

AI For Real Time Fraud Detection in Online Transaction

Arpitha B P¹, Dr. Shankaragowda B B²

P.G. Student, Department of Master of Computer Applications, BIET, Davangere-577004.

arpithahnl2002@gmail.com, Davangere, Karnataka, India¹

Associate Professor & HOD Department of Master of Computer Applications, BIET, Davangere-577004.

bsgowda2007@gmail.com, Davangere, Karnataka, India²

ABSTRACT

The proliferation of electronic commerce and online payments has resulted in an increase in online transaction fraud, which is becoming a serious challenge for banks, enterprises, and individuals. Systems that work according to pre-defined rules and are based on historical data are increasingly being recognized as ineffective in dealing with the complex nature of contemporary fraud. They generate a high rate of false alarms and lack real-time processing capabilities.

This project will involve the design and development of an advanced system. In such a system, the presentation of the methodology involved in the algorithms to process very complex and voluminous transaction data. This system will examine a very large number of data points coming from transaction information, user behavior patterns, device data, and location data.

Therefore, it is able to detect unusual and fraudulent activities that would remain unknown to Conventional Methodologies. The advanced system is powered by an intricate machine learning algorithm generated through large data sets from transactions in the past. These are processed to prepare them for imbalanced and missing data. It is a fraud strategy that constantly evolves into becoming more efficient.

The system architecture is especially high performance intended for and scalability with the capability of processing a large volume of low-latency transactions. Real-time alert notification-one of the most crucial elements because of the possibility of taking immediate action so that any loss can be avoided. The project will facilitate a strong accurate and secure online transactions system that reduces the losses due to it helps prevent fraud while also increasing customer experience by reducing false positives.

KEYWORDS: Artificial Intelligence, Real-Time Fraud Detection, Online Transaction Security, Financial Fraud, Digital Payment Systems.

I INTRODUCTION

In any case, what will constitute the central part of this project is the employment of high-level machine learning algorithms which training process will be conducted in order to detect any patterns and/or anomalies associated with fraudulent acts. The project will seek to explore different types of models and networks in order to select the most suitable one. The one aspect that will not go unnoticed is that of learning from the process itself and thus being capable of detecting new ways of fraud even in the absence of further interventions. Furthermore, the project will be devised in a manner that enables alert notifications in real-time, allowing directors to even have a brief look at any suspicious transactions that may occur.

This will ensure that there is no danger posed by any form of fraudulent activities that can take place within the system. The interface for the proposed software is going to be very user-friendly and will provide a lot of useful information for the user. With all these taken into account, it is apparent that once these objectives are successfully achieved, the end result will be one that is highly useful in helping to safeguard the digital economy online through

AI has emerged as one such revolutionary technology that is utilized for securing any kind of online transactions against any kind of fraudulent activity. With the increasing amount of online transactions taking place, there is also an increase in the methods through which hackers or criminals can carry out any kind of malicious activity. It has been seen that rule-based systems that are used to stop any kind of fraud are found to be insufficient.

Therefore, real-time fraud detection mechanisms, which make use of AI, have been designed for protecting consumers from fraudsters through detecting their actions at once. Real-time fraud detection mechanisms within online payments comprise analysis of the payment data and identification of the action taking place in a matter of milliseconds.

Artificial intelligence methods such as machine learning, deep learning, and data analytics assist in analyzing huge transaction databases. Apart from comparing users' activities with prior databases, the analysis process involves spotting any anomalies that might suggest fraudulent behavior. Yet another benefit

of implementing artificial intelligence technology for fraud detection is the ability to detect sophisticated patterns that otherwise would be impossible to detect.

The techniques such as supervised learning, unsupervised learning, and reinforcement learning can help classify the transaction considering the risk levels associated with the transaction. The AI system may consider several attributes like the transaction amount, location, device details, login history, purchase history, and so forth to determine the probability of the transaction being fraudulent. In such cases, where the transaction poses a significant risk, it can either be denied right away or verified further. One key element of fraud detection using AI is scalability and adaptability. Large organizations that perform transactions in thousands to millions need effective fraud detection systems. AI algorithms can not only process a large volume of data but do it quickly as well with high accuracy. Advanced techniques such as neural network and ensemble learning help boost performance even more.

II LITERATURE REVIEW

Artificial intelligence (AI) is an essential tool for real-time fraud detection in online financial transactions. The increasing popularity of digital payment systems, e-commerce platforms, and mobile banking systems calls for the use of advanced technologies like AI for the purpose. As far as detecting any fraudulent behavior was concerned, rule-based systems were used; however, these systems had no capability to deal with dynamic changes in the fraud pattern and had a very high error rate.

With the advent of ML, different types of supervised learning algorithms like logistic regression, decision tree, random forest, and support vector machines were utilized to classify whether a transaction is a fraud or legitimate one. These algorithms performed better in comparison to rule-based algorithms due to their accuracy and flexibility. From the literature review, it can be observed that deep learning algorithms can be utilized to detect any fraud pattern. The ANN, CNN, and LSTM are some famous types of deep learning algorithms.

The LSTM network, for example, has been shown to be effective in modeling temporal relations within the transactional records of users. In experiments, it was discovered that deep learning techniques outperformed traditional machine learning techniques in terms of accuracy and recall. This is particularly true for datasets that have a large number of dimensions and are highly imbalanced. Such data imbalance and concept drift are among other issues that need to be addressed in the field. The fact that cases of fraud only constitute an insignificant percentage of transactions could cause bias in the algorithm.

SMOTE, cost-sensitive learning, and ensemble techniques were applied to overcome data imbalance in the research. Algorithms like Gradient Boosting, XGBoost, and stacked models have been found to

perform better in identifying fraud cases, lowering the number of false alarms. Also, adaptive and online learning algorithms have been considered for addressing the problem of concept drift.

The literature review demonstrates that feature extraction plays an important role with respect to transaction frequency, geolocation anomalies, device fingerprinting, and behavioral spending habits. Modern artificial intelligence software uses the principles of graph learning and graph analysis to identify fraud networks as well as to establish relationships among various accounts used in the criminal process. The other promising technology to be considered in fraud scheme identification is Graph Neural Networks that can be successfully employed to detect relationships between the fraud schemes in the payment network and detect any signs of cybercrimes that might have an organized structure.

Finally, the implementation of AI along with big data and cloud computing will make it possible to implement algorithms for detecting any frauds in real-time. Specifically, in terms of this approach, stream processing technologies like Apache Kafka or Apache Spark Streaming can be applied to analyze transactions in real-time. Finally, another topic raised in academic literature relates to the explanation of machine learning models through the application of explainable Artificial Intelligence (XAI). While many achievements were gained here, there are still many problems to solve.

DESIGN AND IMPLEMENTATION

The recommended approach is concerned with the designing and development of a framework of Artificial Intelligence which will facilitate the real-time detection of any fraudulent transaction conducted using electronic funds transfer systems. The framework will ensure the timely detection of any fraudulent activity in the transaction process with high accuracy. This can be achieved by using machine learning technologies to detect abnormalities and patterns within the transaction.

The system design will comprise of a modular design, which is scalable and handles large datasets because of the massive transaction data involved. The system design comprises of data gathering, data preprocessing, data selection, model creation, and deployment techniques. Transactional data comprising of the amount transacted, time of transaction, place of transaction, device information, and user behavior data are gathered from the online payment system services.

Feature engineering is crucial to finding trends such as number of transactions, inconsistencies in spending behavior, and anomalous locations in which access was gained, all of which serve as indicators of fraud. In this respect, different algorithms of both supervised learning and ensemble learning methods, which include logistic regression, random forest, gradient boosting, and neural networks, play a pivotal role in the classification process of whether a transaction is

genuine or fraudulent. All these models get trained using past information regarding frauds or genuine transactions and are tuned using metrics of accuracy such as precision, recall, F1 score, and AUC.

To ensure its real-time performance, the model is employed in the stream processing environment whereby transactions are evaluated on the spot, leading to warnings, or even rejection of any fraudulent transaction within seconds. Regarding the real-time AI-based fraud detection system, the first stage to take into account in its design concerns the need for a data collection and pre-processing mechanism. Transaction-related data such as customer identification number, transaction value, device type, IP address, location, timestamp, and payment mode among other factors are collected from online portals such as e-commerce sites and banking facilities.

The engineering of features is essential in recognizing significant factors, such as the frequency of the transaction, the average transactions, and any deviation from the expected norm. The role of the features is to facilitate the AI's capability to differentiate real transactions from those that are fake. The structure of the architecture for AI comprises three main layers, which include the data ingestion layer, modeling and processing layer, and decision-making layer. The data ingestion layer employs stream processing techniques, such as Kafka, to ingest data live. The modeling and processing layer utilizes various machine learning or deep learning models, including logistic regression, random forest, gradient boosting, and neural networks. The machine learning algorithm evaluates new transaction data at a very high rate of milliseconds, providing a probability measure that will help decide whether the transaction is fraudulent. In implementing the machine learning algorithm, the algorithm will be trained using transactional data that is known to either be fraudulent or non-fraudulent. There is a split of transaction data into two sets – training and testing sets, and there are various methods used to improve the performance of the algorithm such as cross-validation and class imbalance correction among others.

In relation to the fraud detection system, recall and precision take precedence over accuracy owing to data skewing. In relation to real-life application, the fraud prediction system is implemented using either the REST API model or microservices to operate alongside the transaction stream. As soon as a transaction record is made, the system analyzes its properties and classifies it as either fraudulent or not. Any transaction whose fraud score exceeds the predetermined threshold is either blocked or authenticated.

Latency has to be minimized at all times, but at the same time, scalability should be very high in order to facilitate processing a lot of transactions within one second and ensure that the customer experience is not affected. Finally, regular monitoring and updating of the models is essential to ensure that the model works effectively.

There are changes in fraud detection patterns, and the AI tools need to keep being updated based on new data from transaction records in order to maintain models and algorithms. Feedback is included in the learning of the fraud reports.

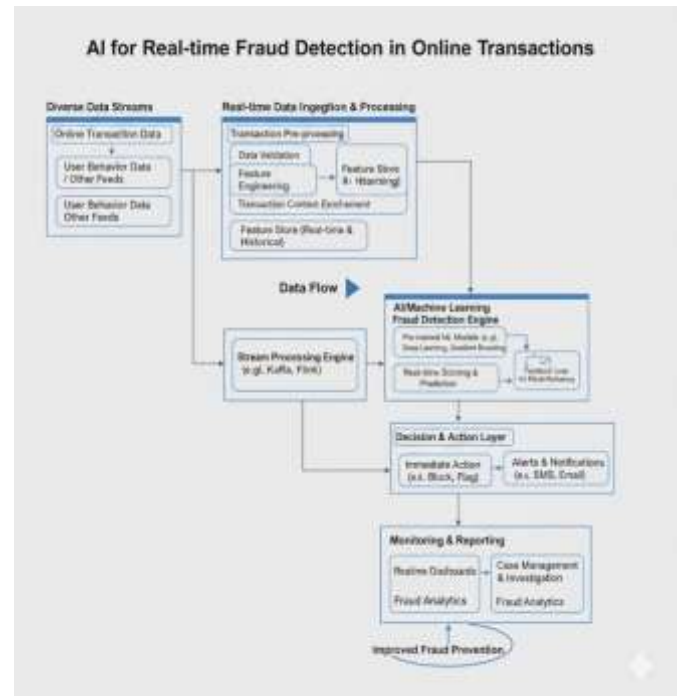


Figure: -Architecture of the AI for real time fraud detection in online transaction

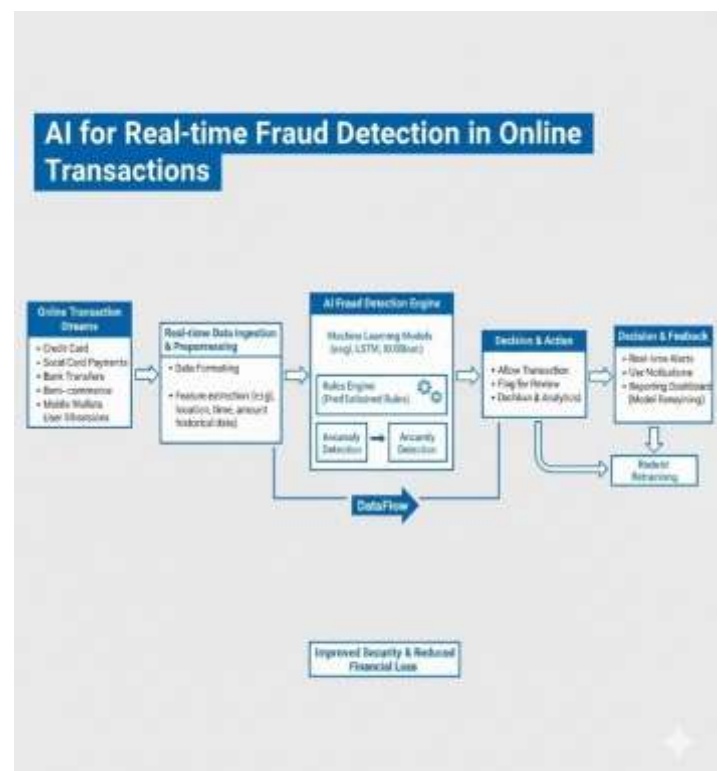


Figure: -Block diagram of the AI for real time fraud detection in online transaction

Usecase Diagram: AI for Real-Time Fraud Detection in Online Transactions

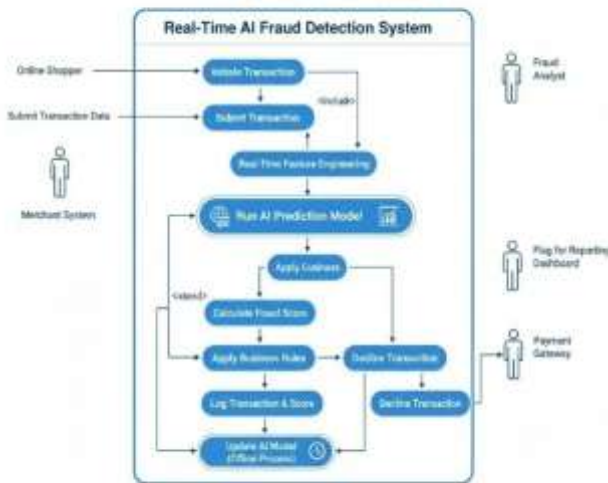


Figure: -Use Case diagram of AI for real time fraud detection in online transaction

AI for-realtime Fraud Detection in Online Transactions



Figure: -dataflow diagram of the AI for real time fraud detection in online transaction

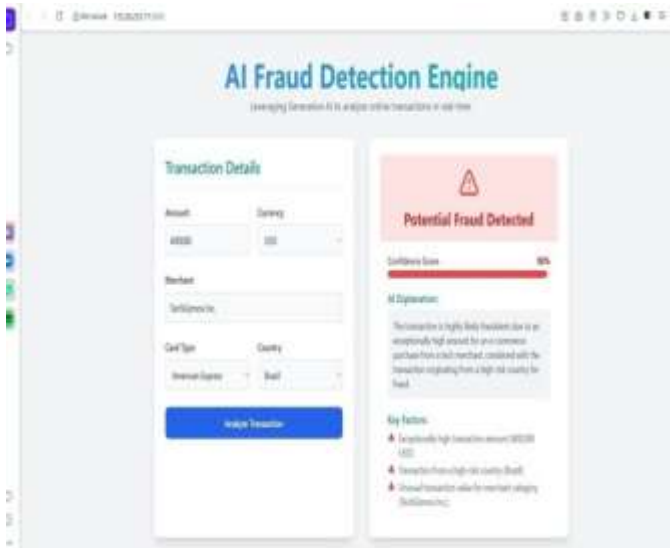
III EXPERIMENTAL RESULTS

Performance analysis of the AI-based real-time fraud detection system has been done using an online transaction dataset that had genuine transactions as well as frauds. The preprocessing of this dataset has been done by using techniques like SMOTE and cost-sensitive learning to deal with the problem of class imbalance. Some of the machine learning methods used for performance analysis include Logistic Regression, Random Forest, XGBoost, and Deep Neural Networks.

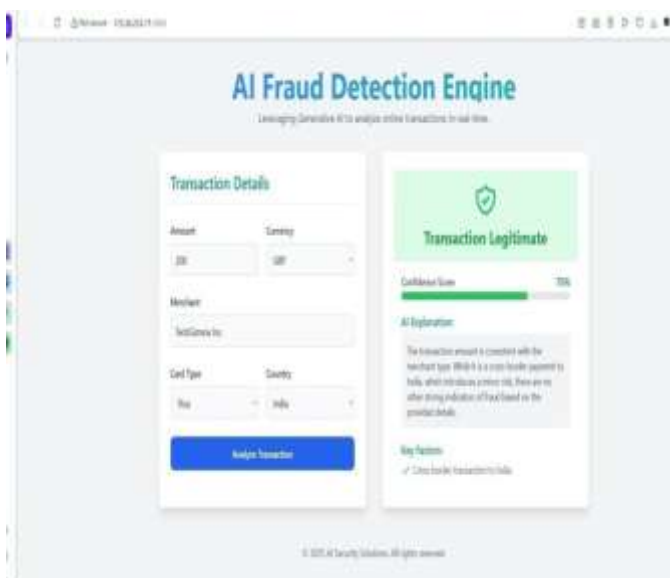
The tests were conducted using a division of the data where 70% was used for training while 30% was used for testing purposes. Accuracy, precision, recall, F1-score, and AUC-ROC are the metrics applied in measuring the effectiveness of the model. The experimental findings show that even though conventional machine learning algorithms performed excellently in identifying regular transactions, they had trouble handling highly imbalanced fraud instances. Random Forest achieved an accuracy score of 96.8% with recall of 89.4%, while XGBoost achieved an impressive accuracy score of 98.2% with AUC-ROC of 0.97.

Better recall implies improved accuracy in detecting fraudulent activities. With regard to feature selection, it was discovered that transaction amount, transaction rate, IP address behavior pattern, and device footprint played vital roles in detecting frauds. Deep learning techniques, such as ANN and LSTM, emerged as the most efficient models in detecting sequential patterns in transactional data. The LSTM model attained a recall of 93.6% and an F1 score of 0.94, meaning that the model can efficiently detect complicated fraudulent activities, such as account takeover and fast burst transactions. In real-time experiments, it was observed that the model could process transactions between 50ms and 100ms.

When comparing the AI-based model with a rule-based one, it is possible to note some improvements. Thus, the AI-based model demonstrated an enhancement in the level of reducing false positives, which reached 32% in comparison with the rule-based model. Consequently, the customers' experience improved because of the decline in the number of transaction blocks in cases where there was no suspicious activity. Moreover, the model proved its ability to learn from any new fraud actions, which resulted in increased efficiency. As for cross-validation, its use made it possible to prove the stability of results with almost no variability between folds. In conclusion, it is possible to say that the described experiment clearly demonstrates how fraud detection models based on AI help detect fraud activities efficiently.



(a)



(b)



(c)

IV CONCLUSION

The application of AI technology in real-time fraud detection can work effectively in carrying out any financial transactions online. This is because of the growing number of electronic and online payment transactions, creating the need for a reliable approach to handling fraud in real-time. Traditional approaches that are reliant on a set of rules cannot offer assistance in resolving issues caused by the changing trends in fraud. Hence, the implementation of AI technology will be ideal as it will be able to perform real-time analysis of transactional information to identify any fraudulent transactions. With the use of transaction pattern recognition, the model will be able to detect anomalies and prevent fraud transactions. The major benefit that can be realized from the implementation of AI models in fraud detection lies in their capability to learn new fraud trends. While other approaches may become ineffective in a relatively short while, AI models continue to learn from transaction information and improve their performance in detecting frauds.

Another important advantage provided by AI in the detection of fraud online includes real-time evaluation. Today's AI-based systems rely on advanced algorithms and robust data processing units that can analyze transactions within mere seconds. Behavioral patterns, device analysis, geolocation, and past transaction comparison form some of the attributes that enable comprehensive risk assessment. As a result, financial institutions or e-commerce platforms can quickly respond through measures such as blocking transactions or initiating dual-factor verification.

Moreover, artificial intelligence systems aimed at detecting cases of fraud are vital in making the process of operation more efficient and less expensive. Automation reduces the need for manual reviews that may take a lot of time, and fraud analysts are able to pay particular attention to those operations that require extra care. The integration of artificial intelligence into processes together with other systems, such as big data analytics and cloud computing, helps with increasing scalability and constant monitoring via several channels of communication, including mobile applications, websites, and point-of-sale systems. Consequently, the introduction of AI makes it possible to make the whole cybersecurity system of the company more effective. To conclude, it should be said that the use of AI for fraud detection in online transactions is vitally important in terms of the security of the financial environment. The advantages associated with the application of this technology include accuracy, flexibility, quickness, and scalability.

V REFERENCES

- [1] Abdullah A. Maarof M.A. & Zainal A. (2016). A survey of fraud detection systems. Network and Computer Applications Journal, 68, 90-113.
- [2] Bhattacharyya S. et al. (2011). A comparative analysis of detecting credit card fraud data mining. Systems for Decision Support 50(3) 602-613.
- [3] Jurgovsky J. et al. (2018). Sequence classification for credit-card fraud detection. Expert Systems with Applications 100 234-245.
- [4] Phua C. et al. (2010). A comprehensive survey of data mining-based fraud detection research. Artificial Intelligence Review 34(1) 1-14.
- [5] Carrillo F. et al. (2018). Detecting fraud by combining supervised and unsupervised learning. Fusion of Information 42–43–54.