chain models, the experimental findings reveal that the USPM-FrauD model has greater performance. This demonstrates that the model has the potential to be practically implemented in online banking systems that are used in the real world. In order to battle the ever-changing world of online banking fraud, financial institutions now have access to a more complex and user-specific tool thanks to the USPM-FrauD framework, which marks a substantial improvement in fraud detection approaches.

Keywords: Financial Institutions; Fraudulent Activities; Online Banking; Fraud Detection Systems; Rule-Based Techniques; Rule Modifications; User-Specific; Sequence Pattern Mining.

1. Introduction

While the introduction of online banking has brought about a transformation in the financial landscape, it has also presented financial institutions with an increasing difficulty in the fight against fraudulent activities[1]. Online banking has provided customers with an unprecedented level of ease. Traditional rule-based procedures are being pushed to their limitations as a result of the expansion of cyber risks and complex fraud schemes, which calls for creative ways to detection[2]. Although rule-based systems do have some efficiency, they struggle to adapt to the dynamic nature of fraud and often do not have the flexibility needed for rule updates that are made in real-time. Personalized Ordering for Each User [3].

Pattern Mining Framework for Online Banking Fraud Detection (USPM-FrauD) is presented in this research in recognition of the limitations that have been identified[4]. As the

https://doi.org/10.70023/piqm244

number of risks in the digital realm continues to rise, it is imperative that fraud detection approaches undergo a paradigm change[5]. This shift should be toward solutions that are not only more adaptable, but also provide a better degree of granularity, allowing detection processes to be tailored to the specific needs of individual users[6]. The critical necessity for financial institutions to remain ahead of the curve in the fight against online banking fraud is the driving force behind this study[7]. Online banking fraud is a growing problem. Due to the fact that standard rule-based tactics have been shown to be insufficient in tackling the complex and ever-evolving nature of fraudulent operations, there is an urgent need for ways that are more sophisticated and customized[8]. This hole is intended to be filled by the USPM-FrauD framework, which incorporates sequence pattern mining methods in order to dive into the complexities of user-specific transaction logs.

The fundamental purpose of this study is to propose a robust and user-specific framework for the detection of fraud that is capable of resolving the inadequacies of traditional rule-based techniques[9]. Aims of the research are to: For the purpose of detecting fraudulent activity in online banking, the User-Specific Sequence Pattern Mining Framework (USPM-FrauD) should be developed. The performance of the USPM-FrauD model should be evaluated in comparison to the performance of standard rule-based approaches and Markov chain models[10]. Determine whether or whether the USPM-Fraud model can be practically applied to online banking systems that are used in the real world[11]. By addressing the limits of current fraud detection approaches and providing a user-specific sequence pattern mining strategy, the purpose of this study is to provide financial institutions with a robust tool that will enable them to traverse the complex environment of online banking fraud[12]. In the following parts, the study will go more into the particular components of this framework, including its creation and the empirical data that supports its effectiveness. This research makes three contributions:

- To develop the User-Specific Sequence Pattern Mining Framework for Online Banking Fraud Detection (USPM-FrauD).
- To evaluate the efficiency of the USPM-FrauD model against traditional rule-based techniques and Markov chain models.
- To assess the practical applicability of the USPM-FrauD model in real-world online banking systems.

A summary of the research is provided below. In Section 2, the current literature and study techniques are thoroughly examined. The proposed methodology and processing procedures are detailed in Section 3. The results analysis is covered in Section 4. Part 5 explores the main conclusion and Future work.

2. Research Methodology

Ni et al. [13] displayed the intricacy of transaction data is putting the credit card industry at greater danger of fraudulent transactions. Due to unequal class distribution and significant feature redundancy, current machine learning models need modification. This work proposes a model for credit card fraud detection that utilizes a fraud feature-boosting mechanism and a spiral oversampling balancing approach (SOBT). The model's decision-making power is improved using a multifactor synchronous embedded method, and correlated and redundant features are weeded out using a compound grouping elimination strategy. By maintaining a steady ratio between the two, the SOBT enhances the model's capacity to distinguish between legitimate and fraudulent transactions.

Kannagi et al. [14] presented the Because data and information are evolving at such a fast pace, it is becoming more difficult for banks and other financial organizations to identify fraudulent activities. Banks need to use fraud detection tools and machine learning techniques to reduce losses. An evaluation of the pseudo-nature of fraudulent transactions may be accomplished using Pattern Recognition based K-Nearest Neighbor (PR-KNN), a non-parametric approach. This method is more effective at identifying fraudulent bank transactions or fewer false alarms when used after the fact. To create chances via dynamic consumer estimate, a thorough customer engagement plan has to be put in place.

Mytnyk et al. [15] suggested the This research looks at the possibility of using AI to detect bank fraud, with a focus on the COVID-19 epidemic. Online banking transaction analysis and recognition using machine learning techniques is the main topic. Using techniques including feature engineering, feature transformation, and managing unbalanced datasets, the study builds models to detect fraudulent transactions and talks about ways to improve detection accuracy. The proposed method, which relies on an artificial neural network, significantly enhances the precision of identifying fraudulent transactions.With a value of around 0.946 for the output AUC, the logistic regression method performs better than other algorithms. This research shows how critical it is for our modern digital society to be able to detect financial fraud using AI algorithms.

Rathor et al. [16] presented ATMs' money and personal data make them susceptible to fraud. Enhance hardware security systems to detect particular fraud, but no protection against future assaults. Security for ATMs doesn't need hardware. Autonomous model generation is used to learn typical behavior patterns from ATM status information, which differs significantly from fraud-indicating behavior. Preprocessing, integrating, and deduplicating data is done, then feature selection trains models using BOA and C-LSTM. Our global and temporal sentence semantics technique beats LSTM and CNN.

Krishna et al. [17] provided the article examines Bayesian network and decision tree data mining methods for credit card fraud detection. subsequently stresses the importance of RF algorithms in detecting credit card fraud and brings attention to data mining issues like performance and user engagement. Data purification, visualization, and clustering-focused machine learning are all included in the study. Enhancement of credit card fraud detection by sequential pattern highlighting.

An RL-based network method for identifying credit card fraud, CATCHM was suggested by Van Belle et al. [18]. This method avoids human feature engineering by considering the transactional connection structure. Thanks to its innovative network design, effective inductive pooling operator, and meticulous configuration of downstream classifiers, CATCHM outperforms state-of-the-art methods on a real-life credit card dataset. This method has been empirically tested on a real-world credit card dataset, demonstrating its applicability for the industry.

Cherif et al. [19] proposed Contactless payment techniques and sophisticated technology have made credit card fraud a major problem. From 2015 to 2021, forty research were reviewed in this article on the detection and prediction of credit card fraud transactions. According to the report, there is a lack of research on deep learning, which means that in order to tackle problems with cloud computing, big data analytics, and large-scale machine learning, further research is required. The research helps academics in both academia and industry assess financial fraud detection systems and develop effective solutions.

The second most valuable digital currency, Ether, which was developed by Md et al. [20], has seen a rapid increase in transactions, leading to a rise in fraud. In order to detect phony accounts, this research recommends employing machine learning techniques. In order to construct a meta-learner, the study's stacking classifier integrates many methods. A robust classifier for detecting fraudulent transactions is formed using Logistic Regression, Decision Trees, Naive Bayes, Random forest models, AdaBoosts, KNNs, SVMs, which and Gradient Boosts. With an F1 score of 97.02% and an accuracy of 97.18%, the stacking classifier outperformed the others. It used Multinomial Naive Bayes, a Random Forest, plus logistic regression as its methods.

3. User-Specific Sequence Pattern Mining Framework for Online Banking Fraud Detection (USPM-FrauD)

One innovative method for detecting online banking fraud is the User-Specific Sequence Pattern Mining Framework for the Purpose of Detecting Fraud (USPM-FrauD). The goal of the framework is to make fraud detection more precise and efficient by defining typical user behavior based on patterns extracted from their transaction logs. For each user, it finds typical transaction sequences using sequence pattern mining algorithms and flags any changes as possible fraud. As new transactions come in, the USPM-FrauD model checks them against each user's known usual patterns in real time. An alert is sent off to notify the system of possible fraudulent conduct if a transaction drastically differs from the user's regular behavior patterns.

The USPM-FrauD framework outperformed more conventional rules-based and Markov chain approaches in identifying fraudulent transactions, according to experimental validation conducted on real-world data from online banking transactions. By tailoring its approach to each individual user, the USPM-FrauD framework improves the speed and accuracy of fraud detection while decreasing the occurrence of false positives and negatives that are typical in rule-based systems. Still, issues like new users' cold start and more contextual data for detection in practical settings require attention. The model's efficiency and scalability might be the subject of future studies aimed at making it more widely used.

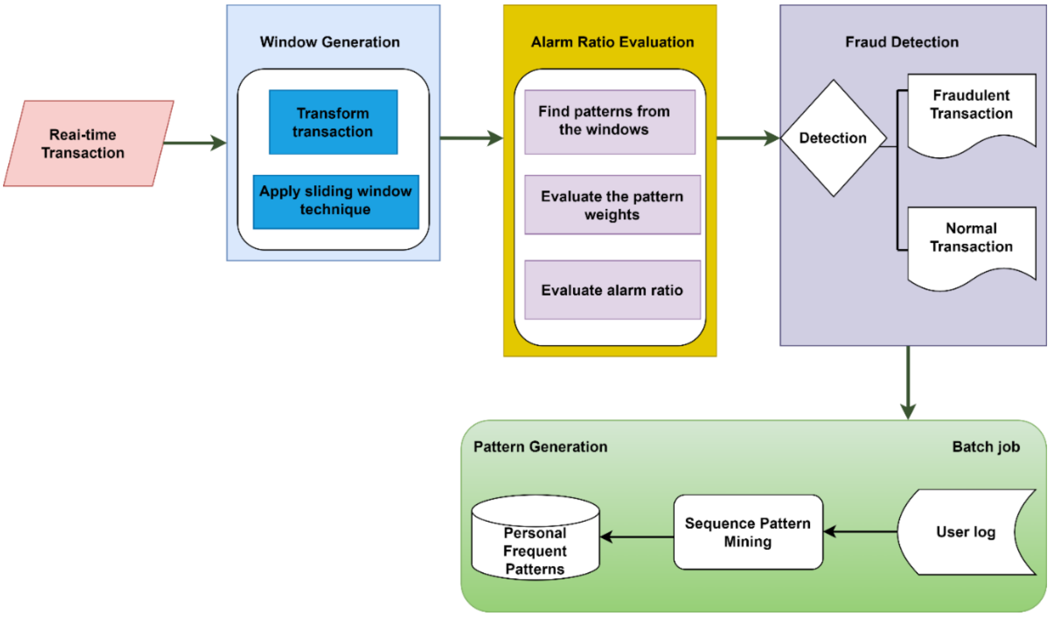

Figure 1: Overview of USPM-FrauD Framework

In figure 1, A overview of an USPM-FrauD model is often characterized by the use of pattern recognition methods for the purpose of identifying abnormalities or deviations from previously defined patterns. In the context of detecting fraudulent conduct in online banking, a pattern-based alert model would examine transaction sequences in order to discover abnormalities that might be indicative of fraudulent activity. The following is a concise explanation of a USPM-FrauD model that may be used to identify fraudulent activity in online banking: Data Collection is to gather transaction data from actions that take place using online banking.

A variety of information, including transaction timestamps, transaction kinds, sums, user identities, and other pertinent facts, are included in this data. Next, the model will extract patterns using the transaction data. This process is known as pattern extraction. The sequences of transactions, the time intervals among transactions, the sorts of transactions that are typical for certain users, and other behavioral patterns might all be examples of these patterns. Pattern analysis involves analyzing the retrieved patterns in order to determine what constitutes typical behavior for each individual user. With the help of the model's awareness of the regular transaction patterns of specific users, it is able to recognize variations that may be indicative of possible fraudulent activity.

Real-Time Monitoring: The pattern mining-based alert model performs continuous monitoring of transactions in real time. When new transactions are made, the model examines them in relation to the patterns that have been formed in order to identify any irregularities or suspicious activity.

Alarm Generation: The alarm model will generate an alert or notice in the event that a transaction exhibits characteristics of fraudulent activity or deviates considerably from the regular patterns. This is done in order to warn the system administrator or users about the possibility of fraud.

Adaptive Learning: The framework can include adaptive learning methods in order to update and modify the patterns that have been developed based on fresh transaction data. Because of this, the model is able to adjust to changing patterns of user activity and emergent fraud tendencies. The efficacy of the pattern-based alarm model is assessed based on parameters such as detection precision, the false positive percentage, false negative rate, and system performance as a whole. Furthermore, the evaluation takes into account the overall performance of the system. Continuous review and improvement are necessary things to do in order to guarantee the model's dependability and effectiveness. In general, a pattern-based alarm framework for bank account fraud detection makes use of pattern recognition methods to improve the identification of fraudulent actions. This is accomplished by examining transaction sequences and finding deviations from known user behavior patterns. By using this preventative strategy, financial institutions may reduce the risks they face and safeguard their customers from the possibility of fraudulent activity in online transactions.

In figure 2, Using the User-Specific Sequence Pattern Mining Framework for Online Banking Fraud Detection (USPM-FrauD), the fraud detection flowchart provides an explanation of the stages involved in identifying fraudulent activity in online banking transactions. This information is based on the information that is supplied in the paper. Based on the information included in the paper, the following is a description of the flowchart that is used for fraud detection:

Information Gathering: The first step in the process is the gathering of transaction information from activities that take place via online banking. Among the information included in this data are transaction timestamps, user identities, transaction kinds, sums, and any other pertinent particulars.In the second stage, known as "Data Preprocessing," the acquired transaction data is put through a series of cleaning and preparation activities in order to get it ready for analysis. In order to do this, it may be necessary to perform data normalization, deal with missing values, and transform the data into a format that is acceptable for further processing.

Sequence Pattern Mining: After the data has been preprocessed, it is next utilized to extract sequential patterns that are unique to each individual user. The use of sequence pattern mining methods allows for the identification of regularly occurring transaction sequences and the establishment of typical behavior patterns for particular users.

Pattern Analysis: The process of defining the typical transaction sequences for each user involves analyzing the patterns that have been retrieved. Through the process of gaining an awareness of the regular actions of users, the system is able to recognize deviations or anomalies that may be indicative of possible fraudulent activity.The system performs continuous monitoring of incoming transactions in real time, which is referred to as "real-time monitoring." When new transactions are introduced, they are compared to the user-specific patterns that have been created in order to identify any anomalies or suspicious activity that may have occurred.

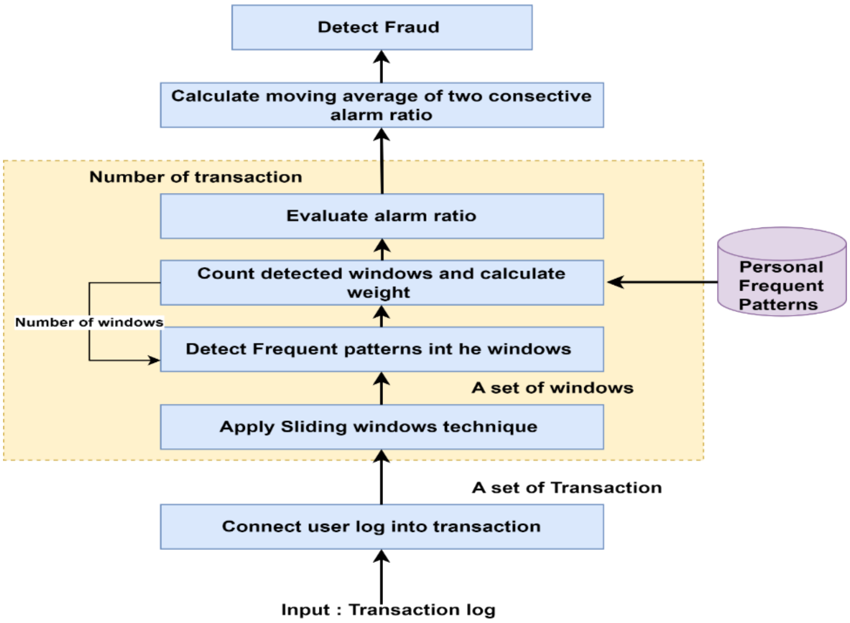
Detect Fraud
Calculate moving average of two consective alarm ratio
Number of transaction
Evaluate alarm ratio
Count detected windows and calculate weight
Personal Frequent Patterns
Number of windows
Detect Frequent patterns int he windows
A set of windows
Apply Sliding windows technique
A set of Transaction
Connect user log into transaction
Input : Transaction log

Figure 2: Flow Chart for Fraud Detection Model

Fraud Detection: The system for detecting fraudulent conduct is activated if a transaction exhibits characteristics of fraudulent activity or deviates considerably from the regular behavior patterns. During this stage, the transaction is identified as carrying the potential for fraudulent activity, and more investigation is initiated.The generation of an alarm occurs when the system determines that a transaction may be fraudulent. This alarm is then sent to the appropriate stakeholders in order to notify them of the situation. The purpose of this alarm is to alert system administrators or users about the questionable conduct, which in turn prompts them to take the right actions.

Continuous Monitoring and Learning: The flowchart for fraud detection places a strong emphasis on the need of continuous monitoring and learning. In order to improve its accuracy and efficiency over time, the system is able to adjust to newly acquired transaction data, update patterns that are personal to the user, and develop its detection skills gradually.

Performance Evaluation: The success of the fraud detection system is assessed based on a variety of indicators, including detection accuracy, the true positive rate, the false negative rate, and the overall performance of the system. Constant assessment is beneficial for determining the dependability of the system and for implementing any adjustments that are required. Finally, the paper's fraud detection flowchart demonstrates a systematic approach to detecting fraudulent behavior in transactions made through online banking via the use of specialized sequence pattern mining techniques. The system's goal is to lessen the risks associated with online banking fraud by improving the precision of fraud detection via the use of real-time monitoring and user-specific trends.

4. Experimental Result and Analysis

To identify fraudulent transactions, a model known as the User-Specific Sequence Pattern Mining Framework for Online Banking Fraud Detection (USPM-FrauD) is used. This framework makes use of data from actual online banking financial transactions. A number of indicators, such as the alarm ratio, accuracy of detection, false positive rate, or false negative rate, are used to assess the effectiveness of the models. The dataset is unbalanced, having a greater number of legitimate transactions than fraudulent ones, which might result in findings that are less accurate than they otherwise would be. When it comes to identifying fraudulent activity, the USPM-FrauD model performs better than both the classic rule-based and Markov chain models simultaneously. The system is able to successfully identify deviations from usual patterns of activity and sends notifications to users or administrators about the possibility of fraud.

The capacity of the model to adapt to the specific patterns of activity of individual users and to identify abnormalities in real time is one of its strengths. This ability contributes to the model's efficacy in limiting the risks connected with online banking fraud. This is advised that more experiments be conducted on other datasets to test the performance of the model across a variety of situations and to strengthen its resilience for applications used in the real world. The capability of the model to adapt to the specific patterns of behavior of individual users and identifying the abnormalities in real time is evidence of usefulness of these model in identifying criminal activities in online banking.

a. Alarm Ratio for USPM-FrauD

A possible indicator of fraudulent behavior is the alert ratio, which shows what percentage of transactions cause an alarm to go off. Figuring out how sensitive the model is to flagging questionable transactions is essential. On the x-axis, analysts may plot various test scenarios or datasets; on the y-axis, they can see what proportion of transactions cause an alert; this allows them to see how the model handles different degrees of fraud. The model's sensitivity to identifying fraud and the threshold for generating warnings may be better understood with the assistance of this depiction.

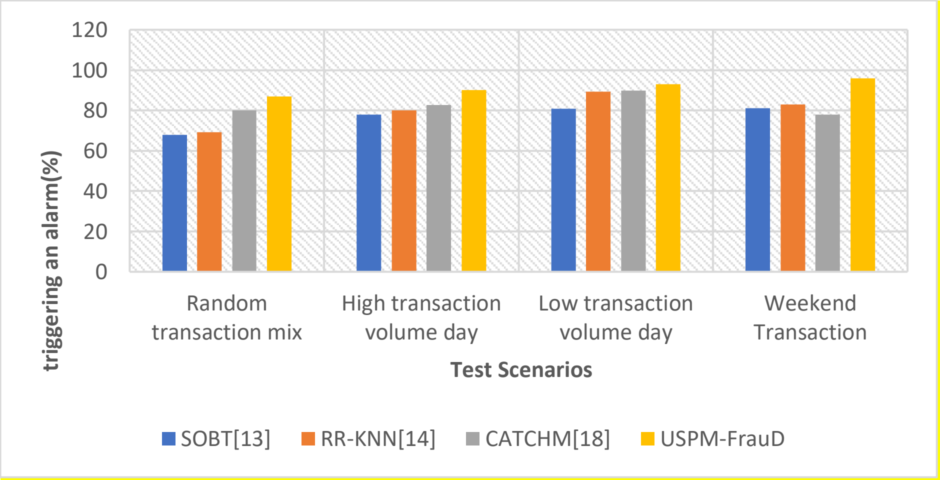

Figure 3: Alarm Ratio for USPM-FrauD

In figure 3, The alarm ratio is essential for analyzing a fraud detection model's sensitivity to fraud. The model's sensitivity to fraud is measured by the proportion of transactions that alert. SOBT, RR-KNN, CATCHM, and USPM-FrauD alarm ratios vary per circumstance. SOBT alerts for 80% of transactions on a high-volume day, indicating moderate to high sensitivity. RR-KNN's alarm ratio varies, with weekend sensitivity high. On high transaction traffic days, CATCHM's alert ratio is 82.6%. USPM-FrauD outperforms or matches other approaches in varied settings due to its great sensitivity.

b. Detection Accuracy for USPM-FrauD

Detection accuracy is a measure of how well a model can spot fraudulent transactions. Out of all the cases of fraud, it measures the proportion of fraudulent transactions that were identified correctly.Researchers may evaluate the model's ability in properly detecting fraud by plotting various test scenarios in the x and y axis for its success %. the study can see how well the model consistently identifies real and fake transactions with this visual aid.

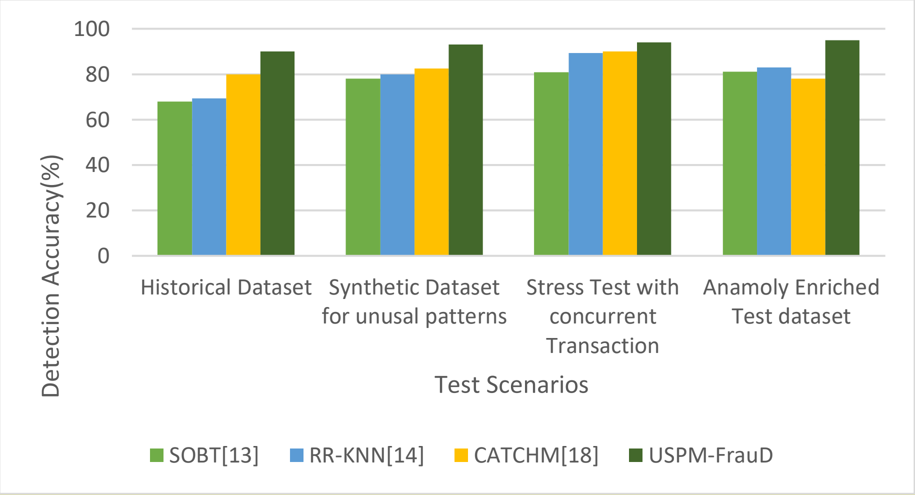

Figure 4: Detection Accuracy for USPM-FrauD

In figure 4, To measure how sensitive a fraud detection algorithm is to possible fraudulent behavior, the alarm ratio is an important statistic to consider. subsequently measures the model's sensitivity to possible fraudulent behavior by quantifying the proportion of transactions that raise an alert. Detection Accuracy vary among situations for several approaches, including SOBT, RR-KNN, CATCHM, and USPM-FrauD. With alerts going off for 80% of transactions on a high-volume day, SOBT shows moderate to high sensitivity in spotting suspicious behavior. RR-KNN's sensitivity is highest on weekends, and it varies among contexts. The alert ratio of CATCHM fluctuates; on days with a large amount of transactions, it reaches 82.6%. USPM-FrauD outperforms or matches the performance of other approaches that were assessed, consistently displaying good sensitivity across varied circumstances.

c. False Positive Rate for USPM-FrauD

To put it simply, the false positive rates is the proportion of legitimate transactions which is wrongly marked as fraudulent. There were fewer false alarms when the false positive rate was lower.Analysts may assess the model's propensity to generate false alarms by plotting different test scenarios on the x-axis and the proportion of false positive detections on the y-axis. In order to improve the model's specificity in detecting fraudulent activity and reduce the number of false positives, this study is useful.

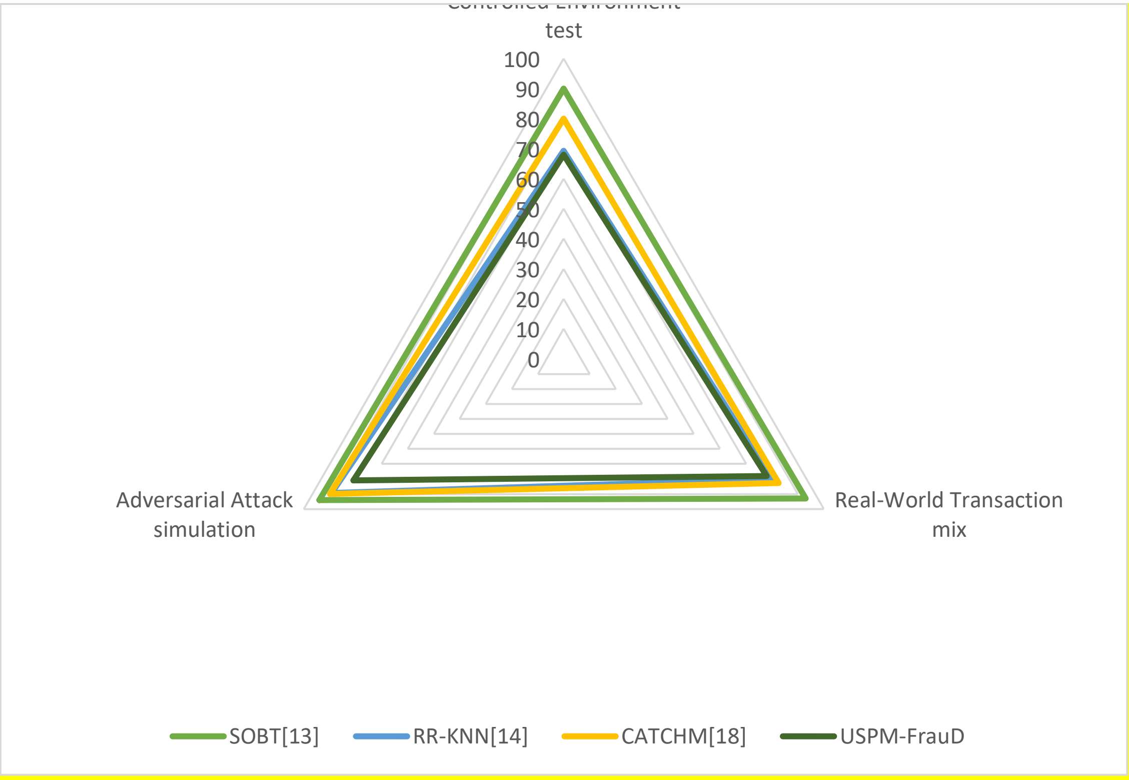

Figure 5: False Positive Rate for USPM-FrauD

In figure 5, To evaluate how well a fraud detection algorithm can avoid falsely identifying legitimate transactions, the false positive rate is an important statistic to consider. The rate in SOBT is greater, in RR-KNN it is lower, and in CATCHM it is lower, although it changes depending on the case. The false positive rates shown by USPM-FrauD are constantly lower; in a controlled environment test, they range from 68% to 78% in a real-world transaction mix. These reduced rates show that the model is good at eliminating needless interventions, keeping users' confidence, and decreasing false alarms for typical transactions.

d. False Negative Rate for USPM-FrauD

The false negative rates is the proportion of fraudulent transactions the model misses. A lower false negative rate indicates greater fraud detection. Research may evaluate the model's fraud detection by plotting test scenarios plotted on the vertical axis and the number of false negatives on the y-axis. This graphic helps highlight places where the model may overlook fraud and directs model adjustments to improve detection.

In figure 6,The false negative rate is an essential statistic that is used to evaluate the capability of a fraud detection model to prevent wrongly identifying transactions that are considered to be normal. The rate changes depending on the circumstance, with SOBT exhibiting a greater rate, RR-KNN displaying a lower rate, and CATCHM displaying a lower rate. During a controlled environment test, USPM-FrauD regularly demonstrates decreased false positive rates, which range from sixty percent to eighty percent when applied to a real-world transaction mix. These decreased rates are evidence that the model is successful in decreasing false alarms for typical transactions, retaining user confidence, and lowering the number of interventions that are not essential.

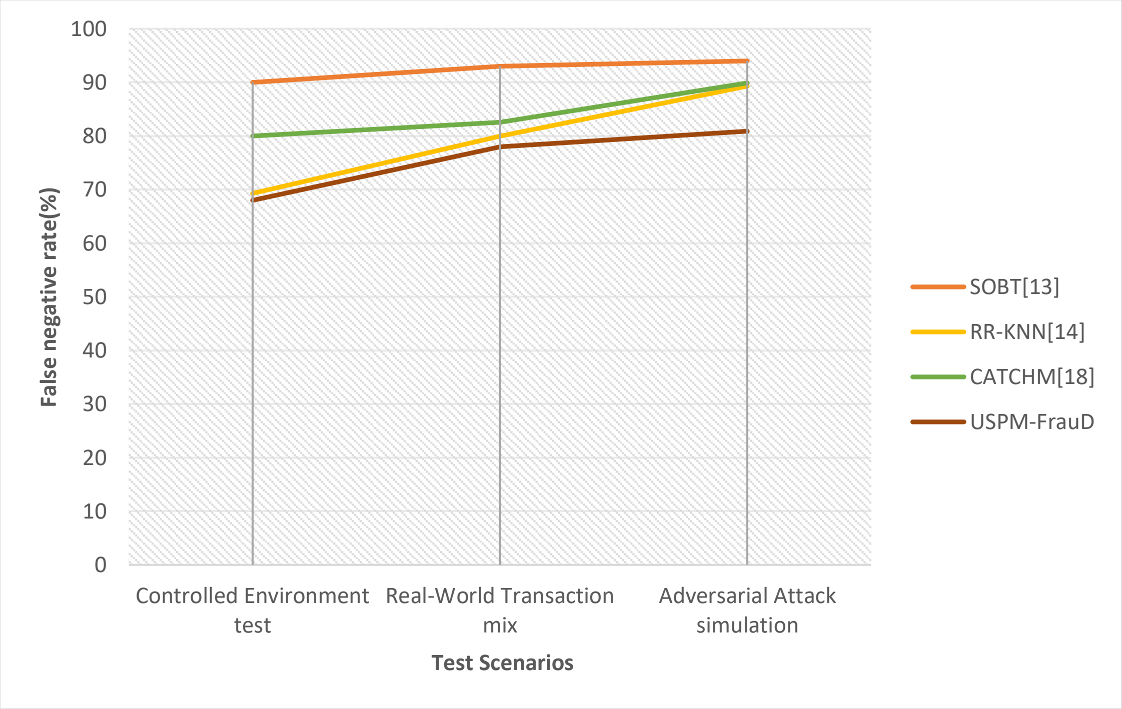

Figure 6: False Negative Rate for USPM-FrauD

5. Conclusion

The assessment metrics of alarm ratio, accuracy of detection, false positive and negative rates provide useful insights into the effectiveness of fraud detection algorithms. These metrics are used to evaluate fraudulent activity. Researchers and practitioners are able to evaluate the model's sensibility, accuracy, false-positive rate, and detection skills over a variety of test scenarios or datasets with the use of these metrics. The evaluation and improvement of fraud detection systems are both significantly aided by the use of these indicators. It is possible that future work may concentrate on improving model creation, real-time monitoring, behavioral analysis, data augmentation, integration of external data, interpretability of models, scalability, and efficiency.Machine learning algorithms, techniques for deep learning, anomaly detection techniques, real-time monitoring, user behavior analysis, data enhancement, other data sources, model interpretability, scalability, and efficiency are all examples of advanced models that might be included. These improvements have the potential to enable the development of systems that are more resilient, precise, and efficient in their ability to prevent financial fraud and enhance security in a variety of fields. Integration of additional data sources, enhancement of model interpretability, and resolving difficulties related to scalability and efficiency might potentially be included in the work that will undergo future development. Researchers and practitioners may make significant strides in the area of fraud detection by concentrating on these future directions. This will result in the development of systems that are more resilient, accurate, and efficient in their fight against financial fraud and in their efforts to improve security in a variety of situations.

REFERENCES

[1]. Hassan, Azeez Olanipekun, et al. "Cybersecurity in banking: a global perspective with a focus on Nigerian Practices." Computer Science & IT Research Journal 5.1 (2024): 41-59.

[2]. Ahmadi, Sina. "Open AI and its Impact on Fraud Detection in Financial Industry." Sina, A.(2023). Open AI and its Impact on Fraud Detection in Financial Industry. Journal of Knowledge Learning and Science Technology ISSN (2023): 2959-6386.

[3]. Patel, Kaushikkumar. "Credit Card Analytics: A Review of Fraud Detection and Risk Assessment Techniques." International Journal of Computer Trends and Technology 71.10 (2023): 69-79.

[4]. Vanini, Paolo, et al. "Online payment fraud: from anomaly detection to risk management." Financial Innovation 9.1 (2023): 1-25.

[5]. Ahmad, Hadeel, et al. "Class balancing framework for credit card fraud detection based on clustering and similarity-based selection (SBS)." International Journal of Information Technology 15.1 (2023): 325-333.

[6]. Esmail, Fahd Sabry, Fahad Kamal Alsheref, and Amal Elsayed Aboutabl. "Review of Loan Fraud Detection Process in the Banking Sector Using Data Mining Techniques." International journal of electrical and computer engineering systems 14.2 (2023): 229-239.

[7]. Xu, Meiling, Yongqiang Fu, and Boping Tian. "An ensemble fraud detection approach for online loans based on application usage patterns." Journal of Intelligent & Fuzzy Systems Preprint (2023): 1-14.

[8]. Bakhtiari, Saeid, Zahra Nasiri, and Javad Vahidi. "Credit card fraud detection using ensemble data mining methods." Multimedia Tools and Applications (2023): 1-19.

[9]. Abd El-Naby, Aya, Ezz El-Din Hemdan, and Ayman El-Sayed. "An efficient fraud detection framework with credit card imbalanced data in financial services." Multimedia Tools and Applications 82.3 (2023): 4139-4160.

[10]. Silva, Matheus Camilo da, et al. "Using Process Mining to Reduce Fraud in Digital Onboarding." FinTech 2.1 (2023): 120-137.

[11]. Singh, Indu, and Rajni Jindal. "Trust factor-based analysis of user behavior using sequential pattern mining for detecting intrusive transactions in databases." The Journal of Supercomputing (2023): 1-33.

[12]. Rangineni, Sandeep, and Divya Marupaka. "Analysis Of Data Engineering For Fraud Detection Using Machine Learning And Artificial Intelligence Technologies." International Research Journal of Modernization in Engineering Technology and Science 5.7 (2023): 2137-2146.

[13]. Ni, Lina, et al. "Fraud feature boosting mechanism and spiral oversampling balancing technique for credit card fraud detection." IEEE Transactions on Computational Social Systems (2023).

[14]. Kannagi, A., et al. "Intelligent mechanical systems and its applications on online fraud detection analysis using pattern recognition K-nearest neighbor algorithm for cloud security applications." Materials Today: Proceedings 81 (2023): 745-749.

[15]. Mytnyk, Bohdan, et al. "Application of Artificial Intelligence for Fraudulent Banking Operations Recognition." Big Data and Cognitive Computing 7.2 (2023): 93.

[16]. Rathor, Ketan, et al. "Intelligent System for ATM Fraud Detection System using C-LSTM Approach." 2023 4th International Conference on Electronics and Sustainable Communication Systems (ICESC). IEEE, 2023.

[17]. Krishna, S. Rama, et al. "Machine Learning based Data Mining for Detection of Credit Card Frauds." 2023 International Conference on Inventive Computation Technologies (ICICT). IEEE, 2023.

[18]. Van Belle, Rafaël, Bart Baesens, and Jochen De Weerdt. "CATCHM: A novel network-based credit card fraud detection method using node representation learning." Decision Support Systems 164 (2023): 113866.

[19]. Cherif, Asma, et al. "Credit card fraud detection in the era of disruptive technologies: A systematic review." Journal of King Saud University-Computer and Information Sciences 35.1 (2023): 145-174.

[20]. Md, Abdul Quadir, et al. "A novel approach to detect fraud in Ethereum transactions using stacking." Expert Systems (2023): e13255.