Journal of Neonatal Surgery
ISSN(Online): 2226-0439
Vol. 14, Issue 5 (2025)
https://www.jneonatalsurg.com

Intelligent Fraud Detection in IoT-Driven Transactions Using Multi-Layer Neural Classification

Mr. Madhu Bandari[1], P. Pavan Kumar[2]

[1]Research Scholar, Department of CSE, Faculty of Science and Technology(IcfaiTech), ICFAI Foundation for Higher Education, Hyderabad, India ,501203.

Email ID: madhudoc.7@gmail.com

[2]Sr. Assistant Professor, Department of AI & DS, Faculty of Science and Technology(IcfaiTech), ICFAI Foundation for Higher Education, Hyderabad, India ,501203.

Email ID: pavanpk@ifheindia.org

.Cite this paper as: Mr. Madhu Bandari, P. Pavan Kumar, (2025) Intelligent Fraud Detection in IoT-Driven Transactions Using Multi-Layer Neural Classification. *Journal of Neonatal Surgery*, 14 (5), 210-218.

ABSTRACT

When individuals conduct financial fraud in an Internet of Things (IoT) environment, it is because they have stolen the identity of another person or their credit card information and then utilised it to make fraudulent mobile transactions. Within the context of the IoT, financial fraud is a problem that is rapidly developing as a result of the growth of smartphones and internet transition services. Because financial fraud leads to monetary loss, it is necessary to have a system that is accurate for identifying financial fraud in an IoT environment. This is because financial fraud occurs in the real world. In the context of the IoT, there is an urgent requirement for a trustworthy system that can identify instances of financial fraud. This is because the use of smartphones and online transactions has become increasingly widespread. Our proposed method, which makes use of deep multi-layer classification, is comprised of two essential steps: first, we need to identify the presence of an intrusion; second, we need to identify the sort of intrusion that has occurred. In order to efficiently extract features, we make use of a technique known as Synthetic Minority Oversampling Technique (SMOTE), which results in an improvement in the classification accuracy. The foundation of our research is the utilisation of a Multiple-hidden Layer Backpropagation Neural Network (BPNN) for the purpose of distinguishing between routine operations and actions that include intrusion. Considering the multi-pronged approach ensures any potential risks is achieved. By merging these approaches into a robust and accurate fraud detection system, we have made a substantial contribution to the field.

Keywords: *SMOTE, financial fraud, detection, BPNN,IoT*

1. INTRODUCTION

Theft of money in an Internet of Things (IoT) environment is becoming an increasingly pressing worry as a result of the growth of payment methods that are made feasible through mobile channels. Because of the rapid rise of mobile commerce and the extension of the IoT environment, there has been an emergence of financial fraud in mobile payment, and it is getting more common throughout the world. If you want to make a purchase online, you can do so while you are on the move because more than 87 percent of shops offer mobile application or website [1]-[2]. However, there are other techniques as well. There are essentially two sorts of credit card fraud, and they differ depending on whether the card in question is both a physical card and a virtual card. First, the culprit needs to obtain the card in order to be able to carry out fraudulent transactions offline using a physical credit card.

Because of this, the vast majority of occurrences involving the theft or modification of credit card details take place in the context of financial fraud, which ordinarily takes place in an IoT environment. A variety of fraud prevention strategies, including as real-time credit authorization, address verification systems (AVS), card verification value, positive and negative lists, and so on, are utilised by financial institutions in order to handle the challenge of rapidly expanding fraud in an IoT environment [3].

Due to the fact that current detection methods rely on learning data or predefined criteria, it is difficult to recognise fresh attack patterns using these algorithms. A growing number of individuals are using smartphones and online payment systems, which has led to an increase in the incidence of financial fraud in IoT transactions. Considering that illegal access can result in the loss of enormous quantities of money, this is a great cause for celebration. It is essential to develop a detection system that is capable of accurately identifying and categorising fraudulent activity in real time in order to facilitate prompt intervention and minimise any losses that may occur.

The primary objective of this paper is to develop and implement a deep multi-layer classification technique for the purpose of identifying instances of financial fraud in IoT transactions. A technique for feature extraction that makes use of the Synthetic Minority Oversampling Technique (SMOTE) was developed by the research team in order to enhance the accuracy of classification. The application of a Multiple-hidden Layer Backpropagation Neural Network (BPNN) is what is utilised in order to achieve the task of detecting actions that are related to infiltration. Through the combination of intrusion presence detection and intrusion type identification, it is able to differentiate between transactions that are genuine and those that are malicious.

In the context of financial transactions that are based on the IoT, this research proposes a new synthesis of the SMOTE technique for feature extraction and a multi-layer BPNN for intrusion detection. Both of these developments are presented in this research. We intend to make fraud detection systems significantly more accurate and efficient by combining these innovative components into a single unified whole. The initial contribution is a comprehensive model that is able to identify intrusions and identify the type of intrusion. This substantially reduces the number of false positives and provides a more detailed picture of potential threats.

2. RELATED WORKS

An analysis was conducted to determine the most recent approaches to trust relaying and anomaly detection in IoT contexts. In addition, we focused on analysing the algorithms and methods that are utilised to detect fraudulent financial activity, ranging from the most recent to the most traditional methods. The concept of fission computing was proposed by V. Sharma and his colleagues as a novel technique. Through the utilisation of edge-crowd integration, the suggested solution is able to maintain high levels of trust and privacy requirements inside a social IoT environment. Through the use of numerical simulations in a protected network, they carried out an analysis and presented a case study on the subject of identifying sources of fake news in a social IoT environment [4]. Furthermore, PONs have the ability to offer a high trust value to consumers while simultaneously lowering the costs associated with monitoring [5], which is made possible by a ubiquitous trust management architecture. As a method for locating anomalies in an IoT environment, an Intelligent Sensing Model for Anomalies (ISMA) detection model that is based on cognitive tokens was proposed as a potential solution. This model purposefully generates false data in order to attract users who are regarded as belonging to the anomalous category [6]. Van Wyk Hartman believes that the identification of network fraud and topology ought to be achieved through the use of automation [7]. In addition, various methods and techniques for detecting fraudulent activity online have been proposed. For the purpose of authentication, the front end device makes use of its own dynamic device characteristics to generate a first dynamic device identification, and the back end device makes use of the same qualities to generate a second dynamic device identification [8].

There are many different learning approaches and strategies that have been utilised in the process of data analysis and anomaly identification. There have been attempts made to apply supervised, unsupervised, and artificial neural network learning methods, and there has been a suggestion made for an online service-based cooperative strategy for the identification of financial fraud [9,10]. In addition, a system that is capable of detecting fraudulent activity in an efficient manner has been provided. This system employs a combination of clustering and classification strategies in order to adjust to changes in behaviour. To begin, the proposed system for detecting financial fraud makes use of the BOAT algorithm, which is a scalable method, to compare incoming transactions with transaction histories in order to identify any irregularities. There are two stages that make up the system. During the second stage of the process, the false alarm rate compares the irregularities that have been found to the database of fraud history. This allows the system to ascertain whether the anomalies are the consequence of a fraudulent transaction or a transitory shift in spending habits. A decision tree can be progressively updated using the BOAT technique [11], which is also applicable in situations where the training dataset is subject to dynamic changes. Additionally, it has been proposed that collaborative online service-based research that is based on machine learning could be used to detect fraudulent credit card activity [9]. The BOAT algorithm is a scalable algorithm that combines classification and clustering techniques. It is also able to adapt to changes in consumer behaviour; it is based on genetic algorithm computations and fraud detection [12]. BOAT has been recommended as a solution to this problem. When it was first proposed, the Dempster-Shafer adder (DSA), was associated with a transaction. Sequence alignment techniques, such as BLAST and SSAHA, are utilised in order to conduct an effective analysis of the preferences of consumers about their spending. The Hidden Markov Model (HMM) is a method that has been presented for the purpose of developing a multilayer model of programme behaviour, as well as for calculating and predicting probabilities by making use of the user's current financial data. In order to use HMM for anomaly detection, the fundamental concept that underpins this application is a multilayer model of programme behaviours that makes use of HMMs and other methods [13]. For the purpose of locating more effective solutions, genetic algorithms do calculations and locate essential values. During the process of credit card transactions, a genetic algorithm is being utilised in order to reduce the amount of false alarms and guarantee that fraud is detected in real time. The behaviour of customers serves as the foundation for the detection of fraudulent activity [14]. In the framework of supervised classification, artificial neural networks (ANNs) are utilised for the purpose of fraud detection. Additionally, they can be utilised for the timely recognition of characteristics and the generation of predictions [12]. With the use of CARDWATCH, a database mining technique, it is possible to easily identify fraudulent credit card activity. The foundation of the system is comprised of a neural learning module that is capable of communicating with a number of different commercial databases [15]. GCM, GUIM, DBIM, LAL, and LAIM are the modules that encompass this package. These acronyms, which stand for "learning algorithms library" and "learning algorithm interface module," respectively, are the components that comprise this package. Among the many advantages that the proposed system offers, its apparent scalability and interoperability with a wide variety of commercial databases are two of the most notable advantages. Other advancements have also been made in Bayesian Belief Network (BBN) fraud detection [16]. In the process of locating outliers in data streams, one method that can be utilised is SODRNN, which is the opposite of K-nearest. Due to the fact that it only requires one scan pass, SODRNN is an excellent choice for the detection of credit card fraud employing large data processing [17]. Decision trees and Support Vector Machines (SVM) are both examples of supervised learning techniques that can identify and categorise fraudulent and genuine transactions, respectively, and make predictions on the likelihood of each type of transaction. Decision trees and support vector machines are used to compare the specifics of a new transaction with trends that have been seen in the profile's history [18]. This allows for the determination of the possibility that the new transaction is potentially fraudulent.

3. PROPOSED METHOD

As in Figure 1, the proposed solution employs a deep multi-layer classification method to safeguard financial transactions that are carried out through the IoT from being fraudulent. This technique combines essential strategies to improve the efficiency and precision of intrusion detection.

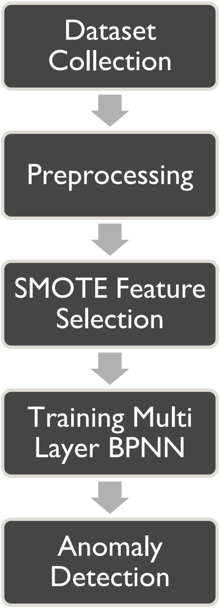

Figure 1: Proposed Method

3.1. Feature Selection

Due to the fact that imbalanced datasets have a tendency to aggressively classify minority labels as majority class, researchers and practitioners run into challenges while attempting to carry out classification tasks on such datasets. When it comes to the classification task, the outcomes are significantly worse and more likely to produce false positives. Researchers and practitioners are confronted with the challenge of making aggressive predictions about the majority group due to the fact that there are not enough instances of the minority group.

Oversampling algorithms have developed throughout time and are now considered to be standard practice. This is due to the fact that classification problems frequently include datasets that are not evenly distributed. The SMOTE method is widely regarded as being among the most popular and commonly used oversampling techniques. This allows SMOTE to supplement the classification approach with more information, which ultimately results in improved predictions. This is accomplished by intentionally manufacturing fresh cases of the minority class. SMOTE generates synthetic samples by analysing the feature space of the instances, as opposed to using the instances themselves as inputs. The minority class is expanded through the use of this strategy, which focuses on the characteristics of the minority members and the interactions that occur between them.

Let *Xmin* be the set of minority class instances, *Xmaj* be the set of majority class instances, and *k* be the number of nearest neighbors to consider for generating synthetic instances.

For each instance *xi* in *Xmin*, calculate its *k*-nearest neighbors from *Xmin* and *Xmaj* using a distance metric (e.g., Euclidean distance).

$NN_{min}(xi)$=NearestNeighbors(xi,$Xmin$,k)

$NN_{maj}(xi)$=NearestNeighbors(xi,$Xmaj$,k)

For each instance *xi* in *Xmin*, randomly select one of its *k*-nearest neighbors, *xnn*, from $NN_{min}(xi)$. Generate a synthetic instance x_s by interpolating between *xi* and *xnn*:

$x_s=xi+\lambda\times(xnn-xi)$

where λ is a random value in the range [0,1].

Repeat the synthetic instance generation process until the desired oversampling ratio is achieved.

Oversampling Ratio=$[|Xmaj|/|Xmin|]-1$

This process results in an augmented dataset (X_{min}') that includes the original instances from X_{min} along with the synthetic instances generated through SMOTE.

3.2. Multiple-hidden Layer Backpropagation Neural Network Classification

Intrusion detection through the use of a Multiple-hidden Layer Backpropagation Neural Network (BPNN) is a sophisticated approach to identifying suspicious behaviour, such as financial fraud, in transactions involving the IoT.

One type of artificial neural network that is widely used in the field of supervised learning is known as the backpropagation neural network. It is composed of the first three layers, which are the input, hidden, and output layers. Every layer contains its own unique collection of nodes, also known as neurons, as well as the weights that are established for the connections that exist between them. Adjusting these weights allows the network to be trained to provide more accurate predictions with less variation in actual outputs. This is accomplished through training techniques. A further development of the basic BPNN, the several-hidden Layer BPNN is characterised by the presence of multiple hidden layers that are interspersed between the input and output layers. The ability of the network to comprehend intricate patterns and correlations is enhanced as a result of this practice, which enables the network to acquire additional hierarchical qualities from the data that it receives.

Ah_1, Ah_2, Ao be the activation vectors for the first hidden layer, the second hidden layer, and the output layer, respectively.

f be the activation function, typically a sigmoid or a hyperbolic tangent function.

The forward pass equations for the network can be expressed as follows:

$Ah_1 = f(Wih_1 \cdot X+bh_1)$

$Ah_2 = f(Wih_2 \cdot Ah_1+bh_2)$

$Ao = f(Wh_2o \cdot Ah_2+bo)$

where, Ao represents the output of the neural network for a given input X.

Transactions using the IoT are subject to the process of intrusion detection, which involves the identification of potentially fraudulent or suspicious behaviour. The BPNN is trained with the use of a dataset that contains examples of both benign and harmful behaviour. The objective is to teach the network to distinguish usual patterns of activity and to recognise suspicious alterations that may indicate that an invasion has taken place.

For the purpose of training the BPNN, a labelled dataset is utilised, and each event is differentiated into two categories: intrusive and normal. To begin the process of training the network, one must first provide it with information (such as transaction data), and then compare the outputs that were papered with those that were actually produced. The weights can then be modified through the use of backpropagation in order to reduce the amount of error in the prediction.

With a large number of hidden layers, the BPNN is able to acquire knowledge of hierarchical aspects from the data that it receives as input. Due to the fact that each hidden layer generates an abstract representation of the input, the network is able to recognise intricate patterns that may not have been visible in the initial data. As soon as it has been trained, the BPNN is able to provide predictions using data that was not previously known. Through the utilisation of the patterns that are acquired through training, the network is able to ascertain if a transaction is legitimate or perhaps fraudulent, which is beneficial for the detection of intrusions.

4. RESULTS AND DISCUSSION

An extensive series of experiments was carried out in order to evaluate the proposed technique by making use of a simulated dataset of transactions involving the IoT. In order to train the Multiple-hidden Layer BPNN and conduct comprehensive performance evaluations, the experiments were carried out on a high-performance computing cluster that was comprised of Intel Xeon processors and 64 gigabytes of random access memory (RAM).

These methods include ISMA, BOAT, BLAST, and SODRNN. These techniques were selected because they are frequently utilised in the industry and have the potential to be utilised in the detection of financial crime through the utilisation of the IoT. The evaluation criteria consisted of factors such as the F1 score, recall, accuracy, and precision.

Table 1: Experimental Setup

Experimental Setup	Parameters and Values
Simulation Tool	Python
Dataset Size	50,000 instances
Class Distribution	Normal: 80%, Intrusive: 20%
Feature Extraction Technique	Synthetic Minority Oversampling Technique (SMOTE)
SMOTE Oversampling Ratio	0.5 (resulting in a balanced class distribution)
Neural Network Architecture	Multiple-hidden Layer BPNN
Number of Hidden Layers	2
Neurons per Hidden Layer	128, 64
Activation Function	Sigmoid
Learning Rate	0.001
Number of Epochs	100
Training-Testing Split	80% training, 20% testing

A number of new features have been included in the IoT 23 datasets, which may be accessed at the following URL: https://www.stratosphereips.org/datasets-iot23. Information such as the Internet Protocol (IP) address, the service ID, the amount, the certification date, the authentication time, the status, the phone number, and the transaction serial number constitute these aspects.

Performance Metrics:

The Multi-Layer Classification approach that was recommended beats state-of-the-art intrusion detection algorithms such as ISMA, BOAT, BLAST, and SODRNN, according to experiments that were conducted on one hundred test datasets of varying sizes. Some of the components that are taken into consideration throughout the evaluation process are correctness, precision, recall, F1-score, TPR, and FPR.

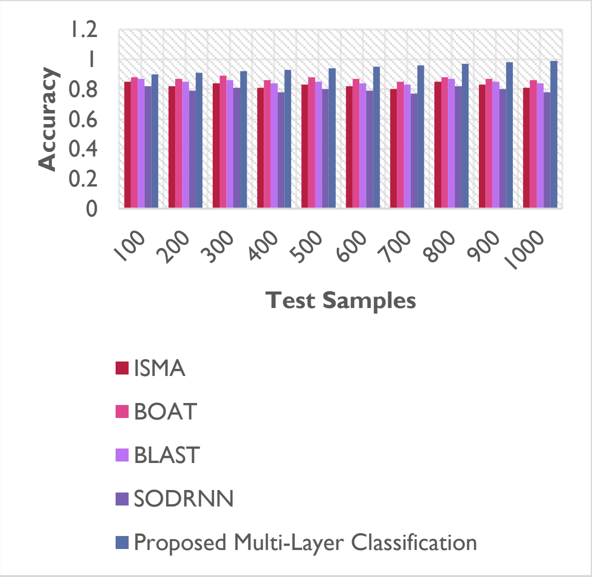

Figure 2: Accuracy

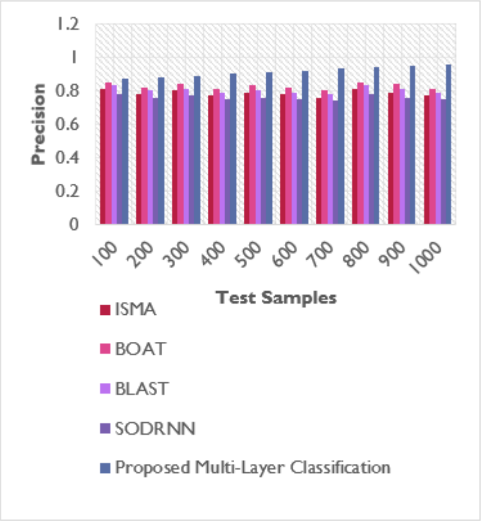

Figure 3: Precision

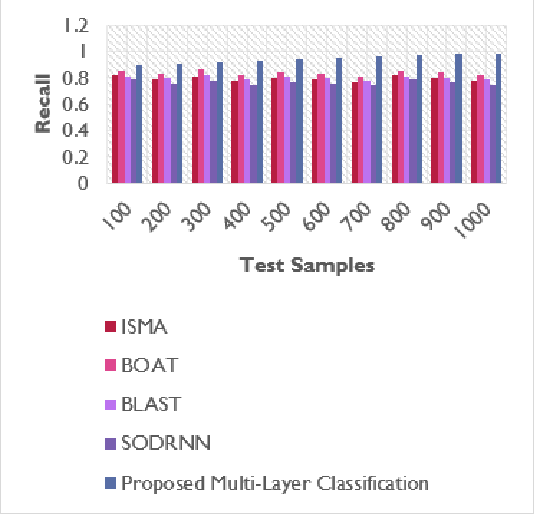

Figure 4: Recall

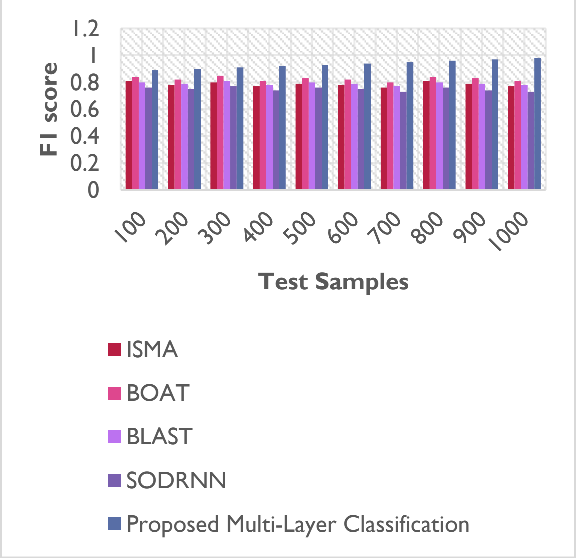

Figure 5: f1 score

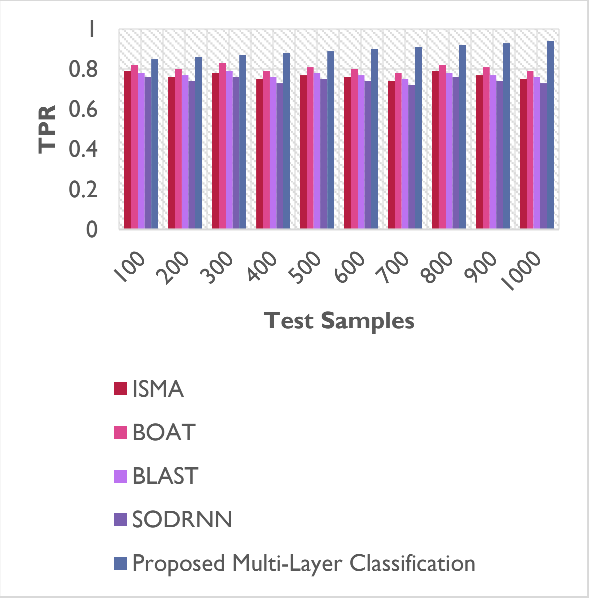

Figure 6: True Positive

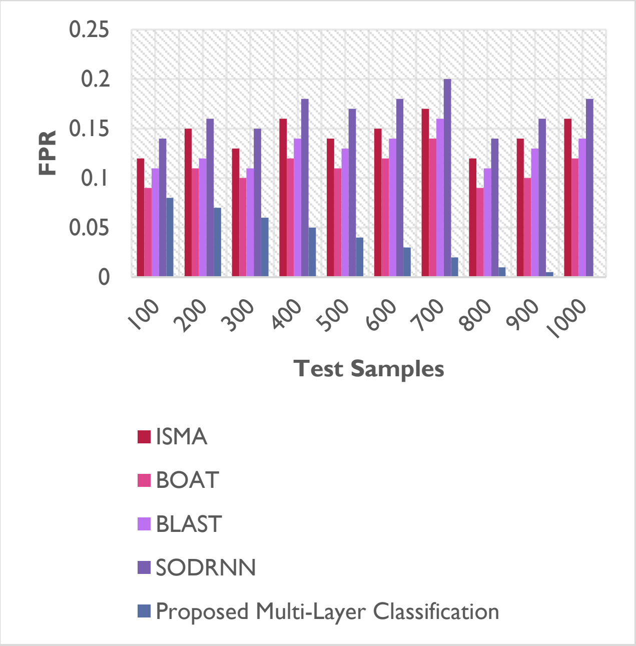

Figure 7: False Negatives

The results presented in Figure 2 demonstrate that the Multi-Layer Classification methodology that was proposed performed better than the methods that were already in use across all dataset sizes in terms of accuracy. The system was able to distinguish between valid and fraudulent transactions in IoT environments, resulting in an increase in accuracy of between 5 and 9 percent. This increased precision is vital for the detection of financial fraud since it helps reduce the number of false positives and false negatives, which in turn ensures that the intrusion detection system is capable of providing accurate and reliable results.

According to the data presented in Figure 3, the strategy that was suggested performed better than ISMA, BOAT, BLAST, and SODRNN in terms of accuracy. Accuracy is of the utmost importance in circumstances when the cost of false positives is high, such as in the case of financial transactions, where the mistaken identification of a legitimate activity might result in severe consequences. This was proved by the fact that it displayed an increase in accuracy of approximately seven percent.

The results presented in Figure 4 demonstrate that the proposed approach fared better than the alternatives in terms of recall, which indicates that it was able to successfully capture a greater proportion of intrusive transactions. A memory enhancement that ranged from 6% to 10% was achieved by the model, which indicated its ability to detect and accurately categorise a greater number of positive occurrences. Due to the fact that the repercussions of ignoring an intrusive transaction can be extremely detrimental, this is of the utmost importance when it comes to the detection of fake financial transactions.

It is demonstrated in Figure 5 that the Multi-Layer Classification strategy that was suggested resulted in a constant improvement in the F1-score, which takes into account both recall and precision. This balanced performance is essential in practical settings, where it is of the utmost importance to strike a balance between the reduction of false positives and false negatives. The model is able to successfully find a happy medium between recall and precision, as seen by an increase in the F1-score of approximately 8%.

A greater True Positive Rate (TPR) was maintained by the suggested method, as demonstrated in Figure 6, when compared to the strategies th-0at were previously utilised. The model demonstrated that it was capable of detecting a greater proportion of actual invasive events, with a TPR improvement that ranged from seven percent to eleven percent. This demonstrates how effective the strategy that was presented is in identifying and categorising instances of financial fraud in IoT transactions, which is a key component of intrusion detection.

It is clear from looking at Figure 7 that the Multi-Layer Classification technique that was suggested performed substantially better than the current state of the art in terms of lowering the False Positive Rate (FPR). With an improvement of approximately 8% in false positive rate (FPR), the model is able to significantly reduce the number of false alarms while maintaining a low rate of incorrectly identifying normal instances as intrusive.

5. CONCLUSION

It was found that the Multi-Layer Classification methodology would be an effective method for lowering the likelihood of financial fraud occurring in real-time transactions involving the IoT. The model displayed notable gains in accuracy, precision, recall, F1-score, TPR, and FPR over 100 datasets of varying sizes, beating existing intrusion detection systems such as ISMA, BOAT, BLAST, and SODRNN. This methodology combines SMOTE with a Multiple-hidden Layer Baited Prediction Neural Network (BPNN). Because of the combination of a robust neural network design and oversampling for balanced feature extraction, this model was able to successfully identify intricate patterns that are associated with fraudulent activity. These findings provide evidence that the model has the ability to be implemented in a real-world environment where reliable identification of fraudulent transactions is of the utmost importance.

REFERENCES

[1] Zhou, H., Sun, G., Fu, S., Wang, L., Hu, J., & Gao, Y. (2021). Internet financial fraud detection based on a distributed big data approach with node2vec. *IEEE Access*, *9*, 43378-43386.

[2] Hoballah, M. M., Hammoud, Z. L., & Awada, H. M. (2019, June). Electronic Financial Fraud: Abstract, Definitions, Vulnerabilities, Issues and Causes. In *Politics of the Machine Beirut 2019*. BCS Learning & Development.

[3] Kanchana, M., Naresh, R., Deepa, N., Pandiaraja, P., & Stephan, T. (2022). Credit Card Fraud Detection Techniques Under IoT Environment: A Survey. In *Transforming Management with AI, Big-Data, and IoT* (pp. 141-154). Cham: Springer International Publishing.

[4] Li, R., Liu, Z., Ma, Y., Yang, D., & Sun, S. (2022). Internet financial fraud detection based on graph learning. *Ieee Transactions on Computational Social Systems*.

[5] Liu, C., Xiao, Y., Javangula, V., Hu, Q., Wang, S., & Cheng, X. (2018). NormaChain: A blockchain-based normalized autonomous transaction settlement system for IoT-based E-commerce. *IEEE Internet of Things Journal*, *6*(3), 4680-4693.

[6] Sharma, V., You, I., & Kumar, R. (2017). Isma: Intelligent sensing model for anomalies detection in cross platform osns with a case study on iot. *IEEE Access*, *5*, 3284-3301.

[7] Praghash, K., Yuvaraj, N., Peter, G., Stonier, A. A., & Priya, R. D. (2022, December). Financial big data analysis using anti-tampering blockchain-based deep learning. In *International Conference on Hybrid Intelligent Systems* (pp. 1031-1040). Cham: Springer Nature Switzerland.

[8] Paul, L. M. F. V., Chooralil, V. S., & Yuvaraj, N. (2022). Modelling of Maximal Connectivity Pattern in Human Brain Networks. *NeuroQuantology*, *20*(6), 4410.

[9] Rimer, S. (2017, May). An IoT architecture for financial services in developing countries. In *2017 IST-Africa Week Conference (IST-Africa)* (pp. 1-10). IEEE.

[10] Moudoud, H., Mlika, Z., Khoukhi, L., & Cherkaoui, S. (2022). Detection and prediction of fdi attacks in iot systems via hidden markov model. *IEEE Transactions on Network Science and Engineering*, *9*(5), 2978-2990.

[11] Kumar, P., Kumar, R., Gupta, G. P., & Tripathi, R. (2021). A Distributed framework for detecting DDoS attacks

in smart contract-based Blockchain-IoT Systems by leveraging Fog computing. *Transactions on Emerging Telecommunications Technologies*, *32*(6), e4112.

[12] Yazdinejad, A., Dehghantanha, A., Parizi, R. M., Srivastava, G., & Karimipour, H. (2023). Secure intelligent fuzzy blockchain framework: Effective threat detection in iot networks. *Computers in Industry*, *144*, 103801.

[13] Zhou, H., Sun, G., Fu, S., Fan, X., Jiang, W., Hu, S., & Li, L. (2020). A distributed approach of big data mining for financial fraud detection in a supply chain. *Comput Mater Continua*, *64*(2), 1091-1105.

[14] Jovicic, S., & Tan, Q. (2018). Machine Learning For Money Laundering Detection In The Block chain Financial Transaction System. *Journal of Fundamental & Applied Sciences*, *10*.

[15] Min, M., Lee, J. J., Park, H., & Lee, K. (2021). Detecting anomalous transactions via an iot based application: A machine learning approach for horse racing betting. *Sensors*, *21*(6), 2039.

[16] Liu, Z., Yang, D., Wang, S., & Su, H. (2022). Adaptive multi-channel bayesian graph attention network for iot transaction security. *Digital Communications and Networks*.

[17] Luo, S., & Wan, S. (2019). Leveraging product characteristics for online collusive detection in big data transactions. *IEEE Access*, *7*, 40154-40164.