International Journal of Development Mathematics Vol 1 Issue 4 Page No. 201 - 213

INTERNATIONAL JOURNAL OF DEVELOPMENT MATHEMATICS

ISSN: 3026-8656 (Print) | 3026-8699 (Online)

journal homepage: https://ijdm.org.ng/index.php/Journals

Sim-Boxing Fraud Detection System Using Artificial Neural Network

Bello M. Thaddeus[a*], Murtala Muhammad[a], Yusuf M. Malgwi[a], and Martin E. Teman[a]

[a]*Department of computer Science, Faculty of Physical Science, Modibbo Adama University Yola*

ARTICLE INFO

Article history:
Received 11 June 2024
Received in revised form 05 September 2024
Accepted 19 October 2024

Keywords:
Sim-boxing, fraud detection system, artificial neural network, call detail record, telecommunication

MSC 2020 Subject classification:
68N01, 68N15

ABSTRACT

The SIM boxing fraud detection system, utilizes artificial neural networks, is designed to detect fraud perpetrated by malicious individuals who use specialized devices known as SIM boxes to bypass legal channels for making international calls. These devices enable scammers to install numerous prepaid SIM cards to the sim box, allowing them to place international calls using local phone numbers in the destination countries and receive calls over VoIP (the Internet). By initiating the call with a local SIM inserted in the SIM box, it appears local to the telecom operators, resulting in significant revenue losses running in billions. This tactic, is also known as SIM-box bypass fraud, poses a serious challenge to telecom operators as it undermines their revenue and operational integrity. Relevant data from telecom Call Detail Records were identified, extracted, and classified into fraudulent and non-fraudulent call. An Artificial Neural Network (ANN) model was designed, and trained using extracted data to more accurately and efficiently identify fraudulent customers; and diverted SIM-Box calls using Customer Detail Records (CDRs) data. The model used multi-layer perceptrons, a class of ANN, to identify patterns indicative of SIM-box operations by analysing Call Detail records (CDRs). The model was trained using 50 iterations on a dataset comprising labelled records of both legitimate and fraudulent calls, using features such as call duration, frequency of calls, timestamp patterns, and originating and terminating number characteristics. The range of prediction accuracy obtained from the developed artificial neural network models starts at 57.04% and improves to 80.01% after 50 iterations with the top layer consisting of 16 nodes. These layers consist of input, hidden and output layers which are 16, 8, and 1 neuron respectively. Thus it is recommended that telecom should adopt the like of this model as it will drastically improve their revenue generation and ensure communication integrity.

1. Introduction

The development of communication technologies has led to a massive expansion of the telecoms sector. The rise in the number of individuals subscribing to mobile services is directly linked to the advancement of reasonably priced technologies. Certain features of the telecommunications industry's growth encourage fraudsters. Fraud methods and techniques are increased in parallel to this massive growth (AlBougha, 2016). Telecom carriers have difficult issues as a result of this increase in fraudulent activities (Sahin, Francillon, Gupta and Ahamad, 2017). Nonetheless, telecom carriers have an obligation to safeguard their clients' money and identity against fraudulent activities.

According to Ekwonwune, Chukwuebuka, Duroha and Duru (2022), Fraud is not only a risk but a highly organized global business that affects telecom operators all over the world. The Communication Fraud Control Association (CFCA) released statistics highlighting the seriousness of the issue. According to the CFCA, global fraud losses in the telecoms industry have surged by 52% since 2003 and now range from US$54 billion to $60 billion annually.

The entire Nigerian economy is rife with fraud, and the mobile telecommunications sector is no exception. With an increasing number of mobile telecommunication carriers, Nigeria's mobile industry is one of the economic sectors that is expanding the fastest (Ogundile, 2013). However, because it has resulted in financial losses for both telecommunication carriers and their subscribers, telecommunication fraud has been a significant obstacle to the industry's rapid growth. Different solutions and services have been employed to curb this menace in the mobile industry, but the more advanced the service or solution, the more susceptible it is to fraud (Ogundile, 2013). Detecting fraud prematurely allows for early corrective action.

Telecommunication fraud happens whenever fraudsters use deception to receive services free of charge or at a reduced rate. Telecommunication fraud is a worldwide problem and causes substantial annual revenue losses for

* Corresponding author. Tel.:
E-mail address
https://doi.org/10.62054/ijdm/0104.16

telecommunication companies (Ogundile, 2013). Fraudsters have long been drawn to telecom fraud since obtaining a subscription using false identification is simple, and mobile terminals are not restricted to certain locations. This allows con artists to operate with a comparatively low chance of detection.

These fraudulent activities negatively impact end users by reducing the quality of service and leading to unexpected charges. Illegal termination of international calls also known as SIM-boxing fraud), and extreme usage scenarios related to international revenue share fraud are two of the major fraudulent activities (Luís, Leopoldo, Francisco, Carlos, Pedro, Helena, Paulo and André, 2023). Traditional fraud detection techniques only focus on detection accuracy and barely focus on detection speed. Fraudsters can therefore go unnoticed for a long period. Once the current connection is blocked, they switch to a new connection due to the decreased cost of doing so. Therefore, to minimize the harm and successfully regulate the fraud, it is crucial to detect these fraudulent activities in close to real-time.

Mobile communication networks have attracted many fraudsters as the subscription is easy to get and the mobile terminal is not bound to a physical place. Illegal high-profit businesses can be set up with minimal investment and technical skills as well as very low risk of getting caught (Abdikarim, Elmi, Ibrahim and Sallehuddin, 2014).

The threat that the SIM-box poses to telecom providers in certain parts of Asia and Africa has grown increasingly serious. As a result, the consequences of SIM-box bypass fraud differ between nations. In comparison to countries where customers can purchase SIM cards for very little or even nothing and where the government does not forbid unregistered subscribers, the effect is lessened in countries where unregistered SIM cards are forbidden and where SIM-box devices are regarded as illegal equipment. The lack of publicly available research on this type of fraud may be explained by the fact that it does not impact all telecom companies worldwide.

According to Zoldi (2015), Call Detail Records () are one of the most valuable data repositories of any telecom operator. The CDRs is a data record that includes details about a single phone conversation or other connected transaction. A CDRs record is produced whenever a transaction passes through a Mobile Switching Centre (MSC) or comparable telecommunication node. Depending on how well the communication nodes function, the level of information in CDRs may change. Most typically, it gives details about the call's beginning and finishing, locations, as well as its length, beginning and ending hours, and destination addresses. The greatest data source to reflect subscriber behavior and calling patterns is the CDRs stream. Some related works use CDRs analysis to detect fraud, but they adhere to the conventional database-based store first, process later paradigm. Furthermore, when making decisions, they take into account gathered over an extended period of time; hence, they lack real-time features and are unable to successfully regulate fraud. Moreover, those systems ignore the time-sensitive call patterns in the CDRs stream, which offer vital information for fraud detection. For this reason, a real-time fraud detection system is required. This programme needs to be able to identify fraud quickly by using time-sensitive call patterns seen in the CDRs stream.

The goal of this work is to find a set of appropriate descriptors and attributes from Costumer Call Detail Records (CDRs) to identify SIM-box fraud. A promising solution to this kind of issue is the Multilayer Perceptron (MLP) in Artificial Neural Networks (ANN), as it can recognize intricate patterns in noisy data (Abdikarim *et al*., 2014).

Telecom carriers lose a lot of money as a result of SIM-Box fraud. Telecom operators must safeguard themselves and their clients from SIM-Box fraud by maintaining a well-organized set of fraud detection procedures and standards. Techniques for detecting telecom fraud look at Call Detail Records () and identify fraudulent activity based on patterns found in them. Telecom operators use a variety of strategies, including rule-based Fraud Management Systems (FMS) and Test Call Generation (TCG), to address the issue.

However, fraudsters can readily defeat TCG and rule-based FMS approaches due to the volume of data created by telecommunication networks and their dynamic behavior (Kou, Lu, Sirwongwattana and Huang, 2004). As was previously noted, fraudsters utilize methods to avoid test calls to avoid being caught. They are able to determine whether incoming voice calls are genuinely originating from subscribers or from a TCG system by looking at the incoming call data and making choices based on established patterns. Furthermore, TCG levies high fees to the operator for conducting trial calls on all international routes. Similarly, scammers developed nifty SIM-Boxes that could imitate the behaviour of regular customers in order to evade detection by rule-based methods.

Furthermore, rule-based systems have high upgrade and maintenance costs and must be upgraded to remain current with modern techniques. Additionally, highly precise definitions of thresholds and parameters are needed for rule-based techniques (AlBougha, 2016).

Telecom giants such as MTN, Globacom, Airtel, and 9mobile representing the major players in the Nigerian telecommunication industry battled with the menace between 2017 and 2020. This according to the Nigerian Communications Commission, which had impacted negatively on security and cost the country about ₦3 billion

losses, according to the Nigerian Communications Commission (NCC) (Ogundile, 2013).

Artificial neural networks can be used to effectively tackle fraud, which will benefit both service providers and subscribers. Benefits include lowering expenses associated with extensive subscription fraud, identifying fraudsters utilising improperly registered services, preventing revenue loss, and identifying unreliable vendors. SIM-box fraud is projected to cost billions of dollars a year in lost income on a global scale. Telecom companies and economies can immediately profit from effective detection, which can greatly decrease these losses. Conventional detection technologies frequently fail to keep up with the increasingly sophisticated ways that fraudsters use. Artificial neural networks (ANNs) provide a dynamic solution that can learn and adapt to intricate and changing fraud patterns, which makes them perfect for today's complicated fraud detection problems. It offers a compelling argument for both academic and industrial investigation since studying ANN-based SIM-boxing fraud detection not only addresses a glaring commercial need, but it also increases our understanding of and proficiency with state-of-the-art machine learning techniques.

2. LITERATURE REVIEW

The content of this section is intended to offer a broader coverage that relates to this topic for better understanding and to showcase what have been done already and what is needed to be done

2.1 SIM Boxing scenario

Every time a subscriber makes a call to a foreign country, several organizations are involved (AlBougha, 2016). It makes sense to first describe the acceptable international call path before discussing the fraud bypass scenario to demonstrate how SIM-Box fraud is carried out. Assume that subscribers A and B reside in different nations, A and B, respectively. In legitimate route of an international call:

i. Subscriber A uses the mobile operator to call subscriber B and pays the service provider for the call.
ii. The subscriber-generated call A directed to the international entrance in A.
iii. The nation's primary international entry point A pays for the call and routes it to a temporary operator.
iv. The temporary operator then directs this call to an international gateway at the destination (country B) and pays the destination international operator a toll.
v. Finally, the call to subscriber B is terminated by country B's international gateway across his network.

Subsequently based on the discussion above figure 2.1 demonstrate the legitimate transaction route for international calls.

Figure 2.1: Legitimate Route of International Call (Ighneiwa and Mohamed 2017)

However, in SIM-Box fraud route of an international call (Murynets *et al*, 2014) is as follows:

i. Subscriber A places a call to subscriber B in the domestic mobile operator network and pays it for the call.

ii. The call generated by subscriber A forwarded to home international gateway in country A.

iii. The home international gateway of country A routes the received call to a transient operator and pays for it.

iv. The transient operator then routes this call to a SIM-Box placed in country B using VoIP and pays a toll to the SIM-Boxer.

v. The SIM-Box then makes a separate connection to subscriber B using its local SIM card on the network of nation B, giving the call the appearance of being local, and pays solely for the local call by eliminating interconnect costs.

vi. Finally, subscriber B in country B receives an international call from abroad but with a local number, it may be amazed.

In this regards, the research work will help to design a SIM-Boxing detection system that will able to mitigate SIM-box fraud as seen in Figure 2.2

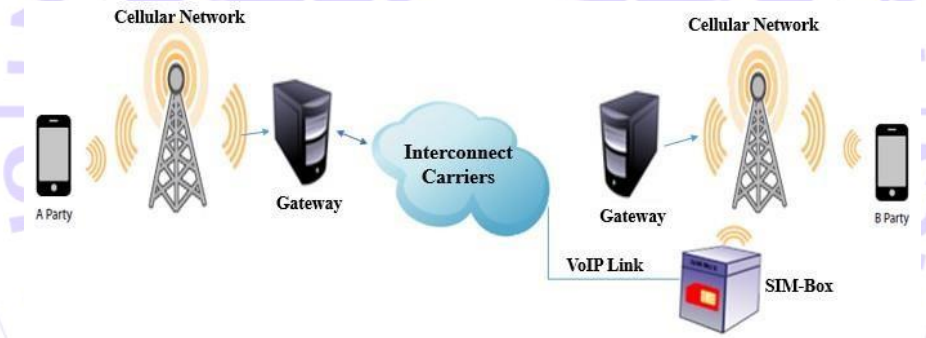

Figure 2.2: SIM-Box Fraud Route of International Call (Ighneiwa and Mohamed 2017)

2.3 Review of Related Literature

Elmi *et al*. (2014) opined that Mobile communication networks have attracted many fraudsters as the subscription is easy to get and the mobile terminal is not bound to a physical place. Illegal high-profit businesses can be set up with minimal investment and technical skills as well as very low risk of getting caught.

Marah *et al.* (2015) analyzed traffic of mobile network data to profile user behavior and identify detection patterns. Fuzzy logic and membership functions were used to determine if SIM cards exhibited potential fraud based on fraud scores. However, without fraud data for testing and verification, the program's results remain unconfirmed. Profiling with fuzzy logic offers flexibility and reliability for handling large amounts of data.

AlBougha (2016) asserts that data mining methods do not differ from the other detection methods in terms of continuous monitoring and that it is impossible for data mining classification algorithms to predict all cases accurately.

Igheniwa *et al.* (2017) developed intelligent algorithms that mine a huge amount of mobile operator's data and detect the SIMs that are used to bypass international calls thereby making it hard for fraudsters to generate revenue and hinder their network.

Luis *et al*. (2021) claim that end users are also affected by these fraudulent actions because they result in atypical rates and a decline in service quality. Two of the most common fraudulent acts are the illegal termination of international calls (also known as SIM-box fraud) and the excessive consumption circumstances associated with foreign revenue

share fraud.
According to Ekwonwune *et al*. (2022), fraud is a broad category of criminal activity in which a person or group of people deceitfully obtains property or benefits financially. Fraudsters employ a variety of tactics to take advantage of opportunities to obtain money, property, time, or information. Employers and individual customers of any age or gender might be considered victims of offenders, who can be people, employees, or managers of businesses in the public or private sectors. Simply put, everyone is impacted by fraud, but those in charge of sizable government and commercial organizations—where the potential losses are greatest—should be especially concerned.
The existing research gaps, based on the reviewed related literature, reveal several areas needing further investigation. These include identifying a suitable set of descriptors and features from CDRs data, classifying the extracted CDRs data, developing an Artificial Neural Network (ANN) model for SIM-Box fraud detection, and simulating the ANN model using Python programming.

3. Material and method

This section outlined the different materials and the methodology employed in implementing the framework.

3.1 Data source

The dataset for the experiments was obtained from the Call Detail Record (CDRs) database, which contains information about every call made over the network, including details of both legitimate and fraudulent subscribers.

3.1.1 Feature Extraction and Handling Missing Data

Call Detail Records () are not used directly for data extraction, as the objective is to extract customer knowledge, not individual call details. The data is aggregated and transformed into a rectangular form to prepare it for extraction algorithms. Customer-related records are condensed to summarize calling habits. Feature selection is crucial for obtaining a useful subscription description. This work will adopt features listed by Abdikarim *et al*. (2014) for detecting SIM-Box fraud.

Table 3.1 Selected Descriptors

	Field Name	Description	Data Type
Identification Field	Call Sub	This is the SIM number which will be used as the identity field	Categorical
Predictor Variables	**Total Calls**	This feature is based on the total number of calls made by an individual subscriber within a day.	Continuous
	Total Numbers Called	This feature represents the total count of unique subscribers that were called by the customer (subscriber) within a day.	Continuous
	Total Minutes	The total duration of the subscriber's calls, measured in minutes, on a single day.	Continuous
	Total Night Calls	The total number of calls made by the subscriber between midnight (12:00 am) and 5:00 am on a single day.	Continuous
	Total Numbers Called at night	The total different unique subscribers called during the midnight (12:00 am to 5:00 am) on a single day	Continuous
	Total Minutes at night	The total duration of all calls made by the subscriber in minutes at midnight (12:00 am to 5:00 am)	Continuous
	Total Incoming	Total number of calls received by the subscriber on a single day	Continuous
	Called Numbers to Total Calls ratio	This is the ratio of the **Total Numbers Called/Total calls**	Continuous
	Average Minutes	The is the average call duration of each subscriber	Continuous

3.1.2 Identifying and Removing Outliers

Outliers, also known as unusual or atypical data values, may be errors or true numbers that differ significantly from the majority of observations. They typically deviate from the overall trend of the data or lie near the extreme boundaries of data ranges (Abdikarim *et al*., 2014). To ensure the quality of models, these outliers will be removed from the data. In this study, outliers will be
detected using descriptive statistics, graphical methods, and Z-score standardization. Numerical predictive variables will be examined for potential outliers, using summary measures like 2 minimum, maximum, range, mean, median, mode, and standard deviation.

Z-score standardization is a common method for identifying outliers. It calculates the difference between a data value and the mean, then scales this difference by the standard deviation, as shown in equation

$$Z\text{–}Score = \frac{x - Mean(x)}{SD(x)} \qquad (3.1)$$

Data values above the mean have positive Z-scores, and values with a standard deviation of ±3 8 from the mean are identified as outliers.

After eliminating outliers, data normalization has been performed to prevent any single 10 characteristics from disproportionately affecting the algorithm's processing due to large numbers. All numerical variables has been normalized and scaled from 0 to 1, as required by Artificial Neural Networks (ANN). Min-max normalization has been applied to the numerical variables, with the 13 normalized value NNN calculated as:

$$N = \frac{X - MIN(X)}{RANGE(X)} = \frac{X - MIN(X)}{MAX(X) - MIN(X)} \qquad (3.2)$$

Normalized values will range from 0 to 1, with the minimum data value normalized to 0 and the maximum to 1.

Finally, the dataset has been divided into training, testing, and validation datasets. The training datasets has been used to train the models, while the testing and validation datasets has been reserved for evaluating the models' effectiveness in predicting the target variable. The data format be prepared according to the requirements of ANN modelling techniques.

3.2 Development of ANN Model

The optimal architecture for a Neural Network depends on the number of hidden layers, neurons in each layer, learning rate, and momentum. Finding the best model requires experimenting with different parameter choices. The number of hidden layers and neurons greatly impacts the network's performance. The back-propagation algorithm is influenced by the learning rate and momentum, which need to be carefully chosen. K-fold Cross-Validation is used to fairly evaluate the models. The training and testing process involves iterative adjustments to the network's weights until a termination condition is met.

3.2 Conceptual Framework for the System

This section aims at explore the interactions among key variables or concepts, which are hypothesized to influence specific outcomes or phenomena. By establishing a conceptual framework, Figure 3.2 provides a structured approach to investigate how these variables interact and contribute to the broader context of Sim-box fraud detection.

The framework and methodology of the system is presented

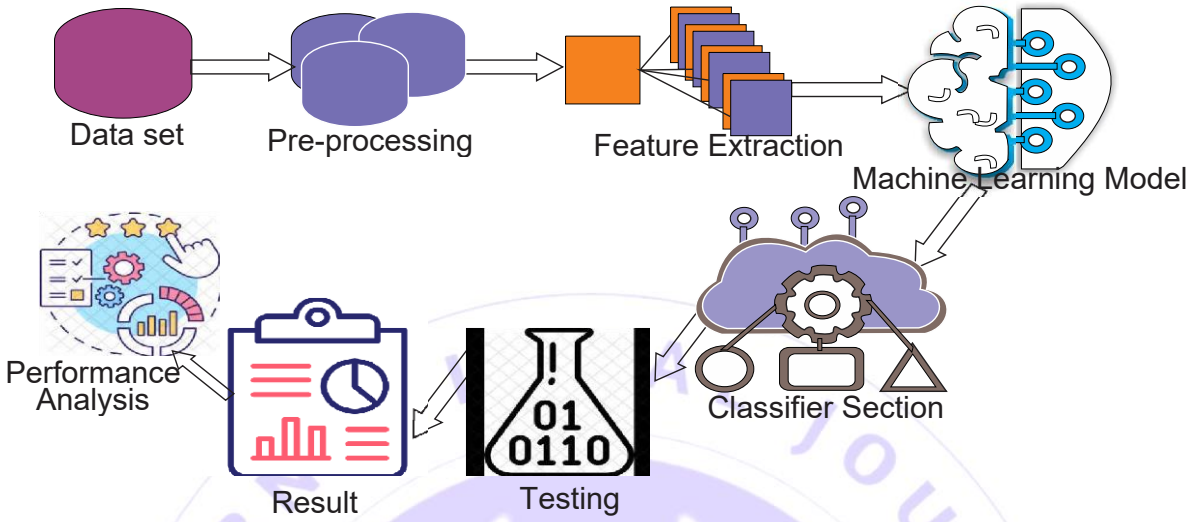

Figure 2.1: The conceptual framework of the system

4. Results and discussions

This chapter presents the empirical investigation, focusing on the outcomes of training and evaluating ANN models using Call Detail Record (CDRs) data. By linking theoretical approaches from earlier chapters with tangible results, this chapter demonstrates the practical application and effectiveness of the models in real-world situations

4.1 Data Description and Preparation

The study utilized data sets obtained from the Call Detail Record (CDRs), which contains information about the calls made by each subscriber. An Artificial Neural Network (ANN) based on a multilayer perceptron was created using a total of 32810 calls made by 6563 subscribers. Since the CDRs data may contain redundant, irrelevant, incorrect and noisy data, the data was subjected to pre-processing, which includes feature extraction, data integration, handling missing data, and the identification and removal of outliers, before using it to train the model. Subsequently, every numerical variable has been standardized and reduced to a 0–1 scale to avoid any one attribute having an excessively high processing power influence on the algorithm due to its big number value.

This chapter presents the empirical investigation, focusing on the outcomes of training and evaluating ANN models using Call Detail Records (CDRs) data. By linking theoretical approaches from earlier chapters with tangible results, this chapter demonstrates the practical application and

	Call Sub	Total Calls	Total Numbers Called	Total Minutes	Total Night Calls	Total Minutes at Night	Total Incoming	Called Numbers to Total Call Ratio	Average Minutes	fraud
0	2.350000e+14	7	3	1318.037710	5	1556.589782	1	0.428571	188.291101	0
1	2.350000e+14	6	6	645.750676	3	624.119509	4	1.000000	107.625113	0
2	2.350000e+14	8	3	1006.582073	1	257.917635	7	0.375000	125.822759	0
3	6.865130e+13	1	1	218.120262	0	0.000000	0	1.000000	218.120262	0
4	2.340000e+14	7	3	1311.082674	5	1331.510356	4	0.428571	187.297525	0

Figure 4.1: Few rows of the dataset displayed

4.2 Model Performance Result on Training Set

Figure 4.2 shows the training accuracy of the model. The training Accuracy measures how well the model performs on the training data. It starts at 57.04% in Epoch 1 and improves over time, reaching about 80.01% by Epoch 50. This indicates that the model learns and adjusts to the training data effectively.

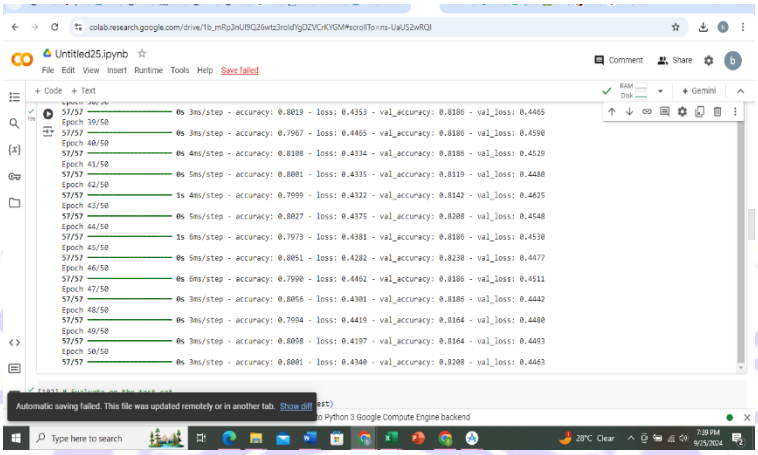

Figure 4.2: Model Performance Result on Training Set

Training Loss measures the model's error on the training data. A lower loss value indicates better performance. It starts at 0.6888 in Epoch 1 and reduces to 0.4340 by Epoch 50, showing that the model becomes more accurate over time in the classification of fraud and none fraud calls.

Validation Accuracy starts at 58.41% in Epoch 1 and improves to around 82.08% by Epoch 50. The validation accuracy closely follows the training accuracy, which suggests that the model generalizes well to new data without overfitting. In the same vein, validation Loss starts at 0.6685 in Epoch 1 and reduces to 0.4463 by Epoch 50. This value decreases consistently and stabilizes near the end.

The model performance is shown in figure 4.3; accuracy graph

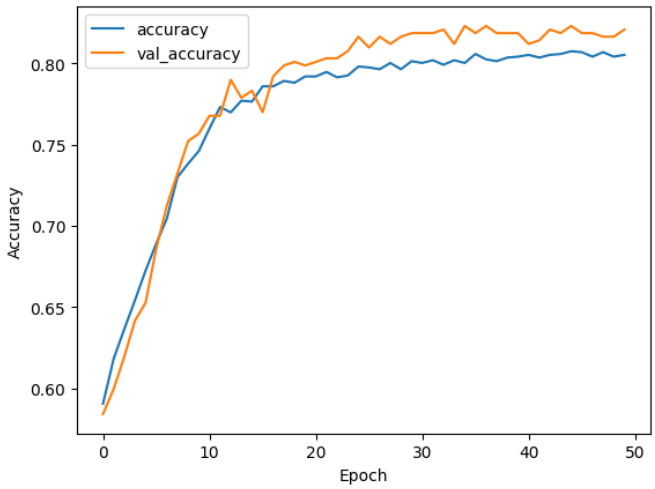

Figure 4.3: Model accuracy graph

The X-Axis (Epoch) represents the number of epochs during training. Each epoch corresponds to one complete pass through the training dataset. Y-Axis (Accuracy) shows the model's accuracy, which is the proportion of correctly classified instances out of all instances in the dataset. As shown in the graph, both lines are increasing, indicating that the model is improving its ability to classify both the training and validation datasets over time. The training accuracy is generally higher than the validation accuracy, suggesting that the model has learned well from the training data although not generalize perfectly to new data.

4.3.2 Convergence

The Lines stabilizes towards the end of the training (around epoch 40-50) Both accuracy lines seem to plateau, indicating that further training may not significantly improve performance. This suggests that the model has learned most of the relevant patterns in the data.

Had it been the training accuracy been significantly higher than the validation accuracy, it could indicate overfitting, where the model learns the training data too well and fails to generalize. In this graph, while there is a gap, it is relatively small, suggesting that the model is not overfitting dramatically.

4.5 Confusion Matrix

The confusion matrix of the model on the test data set is displayed as:

Table 4.1: Confusion Matrix table

True Positive/ True Negative	false Positive/ False Negative	Total
277	180	457
19	493	512

Table 4.1 shows True Negatives (TN) of 277 instances where the model correctly predicted no fraud (class 0). And False Positives (FP) of 180 instances where the model incorrectly predicted fraud (class 1) but it was actually no fraud. In the False Negatives (FN), 19 instances where the model predicted no fraud, but in reality, fraud occurred, and True Positives (TP) of 493 instances where the model correctly predicted fraud. This is clearly indicated in the confusion matrix visualization as shown in Figure 4.3.

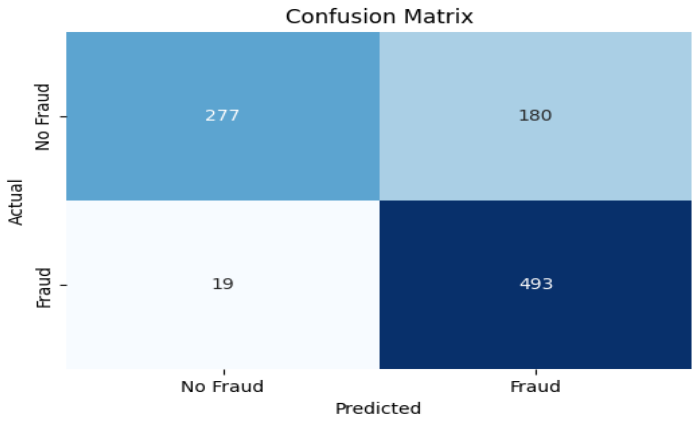

Figure 4.4: Confusion matrix

4.6 Model Classification Result

Classification Report:

Target	Precision	recall	f1-score
0	0.94	0.61	0.74
1	0.73	0.96	0.83

A model Precision is the proportion of positive predictions that were actually correct. From table 4.3, Class 0 precision is 0.94. This indicate all instances predicted as no fraud were correct. Class 1 precision is 0.73, indicating 73% of the fraud predictions were correct.

Recall is the proportion of actual positives that were correctly identified. Class 1: Recall is 0.73, meaning only 73% of the actual no fraud cases were correctly identified, and Class 1: Recall is 1.00, meaning 100% of the actual fraud cases were correctly identified.

Similarly, F1-Score is the harmonic mean of precision and recall. The model class 0: F1-score is 0.74, indicating very good performance in identifying no fraud cases, and class 1 F1-score is 0.83, indicating very excellent performance in identifying fraud cases.

The model's overall accuracy is 87%. This means the model correctly predicted 87% of the cases.

4.6.1 Macro Average

This is the unweighted average of precision, recall, and F1-score across both classes, giving equal importance to both fraud and no-fraud cases.

i. Macro avg precision: 0.83
ii. Macro avg recall: 0.78
iii. Macro avg F1-score: 0.78

4.6.2 Weighted Average

This average takes into account the imbalance in the number of instances in each class, giving more weight to class 1 (fraud), which has more samples.

i. Weighted avg precision: 0.83
ii. Weighted avg recall: 0.79
iii. Weighted avg F1-score: 0.79

4.7 Neural Network Architecture

Neural Network Architecture provides a clear visualization of how information flows through a simple fully connected neural network. It starts with 16 neurons in the input layer, each connected to every neuron in the hidden layer of 8 neurons, demonstrating a dense connection pattern. The hidden layer processes and transforms this

information, which is then fed into a single output neuron. This visualization helps illustrate the internal structure of a basic feed-forward neural network.

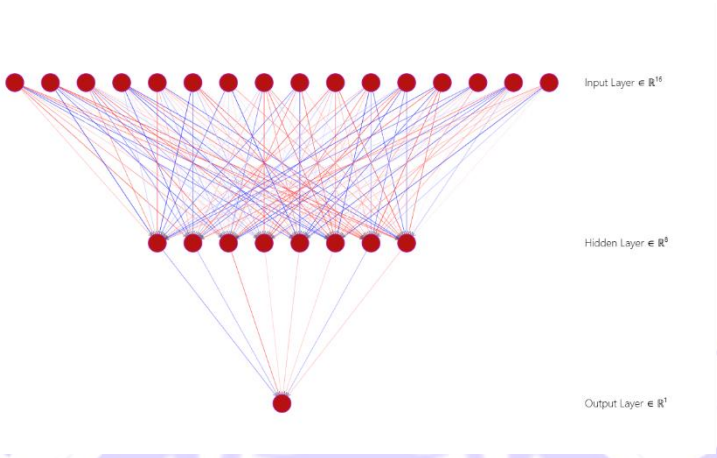

Figure 4.5: Visualized Architecture of Neural Network of the model

4.8 Discussion of the results and findings

The accuracy graphs indicate that the model's performance improves steadily, reaching around 80% accuracy after approximately 15 epochs in the training set, with validation accuracy closely following, suggesting minimal overfitting. By epoch 50, both training and validation accuracies stabilize around 85%, demonstrating good generalization to unseen data.

The confusion matrix shows that the model correctly identified 277 negative and 493 positive instances but misclassified 180 negative instances as positive and 19 positive instances as negative, indicating a tendency towards false positives. For class 0 (negative), the model has high precision (0.94) but lower recall (0.61), suggesting it misses many actual negative instances, reflected in an F1-score of 0.74. In contrast, for class 1 (positive), it achieves a high recall (0.96) but lower precision (0.73), with an F1-score of 0.83.

Overall, the model's accuracy is 87%, with a macro average precision of 0.83 and recall of 0.78, indicating a good balance in performance despite class imbalance. The high recall for class 1 is significant for scenarios prioritizing the identification of positive instances, while the lower recall for class 0 highlights areas for improvement.

Additionally, the neural network architecture features 16 input neurons connected to 8 hidden neurons, illustrating a dense connection pattern leading to a single output neuron, which helps visualize the flow of information in a basic feed-forward neural network.

The ANN models with various hidden layer configurations demonstrated effective performance, highlighting their ability to capture features and learn effectively. Future considerations include verifying the models' generalization beyond the training dataset, optimizing architectures for performance and computational efficiency, and enhancing robustness through regularization to prevent overfitting. Additionally, a detailed analysis of the relationship between model complexity and performance improvements would aid in refining future ANN designs for similar tasks.

5. Conclusion

The primary goal of this paper was to develop a collection of characteristics that could be used to recognize calls coming from SIM box devices as well as an algorithm that could quickly and accurately classify subscribers. A model that can be used to differentiate between genuine and SIM box fraud calls was constructed using nine features that were derived from CDRs data. Calling number, called number, call cost, call length, date and time, location number, total calls made each day, and call detail records are all included in this function. In this work, the overall accuracy of 87% indicates that the model performs well across both classes. Future research in the domain of SIM box fraud detection and prevention can benefit from this paper.

References

Abdikarim, H., Elmi, H., Ibrahim, S., and Sallehuddin, R. (2014). Detecting SIM Box Fraud Using Neural Network. International Conference on Computational Science and Computational Intelligence (pp. 967-971). Springer. doi: 10.1007/978-94-007-5860-5_69.

AlBougha, M. R. (2016). Comparing data mining classification algorithms in the detection of sim-box fraud [Master's thesis, St. Cloud State University]. The repository at St. Cloud State.

Ekwonwune, E. N., Chukwuebuka, U. C., Duroha, A. E., and Duru, A. N. (2022). Analysis of Global System for Mobile Communication (GSM) Subscription Fraud Detection System. International Journal of Communications, Network and System Sciences, 15, 167-180.

Elmi, A., Sallehuddin, R., Ibrahim, S., and Zain, A. M. (2014). Classification of SIM Box Fraud Detection Using Support Vector Machine and Artificial Neural Network. International Journal of Innovative Computing, 4(2), 19-27.

Ighneiwa, I., and Mohamed, H. (2017). Bypass fraud detection: Artificial intelligence approach. arXiv preprint arXiv:1711.04627.

Kou, Y., Lu, C.-T., Sirwongwattana, S., and Huang, Y.-P. (2004). Survey of fraud detection techniques. In Networking, sensing and control, 2004 IEEE international conference (Vol. 2, pp. 749-754). IEEE.Luis, C., Filipe M., António R., Pedro C. "Fraud Management Systems in Telecommunications: a practical approach https://www.telbit.pt/docs/ICT2005_FMS.pdf retrieved 26th September, 2022

Marah, H., Elrajubi, O. M., and Abouda, A. (2015). Fraud detection in international calls using fuzzy logic. In Computer Vision and Image Analysis Applications (ICCVIA), 2015 International Conference (pp. 1-6).IEEE.

Ogundile, O. (2013). Fraud Analysis in Nigeria's Mobile Telecommunication Industry. International Journal of Scientific and Research Publications, 3(2).

Sahin, M., Francillon, A., Gupta, P., and Ahamad, M. (2017). Sok: Fraud in telephony networks. In Security and Privacy (EuroSandP), 2017 IEEE European Symposium on (pp. 235-250). IEEE.

Zoldi, S. (2015). Using anti-fraud technology to improve the customer experience. Computer Fraud and Security, 2015(7), 18-20. https://doi.org/10.1016/S1361-3723(15)30067-1