DOI: https://doi.org/10.61841/tp4k9012 Publication URL: https://nnpub.org/index.php/SSH/article/view/2276

SUBSCRIPTION FRAUD DETECTION USING AUTOENCODER IN CASE OF ETHIOTELECOM

Getahun Wassie
Digital Economy, Policy studies Institute, Ethiopia

Corresponding Author:
getahunws12@gmail.com

To Cite This Article: Wassie, . G. . . (2024). SUBSCRIPTION FRAUD DETECTION USING AUTOENCODER IN CASE OF ETHIOTELECOM. Journal of Advance Research in Social Science and Humanities (ISSN 2208-2387), 10(7), 11-23. https://doi.org/10.61841/tp4k9012

ABSTRACT

Nowadays, telecom services are becoming an essential communication and business facilitators. However, the development of telecom services motivates fraudsters for illegal use. Hence, telecom fraud becomes a serious challenge in telecommunication sector by losing telecom revenue. It also results in poor quality of services for their customers. Telecom data, SMS and voice call are not free from security issues. Despite SMS, and USSD services becomes good options over installable mobile based or web based applications due to lesser cost and real time support, the methods provide fixed amount requirements which is not dynamic way to address the need of these services subscribers. The other challenge of these services is that; the services are not safe from frauds as such, especially in GSM switches. Subscription fraud is one type of fraud in today's telecom business which is a common telecom fraud. The need of fraudsters is to make money illegally or getting telecom services with the intention of not to pay for the service they used. The prime objective of this study is to build a predictive model using deep auto-encoder to detect subscription fraud in case of Ethiotelecom. The performance of fraud detection model is 98.95% validation accuracy on ethiotelecom call detail record dataset using deep neural network autoencoder and CNN-LSTM autoencder algorithms at threshold of 0.0103 and 0173 respectively.

KEYWORDS: Telecommunication, EthioTelecom, Fraud Detection, Deep Learning, Authoencoder

INTRODUCTION

The telecommunication industry has expanded dramatically in the last few years with the development of affordable mobile phone technology and Internet services mainly based on GSM network. With the increasing number of mobile phone subscribers for virtual switching traditional network and Internet telephony (VOIP) services, many users obtain the telecommunication services in both urban and rural areas especially in Covid-19 happening. The LTE/4G Internet is covering many cities of the country. Ethiotelecom also started 5G which is a great jump to accelerate the Internet service provision to its Internet service consumers. However, the global digital continuity disruption problem challenges the Ethiotelecom since it is a global company. One of the means of digital continuity disruption is digital attack [**1**]. We need to strive for an Internet that is safe and secure one that will engender trust when people go online [**2**].To do so , Ethiotelecom needs to implement dynamic based systems to safeguard subscribers data and detect unlawful subscribers at the same time. Subscription fraud becomes one of the challenging problems in Telecoms. During the pandemic, the subscription services of telecom network increases which results Fraud challenge [**3**]. Ethiotelecom defined fraud as it is intentionally deceptive action designed to provide the perpetrator with an unlawful gain or to deny a right to a victim [**4**]. Fraud is an illegal use of telecom services or infrastructure with or without payment intention [**5**].

Data, SMS and Voice call are the common targets of misuse service after subscriptions of customers [**6**]. Telecom data, SMS and voice call are not free from security issues. Despite SMS, and USSD services becomes good options over Installable mobile based or web based applications due to lesser cost and real time support, the methods provide fixed amount requirements which is not dynamic way to address the need of these services subscribers. The other challenge of these services is that; the services are not safe from frauds as such, especially in GSM switches.

Subscription fraud is one type of fraud in today's telecom business which is a common telecom fraud. The need of fraudsters is to make money illegally or getting telecom services with the intention of not to pay for the service they used.

Subscription Fraud has serious impacts on both finances and subscriber relations [**7**]. Thus, the subscription fraud brings the huge loss of revenue as well as it affects the credibility and operators' performance [**8**]. It also results in poor quality of services for their customers. Hence, Ethiotelecom needs more dynamic system to counterattack negative effect of the subscription frauds. Therefore, the prime objective of this study is to build a predictive model using deep auto-encoder to detect subscription fraud in case of Ethiotelecom. The subscription fraud detecting model can be deployed in telecom concerned switches such as multimedia messaging service (MMS) in order to prevent subscriptions tariff, voice and other data frauds.

Telecommunication frauds have different categories on their nature and characteristics. According to Kang and Yang [**9**], It is categorized into two as subscription and superimposed categories whereas Becker and et.al., [**10**], classified telecommunication fraud in to seven groups namely: superimposed, subscription, technical, internal fraud, fraud based on loopholes in technology, social engineering and fraud based on new technology. One of the most common types of fraud is subscription fraud [**11**] which we focus on to detect subscription fraud which shows big negative impact on Ethiopian telecommunication companies' revenue.

Ethio telecom is one of the victim telecom by this subscription fraud. It faces subscription fraud in both prepaid and postpaid service. Ethio telecom registers its customers on the Customer relation Management (CRM) system for billing purpose. However, it cannot detect or predict fraudulent at the time of service request or applications as the current Fraud management system (FMS) of Ethiotelecom is inflexible and non-dynamic to detect and mitigate frauds. The fraud increase the company's revenue loses as well as damages of subscribers' trust relationship. As new fraud behaviors have been happened, Ethiotelecom requires a dynamic way of fraud detection mechanism using the state of the art deep learning technology. Therefore, we propose subscriptions fraud detection method using deep autoencoder approach. The proposed solution detects the fraud early before attack. We extract patterns from subscribers Call Detail Record (CDR) data including Data, SMS and Voice call for detecting fraudulent and non-fraudulent subscriptions.

RELATED WORK

A GSM (Global System for Mobile) service provider sells their services with prepaid and post-payable credits. Customer should buy them to get telephone calls, text messages, and mobile data services. This trade is possible using prepaid or postpaid ways. Today ethioteecom is using Unstructured Supplementary Service Data (USSD) which is eelectronic Top-up solution to send text messages for prepaid or postpaid services [**12**]. USSD uses codes made up of the characters that are available on a mobile phone which are access by users during service request.

The USSD is a session-based, menu-driven, real-time communication technology which is used in sending messages across a GSM network between a mobile client and an application server. It operates much like SMS but it's session-based and has more interactive nature than SMS. Unlike SMS, it does not operate by store-and-forward way. It is faster and very cost effective. It requires asterisks (*) and hashes (#) [**13**]. Examples of USSD services include sports updates, movies, weather information, news, stock market, reservation applications, voting/polling applications, mobile account balance checking and top up, and many others. Ethiotelecom uses the USSD services as it is depicted in figure 2.1.

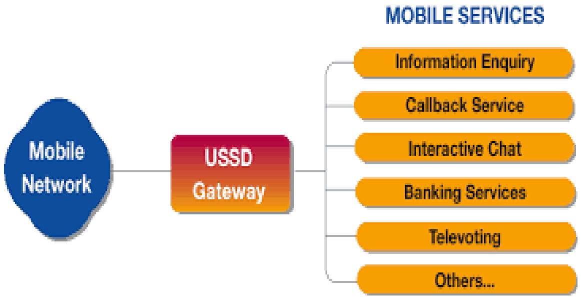


Figure 2. 1 USSD services

SMS has security and user experience shortcomings when it is compared with USSD. When compared to SMS, USSD is considered to be relatively more secure because no copy of the message is stored on customer's phone or at the SMSC switch [**13**].

Usage of USSD is refereed to Smartphone applications due to the fact that Smartphone applications connect users with providers through the internet still exclude the vast majority of the poor [**4**]. Paying mobile bills being on road, homes and offices or getting phone card credited transaction when you need a fast call or message.

Despite the convenience offered by USSD to customers in accessing banking and other services, the security issue has big risk lies on GSM data communication channel is not itself encrypted. If GSM encryption is broken, this data can be then be accessed [**13**] as telecommunication are still suffer from fraud. The presence of frauds is reported by information network security administration (INSA) in 2022. A total of 8985 attacks were tried on 99 institutions in Ethiopia, targeting Ethiotelecom.

PREPAID AND POSTPAID SERVICES

Most of the telecom operators provide two options to their customers, to go for a postpaid or a prepaid connection services. 70%-80% customer services are given as pre-paid services and rest of the customers are under post-paid services [**14**]. Ethiotelecom provides both Prepaid and postpaid services based on fee payments. The operators provide these two options to their customers having postpaid or a prepaid connection. Subscribers of these services are expected to pay service fee as per their agreement in both options.

1) PREPAID SERVICES

Prepaid services are the most popular of the services provided by telecom operators. As the name implies "Pre-paid‘, all transaction in this service needs payment fee before the service is rendered to customers. This service is easy for the operators to maintain in the event of fraud and it is less susceptible to fraud as compared to postpaid services since the expected fee is achievable early [**15**].

Prepay service becomes common today for mobile phones for which credit is purchased in advance of service use. The purchased credit is used to pay for call, SMS, and data services at the point the service are consumed. If there is no credit, then access is denied for the service requester.

2) POSTPAID MOBILE SERVICES

It is the alternative billing method when users enter into short and a long-term contract such as rolling contract or a 30-day contract. The user is expected to pay the service bill after usage of the services.

Network elements like switches, SMSC produce raw usage detail records UDRs or call detail records CDRs, which contain information required by the billing system such as Calling number receiving number call start time, call end time date and time Call duration, call fee, data upload volume, download volume, SMS size etc.

The billing system converts this format into a format understandable by the system to find and map the customer/account to which the call or data usage should be charged and then rate the event accordingly.
Users are usually alerted my messages when the bill dates arrives to compensate the postpaid payment method gap. Any usage above the dead date limit incurs extra charges for subscribers.

The UDRs are then stored in the billing data store and processes to render bill/invoice to subscribers considering the payments amount, taxes, discounts, etc [**16**]. Using postpaid approach, failure to complete the agreement would make the customer liable for early termination fees [**15**].

SUBSCRIPTION FRAUD

Subscription fraud is a contractual fraud between telecom and subscribers. In these kinds of fraud revenue is generated through the normal use of a service without making payment. Fraudsters obtain an account without intention to pay the bill [**17**].

One of subscription fraud call properties is the use of high duration per calls [**16**]. We also consider call Duration as a main feature to detect whether the subscriber pay the fee for the service.

Author in paper [**18**] divided subscription fraud into two subcategories based on intention of making profit or personal usage. In the first category, the fraudster opens a small outfit where he starts up a call center. The fraudster has no intensions of paying his bills but he sells the airtime to people who intend to make cheap long distance calls for cash [**17**] whereas the second Subscription fraud for personal profit.

Author [**19**] also categorizes subscription fraud in to different types based on the nature of the fraud committed. Some of them are Simbox fraud, call and SMS spamming, premium rate service (PRS) fraud, phishing, arbitrage, and stolen goods.

Hence, detecting subscription fraud is very important since it is the most challenging kind of fraud in telecommunication which causes a huge revenue loss for companies [**20**], specifically in developing telecommunication.

Fraud detection and mitigation has been researched using data mining [**17**], machine learning [**19**], neural network [**21**] and deep learning [**22**]. Subscription fraud is also investigated using deep learning in global telecommunications. So there is a need of subscription fraud detection and mitigation investigation for ethotelecom fraud detection task.

Deep learning is the state of the art technology that recently attracted for fraud detection. It has been used to solve real world problems in many areas such as image recognition in Facebook, speech recognition in Apple or Siri, and natural language processing in Google translator and in fraud detection areas [**23**] [**24**].

Deep learning implements many algorithms including Autoencoder(AE), generative adversary network (GAN), deep convolutional neural network, support vector machine, long short term memory (LSTM) on top of back propagation algorithm. AE is detects frauds in unsupervised way so that it does not suffer from class labeling task.

Table 3. 1: Voice attributes

Service num	Total Vol	Dnld vol	Upld vol	Fee

Table 3. 2: Internet Data attributes

calling_num	called_num	start_time	end_time	Duration	Call_Fee

Table 3. 3: SMS attributes

Sender Num	Reciver Num	Start Time	Fee	Procs Time

METHODOLOGY

To achieve the objective of this study, we collected raw CDR Data and identify features. Dataset preparation and feature extraction, workflow and procedures, designing of the proposed system architecture and model emulation mechanisms.

DATA COLLECTION

The data is collected from Ethiotelecom for subscription fraud detection purpose based on usage call patterns, CDR. A three month period from March 25 to June 24, 2021 are collected. CDR is produced by telephone switches on call basis and contains all the information to describe the important characteristics of telephone call and other telecommunication transaction. It contains the fields necessary for billing systems to rate a particular call and bill the subscriber.so that it helps to build a fraud detection model. CDRs give the details of each voice, SMS and Internet data usage transaction, originating from and terminating on a subscriber's device. A Field represents a characteristic or feature of CDR instance. It include, telephone numbers involved in the call, date and time of the call, duration of the call, identification of the cell transmitting the call to the subscriber's Shinde, Pramila P., and Seema Shahmeaning of the records in order to have an overall picture of the data.

FEATURE SELECTION AND DATA PREPARATION

Data preparation becomes a must after data collection for this study. Dataset Preparation was done in line of supervised learning mechanisms. CDR data is extracted from call switch of ethiotelecom and we saved it as CSV file format which leads compatible file format for intended python code of deep learning. In order to prepare the data set, first Voice attributes feature (attributes) is selected as it is displayed in table 3.1 below. Internet Data attributes and SMS attribute are presented in table 3.2. and table 3.3 respectivelyTheoretically, dataset with more attributes in learning process gives better result. However, in practice this may not be always the case [17]. There are many attributes for learning process, some of them feasibly significant, and some are irrelevant or redundant. The problem is identifying a representative set of features from which to construct a classification model. For that reason, the dataset must be preprocessed to select useful attributes. Even though, many learning schemes can select features appropriately and ignore irrelevant ones, but in practice their performance might be selected. Because of the negative effect of irrelevant attributes on most DL algorithms, it is common to precede learning with an attribute selection. More importantly, dimensionality reduction yields a more compact, easily interpretable representation of the target concept, focusing attention on the most relevant features [16].

AUTOENCODER ARCHITECTURE

Fraud detection is represented by neural network based architecture for more proposed system components as it is shown in fig 3.1.

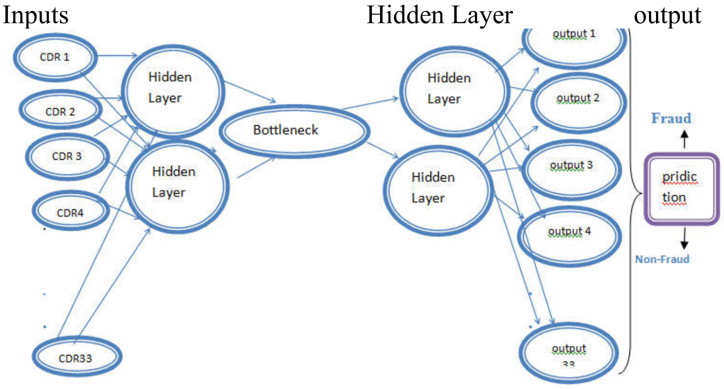


Figure 3. 1: **Auto encoder Architecture**

WORK FLOW OF PROPOSED PROTOTYPE MODEL

The flow of the proposed prototype system takes CDR as an input. We select and extract a feature that suit our study and increases the performance of the model. The dataset is presented as we stated in the data preparation section above. The next task is model construction using a deep learning approach, specifically, we employee auto encoder (AE) method. Finally, we evaluate the performance of the built model.

AutoEncoder is an unsupervised Artificial Neural Network that attempts to encode the data by compressing it into the lower dimensions (bottleneck layer or code) and then decoding the data to reconstruct the original input. The bottleneck layer (or code) holds the compressed representation of the input data. The number of hidden units in the code is called code size. AutoEncoders are widely used in fruad detection. The reconstruction errors are used as the anomaly scores.
The encoder of the model consists of layers that encode the data into lower dimensions. The decoder of the model consists of similar number of layers that reconstruct the input data. Shape of autoencoder
We use an autoencoder network for anomaly detection. The general structure of such a network consists of two components - an encoder and decoder [17]. The goal of the autoencoder is to find optimal model parameters for the minimization of a loss function. For our purpose we use the Mean Squared Error loss function (MSE).
Let us look at how we can use AutoEncoder for fraud detection using TensorFlow on data, voice and SMS attributes. We will use the voice and SMS dataset because it provides artificial time series data containing anomalous periods of behavior. Data are ordered, time stamped, single-valued metrics.so duration of the voice attribute is used as time stamp and fee attribute is chosen as payment value made by subscribers. Process time attribute is chosen for SMS dataset as timestamp with fee attribute as payment values made to detect the fraud using time series Auto encoder mechanism. The simplicity of this dataset allows us to demonstrate fraud detection effectively. The model is compiled with Mean Squared Logarithmic loss and Adam optimizer. The model is then trained with 20 epochs with a batch size of 128. We discussed Model building procedures in figure 3.2 as follows:

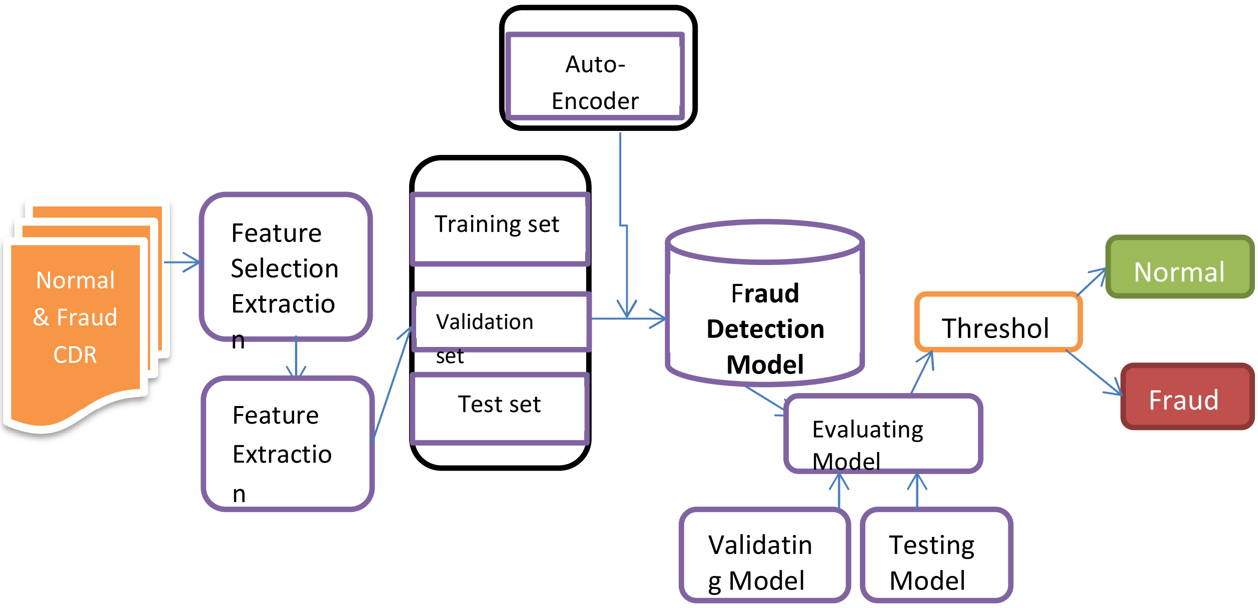


Figure 3. 2: workflow of the research

PERFORMANCE METRICS

Evaluating the trained fraud detection models is an essential part of this work. Fraud based model can be evaluated to check how much the model classifies instances in their corresponding normal or fraud classes. For this purpose, we choose accuracy, precision, recall and F1 measure metrics to measure the performance of the fraud detection model. Accuracy is the most intuitive performance measure among the aforementioned metrics and it is simply a ratio of correctly predicted observation to the total observations. True positive and true negatives are the observations that are correctly predicted. A good classifier minimizes false positives and false negatives values to be used trusted for model implementation for real world environment.

True Positives - TP - These are the correctly predicted positive values which means that the value of actual class is Fraudulent and the value of predicted class is also Fraudulent.
True Negatives - TN - These are the correctly predicted negative values which mean that the value of actual class is legitimate and value of predicted class is also legitimate. False positives and false negatives, these values occur when actual class contradicts with the predicted class..
False Positive - FP – when actual class is negative and predicted class is positive.
False Negative - FN – When actual class is Positive but predicted class in Negative.
Once we understand these four parameters then we can calculate performance of our fraud detection model using four metrics. Classification accuracy is mainly used to measure the performance of our model, however it is not enough to truly judge our model ,so other performance metric tools are also be
used in the evaluation. Performance metrics utilized in this work include accuracy, precision, recall and F1 score [**25**].
Accuracy - Accuracy is what is usually referred to as mean. Accuracy is the ratio of number of correct predictions to the total number of input samples. Accuracy is the measurement used to determine which model is best at identifying relationships and patterns between variables in a dataset based on the input, or training, data. The better a model can generalize to 'unseen' data, the better predictions and insights it can produce. Accuracy is calculated as follows:

$$\text{Acuracy} = 100 * \left(\frac{\text{TP+TN}}{\text{TP+FP+FN+TN}}\right) \quad (1)$$

Precision - Precision is calculated as the ratio between the number of *Positive* samples correctly predicted to the total number of samples predicted as *Positive* (either correctly or incorrectly). The precision measures the model's accuracy in classifying a sample as positive.
If a model makes many incorrect Positive predication, or few correct Positive predication the precision will be small. On the other hand, the precision is high when if the model makes many correct positive predications (maximize True Positive) or when a model makes fewer incorrect Positive predications (minimize False Positive). In general precision reflects how reliable a model is in classifying samples as Positive. Precision is mathematically calculated as follows

$$\text{Precision} = 100 * \left(\frac{\text{TP}}{\text{TP+FP}}\right) \quad (2)$$

Recall - The recall is calculated as the ratio between the numbers of *Positive* samples correctly classified as *Positive* to the total number of *Positive* samples. The recall measures a model's ability to detect *Positive* samples. The higher the recall, the more positive samples detected.
The recall cares only about how the positive samples are classified. This is independent of how the negative samples are classified, for the precision. When the model classifies all the positive samples as Positive, then the recall will be 100% even if all the negative samples were incorrectly classified as Positive. Recall is calculated as follows

$$\text{Recall} = 100 * \left(\frac{\text{TP}}{\text{TP+FN}}\right) \quad (3)$$

F1-score - F1-score is one of the most important evaluation metrics in machine learning. It elegantly sums up the predictive performance of a model by combining two otherwise competing metrics, precision and recall. F1-score is the harmonic mean of precision and recall. It combines precision and recall into a single number. We want to maximize both precision and recall but in practice, it is not possible to maximize both precision and recall at the same time because of the trade-off between precision and recall. F1-score is calculated as follows:

$$\mathrm{F1-score} = 100 * 2\left(\frac{\mathrm{presion*recall}}{\mathrm{presion+recal}}\right) \quad (4)$$

EXPERIMENTATION AND EVALUATION

As aim of this study is to build a model that performs best in detecting fraudulent subscribers. Fraud detection is the process of finding illegal use of telecom services. Abnormal data is defined as the ones that deviate significantly from the general behavior of the data. We understand from the collected dataset that subscribers who did not pay while they talked, uploaded, downloaded data using telecom services, but they did not bill for the services. The calling fee, SMS fee and data fee becomes zero. This means subscribers are used the services illegally.

To meet this goal, features from CDR data were collected and extracted; auto-encoder is selected for training and testing the model.

Table 4. 1 dataset for service type

	Service type	No of records
1	Voice	1048576
2	Data	1048576
3	SMS	1048576

As shown in Table4.1 above, a total of 1048576 for each CDR records were used in the experimentation process.

The lack of publicly available database has been a limiting factor for the publications on ethiotelcom fraud detection i.e creating a proper data set for this purpose is very difficult and there are no standard techniques to do this.

Deep learning based unsupervised learning models were implemented on the collected from telecom directly. Specifically, auto-encoder algorithm is used to determine the accuracy of the model. Auto encoder model was developed in python programming using keras and tensor flow and experimental results were obtained from fraudulent behavior of the dataset.

EXPERIMENTAL SETTING

Experiments have three categories, experiment I, experiment II and experiment III. Experiment 1 was evaluating Fraud detection models using variety of auto-encoder algorithms on three CDR Dataset with parameters mainly duration and fee. Experiment II, the experimentation was undertaken to obtained best performance result based on optimal threshold value. Experiment III, tried to identify the optimal epoch identification whether the trained model if free from under-fit and over fit problems.

DATA COLLECTION AND DATA PREPARATION

We collected and organized the collected dataset assuming that testing the fraud detection task on different service types messaging, calling and internet access from fixed network.

The lack of publicly available database has been a limiting factor for the publications on ethiotelcom fraud detection i.e creating a proper data set for this purpose is very difficult and there are no standard techniques to do this.

TOOLS USED

We installed Anaconda version 3 on Dell core i7 labtop computer. We also installed components that help us to implement the deep learning experimentation on notebook Editor. Some of the components are numpy, pandas, matplotlib for the sake of handling array of data and visualize the experimental results graphically. Keras and tensorflow modules were installed on the anaconda in order to obtain deep learning based autoencoder libraries. We also run varieties of auto-encoder algorithms on colab laboratory. The hardware capacity and other tools of colab that we used is presented as follows.

Computer network name: 8a7d49035982
Machine type: x86_64
Processor type: x86_64
Platform type: Linux-5.4.188+-x86_64-with-Ubuntu-18.04-bionic
Operating system: Linux
Operating system release: 5.4.188+
Total RAM installed: 13.62 GB

SYSTEM EVALUATION

The proposed model is evaluated using accuracy, precision, recall and F1-score on 20% of test set. The built model is also evaluated using validation set. Validation set is the set of CDR examples used for fraud detection model selection. If you have a total of 100 instances, you're probably stuck with cross validation as no single split is going to give you satisfactory variance in your estimates. If you have 100,000 instances, it doesn't really matter whether you choose an 80:20 split or a 90:10 split [**26**]. Accordingly, we split the dataset into 90 training set and 10% validation set which is 90:10 ratios after we subtract 20% test set from a record of 1048576 dataset.

Table 4. 2: Training set, validation set and test set split

sn	Dataset and its split	No of records	Data size
1	Total dataset	1048576	100%
2	Training set	838860	80% of total dataset
2	validation set	754974	90% of training set
3	test set split	209715	20% of total dataset

As shown in Table 4.2 above, a total of 1048576 records for each CDR Dataset were used in the experimentation process.

The validation set provides an unbiased evaluation of each model fit on the training set. Furthermore, it is used to compare performance of the different models and decide which one to implement and use in telecommunication switches [**26**]. A classification outcome has four cases, True Positive (TP), False Positive (FP), True Negative (TN) and False Negative (FN).

EXPERIMENTAL RESULT AND MODEL EVALUATION

EVALUATING FRAUD DETECTION MODELS USING VARIETY OF AUTO-ENCODER ALGORITHMS ON THREE VOICES, DATA AND SMS CDR DATASETS

Auto-encoder learns the reconstruction function that works with normal data, and we can use this Model for fraud detection [**27**]. We get low reconstruction error for normal data and high for abnormal data (minority class). Autoencoder learn to reconstruct normal subscription payment, and hence we can classify those CDR as fraud if the reconstruction error exceeds some threshold [**28**] following a threshold based system for prediction probability to filter out untrustworthy predictions [**29**]. Accordingly, we trained the auto-encoder model and evaluated DNN auto-encoder, stacked DNN auto-encoder, LSTM auto-encoder, stacked LSTM auto-encoder and CNN LSTM auto-encoder models using accuracy; precision, recall, and F1 score metrics.

EVALUATION OF DEEP NEURAL NETWORK(DNN) AUTO-ENCODER MODEL

The DNN auto-encoder model training uses dense layer after data preparation. For evaluating the autoencoder's model, the training loss and validation loss were computed per each autoencoder's model proposed. Best validation accuracy is 98.95% at threshold value of 0.0103. The performance score obtained becomes 92.75% test accuracy, 92.75% test precision, 100% test recall, 96.24% Test f1 score. DNN auto-encoder model reconstruction loss distribution visualization and loss decreases smoothly and approaches to zero as its training history is seen in figure 4.1. Specifically, loss decreases from 0.0008 to 0.0003.

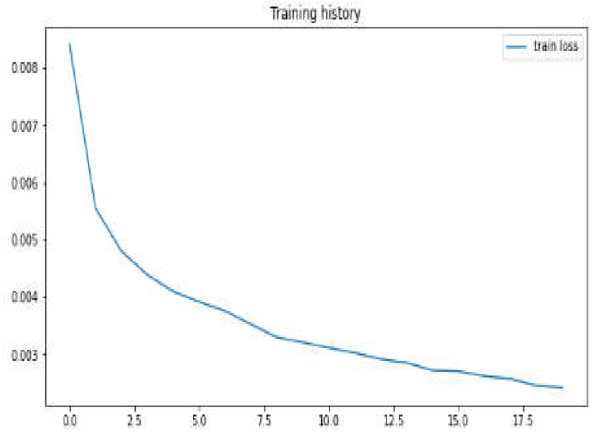


Figure 4. 1: DNN auto- encoder model training history

Data visualization is vital to understanding the relationship between normal and fraud CDR variables. Based on the threshold values, 0.0103, DNN auto-encoder model correctly predicted normal and fraud data true positive and true negative CDR record is corrected classified to the intended target class (normal).

EVALUATION OF STACKED DNN AUTO-ENCODER MODEL

The best validation accuracy obtained was 98.94% on threshold value of 0.046. The stacked DNN training history is illustrated in figure 4.2. We also tested the model and the performance results were test accuracy 93.45%, 93.45% precision, 100% recall, and 96.61% F1 score using the stacked DNN auto-encoder.

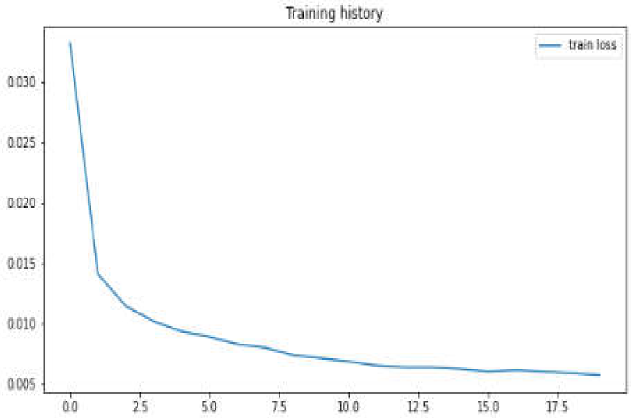


Figure 4. 2: Stacked DNN autoencoder model training history

The stacked DNN autoencoder model correctly predicted normal and fraud data, threshold for fraud detection was 0.046 after the loss diminishes from 0.03 to 0.005 as it is presented in figure 5.10. Stacked DNN auto-encoder can identify correctly labeled/predicted normal and fraud data as well as misclassified normal and fraud data [**29**]. This model detects and classifies false positive and false negatives CDR data.

EVALUATION OF LSTM AUTO-ENCODER MODEL

LSTM auto-encoder is one of the mix deep learning auto encoder algorithms which compress the input in to minimized dimension and classification task is undertaken on top of the compressed data. The LSTM model will use the CDR sequence from the train set as input and output for LSTM Autoencoder. Threshold selection is done with an aim of maximizing the accuracy of the model; best validation accuracy of 98.94% is obtained on threshold value of 0.0258.

The loss diminishes with the same quantity as stacked auto encoder model from 0.03 to 0.005 due to the integration of auto-encoder over LSTM as it is shown in figure 4.3 below.

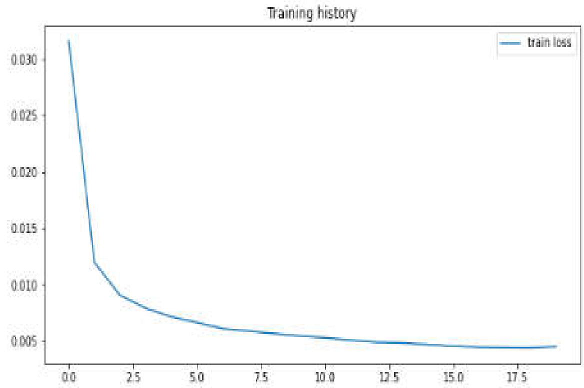


Figure 4. 3: Loss using LSTM-AE

Accordingly, we trained and tested the LSTM auto encoder on our CDR Dataset. The performance of the model is tested as 92.21% test accuracy, 92.1% precision, 100% recall, and 95.89% F1 score. These high performance score is due the integration the state-of-the-art LSTM algorithm with auto-encoder. LSTM Autoencoder learned some patterns from CRD training data and tried to recreate them in each sequence.

EVALUATION OF STACKED LSTM AUTO-ENCODER MODEL

The model training in the stacked LSTM involves the same data preparation and loading and training steps as LSTM Autoencoder. The feature set is further reshaped to be fit to a stacked LSTM and training the stacked LSTM model is trained from the train set as input. The reconstruction sequences of the stacked LSTM Autoencoder model are similar to the reconstruction sequences of the stacked autoencoder model.

The output of stacked auto encoder at bottleneck layer is given to LSTM. Stacked LSTM auto-encoder reconstructs loss on training data was recorded. Threshold selection is done with an aim of maximizing the accuracy of the model. Best validation accuracy was registered is 98.94% for threshold value of 0.0258.

As it is demonstrated in figure 4.4, the loss is decreasing from 0.030 to 0.005 since loses are eliminated in order to increase the performance of the model.

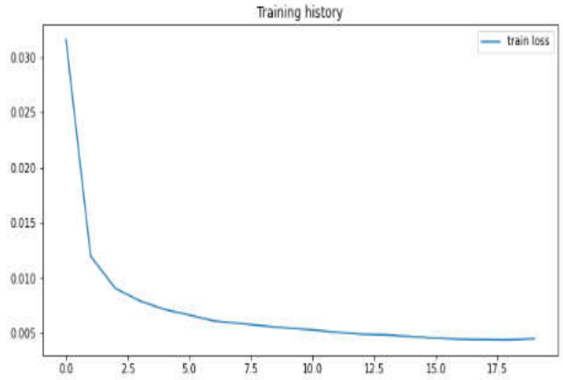


Figure 4. 4: Loss using Stacked LSTM-AE

The reconstruction sequences of the stacked autoencoder model are similar to the reconstruction sequences of the stacked LSTM Autoencoder. The test evaluation performance of the stacked LSTM model is 93.45% accuracy, 93.45% precision, 100% recall, and 96.61% F1 score.

EVALUATION OF CNN-LSTM AUTO-ENCODER MODEL

CNN-LSTM model was trained on CDR dataset and tested with previously unseen test data. Best validation accuracy achieved is 98.95% for threshold of 0.0173. The performance of the CNN-LSTM autoecncoder model is evaluated automatically using accuracy, precision, recall, and F1 score. Test performance results are 94.7% accuracy, 94.7% precision, 100% recall, and 97.73% F1 score. The CNN LSTM autoencoder training history is demonstrated in figure 5.5 is as follows.

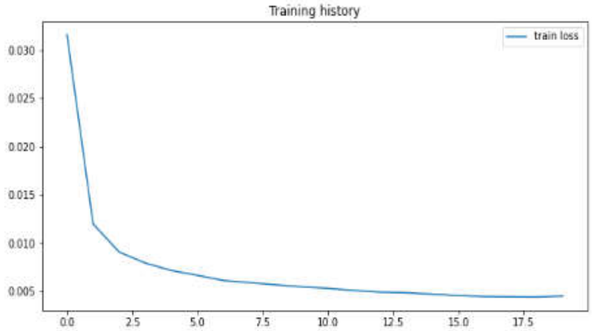


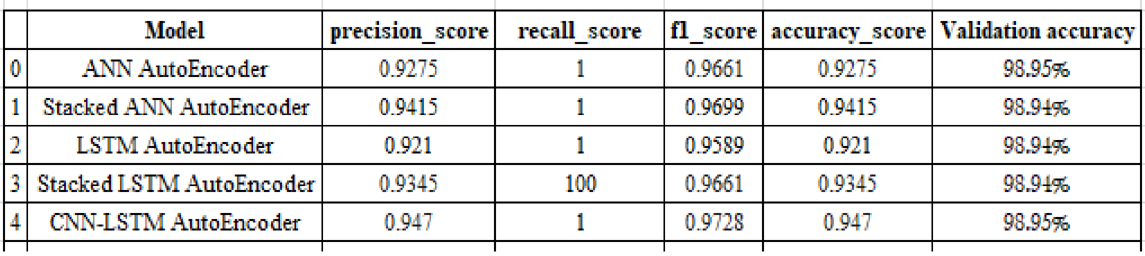
Figure 4. 5: CNN -LSTM auto-encoder loss history

The training also loss decreases from 0.030 to 0.005 which very closer to zero (x-axis).

FINDINGS

We trained five models to demonstrate the the effectiveness of auto encoder based unsypervised learning over the laber intensive way of supervised learning methods. Autoencoder uses the loss function to determine the threshold hyper plane value. The first model has the same structure as well as MSE loss function. Furthermore, we compares the the five autoncoder performance results with best agreed metrics on top of Loss functions which are often designed to be differentiable, and preferably convex and smooth [**30**]. If the reconstruction loss for a sample is greater than this threshold value, then we can infer that the model is seeing a pattern that it isn't familiar with. We label this sample as a fraud.

As it is presented in table 5, the highest performance result gained was high as 98.95% in validation accuracy using CNN-LSTM auto-encoder and ANN auto-encoder despite the rest algorithms perform almost the same validation performance result, 98.94%. Test performance also assures whether the validation performance is trustworthy or not. The test results are greater than 92% using the four implemented metrics, precision, recall, f1 score and accuracy.



	Model	precision_score	recall_score	f1_score	accuracy_score	Validation accuracy
0	ANN AutoEncoder	0.9275	1	0.9661	0.9275	98.95%
1	Stacked ANN AutoEncoder	0.9415	1	0.9699	0.9415	98.94%
2	LSTM AutoEncoder	0.921	1	0.9589	0.921	98.94%
3	Stacked LSTM AutoEncoder	0.9345	100	0.9661	0.9345	98.94%
4	CNN-LSTM AutoEncoder	0.947	1	0.9728	0.947	98.95%

Table 4. 3: Final model evaluation results

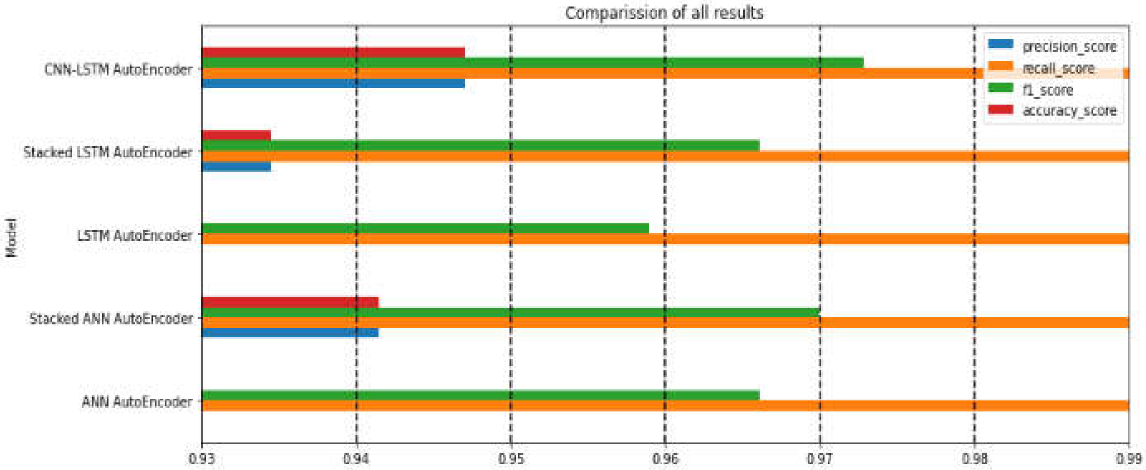


Figure 4. 6: Final model evaluation results

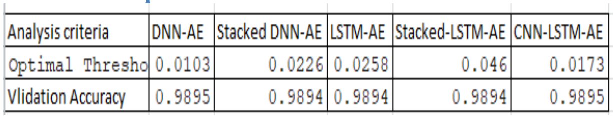
From the figure 4.7 demonstrated, we evaluate the five auto-encoder methods using four metrics for auto-encoder methods comparison.

The overall performance of each autoencoder model is affected at every stage or components. In general, all autoencoder models performed very well in detecting fraud in CDR, as it can be seen all implemented algorithms perform greater than 98% validation accuracy. The testing accuracy is grater that 92% validation accuracy.
DNN auto-encoder, stacked DNN auto-encoder, LSTM auto-encoder, CNN-LSTM auto-encoder is promising to develop and integrate in to ethioteclom swishes. The performance of the model is presented in figure 4.6.

We used threshold of analysis to identify the subscription data is fraud or not. After the model is built and looking at the reconstruction error on our training and validation set, we are able to decide a Threshold for fraud detection firstly taking into account only the reconstruction loss after passing a concrete subscription data through the autoencoder. The chosen threshold values in line of the implemented auto-encoder types are presented in table 4.4 which is going to be precise enough to detect frauds. The losses that would be obtained from CDR fraud after passing through the auto-encoder are analyzed. Firstly, we have divided the CDR dataset" in three different types of dataset (training set, validation set and test set) to evaluate how the system reacts and how good is the threshold decision for each one of them. Here test set is the unseen data from training set to evaluate the best threshold values. We formulate ten threshold values and the optimal threshold value is chosen to identify frauds from normal subscriptions.

Once we evaluated which is the best threshold for our fraud detection model formulation, we able to turn the problem as a simple binary classification task: If the reconstruction error of a CDR data is below the threshold, the CDR record is classified as a normal. Otherwise, if its loss value is higher than the threshold, the formulated model decides that it is a fraud. The optimal thresholds among ten experimented thresholds is selected and used for fraud detection task. The optimal thresholds used using the five employed auto-encoder algorithms are presented as it is seen in Table 4.4.

Table 4. 4: optimal thresholds



Analysis criteria	DNN-AE	Stacked DNN-AE	LSTM-AE	Stacked-LSTM-AE	CNN-LSTM-AE
Optimal Thresho	0.0103	0.0226	0.0258	0.046	0.0173
Vlidation Accuracy	0.9895	0.9894	0.9894	0.9894	0.9895

The frauds that were analyzed are the following ones: we could also get a threshold for detecting anomalies. In this case, if we compute the sum of the MSEs of the anomalous audios data set, we get the histogram

CONCLUSION AND RECOMMENDATION

CONCLUSION

In this paper, we have proposed deep autoencoder technique for subscription fraud detection. Our implementation for fraud detection combined state-of-the-art deep learning and data preparation routines. We adopted those techniques based on their automatic learning capability. We investigated five autoencoder algorithms on CDR, voice, data and sms datasets. Our auto encoder technique achieves the excellent result of 98.89% validation accuracy. We used the auto-encoder subscriber's fraud detection mechanism for EthioTelecom ISP. Our results show that discriminative approaches that leverage descriptors of retrained networks outperform methods that learn CRD feature representations from scratch solely on the payment-free and payment-full training data. Furthermore, we have discussed properties of common evaluation metrics and threshold estimation techniques for fraud segmentation and have highlighted their advantages over pure supervised learning algorithms such as CNN, LSTM. The reason is that supervised learning requires human labor to label their classes. FROM our experiment, both the training error keeps going down. This is a sign that the learning process is going well.

RECOMMENDATIONS

- The fraud detection task shall better be tested using generative adversarial network (GAN) because GAN shows good performance for fraud detection today.
- Ethitelcom needs not only subscription detection mechanisms but also other studies type of frauds are recommended on dynamic detecting and mitigating those frauds types continuously is very important.

REFERENCE

[1] Berhan Oumer Adame, "The Ethiopian Telecom Industry: Gaps and Recommendations towards Meaningful Connectivity and a Thriving Digital Ecosystem," *HELIYON*, 2021.

[2] International Telecommunication Union Development Sector, "Global Connectivity Report," 2022.

[3] Hendrik Wiersma and Ferdinand Nijboe, "The need for speed, THINK Economic & Financial Analysis," 2021.

[4] ethiotelecom, "https://www.ethiotelecom.et/fraud-awareness/: Accessed on 08/06/2022," 2022.

[5] Hailemeskel G/Tsadik, "Constructing Subscription Fraud Detection Model Using Machine Learning Algorithms: The Case of ethio telecom, ," *unpuplished, Addis Ababa, Ethiopia*, 2021.

[6] Alae, and EL Hassane Ibn EL Haj Chouiekh, "Convnets for fraud detection analysis," *Procedia Computer Science* , 2018.

[7] Mais, Abdallah Qusef, and George Sammour Arafat, "Detection of wangiri telecommunication fraud using ensemble learning," *2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT). IEEE*, 2019.

[8] AlBough and Mhd Redwan., "Comparing data mining classification algorithms in detection of simbox fraud,"

2016.

[9] N. Kang, and L. Yang S. Wu, "Fraudulent behavior forecast in telecom industry based on data mining technology," *Communications of the IIMA*, 2007.

[10] Richard A., Chris Volinsky, and Allan R. Wilks. Becker, "Fraud detection in telecommunications: History and lessons learned," *Technometrics* , 2010.

[11] H. Farvaresh and M. M. Sepehri, "A data mining framework for detecting subscription fraud in telecommunication," *Engineering Applications of Artificial Intelligence* , 2011.

[12] MEKALA.SAKETHA RAM, "MOBILE CREDIT USING GSM NETWORK TOPUP FOR MOBILE PHONES," *Faculty of Computing Blekinge Institute of Technology SE-371 79 Karlskrona Sweden* , 2015.

[13] Anael Sam, Loserian S. Laizer Baraka W. Nyamtiga, "Security Perspectives For USSD Versus SMS In Conducting Mobile Transactions: A Case Study Of Tanzania," *INTERNATIONAL JOURNAL OF TECHNOLOGY ENHANCEMENTS AND EMERGING ENGINEERING RESEARCH, VOL 1, ISSUE 3 38*, 2013.

[14] ABHISHEK SINGH and et al., "Factors Influencing Prepaid Consumer Behavior in Mobile Telecom Industry of Bihar & Jharkhand," *ICFAI UNIVERSITY, JHARKHAND RANCHI*, 2019.

[15] Godfred Yaw, et al. Koi-Akrofi, "Global telecommunications fraud trend analysis," *International Journal of Innovation and Applied Studies*, 2019.

[16] Yongjun Liao and et al., "Prepaid or Postpaid? That is the question.Novel Methods of Subscription Type Prediction in Mobile Phone Services," *arXiv:1706.10172v1 [cs.SI]*, 2017.

[17] Sen, Naidong Kang, and Liu Yang Wu, "Fraudulent behavior forecast in telecom industry based on data mining technology," *Communications of the IIMA* , 2007.

[18] Ledisi G., Domaka N. Nanwin, and Edikan Uduak Nquoh Kabari, "Telecommunications Subscription Fraud Detection Using Naïve Bayesian Network.," *International Journal of Computer Science and Mathematical Theory*, 2016.

[19] Kelemework Abebe., "Comparison of Supervised Machine Learning Algorithms on Detection of Signalling DoS attack to the 3G (UMTS) mobile network-in the case of ethio telecom," *Diss. Addis Ababa University, Addis Ababa,Ethiopia*, 2020.

[20] Derebe Tekeste, "Comparative Analysis Of Machine Learning Algorithms For Subscription Fraud Detection: The Case Of Ethiotelecom ," *Unpuplished paper,Addis Ababa University, Ethiopia*, 2020.

[21] Pablo A., Claudio M. Held, and Claudio A. Perez Estévez, "Subscription fraud prevention in telecommunications using fuzzy rules and neural networks," *Expert Systems with Application*, 20006.

[22] Apapan, and Yan Liu Pumsirirat, "Credit card fraud detection using deep learning based on auto-encoder and restricted boltzmann machine," *International Journal of advanced computer science and applications 9.1*, 2018.

[23] Yew Kee Wong, "The Difference Of Machine Learning And Deep Learning Algorithms," *School of Information Engineering, HuangHuai University, Henan, China*.

[24] Pramila P., and Seema Shah Shinde, "A review of machine learning and deep learning applications," *2018 Fourth international conference on computing communication control and automation (ICCUBEA). IEEE*, 2018.

[25] Željko Đ. Vujović, "Classification Model Evaluation Metrics," *(IJACSA)International Journal of Advanced Computer Science and Applications*, 2021.

[26] TomZahavy and Shie Mannor Guy Tennenholtz, "TRAIN ON VALIDATION: SQUEEZING THE DATA LEMON," *rXiv:1802.05846v1* , 2018.

[27] Guansong, et al. Pang, "Deep learning for anomaly detection: A review," *ACM Computing Surveys (CSUR)*, 2021.

[28] Celia, et al. Cintas, "Anomalous Pattern Detection in Activations and Reconstruction Error of Autoencoders," *Under review as a conference paper at ICLR 2020*, 2020.

[29] Limin, et al Yang, "CADE:Detecting and Explaining Concept Drift Samples for Security Applications," *0th USENIX Security Symposium (USENIX Security 21*, 2021.

[30] J. Zhu, "Deep Learning-Based Autoencoder for Data-Driven Modeling of an RF Photoinjector," *arXiv:2101.10437v1*, 2021.