International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 11 Issue 4 ǁ April 2023 ǁ PP. 459-469

Advance decision support system for detection and prevention of frauds in online banking systems

Sadaf Zuberi
Department of Data Science
University of Europe for Applied Science
Potsdam, Germany
sadaf.zuberi@ue-germany.de

Prashantkumar Mishra
Department of Data Science
University of Europe for Applied Science
Potsdam, Germany
prashantkumar.mishra@ue-germany.de

Girish Vasudev Shetty
Department of Tech &Software
University of Europe for Applied Science
Potsdam, Germany
girishvasudev.shetty@ue-germany.de

Mohammed Nazeh Alimam
Department of Tech & Software
University of Europe for Applied Science
Potsdam, Germany
mohammednazeh.alimam@ue-germany.de

ABSTRACT: *This article describes a decision support system designed to detect and prevent fraud in online banking transactions. The system utilizes an optimization model that takes into consideration a range of metrics, including security, identification, location, and account information to determine whether or not a transaction should be accepted. The three-tier system design boasts a dynamic user interface, cutting-edge IT system, and an efficient operations management. The system uses two types of data processing techniques: Online Analytical Processing (OLAP) and Online Transaction Processing (OLTP). When a transaction is initiated, the OLTP system captures & stores the relevant data and then it is transferred to the Online Analytical Processing (OLAP) system for analysis. Before diving into analysis, the data undergoes a rigorous cleaning and preparation process. This paper applied Random Forest decision tree Model, a supervised machine learning model that is highly efficient in improving the detection of frauds in online banking system and has significant real world impact. The system and data are continuously monitored to ensure proper performance and timely handling of deviations. Discovering the true nature of risks in online banking transactions involves various factors, including security, identity, location, and account-based metrics. The workflow involves extracting data from OLTP systems, cleaning and transforming it, loading it into a data warehouse, integrating it with other data sources and then apply a Machine Learning model for further analysis. The goal of the system is to build a decision support tool that can catch financial crimes before they happen. The system employs cutting-edge optimization models and advanced criteria to thoroughly analyze every aspect of a transaction, ensuring that clients are protected from any potential financial loss.*

Keywords— *Fraud detection & prevention, OLAP & OTLP, Decision Support System, Random Forest Model, Online Banking System*

Date of Submission: 06-04-2023 Date of acceptance: 18-04-2023

I. INTRODUCTION

With the rise of internet & mobile banking, financial institutions face every day new challenges in assuring the security of their client's transactions from cyber criminals. Online banking fraud describes any unauthorized or illegal actions intended to manipulate the online banking system for personal or financial gain. Online banking fraud comes in many different forms, such as phishing, malware, account takeover, identity theft, card skimming, and money mulling.

It is crucial to find fraud in online banking systems to safeguard customers' assets, preserve the

reliability of the banking system, adhere to legal requirements, and stop fraud in the future.

This paper presents a rule-based DSS that employs a three-tier design to detect and prevent fraud. The three tiers are the user, the IT system, and the operation management. The user tier includes the end-users who are authorized to access the system, the IT system tier includes the hardware and software infrastructure that supports the DSS, and the operation management tier includes the decision-makers who are responsible for managing the DSS. The system uses a range of decision-making characteristics such as user demographics, account information, location, and transactional history to identify suspicious behavior patterns and take appropriate actions. By analysing these characteristics, the DSS can prevent potentially fraudulent activities and protect the organization from losses and reputational damage.

Random Forest Algorithm gives better accuracy of results in fraud detection and prevention in online banking transaction. This model works for classification and regression of dataset which are performed by developing combination of decision trees to construct a transaction as fraud or non-fraud. It is highly versatile, can be trained quickly and capable of addressing classification errors that arises from highly imbalanced data in the detection of fraudulent transactions. These performance abilities demonstrated its superiority over other models.

A transaction risk is evaluated using metrics like security, identity, location, and account factors, and a decision is made regarding whether to approve the transaction, rejection or flag it for additional investigation. OTP tries, password resets, and the status of multifactor authentication are all security metrics. Social Security number, address matching, and user age are examples of identity metrics. Location metrics also include red/green alert countries and transaction origin and destination checks. Transaction history, daily transaction totals, threshold amounts, rejected, and suspicious transactions are just a few examples of account metrics. By using these metrics, one can assess the risk involved in a transaction and make wise choices.

The paper proposes a Rule-Based decision support system to prevent online banking fraud. The system uses four categories with equal weightage, and a score of 99.96% is required for a successful transaction. A simulation is designed with a pseudo code to reflect the process flow. This approach allows banks to make informed decisions on approving, rejecting, or flagging a transaction as suspicious based on set criteria. Later an anti-money laundering team investigates suspicious transactions, and an operation manager grants final approval. The system evaluates transaction risk using variables like OTP attempts, password resets, and transaction amounts to reduce fraud and illegal transactions in online banking. Data is processed from OLTP and OLAP data warehouse which further gets through a machine learning RFA algorithm. The system is regularly monitored for compliance and client protection.

Unleashing the power of technology, this decision support systems (DSS) can help banks identify and combat the malicious crime of online fraud. By gathering data, implementing rules-based systems, and monitoring online activity in real-time, DSS empowers banks to detect fraud and prevent it from happening. With user feedback contributing to the mix, banks can not only keep up with legal requirements, but also enhance their ability to stop fraudulent transactions in their tracks.

II. LITERATURE REVIEW

The banking industry shifts towards digitization has sparked a significant rise in digital fraudulent activities. Currently, e- banking fraud is a global issue that has evolved into a thriving industry for cyber criminals who employ sophisticated techniques including denial-of-service attacks, malware, phishing, trojans, viruses, and identity theft study was carried by S. I. Ifitikhar Ahmad [1]. Different studies highlighted the security challenges faced by customers during e-banking operations. Saussalito [2] researched that until now, the combined threats have resulted in a total loss of 6 billion dollars for both clients and organizations.

A study conducted by C.J. Wei et al. [3] over one of the largest Australian bank and its findings indicated that a majority of them possess the following traits and encounter similar difficulties as below

i) Detecting fraud in e-banking system can be a challenging task due to the highly imbalanced nature of the large dataset, with usually millions of transactions and only a few occurrences of fraud on a daily basis.

ii) Real-time fraud detection is necessary in certain online banking transactions to prevent monetary losses.

iii) Online banking security measures are continuously challenged by cyber criminals who constantly enhance their methods to bypass them. Due to complexity and diversity of these attacks, it has become impossible for a simple fraud detection model to effectively protect against them.

iv) The variations in online transaction pose a challenge to identify the fraud activity

Since fraudsters frequently alter their behavior to mimic genuine customer transactions, making it difficult to distinguish between fraudulent and legitimate activity, and stay ahead of advancements in fraud detection. Systematic and structured security models are needed by electronic banking systems to identify authentic users, authorize transactions and ultimately to reduce the fraud risk was proposed by S. M. Emad Abu-Shanab [4]. Various models have been introduced to highlight the fraud activities prevalent among the online banking systems, however a little work was done to provide the preventive measures that means actions are taken only after a fraud has occurred rather than implementation of preventive measures in advance by S. J. R. Peotta et. Al. [5]. The study on fraud prevention explained by H. D. Bolton as to adopt security measures to protect the customers or clients from being hostage by unauthorized online transaction[6].

Multiple decision support systems have been proposed to curb and prevent fraudulent activities. As described by S.Saagari et.al [7] a Decision Support System (DSS) refers to a tool that enhances the decision-making process in complicated systems. It can vary from a basic system that responds to simple inquiries and facilitates a decision to a complex system that utilizes artificial intelligence and offers correlated datasets. Sunil S & L.M.R.J put forwarded a decision support system for internet banking fraud detection and prevention using Hidden Markov Model algorithm using one time password generated by bank server and set to customer mobile via SMS [8]. Another study by Ashwini and Zinjurde introduced a new approach which requires two step authentication using OTP and facial recognition mechanism to make efficient e-banking safer transactions [9].

Current trend of research emphasizes transition of decision support system towards using data warehouse, Machine Leaning and Big Data which are able to provide high quality information, centralized and integrated repository of data, consistent and valid data transformational rules and improved accuracy of decision making by Saagari [7]. Most of the studies are related to find the Credit card fraud in online banking system. The most commonly and successfully applied used Machine learning technique is Supervised Learning Random Forest Model where the best result outputs were achieved in terms of accuracy and coverage but limited to account variables, geographical areas, customer behavior and risk ranges proposed by E. A. &. M. G. Minastireanu [10].

Harjanto highlighted that research trends are shifting towards use of big data and every single online banking data is captured and stored in operational database and big data [11]. One of the most recent approaches in the field is integration of Online Analytical Processing (OLAP), Online Transactional Processing (OLTP), and data warehouse systems to detect fraud in online banking systems.

According to Mathur et. al. [12] data stored in a data warehouse is utilized for strategic choices by combining heterogeneous data from many sources into a single storage location, where it is used for querying and analysis. With technological advancements, business analytics and business intelligence are increasingly being employed in the financial industry for anticipating business choices. Many On-Line Analytical Processing (OLAP) systems that can aid in corporate decision-making are being extensively researched. According to study by Amandeep Kour [13], the data warehouse enables online analytical processing (OLAP), which has very different functional and performance requirements than the online transaction processing (OLTP) applications usually handled by operational databases. Data warehouses provide OLAP capabilities for the interactive study of multidimensional data at various granularities, making efficient data mining possible. Data warehousing and OLAP are critical components of decision support, which has grown in importance in the database business.

Many researchers proposed work based on different machine learning models to detect and prevent frauds in online banking transactions. Fang et. Al [14] introduced a CNN-based approach for identifying fraud, which uses the marked data to recognize the underlying fraudulent patterns. Wang [15]work is based on UCI public dataset using data mining algorithm. Zhang et al [16] research work proposed transaction aggregation strategy by generating a fresh group of characteristics through the application of the von Mises distribution, which involves studying the recurring patterns found in transaction timestamps. Bhusari and Patil [17]used Hidden Markov Model to achieve a high level of protection against fraudulent activity while minimizing the frequency of false alarm. According to Wang , Yu and Ji [14] these methods lack sufficient data and feature processing to create a robust, fast and accurate fraud detection and prevention system for real world examples.

Finally, this research shows that integrating OLTP, OLAP in DSS and applying Random Forest Algorithm for fraud detection in online banking systems, is a promising method. To detect fraud activity in online banking system, the OLAP system analyses historical stored data from data warehouse and OLTP system validates the patterns by analyzing current transaction data. Furthermore, the application of data mining and machine learning techniques significantly improve the accuracy of fraud detection allowing for a more accurate and complete analysis of the transaction data, which is critical for fraud detection and prevention.

III. PROPOSED SYSTEM

The proposed model involves the following steps: data collecting, cleaning, preprocessing, and applying the model to obtain the desired output.

A) System Overview

The initial phase of this study involves the pinpointing of the problem at hand, which necessitates the determination of the paramount objective of the analysis as well as the data that will be harnessed to attain it. The utilization of Online Analytical Processing (OLAP) and Online Transaction Processing (OLTP) databases are employed in the data analysis process, where OLAP is utilized to analyze multidimensional data, and OLTP is utilized for transactional processing. Subsequently, the process of data curation commences, which is accomplished by extracting data from OLTP systems and transferring it to an OLAP system for analysis. Before data can be analyzed, it must go through the process of data purification, which includes the elimination of duplicate or irrelevant data and ensuring that the data is in a format that is easily examinable. Figure 1 shows an overview of the model.

The OLAP system employs a rule-based framework using RFA algorithm to evaluate the data and find trends or deviations. The data is analyzed using a plethora of tools and techniques, such as data visualization, statistical analysis, and machine learning. The final stage of the analysis is to draw conclusions and develop recommendations based on the outcomes of the analysis. This involves determining the potential causes of any deviations discovered and offering suggestions for rectifying them. By comparing the transaction data to the established rules, the machine learning model may detect any departure from the transaction, which can aid in the detection of potential faults or fraud in the transaction. A report is prepared that encapsulates the study's findings and recommendations for correcting any abnormalities that were discovered. The solutions are implemented, and the process is monitored to ensure that the analysis's objectives are satisfied, and the system and data are continuously monitored to verify the rule-based approach

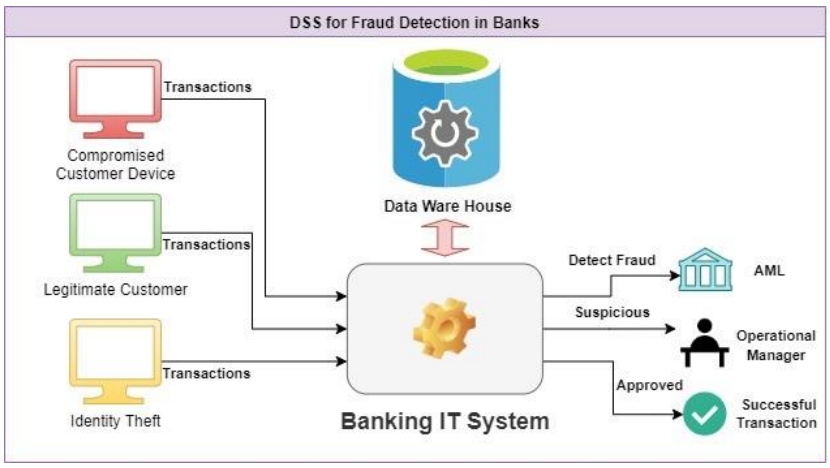

Fig. 1. Overview of model

B) Metrics

The evaluation of a transaction's risk and the determination of its approval require the assessment of various factors such as security, identity, location, and account elements. The security metrics encompass the quantification of One-Time Password (OTP) attempts, the enumeration of password resets, and the status of the multifactor authenticator, whether it is active or inactive. These metrics prove crucial in appraising the security level associated with both the transaction and the user's account. The identity metrics comprise the social

security number or tax number of the receiver, the criteria for matching the billing address to the home address, and the age of the user. The application of these metrics is vital in verifying the identity of the recipient and preventing the occurrence of any fraudulent activities or imposters.

The location metrics encompass the evaluation of the transaction origin and destination, ranging from red alert countries to green countries. Red Alert Countries represent regions that are prone to a high risk of money laundering and fraud activities such as Syria, Iraq, Afghanistan, Nigeria, Cuba, Sudan, and many more, while Green Alert Countries are considered safe and secure countries such as the USA, Australia, European countries, and the like. Additionally, the criteria for matching the billing address to the home address fall within this category. Account metrics involve evaluating the customer's transaction history, the count of daily transactions, the threshold amount, rejected historical transactions, and suspicious historical transactions. These metrics aid in analyzing the customer's account history, account activity, and overall transaction behavior. For instance, setting a maximum of $1000 for a customer who attempts to transfer a large amount of money.

Overall, the metric data can be summarized as below

- **Security**: Count of OTP attempts, count of password resets, status of multifactor authenticator.
- **Identity**: Recipient's social security or tax number, criteria for matching billing address to home address, user age.
- **Location**: Transaction origin and destination criteria, red alert and green alert countries
- **Account**: Total transaction history of the customer, count of transactions per day, threshold amount, rejected historical transactions, suspicious historical transactions

C) Criteria for defining a fraud activity

In an online financial system, fraud can be specified as any deception or misrepresentation made with the intent to proceed with something (e.g., money or access to sensitive information) through unlawful means. To detect and prevent fraudulent activities, a system can use several criteria, such as the number of attempts to enter the one-time password (OTP), the number of password reset attempts, the status of the multifactor authenticator, the provided social security or tax number, the matching of the billing address to the home address, the age of the user, the origin and destination of transactions, transaction history, transaction frequency, the count of suspicious and rejected transactions, and the transaction threshold amount. For example, if the number of OTP attempts exceeds three chances, it may indicate that someone is trying to proceed with unauthorized gain to the account. Similarly, if a transaction originates from a "red zone" country, it might imply that the transaction was carried out by a criminal or terrorist group. By using these criteria, an online financial system can create an increasingly robust and sophisticated fraud detection system that can process and investigate large amounts of data in real time, enabling early detection of fraudulent activities and ultimately reducing the risk of financial losses.

D) Random Forest decision tree model

Random forest decision tree algorithm is best suitable model for the purpose of classification and regression task. The algorithm is simple to understand and flexibility to handle different types of attributes. Ease of implementation and high accuracy are some reasons why this model is selected for the detection and prevention of fraud in online banking.

A variety of tree predictors are combined together to make random forest techniques. In this method, each tree depends on a random & unbiased dataset and every tree in the forest has the same dispersion. The effectiveness of a random forest is defined by the correlation between different trees as well as the confidence of each individual tree. As the tree forest grows, it produces an internal, unbiased estimate of the generalization error.

The workflow of RF model consists of different criteria checked by multiple decision trees. Random datasets are pushed to train the model and based on this training each decision tree provides the likelihood results of a transaction being classified as 'fraudulent' or 'legitimate'. On the basis of all the criteria results, the final prediction is made by using each decision tree result. Different information parameters of a transaction request such as card number, location of the receiver and sender, date, time, IP address, amount, frequency, age are examined by filling all the information in fraud detection algorithm which selects variables from the data that aid in splitting it up. Figure 2 showcase the above mentioned flow.

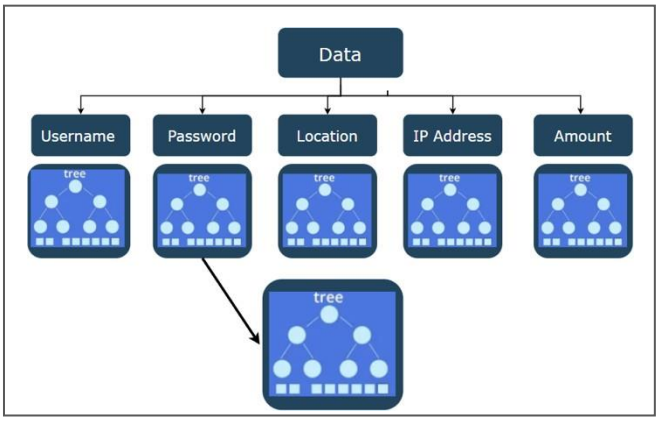

Fig. 2. Random forest model overview

The sub-tress represents variables and corresponding conditions that are set to check a legitimacy of a transaction. After validating all the conditions of the sub trees and combining all the results, the model label the transaction as fraudulent or legitimate.

Below mathematical concept explains about the model where *leftCenter* and *rightCenter* denotes the class 0 & 1 respectively. With help of below computational formulae (1) and (2), *k*th element of center can be calculated

$$leftCenter[k] = \frac{1}{n} \sum I(y=0) \quad (1)$$

$$rightCenter[k] = \frac{1}{n} \sum I(y=1) \quad (2)$$

Where $I(y=0)$ and $I(y=1)$ denotes the dictator functions. Each dataset record is assigned to the corresponding class at the current node based on the Manhattan distance between the record and the center, as shown in formulae (3).

$$dist(center, record) = \sum | center[i] - record[i] | \quad (3)$$

Here *sub* denotes the subset of attributes which are randomly selected from X where size is square root of $m = |X|$

E) Workflow

The online banking system's OLTP system collects and stores massive volumes of transactional data in the data warehouse. This information consists of details such as account numbers, transaction dates, amounts, and places. This data can then be analyzed using online analytical processing (OLAP) to identify patterns and trends that can be used to inform business decisions. The data warehouse stores all historical data from numerous sources, such as account activity, user profiles, and transaction trends. OLAP will utilize fraud detection approaches like rule-based systems to detect any transactions that differ considerably from usual behavior. These transactions are flagged as potential fraud. OLAP can moreover use rules and values, such as those related to suspicious IP addresses, abnormal transaction patterns, and suspicious account profiles, to detect fraudulent transactions. Figure 3 shows the data warehouse design and workflow.

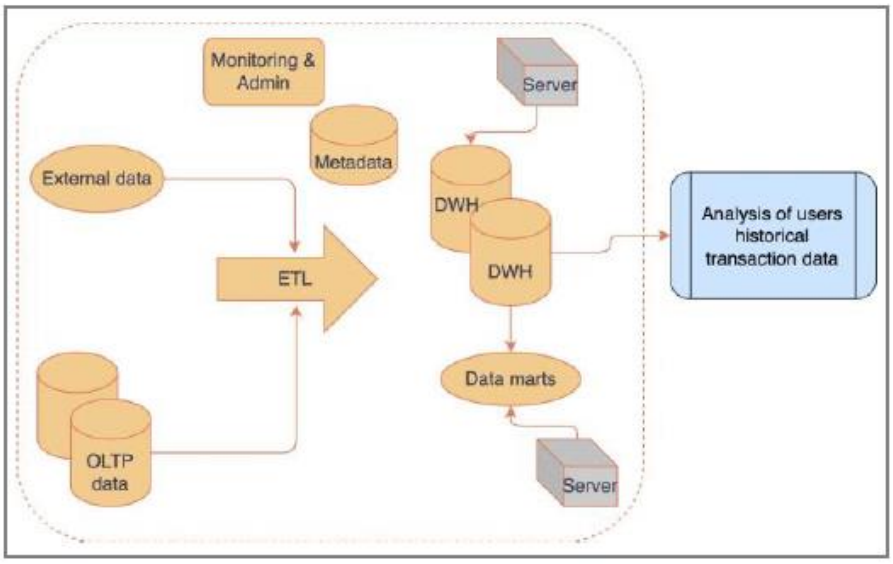

Fig. 3. Datawarehouse workflow

In online financial systems, there are several criteria that can be used to identify and flag potential instances of fraud. One such criterion is the identification of suspicious IP addresses. This can include blocking or flagging any IP address that is known to be associated with fraudulent activity, such as a known hacking group or a known source of spam. Additionally, flagging any IP address that is associated with a high number of failed login attempts or a high number of transactions or account changes in a short period of time can moreover indicate potential fraud. Another criterion for identifying potential fraud is abnormal transaction patterns. This can include flagging any worth that has a high number of small transactions in a short period of time or any worth that has a high number of transactions that deviate from the user's typical behavior. Additionally, flagging any worth that has a high number of transactions from unfamiliar or suspicious locations can moreover indicate potential fraud. Lastly, suspicious account profiles can moreover be a criterion for identifying potential fraud. This can include flagging any account that was created with fake or incomplete information, any worth that has a high number of changes to personal information, or any worth that is associated with a high number of failed login attempts. These criteria can be used in combination with other techniques, such as data analytics, to detect and prevent fraud in online financial systems.

JavaScript programs can be utilized in online financial systems to detect fraudulent transactions using online analytical processing (OLAP) techniques and a rule-based system. The process begins with data extraction and pre-processing. As soon as a transaction is triggered, the JavaScript program extracts other required data from the data warehouse and processes it to remove any irrelevant or indistinguishable information. By applying criteria versus the transaction, unrepealable metrics are generated, and then numbering is washed-up to find the weight versus the predefined metrics. The program then implements a rule-based system to identify the authenticity of the transaction. These rules are based on expert knowledge and are used to detect specific types of events or activities that are considered suspicious or indicative of fraud. The program uses the data in the OLAP and the predefined rules to identify patterns of fraudulent activity. When a match is found, the system triggers an alert or flag to indicate that advance investigation is needed. Finally, based on the results of the fraud detection, the JavaScript program makes decisions about which transactions to flag for advanced investigation. This process helps in providing a secure online financial system and minimizing the risk of fraudulent activities.

If the OLAP system discovers any potentially fraudulent activity, it will flag them and provide information to the investigative team for an advance examination. By examining the customer's prior transactions, location, and other pertinent data points, they can use the OLTP system to retrieve detailed transaction data and personalize the flagged transaction. The OLTP system plays a crucial role in detecting and preventing fraud in online financial systems. It is responsible for recording and tracking individual transactions in real-time, capturing and storing all the necessary data related to the transactional details such as account numbers, dates, amounts, and locations. This data is then fed into a data warehouse where it can be analyzed using Online Analytical

Processing (OLAP) techniques. If the OLAP system detects any potentially fraudulent activity, it will flag these transactions and send them to the investigation team for an advance examination. The investigative team can then use the OLTP system to wangle the detailed transaction data and verify the flagged transaction. They can do this by looking at the customer's previous transactions, location, and other relevant data points to personalize if fraudulent activities have taken place.

The prevention of fraudulent activities is a crucial step in the overall process of detecting and combating fraud. If a flagged transaction is confirmed to be fraudulent, the OLTP system can be used to immediately freeze or flag the worth in question to prevent remoter fraudulent activity. This whoopee is taken to prevent the possibility of the worth stuff being used for spare fraudulent transactions. In wing to freezing or flagging the account, the investigation team can moreover take towardly measures to prevent similar activities from occurring in the future. This can include updating rules, blocking the user, or taking any other towardly measures to ensure the security of the online financial system.

Combining the power of OLTP and OLAP systems allows for an increasingly robust and sophisticated fraud detection system. By processing and analyzing large amounts of data in real time, the system can detect fraudulent activities early on and ultimately reduce the risk of financial losses. This process ensures that an online financial system is protected from potentially fraudulent activities, providing customers with a protected and secure financial experience.

IV. RESULTS & DISCUSSION

To effectively evaluate and process transactions in the system described above, a decision model was developed that considers various metrics such as security, identity, location, and account information. Each of these metrics is assigned a weight to prioritize and determine their relative importance in the decision-making process. The weightage of each metric is set to 25% as it is deemed that each part is important to process a successful transaction. A pseudocode was created to implement this weightage system. The pseudocode defines a method named "getWeight" which accepts a string input named "metricType" and returns the weight prescribed to that specific metric using a switch statement. If the input metricType is not recognized, the method returns a value of 0.

In this way, the decision model can consider the specific weights prescribed to each metric, permitting an increasingly well- judged and efficient evaluation of transactions. This tideway helps to ensure that all important factors are considered and prioritized in the decision-making process, leading to an increasingly reliable and secure system.

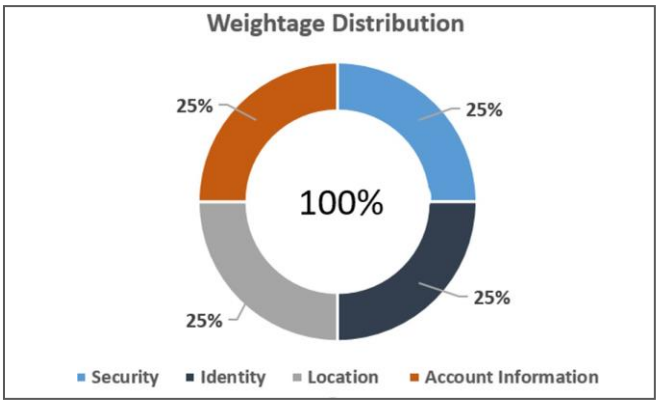

Fig. 4. Weightage of Metrics in percentage

A decision matrix is used to evaluate options and make decisions based on specific criteria. In this case, the matrix is used to determine the outcome of a transaction by analyzing various data points and metrics. The matrix assigns a weight to each metric and calculates a final score, which is then used to determine the overall outcome of the transaction. If the final score is greater than or equal to 99.60, the transaction is considered a "Passed" and is approved. If the final score is greater than or equal to 90 but less than 99.60, the transaction is considered "Suspicious" and requires remoter investigation by an operation manager. If the final score is less than

90, the transaction is considered "Rejected" and is forwarded to the AML team for remoter review. In this case, the consumer will moreover be required to contact the bank. This matrix provides a well-spoken and objective method for evaluating and making decisions based on the data and metrics provided.

The proposed method for detecting fraud in an online banking system involves utilizing a set of factors to calculate a final score for each transaction. These factors include customer name, transaction ID, count of OTP attempts, count of password resets, the status of the multifactor authenticator, instances used by the customer with a social security or tax number, criteria of matching billing address to home address, age of the user, transaction origin and destination, total transaction history of the customer, total count of transaction frequency in a day, and total transaction threshold amount.

A pseudocode for implementing the final score calculation is provided, which includes a function that takes in a point and applies weights to each of the aforementioned factors. The function first initializes the weights for each factor and then checks for certain conditions, such as the number of OTP attempts, password resets, and instances used by the customer being above a certain threshold. If these conditions are met, the function returns a score of 0, indicating potential fraud.

Additionally, the function also includes checks for transaction origin and destination, utilizing a search zone function to determine if the transaction is in a red or green zone. If the transaction is in a red zone, the weight for that factor is set to 0, while if it is in a green zone, it is given a weight of 0.0833. The function also includes checks for transaction history, transaction frequency, and transaction threshold amount, again returning a score of 0 if these conditions are met.

Finally, the function calculates the final score by adding up the weights for each factor and returning this value. The final score can then be used to decide on the transaction, such as whether it is approved, suspicious and requiring further inquiry, or rejected and forwarded to the AML team.

TABLE I. DECISION MATRIX RESULTS

Final Score (%)	**Criteria**	**Decision**
**X > = 99.6	Passed	Approved transaction
X < 90	Rejected	Forward case to AML team
91 < X < 99.6	Suspicious	Operation team contacts customer

**X = Final Score of transaction

Weights refer to the relative importance or influence of different data points or variables in the simulation. These weights may be used to adjust the relative impact of different factors on the simulated outcome. A sample transaction with the following attributes were simulated: customer name, transaction id, security, identity, location, and account information. The weights used in this example are 0.249, 0.16, and 0.249. The simulation resulted in a score calculation, final score, conversion to percentage, criteria, and decision for each transaction. For example, the transaction with customer name Roger, transaction ID 1123589, and weights 0.249, 0.249, 0.249, and 0.249 resulted in a final score of 1, a conversion to a percentage of 99.60%, and a decision of "approved transaction." The transaction with customer name Sarah, transaction ID 1123783, and weights 0.16, 0.16, 0.249, and

0.249 resulted in a final score of 0.82, a conversion to percentage of 82%, and a decision of "forward the case to the AML team and the customer needs to contact the bank." The transaction with customer name John, transaction ID 1023587, and weights 0.249, 0.16, 0.249, and 0.249 resulted in a final score of 0.91, a conversion to a percentage of 91%, and a decision that "the operations manager needs to contact the customer for further inquiry".

Basic measures and Performance measures are described in below table and mathematical formulae. Positive reflects to fraud instances and negative value corresponds to normal instances.

TABLE II. BASIC MEASURES

Predict\Real	**Positive**	**Negative**
Positive	True Positive	False Positive
Negative	False Negative	True Negative

Precision gives an idea about the prediction results while recall rate measures all fraud detection cases. Intervention rate represents the measure of degree of intercept of normal instances.

$$\text{Accuracy} = \frac{TP + TN}{TP + FP + TN + FN} \quad (4)$$

$$\text{Precision} = \frac{TP}{TP + FP} \quad (5)$$

$$\text{Recall} = \frac{TP}{TP + FN} \quad (6)$$

$$F - \text{measure} = \frac{2 \times \text{precision} \times \text{recall}}{\text{precision} + \text{recall}} \quad (7)$$

$$\text{Intervention} = \frac{FP}{TN + FP} \quad (8)$$

V. CONCLUSIONS AND FUTURE WORK

The fundamental driving force behind the research work is to enhance the online banking systems by implementing a mechanism that detects and prevents the suspicious activities. The investigation presents the deployment of an integrated approach employing the techniques of Online Analytical Processing (OLAP) and Online Transaction Processing (OLTP). Now a Machine Learning supervised model known as Random Forest Algorithm applied to data to arrive at conclusive verdicts on the transactional data stored in a data warehouse. The ultimate objective is to make a decision-making model that prioritizes a diverse array of metrics such as security, identity, location, and account information, so as to efficiently and reliably recognize questionable transactions and forestall monetary losses due to fraudulent activity. By realizing this approach, the research strives to make a noteworthy contribution to the advancement of efficacious fraud detection systems for online banking, thereby fostering customer confidence and trust in online banking services.

Various patterns and trends are identified and decoded within the transactional data, the proposed method has the capacity to effectively and accurately detect potential instances of fraud. This method achieves its goal by utilizing established trending Machine Learning technique that can flag potential cases of fraudulent activity. Depending upon the final achieved score, if the result is lower, then it considers as suspicious transaction and send for further investigation. The efficacy and reliability of this decision model are unequivocal, as demonstrated by the simulation results. Overall, the proposed RFA model has undoubtedly achieved its intended objective of enhancing the security of online banking systems. Its success can be attributed to its ability to efficiently and reliably detect and prevent fraudulent undertakings. This feat was accomplished through the integration of advanced techniques that set a precedent for the security of online banking systems in the future.

Looking towards the future work, this model can be applied on different broad financial business sectors like credit card payment, e-commerce transaction, Unified Payment Interface system. Also, further research can be done on using advance data warehousing options like Cloud Based and Big Data. Additional data sources, like social media or device data, could be incorporated to improve fraud detection.

REFERENCES

[1]. S. I. Ifitikhar Ahmad, "A Systematic Literature Review of E-Banking Frauds: Current Scenario and Security Techniques," LINGUISTICA ANTVERPIENSIA, no. 2, p. 3509 – 3517, 2021

[2]. Sausalito, "Cyberwarfare In The C-Suite," Cybercrime Magazine., 2020

[3]. W. L. J. C. L. O. Y. &. C. J. Wei, "Effective detection of sophisticated online banking fraud on extremely imbalanced data.,"

World Wide Web, vol. 16, no. 4, pp. 449-475, 2012

[4]. S. M. Emad Abu-Shanab, "Security and Fraud Issues of E-banking," International Journal of Computer Networks and Applications , vol. 2, no. 4, p. 182, 2015

[5]. L. H. M. D. B. D. F. &. S. J. R. Peotta, "A Formal Classification of Interest Banking Attacks and Vulnerabilities.," International Journal of Computer Science & Information Technology , vol. 3, no. 1, pp. 186-197, 2011

[6]. R. &. H. D. Bolton, "Statistical fraud detection: A review.," Statistical Science, vol. 17, no. 3, pp. 235-255, 2002.

[7]. P. A. C. P. V. S.Saagari, "Data Warehousing, Data Mining, OLAP and OLTP Technologies Are Essential Elements to Support Decision-Making Process in Industries," International Journal of Innovative Technology and Exploring Engineering, vol. 2, no. 6, pp. 88-93, 2013

[8]. L. L. Sunil S Mhamane, "Internet Banking Fraud Detection Using HMM," Third International Conference on Computing, Communication and Networking Technologies, pp. 1-4, 2012.

[9]. V. K. Ashwini. M. Zinjurde, "Credit Card Fraud Detection and Prevention by Face Recognition," International Conference on Smart Innovations in Design, Environment, Management, Planning and Computing (ICSIDEMPC), pp. 86-90, 2020

[10]. E. A. &. M. G. Minastireanu, "An Analysis of the Most Used Machine Learning Algorithms for Online Fraud Detection," Informatica Economica, vol. 23, no. 1, pp. 5-16, 2019

[11]. Harjanto Prabowo, "Learning fraud detection from big data in online banking transactions: A systematic literature review.," Journal of Telecommunication, Electronic and Computer Engineering, vol. 8, no. 3, pp. 127-131, 2016

[12]. Mathur, S., Lal Gupta, S., & Pahwa, P. (2021). Optimizing OLAP Cube for Supporting Business Intelligence and Forecasting in Banking Sector. Journal of Information Technology Management, 13(1), 81-99

[13]. Kour, Amandeep. "Data Warehousing, Data Mining, OLAP and OLTP Technologies Are Indispensable Elements to Support Decision-Making Process in Industrial World." International Journal of Scientific and Research Publications 5.1 (2015): 1-7

[14]. Fang, Y., Zhang, Y., & Huang, C. Credit Card Fraud Detection Based on Machine Learning

[15]. Wang, M., Yu, J., & Ji, Z. (2018). Credit Fraud Risk Detection Based on XGBoost-LR Hybrid Model

[16]. Zhang, Y. , Tong, J. , Wang, Z. , & Gao, F. . (2020). Customer Transaction Fraud Detection Using Xgboost Model. 2020 International Conference on Computer Engineering and Application (ICCEA)

[17]. Bhusari, V., & Patil, S. (2016). Study of hidden markov model in credit card fraudulent detection. In 2016 World Conference on Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave) (pp. 1-4). IEEE