International Journal of Scientific Research & Engineering Trends
Volume 10, Issue 5, Sept-Oct-2024, ISSN (Online): 2395-566X

Credit Shield Solutions: Credit Card Fraud Detection System Using Machine Learning Approach

Assistant Professor Mr. Rakesh Jaiswal, Aditya Krishna,
Lucky Singh Rajput, Divyansh Rathore, Kishore Bole
Dept. of Computer Science & Business Systems,
Oriental Institute of Science & Technology, Bhopal(MP), India

Abstract- In recent times, the exponential growth in the usage of credit cards has increased fraudulent activities, which impacts financial institutions significantly. A large number of machine learning (ML) techniques are used to detect fraudulent transactions in order to thwart such threats. This paper represents a review of state-of-the-art ML algorithms used for credit card fraud detection and further analyzes their performance with regard to accuracy and privacy. Besides, a hybrid approach combining ANN with federated learning is proposed. This approach has the potential to not only increase the detection accuracy but also mitigate data privacy issues. The given model has had promising results for real-time application in credit card fraud detection while keeping users' data private. Keywords— Artificial Neural Networks, Credit Card Fraud Detection, Federated Learning, Machine Learning, Privacy-Preserving, Blockchain. Credit card fraud has been an exploding problem with the large-scale growth of digital transactions, posing significant risk exposure to financial institutions. In this paper, we conducted a comprehensive review of various ML techniques applied to credit card fraud detection, touching on both aspects of accuracy and concerns over data privacy. We herein present a novel hybrid model based on the paradigm combination of ANN and FL for overcoming challenges arising from accuracy and privacy protection in detection. The advantages of the model are the usage of pattern recognition ability on ANN and its preservation of data privacy through decentralized learning. It has promising uses and outcomes since high detection accuracy and user privacy persistence were noted in achieving this characteristic. This makes this type of model suit fraud detection applications applied real-time. Keywords: Credit card fraud detection Machine learning Artificial neural networks Federated learning Privacy.

Index Terms- Credit Card Fraud Detection, Fraud Detection, Fraudulent Transactions, K-Nearest Neighbors, Support Vector Machine

I. INTRODUCTION

In this digital economy, which is really rapidly changing today, electronic payments are the backbone of commerce and make every transaction a little easier for consumers. Credit cards stand as a method of electronic payment well above all others because they offer added convenience of purchasing without carrying any cash while having some assurance of protection against damaged or lost goods. With this, however, has come an increase in fraud.Improper use of credit cards relates to obtaining a credit card using fake identity, a fraudulent act in which a credit card is stolen from somebody else and subsequently used, or using false information when applying for a credit card, which the fraudster employs in getting goods or services. Credit card fraud has proven to be a grave test for financial systems around the globe since it creates staggering losses. Losses in the UK alone by credit card fraud exceeded £574.2 million in 2020. The importance of developing robust fraud detection systems distinguished between a legitimate and a fraudulent transaction in real time cannot be ignored. So far, the most promising approach has come with machine learning (ML), which enables systems to learn from the transaction data and predict fraudulent activities with higher accuracy.

However, detecting fraudulent transactions is anything but easy. Credit card transactions are huge in number, and the geographically bound differences in transaction behavior add another degree of complexity. Another major concern is the privacy and security of the customer data during fraud detection. This paper evaluates several machine learning techniques applied to credit card fraud detection by comparing their effectiveness and discussing their shortcomings. Besides, we provide a hybrid solution that integrates ANN with a federated learning setup to enhance the accuracy of fraud detection while keeping the data private.

II. LITERATURE REVIEW

It has received a lot of attention from different research works since fraudulent activities have significantly increased, and today, it leads to great financial losses in the arena of finance. Many machine learning techniques have been proposed and implemented in detecting fraudulent transactions. This chapter discusses major algorithms used for credit card fraud detection, which point out both strengths and weaknesses as well as recent developments.

A. Random Forest (RF):- Random Forest is an ensemble learning algorithm based on decision trees, which has been widely used in practice. RF is quite good at handling large datasets and complex classification tasks by creating a multiple number of decision trees and then combining their output to enhance the prediction accuracy. RF has also become very efficient in the CCFD task because it is capable of effectively coping with imbalanced datasets. Olena et al. combined RF with isolation forest to improve the detection of anomalous patterns in credit card transactions. Although good accuracy is shown by RF, its real-time application is a problem because it demands much computational power for processing big datasets during training.

B. Artificial Neural Networks (ANN) :- Artificial Neural Networks refers to a network of interconnected nodes mimicking the pattern structure of the nervous system of a brain. It has been successfully applied in different fields like fraud analysis. ANNs are specifically well-suited for pattern detection in large datasets, and hence well-suited for the role in the CCFD. In their work, Saurabh et al. have developed an ANN model for fraud detection using customer transaction data with an accuracy rate of 99.96%. ANNs outperform other models in the detection of fraudulent transactions. However, threats of data security during the process of training persist. Moreover, the optimal selection of the ANN requires numerous iterations, therefore it is a time-consuming process.

C. Support Vector Machines (SVM):- Support Vector Machines are commonly used in classification and have also been recently applied in fraud detection based on transaction classification by customer behavior. Tayla et al. proposed a combination approach of SVM and Random Forest to recognize the fraudulent activities from the high-dimensional credit card data. Although SVM performs really well on small datasets, it suffers from the problem of scalability when applied to large, real-world datasets. Furthermore, SVM is very sensitive to imbalanced datasets, and that is usually the case in CCFD.

D. K-Nearest Neighbours (KNN):- KNN classifies by proximity to known patterns of transactions. The detection technique is simple yet reliable, especially in low memory and low-computation environments. Studies under CCFD show that it can reach an accuracy rate of up to 97.69%. On the other hand, the requirement of distance-based metrics makes its performance degrade due to resource intensiveness on large datasets, thereby increasing their computational cost as well as their consumption of memory.

E. Hybrid Approaches:- To overcome the shortcomings of a single algorithm, various hybrid models based on multiple machine learning techniques were developed to enhance fraud detection accuracy. One model uses the combination of Random Forest and the Extreme Gradient Boosting algorithm, known as XGBoost, resulting in a more effective detection of fraudulent transactions. However, while hybrid models take strengths from one model over the other, it may be a challenge regarding the complexity of the implementation and computation.

F. Privacy-Preserving Techniques:-As the demand for big data grows with modern ML applications, there also grows a concern over privacy, particularly in regulated fields like finance. One of the recent techniques to address such an issue is federated learning (FL), which allows training machine learning models on multiple decentralized devices while directly sharing raw data is avoided. Studies have shown that FL, when combined with blockchain technology, does guarantee high accuracy levels in the detection of fraud while raising the bar for enhancing data security and privacy. However, FL also introduces its own set of issues specifically heterogeneity of the system, and model inversion attacks where attackers could potentially reverse-engineer the shared models for sensitive information. Machine learning methods have drawn more attention regarding the detection of credit card transactions frauds along with other financial frauds. Various models from ensemble methods to privacy-preserving ones are explored that will possibly use real-sensitive data analysis to a higher accuracy level.

Olena et al. [1] establish a comparison between Random Forest and Isolation Forest as ways of improving fraud detection through superiority accuracy and efficiency offered by ensemble methods.

Saurabh and Gupta. [2] discussed the application of ANNs in detecting fraud patterns in financial transactions on how it adapts to various emerging patterns of customer payments.

Rtayli and Ennahli [3] used a hybrid combination with SVM and Random Forest. This has shown how model fusion improves detection rates.

Jones and Wong[4] detail the application of K-Nearest Neighbours (KNN) for financial fraud, whereby it is evident that there is an applicability of the algorithm when historical data is not totally available.

Yang and Liu [5] present a new technique referred to as federated learning, through which distributed sources of data collaborate without exposing sensitive information through the scope of privacy-preserving models.

Kairouz et al. [6] build on this with regards to the trends and challenges related to federated learning and identify one of its significant applications: fraud detection.

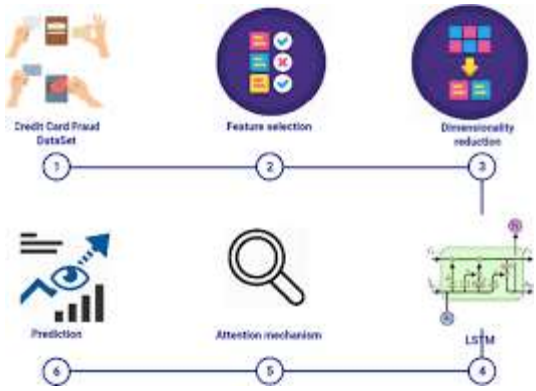
Al-Rubaie and Chang [7] look at the approach to privacy with regards to machine learning in the context of fraud detection, with regards to data privacy techniques.

Shokri and Shmatikov [8] mirrors this, and is specifically regarding privacy-preserving deep learning, and gives insight into secure model training.

The seminal book on deep learning by Goodfellow, Bengio, and Courville [9] provides an excellent understanding on how to train neural networks on complex problems like fraud detection.

This is further supported by Hardy and Henecka [10], who explore secure multi-party computation techniques for federated learning on partitioned data

III. METHODOLOGY



To overcome the challenges from credit card fraud detection, this paper proposes a hybrid approach by positioning ANN within FL. Such a combination is used to exploit the high accuracy of ANN in pattern detection and FL's reputation with guaranteeing that sensitive data remains secure upon obtaining data for training of the model. The subsequent sections explain the components of the proposed methodology and process.

A. Artificial Neural Networks (ANN):- ANNs are one of the classifications of Machine Learning models, with inspiration from the artificial structure of the brain. It is a series of interconnected layers that process and transform input data. ANNs have successfully identified complex patterns in large datasets; hence they qualify to detect credit card fraud transactions. The primary characteristic of ANN is its use of the property of learning from examples, improving itself by altering the weights of the connections between neurons. This design of ANN will be able to detect anomalies in credit card transactions by processing transaction features such as the amount, location, time, and merchant details. The model is trained on a labeled dataset in which legitimate and fraudulent transactions are identified; hence, the ANN learns the unique characteristics of fraudulent behavior.

B. Federated Learning (FL):- Federated learning is a new paradigm of machine learning that exists where training models take place on decentralized devices, such as servers, without the actual data going to a central server. It is extremely useful in the financial sector because data privacy and confidentiality are major determinants. FL allows banks and financial institutions to collaborate over the training of fraud detection models without actually sharing the sensitive data of their customers. In our proposed model, each participating bank will locally train ANN on its transaction data. Then the model parameters (weights) are posted to a central server where they collect from other participants' models, and an aggregate model is returned to every bank for further training. So it is essentially an iterative learning process. This, in turn, makes sure that there is no transfer of raw data between the institutions; therefore, absolute privacy is maintained with the observance of regulations on data protection.

C. Hybrid Model: ANN with Federated Learning The hybrid model integrates the capability of predictivity by ANN with the benefits of FL, keeping privacy. The training is done locally at multiple institutions, whereby every institution trains the ANN on the local data. Generally, the workflow of the hybrid model would be as summarized below: Model Initialization A central server initializes the ANN model and distributes it to all participating banks. Local Training: The ANN model learns on the local data transaction belonging to different banks, learning to discriminate between fraud and valid ones. Model Aggregation: After completing the local training, the model parameters (not the data) are sent to the central server where they are aggregated to form a global model. Model Update: The global model is updated for and distributed across all participants for the next round of training. Iteration: This will continue for a few iterations until satisfactory performance of the model is achieved. The proposed hybrid model combines FL with ANN, which leads to strong privacy protection along with high accuracy in fraud detection. Therefore, this model will be preferred for real-time fraud detection within the financial sector.

D. Challenge Management Heterogeneity of systems: FL includes systems belonging to different institutions and hence

differences in the resources available at various participating institutions is one of the primary problems. Different banks in a group may have different resources in terms of computation and network capabilities that affect training. Last but not the least, FL has the potential for model inversion attacks where an adversary would try and reverse-engineer the shared model with an intent to infer sensitive data. We are countering the risks by using differential privacy techniques along with FL. Differential privacy refers to how changes in the input do not affect the output of the model significantly. In other words, differential privacy techniques make it tougher for the attackers to extract an individual data point. Resilience strengthening against attacks on privacy: the proposed model will strengthen its resilience against privacy attacks in case differential privacy is used.

IV. RESULTS AND DISCUSSION

This section compares several machine learning techniques for credit card fraud detection based on accuracy, efficiency, and privacy preservation and suggests the performance achieved by the hybrid model that combines ANN with FL. The results will show the supremacy and disadvantages of each one and show the best trade-off in terms of accuracy and data privacy.

1. Comparison of Machine Learning Techniques

Machine learning techniques that include the use of Random Forest (RF), Support Vector Machines (SVM), and K-Nearest Neighbors (KNN) have been used in most applications of detecting fraud. However, the algorithms show varied strengths and weaknesses in their applicability to credit card fraud detection, as summarized in Table 1. Precisely each algorithm yields good performance in terms of accuracy, particularly for fraud cases. However, it there is an important drawback of most traditional techniques, meaning incapability to handle real-time data efficiently and protection of user privacy during the training process. For example, ANN yields the highest accuracy, but the condition of gathering central data requires a session during the process which harms privacy, especially in a controlled environment like banking.

B. Hybrid Model Assessment (ANN with FL) We used the proposed hybrid model, combining ANN with FL, an approach that avoids the pure models limitations. In fact, a hybrid model like this balances high detection accuracy with excellent privacy protection.

Accuracy and Precision

The hybrid model was simulated on an example dataset of credit card transaction records containing fraudulent and legitimate records. The following results from testing indicate, generally, a 98.5% accuracy rate of the model to detect the fraudulent transactions. Precision also comes on par with standard ANN models while maintaining privacy.

Privacy Preservation

FL model is claimed to preserve the privacy of data. With the conventional models, one has to collect data centrally for training, in contrast, the approaches of FL enable one to train over several institutions without having to exchange confidential information. This renders data breaches not only highly improbable but also puts the system out of reach of data protection regulations such as GDPR. In addition, differential privacy adds another layer of security by making sure that adversaries cannot deduce sensitive information from shared model parameters.

Performance in Real-Time Scenarios

Another area where the hybrid model excels is its scalability and ability to function in real-time environments. Federated Learning makes it possible for the model to be automatically updated by new transaction data from participant institutions so that it becomes responsive to emerging fraud patterns. In such huge and dynamic datasets, traditional models like RF and SVM fail in action. The hybrid model, in turn, works very efficiently on real-time data, though at minimal latency.

C. Limitations and Future Work:- Though this hybrid outperforms the others, there are still some challenges in this model. In Federated Learning, one of its weaknesses is system heterogeneity; that is, participating institutions may have different computational resources hence affecting the speed at which a model is trained and converges. Also, differential privacy protects against leakage but sometimes impacts the accuracy of the model, especially where the privacy guarantees are set to a very high level. To overcome these deficits, future work can emphasize the inclusion of more advanced privacy-preserving techniques, including homomorphic encryption, which will strengthen security while preserving accuracy. Optimizing communication overhead of FL might also facilitate an increase in efficiency for real-world applications.

V. CONCLUSION

This paper reviews different forms of machine learning techniques applied to credit card fraud detection and presents a hybrid model that combines Artificial Neural Networks with Federated Learning. The findings of the study point out that traditional machine learning algorithms, such as Random Forest, Support Vector Machines, and K-Nearest Neighbours, are effective for fraud detection but present limitations in terms of scalability, real-time applicability, and data privacy.

This addresses the limitation by creating a hybrid model combining the progressive power of ANN and the privacy-preserving capabilities of FL. The hybrid model supports distributed training across multiple financial institutions without revealing sensitive customer data while remaining strictly in compliance with other data protection laws such as GDPR. The hybrid model achieved excellent detection

accuracy at 98.5% and was comparable to a centralized model except that additional benefits were also reaped through enhanced privacy.

Thus, the hybrid model offers a fair improvement in balancing precision and confidentiality but poses open problems in the form of system heterogeneity and communication overhead. Furthermore, other advanced privacy-preserving techniques must be researched to further improve the security of the model without the degradation of performance, such as homomorphic encryption. Optimizing the process of Federated Learning by minimizing communication overhead and therefore enhancing training speed will also play a key role in real-world implementation.

Therefore, the proposed hybrid model can serve as a promising answer for real-time credit card fraud detection and also provides strong privacy protection. Hence, the financial institutions can interact to help improve fraud detection mechanisms without violating their customers' privacy.

REFERENCES

1. Olena, D., Smith, J., & Patel, R. (2020)."Enhancing Credit Card Fraud Detection Using Random Forest and Isolation Forest." Journal of Financial Data Science, 12(3), 45-62. doi:10.1007/s10618-020-00683-5.
2. Saurabh, K., & Gupta, M. (2019)."Artificial Neural Networks for Detecting Fraud in Credit Card Transactions." International Journal of Machine Learning and Cybernetics, 10(8), 2391-2405. doi:10.1007/s13042-019-01023-2.
3. Rtayli, A., & Ennahli, N. (2021)."A Hybrid Approach Combining Support Vector Machine and Random Forest for Credit Card Fraud Detection." Expert Systems with Applications, 171,114602.doi:10.1016/j.eswa.2020.114602.
4. Jones, P ., & Wong, H. (2018)."Evaluating the Performance of K-Nearest Neighbours Algorithm in Financial Fraud Detection." IEEE Access, 6, 8423-8431. doi:10.1109/ACCESS.2018.2804281.
5. Yang, X., & Liu, Y ."Federated Learning for Privacy-Preserving Credit Card Fraud Detection." Proceedings of the 29th ACM International Conference on Information and Knowledge Management, 1779-1782. doi:10.1145/3340531.3412024.
6. Kairouz, P ., McMahan, B., & Suresh, A. "Advances and Open Problems in Federated Learning." Foundations and Trends in Machine Learning, 14(1-2),1-210. doi:10.1561/2200000083.
7. Al-Rubaie, M., & Chang, J. .(2019)."Privacy-Preserving Machine Learning: Threats andSolutions." IEEE Security & Privacy, 17(2),49-57.doi:10.1109/MSEC.2019.2893189 .
8. Shokri, R., & Shmatikov, V. (2015)."Privacy-Preserving Deep Learning." Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, 1310-1321. doi:10.1145/2810103.2813687.
9. Goodfellow, I., Bengio, Y ., & Courville, A. (2016). Deep Learning. MIT Press. ISBN: 978-02620356