UNIVERSITY OF NAIROBI

SCHOOL OF COMPUTING AND INFORMATICS

Mobile network Fraud Detection Using Artificial Neural Networks

BY

Mundia James Gichuki

P58/76399/2012

Supervisor

Mr. Evans Miriti

Sept 2014

Submitted in partial fulfillment of the requirements of the Master of Science in Computer Science

DECLARATION

I declare that this project is my original work and, to the best of my knowledge, the work has not been submitted for any other award in any University.

Signature _____________________________ Date ____________________

Mundia James Gichuki

Reg. No: P58/76399/2012

This project report has been submitted in partial fulfillment of the requirement of the Master of Science Degree in Computer Science of the University of Nairobi with my approval as the University supervisor.

Signature _____________________________ Date ____________________

Mr. Evans Miriti

School of Computing and Informatics

University of Nairobi

DEDICATION

This project is dedicated to my family, my dear parents and my siblings. Your love, patience and motivation have kept me going.

ACKNOWLEDGEMENT

I am indebted to all those who helped, inspired and supported me to complete my studies.

Firstly I thank the almighty God for the good health during my study, financial blessings to pay my fees among others and strength to keep on going against all odds.

My sincere gratitude goes to my supervisor Mr. Evans Miriti for creating time to guide me despite his busy schedule. His dedication and commitment to ensure that I stay on the right path of research was highly noted and appreciated.

I am thankful of my family for being there for me even when I have less time for them. I also give thanks to the school of computing and informatics lectures who gave their time to educate and advise me on various aspects of my study.

Finally I thank the School of Computing and Informatics community, for giving me a favorable environment to successfully carry out this study.

ABSTRACT

The past decade has witnessed the rapid deployment and evolution of mobile cellular networks, which now support billions of users and a vast diverse array of mobile devices from smartphones, tablets, to e-readers and smart meters

Due to this high number of mobile devices and low mobile phone service connection rates Mobile phone communication is now faced with two major threats which are Voice-related security threats, ranging from conventional voice scams similar to those on landlines, e.g., stealing customers privacy information or defrauding users of money through various social engineering techniques, the new forms of voice fraud that utilize the data functionality of smartphones for voice-related trickeries. The other threat is the SMS-related security threats which range from sending threatening messages to other mobile phone users to extort money from them to sending '*false win'* messages to other subscribers and demand funds in return.

Detecting and rooting out voice-related and SMS-related fraud activities, is not an easy task, due to the large user population, the vast phone number space and limited data which is recorded when a call is made or an SMS is send.

The objection of this study was to determine the performance of Artificial Neural Networks in classifying and detecting the fraud rent activities. We developed a system that uses Artificial Neural Network to classify phone numbers and detect the once being involved in the fraud rent activities using the call attributes captured by the mobile service provider. The system was tested using the data captured in a span of three months and the results compared with actual fraud rent cases reported to the service provider. In the model different time variant datasets were used to train the network and perform the classification. Also training the Network using different size variant dataset was performed. This was to examine the correct data size and age that is optimum and accurate in the classification.

We found out that Artificial Neural Network was an optimum tool when it comes to classifying these fraud rent activities due to its ability to dynamically learn fraud rent patterns that change day by day. We also found out that Training data size and age were major factors that affected the accuracy in classification

TABLE OF CONTENTS

LIST FIGURES

LIST OF TABLES

ACRONYMS

GSM	Global System for Mobile
RSS	radio subsystem
NSS	network and switching subsystem
OSS	operation subsystem
MS	mobile station
BS	base station
MSC	Mobile Services Switching Center
IWF	Interworking Functions
ISDN	Integrated Services Digital Network
PSTN	Public Switched Telephone Network
PSPDN	Packet Switched Public Data Net
CSPDN	Circuit Switched Public Data Net
NS	Network Subsystem
MSC	Mobile Switching Center
HLR	Home location register
VLR	Visitor location register
AuC	Authentication center database
EIR	Equipment identity register database
MCL	Markov Clustering
SMS	Short Message Service
CCK	Communication commission of Kenya
MSC	mobile switching center
LR	location register

Chapter 1: INTRODUCTION

1.1 Introduction

The past decade has witnessed the rapid deployment and evolution of mobile cellular networks, which now support billions of users and a vast diverse array of mobile devices from smartphones, tablets, to e-readers and smart meters. It was reported (BBC,2013) that in 2013 there were over 5 billion mobile phones in operation, in comparison to the total world population of 6.8 billion. Mobile phones and tablets are gradually replacing traditional wire-lines as well as personal computers, and are becoming an indispensable component in our daily life. With breath-taking advances in smart mobile devices and the growing sophistication in the mobile applications (apps) and services (e.g., location services and cloud services) they spur, we are now entering in a new era of mobile computing.

With their wide adoption, smartphones, while providing valuable utility and convenience to mobile users, also bring with them new security threats. Little work has been devoted to detecting and understanding various voice-related and SMS-related fraud activities targeting mobile users. Voice-related and SMS-related fraud activities can have a much wider impact on the cellular network, as potentially all mobile users can be victims of such activities. Another form of fraud occurs when a mobile user pretends to be a genuine user but spreads threats using either Voice or SMS or even both with an aim of extorting money or other benefits from other mobile phone users. Detecting and rooting out such voice-related and SMS-related fraud activities, especially those that target users through the data plane triggered voice fraud, is not an easy task, due to the large user population, the vast phone number space and limited data.

As a result an efficient approach needs to be adopted due to the scanty and noisy data to be dealt with.

There are approximately 28.08 Million mobile subscriptions in Kenya (CCK, April 2013), representing a mobile penetration rate of 71.3%. It is assumed that this number represents that of active SIM cards, those that have been used in the past three months or so. The mobile subscription rates in Kenya have been rising exponentially since the introduction of the fourth mobile phone operator, early in the last decade. In the past year, mobile penetration in Kenya has increased by more than 12% (CCK, April 2013).

With this number of mobile penetration, fraud becomes one on the major concern to the government, mobile phone operators and even mobile users.

1.2 Problem Statement

Two major mobile network security threats being experienced today are - :

1) Voice-related security threats, ranging from conventional voice scams similar to those on landlines, e.g., stealing customers privacy information or defrauding users of money through various social engineering techniques, the new forms of voice fraud that utilize the data functionality of smartphones for voice-related trickeries.
2) SMS-related security threats: - These threats rage from sending threatening messages to other mobile phone users to extort money from them to sending '*false win*' messages to other subscribers and demand funds in return. These threats can also be seen on the on the glasses on spreading hate speeches and other forms messages that can result to violence and social instability.

Detecting and rooting out voice-related and SMS-related fraud activities is not an easy task, due to the large user population, the vast phone number space and limited data which is recorded when a call is made or an SMS is sent. Another challenge arises on the resources required to perform such analysis where by huge chucks of memory and CPU are required. So far most research efforts have focused on applying and developing anomaly detection and prevention techniques using classification tools.

1.3 Objectives

The main objective of this research was to test and evaluate the performance of Artificial Neural Networks in detecting mobile fraud. The specific objectives were to:

i) Build a system that uses Artificial Neural network in detection of mobile phone fraud by using the call and SMS record attributes

ii) Establishing the mobile phone fraud patterns and the calls' attributes influence in fraud detection

iii) Establishing how training data age and size affect the accuracy of a Neural Network used in mobile phone fraud detection

1.4 Justification

It was reported (CCK, April 2013) that over 200,000 cases of fraud-rent or attempted fraud-rent activities were reported between Jan 2012 to Feb 2013 with Safaricom being hit hard by this menace with over 75% of these cases. This was attributed to its vast network coverage combined with inadequate knowledge among its customers. Celtel Kenya followed in the ranking with the other mobile providers (Yu and Orange) following closely.

Most of these activities originated for certain locations with the prison and the slum areas leading in the list. They were carried out using one SIM card where by broadcast SMSs or calls are made targeting the less informed customers. The menace is aggravated by the dynamic nature of the fraudsters' behavior whereby they develop new tactics and tricks to carry their activities. Some of these fraud-rent activities originate from an Internet driven messaging or calling systems which makes it difficult to track them

As a result a fraud detection technique that adapts and learns fraud-rent activity patterns will be appropriate. In addition the technique should be capable of analyzing the data from the network, even if the data is incomplete or distorted. In other words, the system would possess the ability to conduct an analysis with data in a non-linear fashion. In addition, because some attacks may be conducted against the network in a coordinated assault by multiple attackers, the ability to process data from a number of sources in a non-linear fashion is important.

1.5 Scope of the Research

The scope of this research is limited to the call records provided by the one of the service provider in Kenya. Each call record consists of 8 attributes which characterize location, call duration and the caller details. In addition the number of records to be used for both training and testing will not exceed 500,000 records due to resource limits

A more accurate analysis can be achieved if more detailed attributes were available, for instance SIM card swapping and calling history which can highly define and influence the calling patterns

Chapter 2: LITERATURE REVIEW

2.1 Introduction

In this section we will look on detailed mobile network architecture and components (Michael, 2013) its growth shedding more light on the Kenyan market. This will enable us to understand and locate fraud point and the weak point area. Will also review previous algorithms used in fraud detection and their limitation.

2.2 GSM Network Architecture

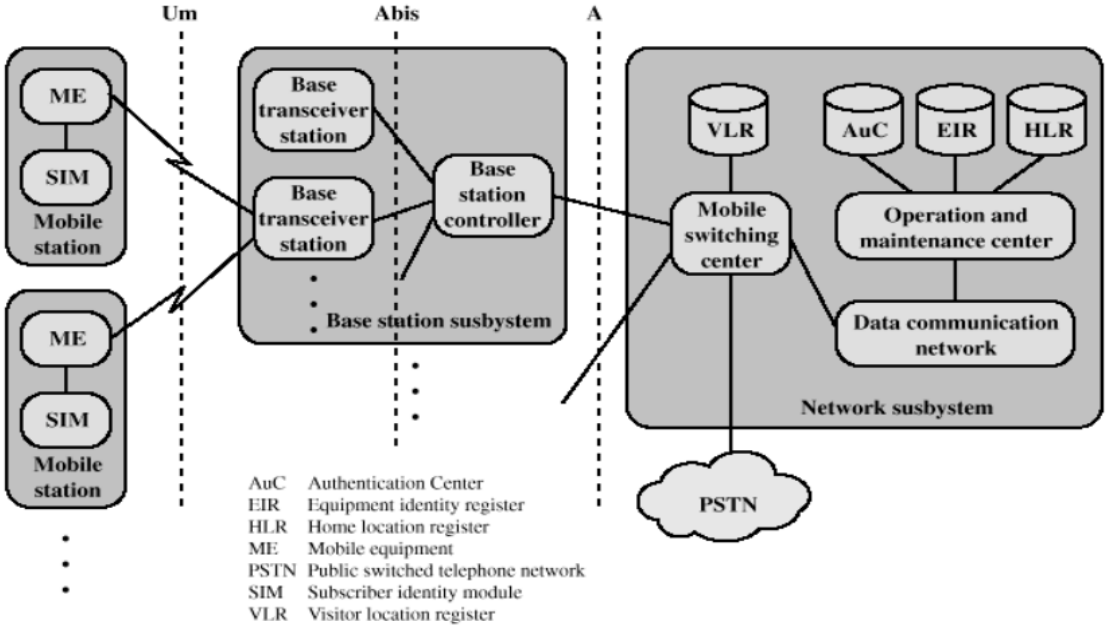

Um
Abis
A
ME
SIM
Mobile station
ME
SIM
Mobile station
Base transceiver station
Base transceiver station
Base station controller
Base station susbystem
VLR
AuC
EIR
HLR
Mobile switching center
Operation and maintenance center
Data communication network
Network susbystem
PSTN
AuC Authentication Center
EIR Equipment identity register
HLR Home location register
ME Mobile equipment
PSTN Public switched telephone network
SIM Subscriber identity module
VLR Visitor location register

Figure 1: Overall GSM Network. Source: (Michael, 2013)

Several providers setup mobile networks following the GSM standard within each country

2.2.1 Components

- MS (mobile station)
- BS (base station)
- MSC (mobile switching center)
- LR (location register)

2.2.1.1 Subsystems

- RSS (radio subsystem): covers all radio aspects
  - Base station subsystem
- NSS (network and switching subsystem): call forwarding, handover, switching
- OSS (operation subsystem): management of the network

2.2.2 GSM: Elements and Interfaces

The below figure show a high level interfaces' integration in a Mobile network architecture

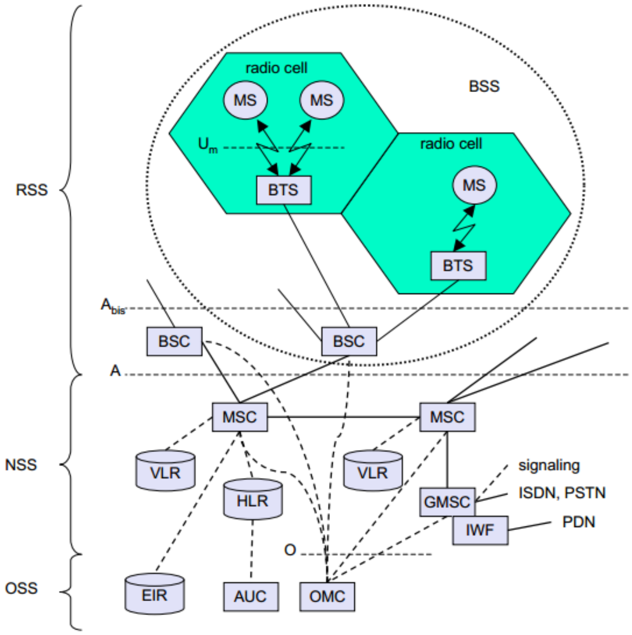


Figure 2: GSM Elements and Interfaces. Source: (Michael, 2013)

2.1.3 GSM: Detailed System Architecture

The GSM systems is built from three major components: - Radio Subsystem, Network and Switching Subsystem and Fixed Partner network as per the figure below

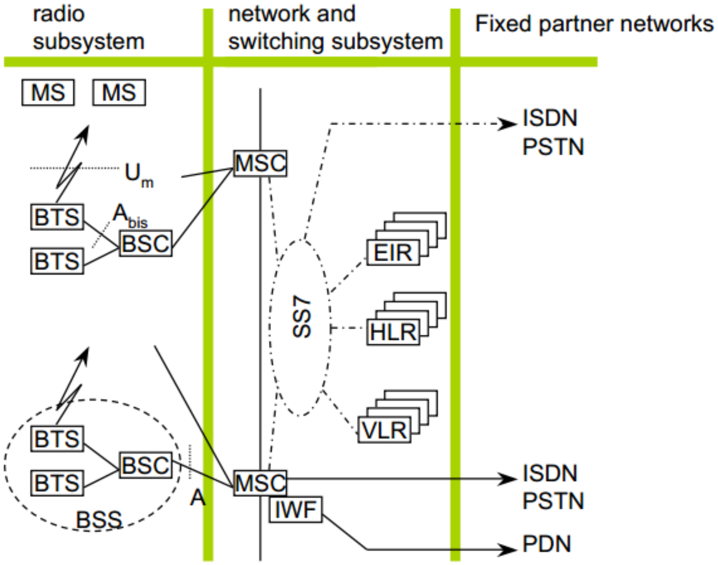
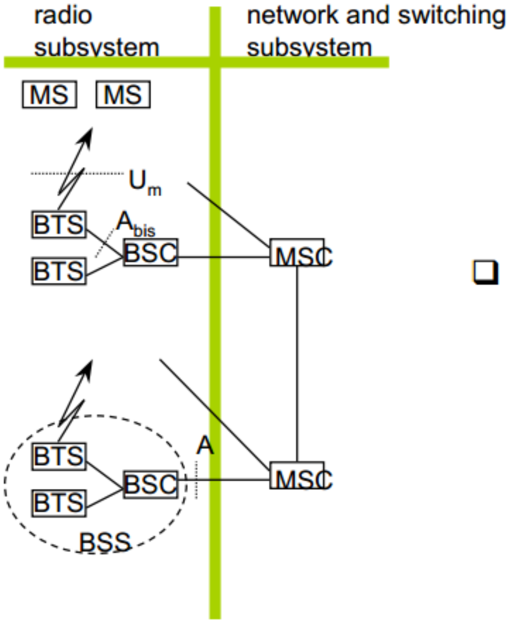


Figure 3: GSM System Architecture. Source: (Michael, 2013)

2.2.3.1 Radio Subsystem:



❑

Figure 4: GSM Radio Subsystem Source: (Michael, 2013)

The Radio Subsystem consists of the below components:-

Mobile Station

Mobile station communicates across Um interface (air interface) with base station transceiver in same cell as mobile unit

Mobile equipment (ME):– physical terminal, such as a Mobile phone, Tablet etc. ME includes radio transceiver, digital signal processors and subscriber identity module (SIM)

- **Base Station Subsystem (BSS)**

BSS consists of base station controller and one or more base transceiver stations (BTS). Each BTS defines a single cell, which consist of radio antenna, radio transceiver and a link to a base station controller (BSC). BSC reserves radio frequencies, manages handoff of mobile unit from one cell to another within BSS, and controls paging

2.2.3.2 Network and Switching Subsystem:

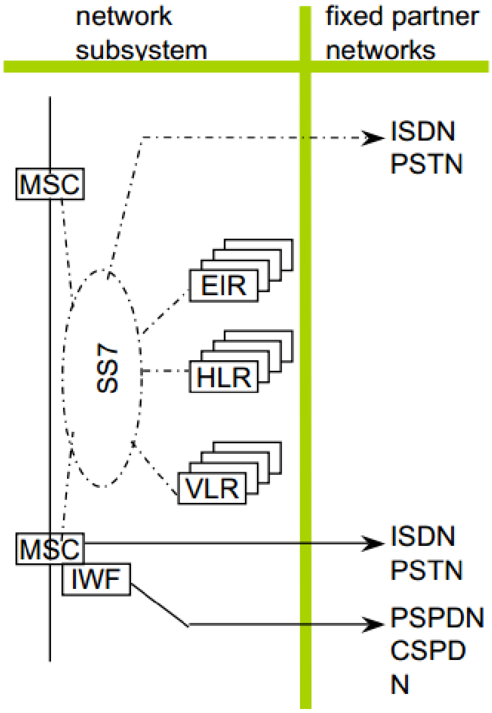


Figure 5: GSM Network and Switching Subsystem. Source: (Michael, 2013)

The Network and Switching Subsystem consists of the below components:-

- MSC (Mobile Services Switching Center):
- IWF (Interworking Functions)
- ISDN (Integrated Services Digital Network)
- PSTN (Public Switched Telephone Network)
- PSPDN (Packet Switched Public Data Net.)
- CSPDN (Circuit Switched Public Data Net.)

Network Subsystem (NS) is responsible for the below roles

- Provides link between cellular network and PSTNs
- Controls handoffs between cells in different BSSs
- Authenticates users and validates accounts
- Enables worldwide roaming of mobile users
- Central element of NS is the mobile switching center (MSC)

This layer also consists of Mobile Switching Center (MSC) Databases

- Home location register (HLR) database – stores information about each subscriber that belongs to it
- Visitor location register (VLR) database – maintains information about subscribers currently physically in the region
- Authentication center database (AuC) – used for authentication activities, holds encryption keys
- Equipment identity register database (EIR) – keeps track of the type of equipment that exists at the mobile station

2.1.4 GSM Speech Processing

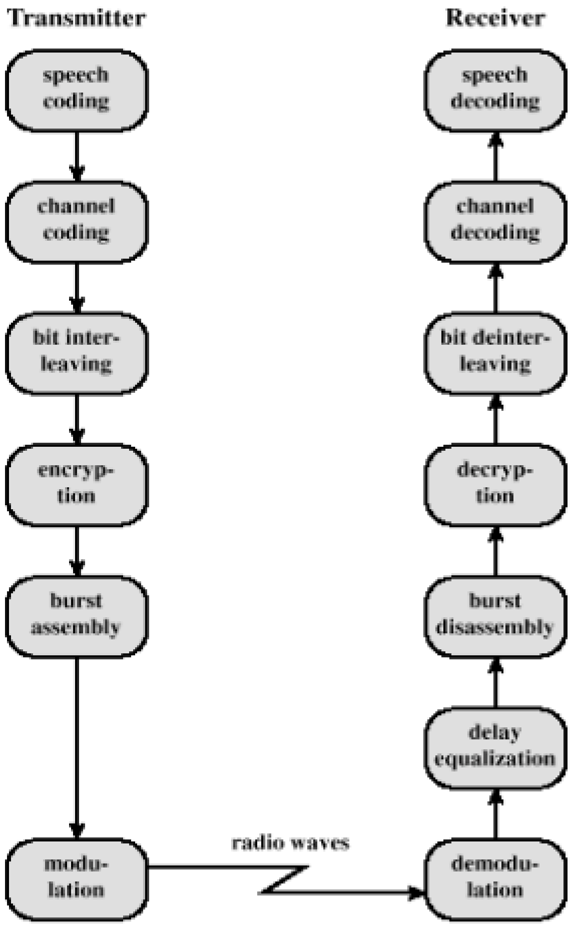


Figure 6: GSM Speech Signal Processing

GSM Speech Processing Steps

- Speech compressed using a predictive coding scheme
- Divided into blocks, each of which is protected partly by CRC and partly by a convolutional code
- Interleaving to protect against burst errors
- Encryption for providing privacy
- Assembled into time slots
- Modulated for analog transmission using FSK

2.2.5 Mobile Terminated Call Process

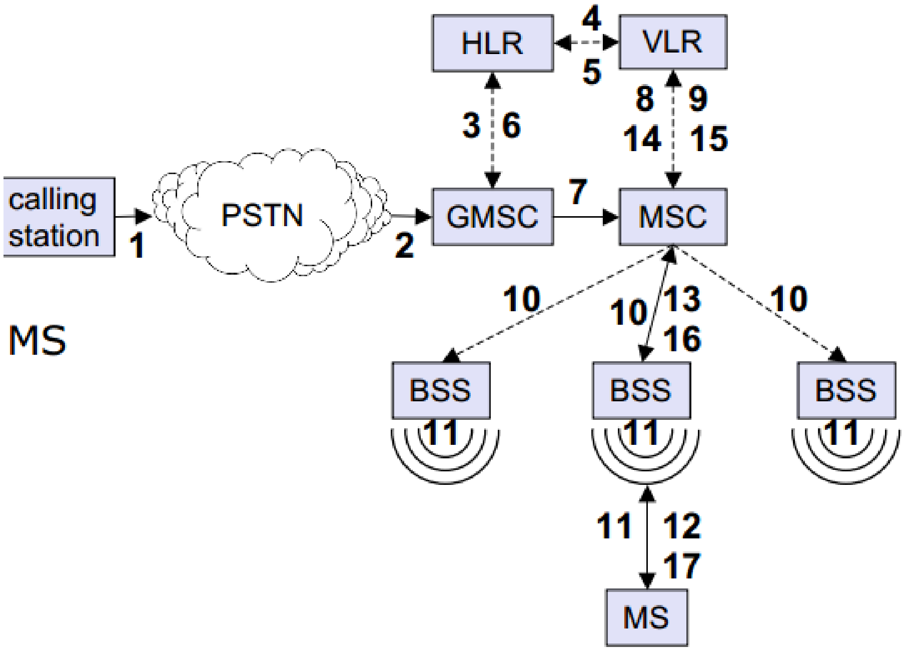


Figure 7: GSM Call Termination Process Source: (Michael, 2013)

Below are the steps involved in a call termination

1: calling a GSM subscriber

2: forwarding call to GMSC

3: signal call setup to HLR

4, 5: connect with current VLR

6: forward responsible MSC to GMSC

7: forward call to current MSC

8, 9: get current status of MS

10, 11: paging of MS

12, 13: MS answers

14, 15: security checks

16, 17: set up connection

2.2.6 Mobile Originated Call

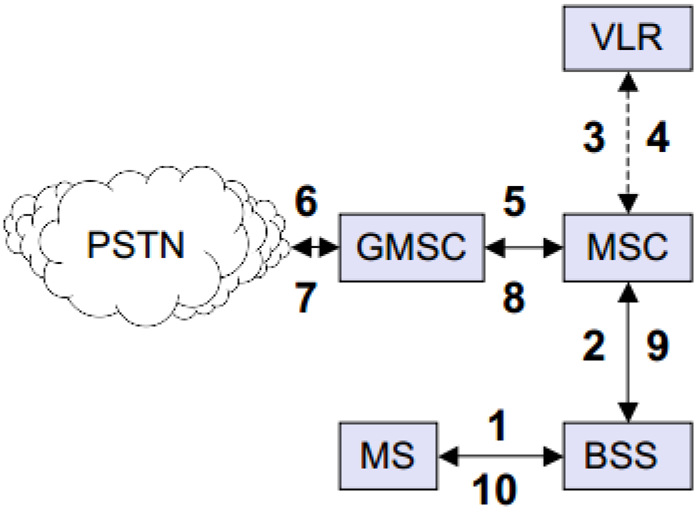


Figure 8: GSM Call Originating Process. Source: (Michael, 2013)

Below are the steps involved in to originate a call

1, 2: connection request

3, 4: security check

5-8: check resources (free circuit)

9-10: set up call

2.2.7 Mobile Terminated Call/ Mobile Originated Call combined process

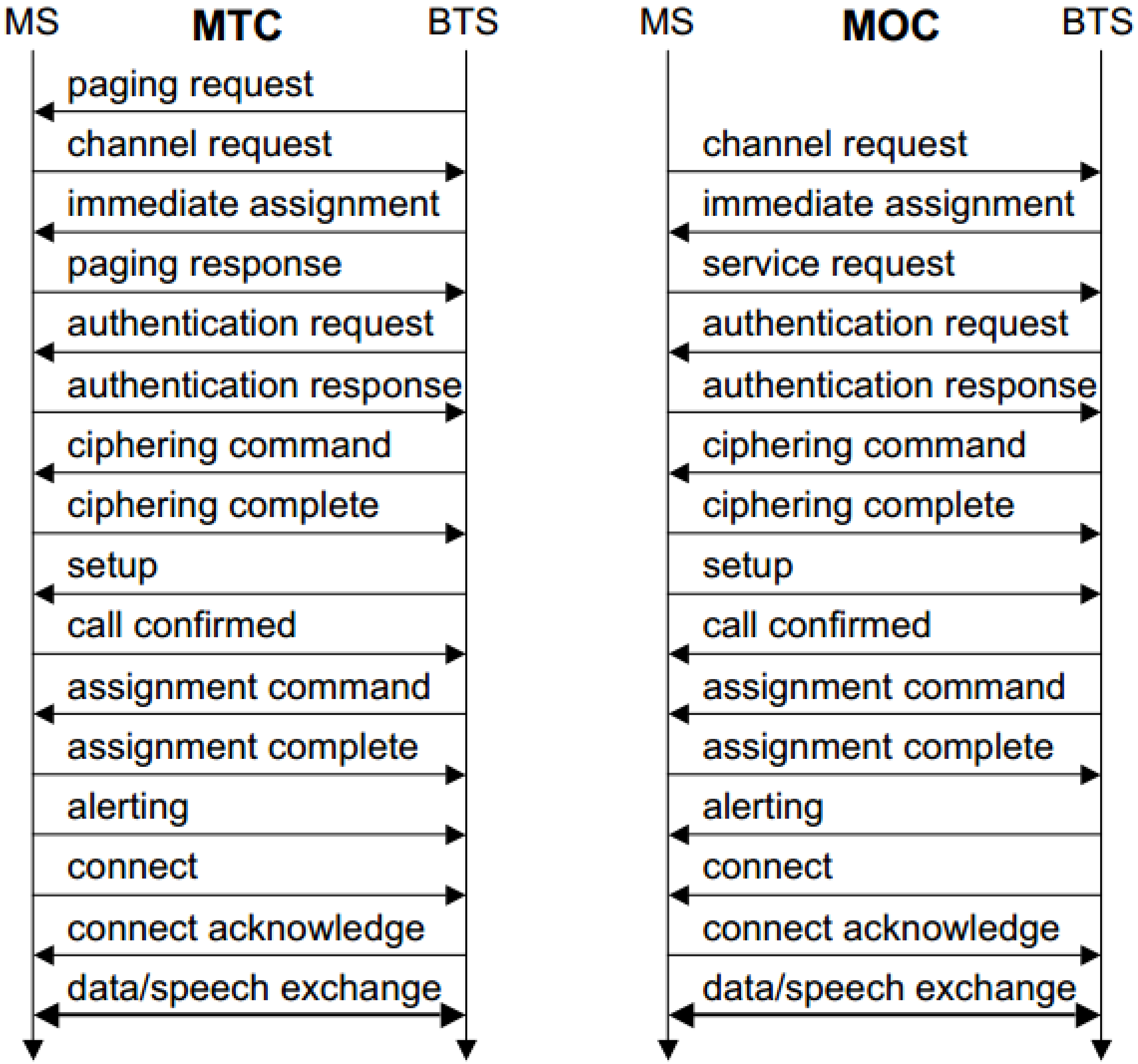


Figure 9: GSM complete Call Processing Cycle. Source: (Michael, 2013)

2.2.8 Security in GSM

Security in GSM architecture is paramount and is categorized into the below services

- Access control/authentication:- this is embedded on the user SIM (Subscriber Identity Module): secret PIN (personal identification number) and SIM network: challenge response method
- Confidentiality:- voice and signaling encrypted on the wireless link (after successful authentication)
- Anonymity:- this is embedded on temporary identity TMSI (Temporary Mobile Subscriber Identity), newly assigned at each new location update (LUP) and encrypted transmission

2.3 Mobile phone growth in Kenya

There are approximately 28.08 Million mobile subscriptions in Kenya, representing a mobile penetration rate of 71.3%. It is assumed that this number represents that of active SIM cards, those that have been used in the past three months or so. The mobile subscription rates in Kenya have been rising exponentially since the introduction of the fourth mobile phone operator, early in the last decade. In the past year, mobile penetration in Kenya has increased by more than 12% (CCK, April 2013).

On the other hand there are 283,546 fixed lines in use in the country, a number that has been drastically reducing as the mobile penetration increases. This represents a fixed line tele-density of 0.72%.

It is expected, according to the CCK analysis that total mobile subscriptions in the country will reach 39.5 million by 2016, a penetration rate of 83.1%. [Business Monitor International, May 2013]. Majority of usage of mobile phones in Kenya is via feature and basic phones (those with EDGE capabilities and below). Based on various sources, the most commonly used phone in Kenya for online use is the Nokia phone (the S40 series).

Data from (Admob, 2013) showed that Nokia was the leading handset manufacturer in Kenya in February 2013 with 57% of mobile web users using it to access internet. This was followed by Samsung with 13% of the market, MAUI (a smart-phone operating system used on MediaTek based devices [Chinese Handsets]) with 6% while Android based devices with 4% share. Sony Ericsson also had 4% market share while Alcatel and Huaweii each had a 3% share. Apple's market share then was at 2% similar to Motorola's while LG 1%. In this Survey, RIM and ZTE did not make it to the top 10.

A similar dataset obtained from StatCounter shows that in May 2013, the Symbian OS was the most commonly used mobile OS to browse the web followed by Nokia S40 series. It is to be noted that many Nokia phones have a Symbian OS.

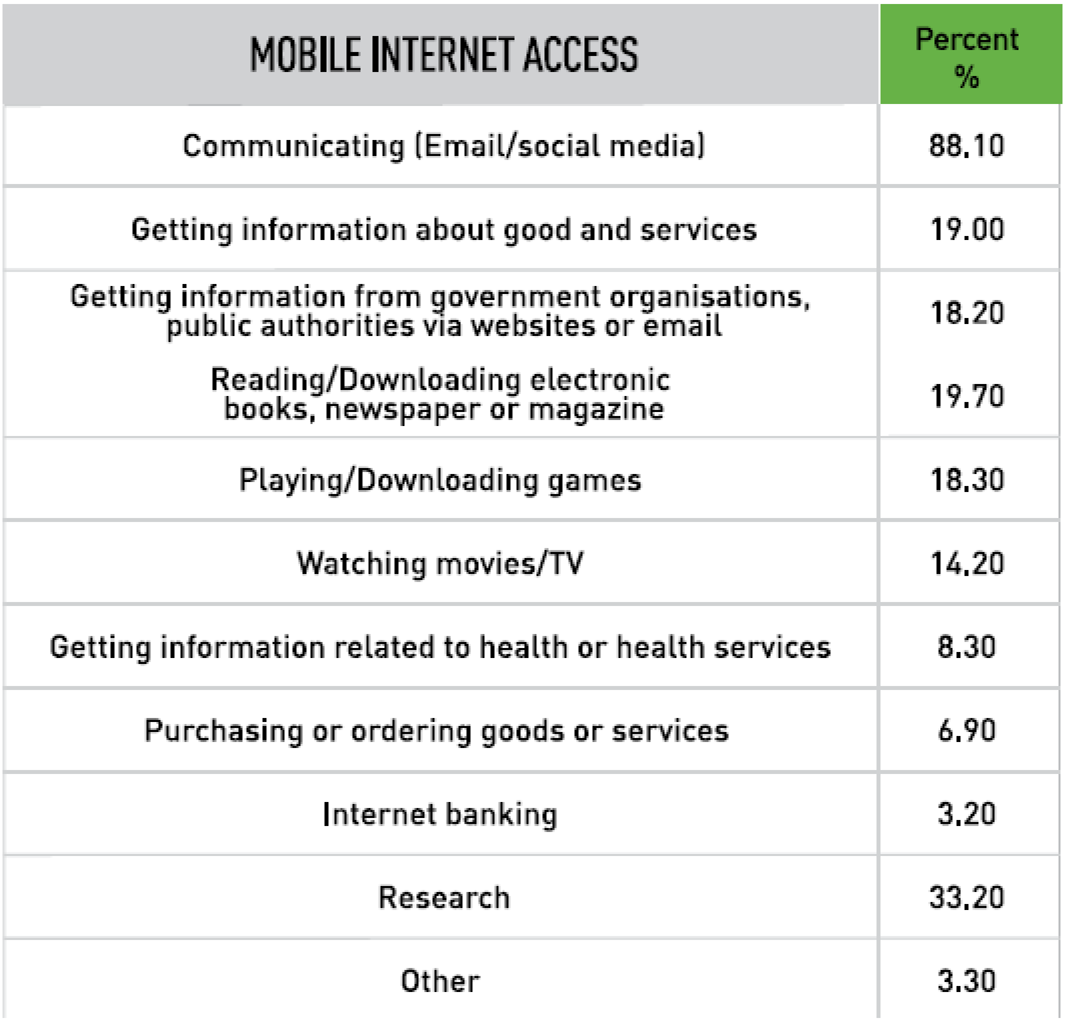
Most Kenyans subscribe to the pre-paid option. In fact, 99% of the 28 million subscribers (27.8 million) are on pre-paid. Less than 300,000 subscribers are on the post-paid subscription. (CCK, April 2013).

The largest distinguishing factor of mobile in Kenya as compared to the rest of Africa and the world is the massive adoption and use of mobile money. Of the 24 million mobile subscribers, more than 70% (28.08 million users) are subscribed to mobile money, transferring more than Kshs. 176 Billion (2 Billion USD) between October and December 2013. The success of Mobile Money in Kenya has been attributed to the fact that it has provided the much needed financial facilities to a large number of the country's unbanked population.

There are increased investments in the mobile sector to finance growth of technology infrastructure and improved provision of mobile services. Further, revenues from the mobile sector feature largely in the 20% contribution of the ICT sector to the Kenyan Economy. This is further supported by a favorable regulatory framework in existence that promotes healthy competition based on demand and a favorable mobile market.

The local sector regulator CCK, as well as a number of independent research organizations, has studied how Kenyans use their phones. These studies are not conclusive in themselves but give a general insight into the use of mobile phones.

According to the latest statistics from CCK, 99% of internet access is from a mobile device (phone, modem, tablets etc.) This represents about 17 million internet users in Kenya. Further, CCK carried out a National ICT survey in 2013 and the findings report is illustrated in the table below:



MOBILE INTERNET ACCESS	Percent %
Communicating (Email/social media)	88.10
Getting information about good and services	19.00
Getting information from government organisations, public authorities via websites or email	18.20
Reading/Downloading electronic books, newspaper or magazine	19.70
Playing/Downloading games	18.30
Watching movies/TV	14.20
Getting information related to health or health services	8.30
Purchasing or ordering goods or services	6.90
Internet banking	3.20
Research	33.20
Other	3.30

Figure 10: Mobile Internet Access. Source (CCK, 2013)

Companies in Kenya have diversified their marketing campaigns by making use of all available platforms to advertise and market their products and services. There is increased adoption of mobile marketing campaigns with companies taking advantage of USSD, text, apps and mobile web to advertise.

All the Mobile Network Operators have been using SMS campaigns to promote new and existing services. Further whenever a user queries via USSD for airtime balance, the reply may come with a text promoting a service. Similarly, independent companies have collaborated with these network providers to advertise their products via text.

Majority of text campaigns are not opt-in lists and there have been numerous of complaints on unsolicited marketing text messages by subscribers.

There are four mobile network operators in Kenya: Safaricom, Airtel, Orange, Essar Yu. and have provided an enabling environment for development of mobile applications through the friendly call, text and data rates (all below 5cts US per unit) as well as the availability of mobile money services. This is promoting greater use of these mobile products as they are more affordable than ever to the general population.

Further, Safaricom is launching a sandbox for developers to create even more useful applications on the mobile sphere, the Safaricom Service Delivery Platform (SDP). This is with the hope that the developers will create more applications for mass usage that will ride on the mobile network operator. Moreover, Safaricom also has plans to release a local apps store so as to increase levels of access to locally developed applications while at the same time giving the developers great traction of their products.

2.4 Mobile Phone Fraud

Due to this increase of the mobile phone usage, security issues arises where by different fraud rent activities are exhibited

2.4.1 What entails mobile phone fraud?

Mobile phone fraud involves a variety of scams that either persuade you to buy phone-related products/services that turn out to be substandard or non-existent; or to make phone calls or texts to premium services by accident; or to unknowingly sign up to expensive subscription services. It also involves issuing threatening calls or text in the aim of extorting money or other benefits from other unknowing subscribers

Below are major fraud rent activity of a major concern to both the Kenyan Government and the mobile operators

1. Sending ‘false win’ text or making calls to other mobile phone users informing them that they have won something and solicit funds in return :- In this form of fraud the attacker send similar text to thousands of unsuspecting mobiles user expecting some of them especially the less knowledgeable to action by sending the demanded funds

2. Sending threatening messages or threatening calls demanding funds: - in this form of fraud the attacker will send threatening messages and call to unsuspecting phone users and demand fund or else suffer the indicated consequence.

3. Another form of fraud is stealing customers privacy information or defrauding users of money through various social engineering techniques, the new forms of voice fraud that utilize the data functionality of smartphones for voice-related trickeries. For instance, fraudsters deploy malicious apps, disguised as interesting games and other applications to entice users to download them; when invoked, these apps automatically – and without users' knowledge – dial certain (international) phone numbers which charge exorbitantly high fees.

The above are some of the major fraud rent activities exhibited in the mobile phone infrastructure

2.5 Previous Works

Several algorithms have been developed to detect these forms of fraudrent activities.

We will look on them and their short coming

2.5.1 A Markov Clustering Based Fraud Detection Algorithm

In this section, we look at a Markov Clustering (MCL) based algorithm for decomposing voice graphs and identifying potential fraud activities.

Alg. 1 shows the MCL algorithm, where we iteratively apply the MCL algorithm to large subgraphs which contain more than N edges (N = 2, 000). For subgraphs with fewer than 2K edges, we can extract community structures with little cost.(Nan et al. ,1998)

Algorithm 1 Decomposing voice call graphs with MCL.

```
Input: G, N = 2, 000, _ = 2;
Extract disconnected subgraphs G := {Gi} from G, where
ON = [iONi, T N = [iT Ni and E = [iEi;
```

```
3: for each Gi 2 G do
    4: if Ei > N then
        5: Construct symmetric adjacency matrix A from Gi;
        6: repeat
            7: Normalize rows in A;
            8: A := A2; //expansion
            9: aij := a_
            ij , for all entries in A;//inflation
        10: until A converges
        11: Extract disconnected subgraphs GA from A;
        12: G = G [GA − {Gi};
    13: end if
14: end for
```

The MCL algorithm is developed for graph partitioning, which is based on the assumption that random walks tend to stay within the same cluster for a longer time rather than traversing across clusters. MCL iterates two processes: expansion and inflation (line 8 and 9 in Algorithm). Expansion takes the power of the Markovian matrix using regular matrix product. For instance, taking the square of the matrix will compute random walks of length two. Since higher length paths are more common within clusters than between different clusters, expansion will increase the probabilities of intra-cluster walks. Inflation is the element-wise power to _ followed by a diagonal scaling (to make the resulting matrix Markovian).Inflation changes the probabilities associated with the collection of random walks departing from one particular edge by favoring more probable walks. MCL terminates when the two processes converge. Cluster memberships can be identified by extracting connected components from the MCL result. We select MCL to decompose voice graphs for two reasons. First, in MCL, we do not need to specify the expected number of clusters. Second, MCL can scale up to large graphs consisting of millions of edges. The standard MCL algorithm only takes regular (non-bipartite) undirected graphs as input. However, voice call graphs are bi-partite undirected graphs. Therefore, for each subgraph up to decomposition, before feeding it to MCL, we need to create its corresponding non bi-partite version. For example, let Aasym be the adjacency matrix corresponding to a voice graph G, we construct a symmetric adjacency matrix A from Aasym as follows:

$$A = \begin{pmatrix} 0 & A_{asym} \\ A_{asym}^T & 0 \end{pmatrix}$$

The MCL algorithm then operates on A and finally decomposes G into a series of sub-graphs after iterating the expansion and inflation steps. We have tested different selections of B and B= 2 yields the most stable and interpretable results, which is the default parameter setting that we use throughout this paper. By the end of the algorithm, all voice graphs larger than N will be decomposed and the remaining sub-graphs are of less than N edges. We next isolate fraud activities from these sub-graphs.

The major challenges of MCL are:

Identifying all community structures is still a challenging task. This is mainly due to the appearance of random edges or weak connections which connect different communities, thereby forming large sub-graphs mixed with different fraud activities.

The other issue was that the algorithm could not correlate test messages to map up a fraud rent activity:- MCL is based on correlation of the sources and the destinations of the voice calls or text messages and do not go ahead to fetch the content of the text and this made this algorithm unpopular in detecting modern fraud activities

2.5.2 Rule Based Fraud Detection Algorithm

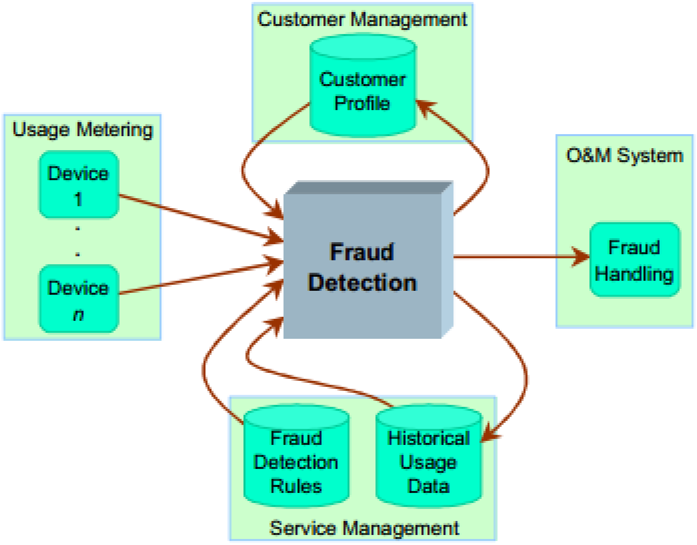


Figure 11: Rule Based Fraud Detection Algorithm. Source (Jimmy, 1998)

With rules based detection, usage data is verified against specified rules. These rules may be absolute or differential. The former are based on simple thresholds, which may or may not be customer-dependent. The latter are based on observed statistical anomalies, the identification of which can be based on customer profile, time of day or other factors. A statistical anomaly occurs when there is a perceived difference between observed behavior and "normal" behavior.

Rules based fraud detection is usually implemented by some kind of predicate logic that works on input data. (Jimmy, 1998)

Major challenges of Rule Based Algorithm are:

The main implementation issues for rules based detection are mediation of this input data to some standard format, choice of rules engine, and provision of flexible tools for specification of arbitrarily complex rules.

Another major design question for rules-based fraud detection systems is how rules are stored and edited.

If fraud detection rules are static then their effectiveness is reduced, firstly as this implies that they cannot be tailored to one-off or rapidly changing services, and secondly as perpetrators of fraud tends to get to know the rules and develop workarounds. Thus it is paramount that rules are easily editable, and are highly customizable, either per-service or per-user. An ideal scenario is where the customer is actively involved in rules specification (e.g. "I rarely make

international calls, and when I do they're almost always to Kenya").

Furthermore, for maximum effectiveness, fraud detection rules should be able to be dependent on any input data – i.e. arbitrary choice of IPDR fields and other input data, and it should be possible for these rules to be almost arbitrarily complex. Formally, we can write this as:

Detection Result = f(IPDR fields, Historical Usage Data, Customer Data), where f is an arbitrary, non-linear function.

The challenge for the implementation of a fraud detection system is to define a representation of rules that is flexible and user-friendly

Also due to their supervised nature meaning that there could only detect fraud that is already known and they cannot learn new fraud tactics makes it unpopular in adjusting to the todays' ever changing fraud tactics

Based on the above challenges we propose the use of Artificial Neural Network as mobile network fraud detection technique

2.6 Artificial Neural Network (ANN)

An Artificial Neural Network (ANN) is an information processing paradigm that is inspired by the way biological nervous systems, such as the brain, process information. ANNs, like people, learn by example. An ANN is configured for a specific application, such as pattern recognition or data classification, through a learning process.

Algorithms are used as a straight forward application of optimization theory and statistical estimation. Gradient Descent Algorithm and Least Mean Square Algorithm will be used in this study. There is use of learning algorithm to make the network learn and there is training algorithm to train the network. Learning rate (µ) is an important consideration to change the weights at each step. If µ is small it will take long time to converge and if it is very large error surface may bounce out of control i.e. lead to divergence.

2.6.1 Gradient Descent Algorithm

It is an optimization algorithm that is used to reach a local minimum function by taking steps proportional to the negative of the gradient of the function at the correct point. It is also known as steepest descent. The algorithm terminates once it is sufficiently near to the minimum of the error function and that point algorithm is said to be converged. (Haykin, 1994)

Let us illustrate this process by the example given below. Here *F* is assumed to be defined on the plane, and that its graph looks like a hill. The concentric curves are the contour lines, that is, the regions on which the value of *F* is constant. An arrow originating at a point shows the direction of the gradient at that point. Note that the gradient at a point is perpendicular to the contour line going through that point. We see that gradient ascent leads us to the top of the hill, that is, to the point where the value of the function *F* is largest.

To have gradient descent go towards a local minimum, one needs to replace γ with − γ.

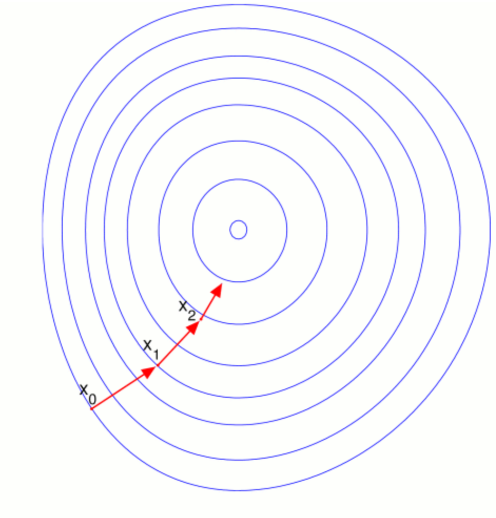


Figure 12: Gradient Descent Algorithm. Source (Haykin, 1994)

2.6.2 Least Mean Square Algorithm

The LMS algorithm is used to producing the least mean squares of the error signal (difference between the desired and the actual signal). The idea behind LMS is to use the method of steepest descent to find a coefficient vector which minimizes a cost function (Nan et al. ,1998).

Input is given to the network and output from the network is actual output (di) of the network. If the actual output of the network does not match with the desired output (d), feed back the error (εi) to the network as follows:

$$d_i = \mathrm{sgn}(wx_i + b)$$

$$\varepsilon_i = d - d_i$$

Calculate average sum of all the errors as

$$J = \frac{1}{2N}\sum \varepsilon_i^2$$

J is to be minimized by differentiating it with respect to weight and bias as these are the only scalar quantities which can vary. Here N is the number of samples used. To modify the weight on each iteration, following equation will be used:

$$w(k+1) = w(k) - \mu \nabla J(k)$$

$$\nabla J(k) = \frac{\partial J}{\partial w}(k) = -\varepsilon(k)\, x(k)$$

$$\text{So, } w(k+1) = w(k) + \mu\, \varepsilon(k)\, x(k)$$

Other algorithms can also be used depending upon the architecture of network used.

In this study **MLP** (Multi-Layer Perceptron) Network Architecture has been used.

2.6.3 Multi-Layer Feed Forward Network

In this type of network, Neurons are arranged in layers, with the first layer taking in inputs and the last layer producing outputs. The middle layers have no connection with the external world, and hence are called hidden layers. The activity of each hidden unit is determined by the activities of the input units and the weights on the connections between the input and the hidden units (Haykin, 1994)

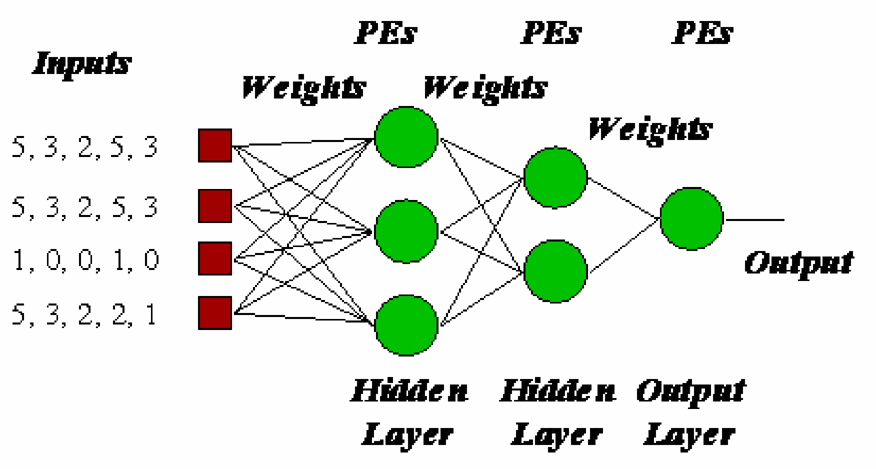


Figure 13: Multi-Layer Feed Forward Network. Source (Haykin, 1994)

Using this used architecture, inputs will flow in the network and it will be trained to output the desired outputs. Different static controllers will be there in the simulation board to conduct the data flow. Then network will be made to run for testing and cross validation of the output. Data has been tagged for, training, cross validation and testing.

In this study the problem is a classification problem. In this faults will be authenticated as 'YES' (if it's a fraud) and 'NO" (if it's not a fraud).

Here are some of the advantages of using neural networks as compared to other algorithms

The advantage in the utilization of a neural network in the mobile phone fraud detection would be the flexibility that the network would provide. A neural network would be capable of analyzing the data from the network, even if the data is incomplete or distorted. Similarly, the network would possess the ability to conduct an analysis with data in a non-linear fashion. Both of these characteristics are important in a networked environment where the information which is received is subject to the random failings of the system. Further, because some attacks may be conducted against the network in a coordinated assault by multiple attackers, the ability to process data from a number of sources in a non-linear fashion is especially important.

The inherent speed of neural networks is another benefit of this approach. Because the protection of computing resources requires the timely identification of attacks, the processing speed of the neural network could enable intrusion responses to be conducted before irreparable damage occurs to the system.

Because the output of a neural network is expressed in the form of a probability the neural network provides a predictive capability to the detection of instances of mobile phone fraud.

A neural network-based fraud detection system would identify the probability that a particular event, or series of events, was indicative of an attack against the system. As the neural network gains experience it will improve its ability to determine where these events are likely to occur in the attack process. This information could then be used to generate a series of events that should occur if this is in fact an intrusion attempt. By tracking the subsequent occurrence of these events the system would be capable of improving the analysis of the events and possibly conducting defensive measures before the attack is successful.

However, the most important advantage of neural networks in misuse detection is the ability of the neural network to "learn" the characteristics of the fraud and identify instances that are unlike any which have been observed before by the network. A neural network might be trained to recognize known suspicious events with a high degree of accuracy. While this would be a very valuable ability, since attackers often emulate the "successes" of others, the network would also gain the ability to apply this knowledge to identify instances of attacks which did not match the exact characteristics of previous intrusions. The probability of an attack against the system may be estimated and a potential threat flagged whenever the probability exceeds a specified threshold.

Chapter 3: METHODOLOGY

3.0 Overview

This section describes the system analysis, system requirements, collection and grouping of datasets, analysis and evaluation of data and finally system implementation.

It also describes the system in narrative form using non-technical terms by providing a high-level system architecture diagram showing a subsystem breakout of the system. The high-level system architecture or subsystem diagrams also show interfaces to external systems

3.1 System Analysis

The section will reveal call record attributes overview, non-DBMS files associated with the system under development and high level design highlighting levels involved in the system development.

Raw Call Records data (non-DBMS file):- This is a pipe separated text file that contains all the attributes of a call or the SMS and generated by the GSM Network. The file contains all attributes of a call or SMS record captured when a call or an SMS is initiated

Below are the attributes captured when a call is initiated:-

- *Orgn number :*-This represents the call originating number
- *Dest number:*-This represents the call destination number
- *Call_location:*-This represent the geographical location of the originating call
- *Call duration:*- This represent the amount of time in seconds the call lasted
- *Phone model:*-This represent the phone model/type of the call initiator
- *First_name:*-This is the Initial name of the call initiator
- *Last_name:*-This is the last name of the call initiator
- *Rating:*-This is the call initiator rating assigned by the service provider which is based on the amount of revenue generated from the number
- *Line life time:*-this represent the number of days the number have been active
- *Number of calls received in minute:*- this represent the number of calls received by the call originating number
- *Number of calls made in a minute:*- this represent the number of calls made by the call originating number

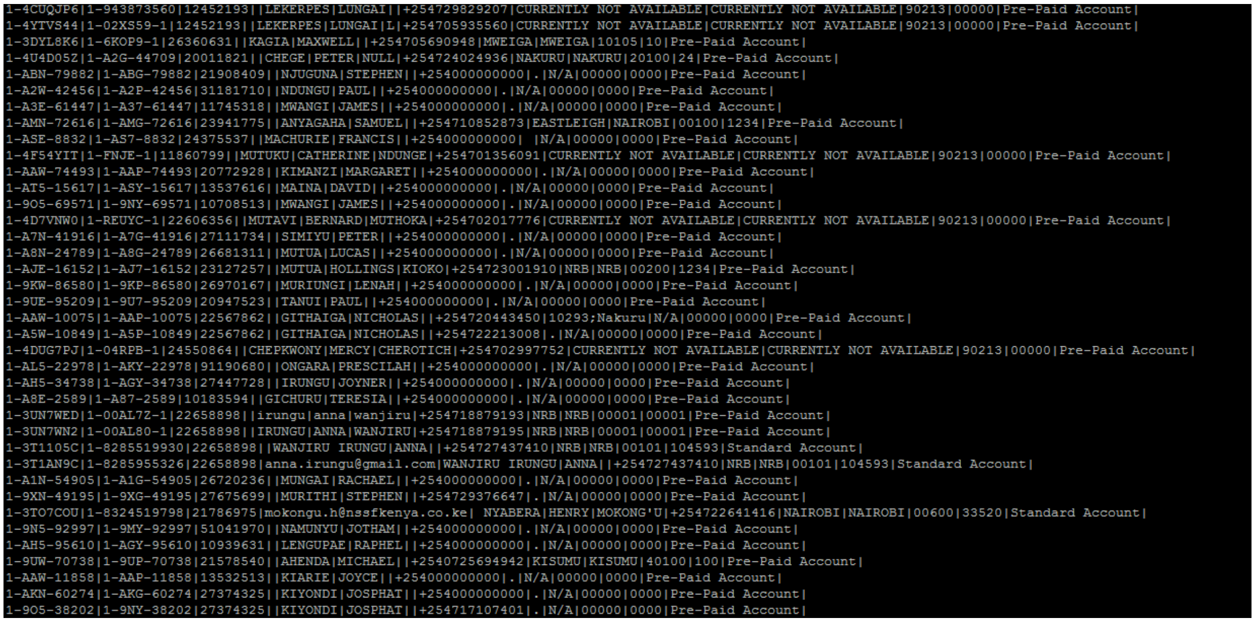
- *Known status:-*This represent the know status of the originating number which indicates whether the number have been previously involved in a fraud rent activity

Below are the attributes captured when an SMS is initiated:-

- *Orgn number :-*This represents the call originating number
- *Dest number:-*This represents the SMS destination number
- *SMS_location:-*This represent the geographical location of the originating SMS number
- *Key word status:-* This indicates whether a fraud related word appears on the SMS send
- *Phone model:-*This represent the phone model/type of the call initiator
- *First_name:-*This is the Initial name of the call initiator
- *Last_name:-*This is the last name of the call initiator
- *Rating:-*This is the call initiator rating assigned by the service provider which is based on the amount of revenue generated from the number
- *Line life time:-*this represent the number of days the number have been active
- *Number of SMS received in minute:-* this represent the number of SMS received by the call originating number
- *Number of SMS send in a minute:-* this represent the number of SMS send by the call originating number

- *Known status*:-This represent the know status of the originating number which indicates whether the number have been previously involved in a fraud rent activity

Below is a sample raw Call Record data file



```
1-4CUQJP6|1-943873560|12452193||LEKERPES|LUNGAI||+254729829207|CURRENTLY NOT AVAILABLE|CURRENTLY NOT AVAILABLE|90213|00000|Pre-Paid Account|
1-4YTVS44|1-02XS59-1|12452193||LEKERPES|LUNGAI|L|+254705935560|CURRENTLY NOT AVAILABLE|CURRENTLY NOT AVAILABLE|90213|00000|Pre-Paid Account|
1-3DYL8K6|1-6KOP9-1|26360631||KAGIA|MAXWELL||+254705690948|MWEIGA|MWEIGA|10105|10|Pre-Paid Account|
1-4U4D05Z|1-A2G-44709|20011821||CHEGE|PETER|NULL|+254724024936|NAKURU|NAKURU|20100|24|Pre-Paid Account|
1-ABN-79882|1-ABG-79882|21908409||NJUGUNA|STEPHEN||+254000000000|.|N/A|00000|0000|Pre-Paid Account|
1-A2W-42456|1-A2P-42456|31181710||NDUNGU|PAUL||+254000000000|.|N/A|00000|0000|Pre-Paid Account|
1-A3E-61447|1-A37-61447|11745318||MWANGI|JAMES||+254000000000|.|N/A|00000|0000|Pre-Paid Account|
1-AMN-72616|1-AMG-72616|23941775||ANYAGAHA|SAMUEL||+254710852873|EASTLEIGH|NAIROBI|00100|1234|Pre-Paid Account|
1-ASE-8832|1-AS7-8832|24375537||MACHURIE|FRANCIS||+254000000000| |N/A|00000|0000|Pre-Paid Account|
1-4F54YIT|1-FNJE-1|11860799||MUTUKU|CATHERINE|NDUNGE|+254701356091|CURRENTLY NOT AVAILABLE|CURRENTLY NOT AVAILABLE|90213|00000|Pre-Paid Account|
1-AAW-74493|1-AAP-74493|20772928||KIMANZI|MARGARET||+254000000000|.|N/A|00000|0000|Pre-Paid Account|
1-AT5-15617|1-ASY-15617|13537616||MAINA|DAVID||+254000000000|.|N/A|00000|0000|Pre-Paid Account|
1-9O5-69571|1-9NY-69571|10708513||MWANGI|JAMES||+254000000000|.|N/A|00000|0000|Pre-Paid Account|
1-4D7VNW0|1-REUYC-1|22606356||MUTAVI|BERNARD|MUTHOKA|+254702017776|CURRENTLY NOT AVAILABLE|CURRENTLY NOT AVAILABLE|90213|00000|Pre-Paid Account|
1-A7N-41916|1-A7G-41916|27111734||SIMIYU|PETER||+254000000000|.|N/A|00000|0000|Pre-Paid Account|
1-A8N-24789|1-A8G-24789|26681311||MUTUA|LUCAS||+254000000000|.|N/A|00000|0000|Pre-Paid Account|
1-AJE-16152|1-AJ7-16152|23127257||MUTUA|HOLLINGS|KIOKO|+254723001910|NRB|NRB|00200|1234|Pre-Paid Account|
1-9KW-86580|1-9KP-86580|26970167||MURIUNGI|LENAH||+254000000000|.|N/A|00000|0000|Pre-Paid Account|
1-9UE-95209|1-9U7-95209|20947523||TANUI|PAUL||+254000000000|.|N/A|00000|0000|Pre-Paid Account|
1-AAW-10075|1-AAP-10075|22567862||GITHAIGA|NICHOLAS||+254720443450|10293;Nakuru|N/A|00000|0000|Pre-Paid Account|
1-A5W-10849|1-A5P-10849|22567862||GITHAIGA|NICHOLAS||+254722213008|.|N/A|00000|0000|Pre-Paid Account|
1-4DUG7PJ|1-04RPB-1|24550864||CHEPKWONY|MERCY|CHEROTICH|+254702997752|CURRENTLY NOT AVAILABLE|CURRENTLY NOT AVAILABLE|90213|00000|Pre-Paid Account|
1-AL5-22978|1-AKY-22978|91190680||ONGARA|PRESCILAH||+254000000000|.|N/A|00000|0000|Pre-Paid Account|
1-AH5-34738|1-AGY-34738|27447728||IRUNGU|JOYNER||+254000000000|.|N/A|00000|0000|Pre-Paid Account|
1-A8E-2589|1-A87-2589|10183594||GICHURU|TERESIA||+254000000000|.|N/A|00000|0000|Pre-Paid Account|
1-3UN7WED|1-00AL7Z-1|22658898||irungu|anna|wanjiru|+254718879193|NRB|NRB|00001|00001|Pre-Paid Account|
1-3UN7WN2|1-00AL80-1|22658898||IRUNGU|ANNA|WANJIRU|+254718879195|NRB|NRB|00001|00001|Pre-Paid Account|
1-3T1105C|1-8285519930|22658898||WANJIRU IRUNGU|ANNA||+254727437410|NRB|NRB|00101|104593|Standard Account|
1-3T1AN9C|1-8285955326|22658898|anna.irungu@gmail.com|WANJIRU IRUNGU|ANNA||+254727437410|NRB|NRB|00101|104593|Standard Account|
1-A1N-54905|1-A1G-54905|26720236||MUNGAI|RACHAEL||+254000000000|.|N/A|00000|0000|Pre-Paid Account|
1-9XN-49195|1-9XG-49195|27675699||MURITHI|STEPHEN||+254729376647|.|N/A|00000|0000|Pre-Paid Account|
1-3TO7COU|1-8324519798|21786975|mokongu.h@nssfkenya.co.ke| NYABERA|HENRY|MOKONG'U|+254722641416|NAIROBI|NAIROBI|00600|33520|Standard Account|
1-9N5-92997|1-9MY-92997|51041970||NAMUNYU|JOTHAM||+254000000000|.|N/A|00000|0000|Pre-Paid Account|
1-AH5-95610|1-AGY-95610|10939631||LENGUPAE|RAPHEL||+254000000000|.|N/A|00000|0000|Pre-Paid Account|
1-9UW-70738|1-9UP-70738|21578540||AHENDA|MICHAEL||+2540725694942|KISUMU|KISUMU|40100|100|Pre-Paid Account|
1-AAW-11858|1-AAP-11858|13532513||KIARIE|JOYCE||+254000000000|.|N/A|00000|0000|Pre-Paid Account|
1-AKN-60274|1-AKG-60274|27374325||KIYONDI|JOSPHAT||+254000000000|.|N/A|00000|0000|Pre-Paid Account|
1-9O5-38202|1-9NY-38202|27374325||KIYONDI|JOSPHAT||+254717107401|.|N/A|00000|0000|Pre-Paid Account|
```

The records contained in these files need to be transformed and loaded in to a database in readable format to acted upon by the Neural Network.

3.1.1 Application Analysis:-Fraud Detection Engine

The Fraud detection engine that act upon voice and the SMS database stored in the database should run four levels, this is to ensures that the classification refined

The levels are described below:-

LEVEL 1: Event Refinement:

This is the first level where all the entries that match a particular fraud rent pattern are detected

This can be a general attribute such as a location or a certain phone number. In this stage all the detected events my not necessarily be fraud rent but they match a certain fraud rent attribute

Eg. A location like a prison area is highlighted to be a source of frauding calls but not all calls originating there are fraud calls

LEVEL 2: Situation Refinement:

This is the second level all the event raised in level 1 are passed again to the engine with additional attributes to assess whether they are really fraud-rent activities

LEVEL 3: Impact Assessment:

In this level the impact of the fraud rent activity it positive is evaluated. This can be measured using additional attribute like amount of money being involved the number of casualties etc.

LEVEL 4: Process Refinement:

In this level, an evaluation of all the three levels is done to determine whether an event is truly fraud rent. The neural network should detect this based on the previous cases and the training acquired

3.2 System requirements

The requirements for this study were:

- Transformation of Raw Call Data Records (CDRs): (unprocessed call records as captured by the network subsystem) to a readable format that can be analyzed.
- Build an Artificial Neural Network the read the transformed data stored in the database and classifies it into fraud-rent and non-fraud-rent cases
- Train the Artificial Neural Network: - This is the passing of the already classified data (both the call attributes and the outcome) through the Network to learn so that the Network will classify the unknown cases. Different time and size variant data should be used in the Network training
- Test the Artificial Neural Network: - This will involve passing on unclassified data (call attributes only) through the already trained Network for classification. The classified cases are then compared with the actual data as provided by the service provider to assess the accuracy of the Network. Different time variant data sets should be used in the testing process.

3.3 System Design

In this section, describe the overall system software and organization. In this project an out of box software RapidMiner was used to build the neural network and read data read from the database.

RapidMiner is a software platform developed by the RapidMiner Co. that provides an integrated environment for machine learning, Data mining, text mining and predictive analytics.it is built on a

Java programming language and widely used for business and industrial applications as well as for research, education, training, rapid prototyping, and application development and supports all steps of the data mining process including results visualization, validation and optimization. *RapidMine*r is developed on a business source model which means the core and earlier versions of the software are available under an OSI-certified open source license on *Sourceforge* A Starter Edition is available for free download

RapidMiner can be used to build, train and test Artificial Neural Networks as It consists of the below tools that are used to read, transform and manipulate data that is used for training or testing

Training data input*:* This function provide the input on the training data to the network

Nominal converter: This function converts invalid inputs to readable values

Replace Missing: This function replaces the missing values with predefined once if any

ANOVA Matrix function: This smoothens the data before feeding it to the network

Neural Net: This is the actual function that does the training

Test Data Input: This function provides the input for both Testing and the actual CDR data

Apply mode Function**:** This function applies the model to the data

RapidMiner is very flexible when it comes to Network training as it allows parameter adjustments depending on the type and size of data being passed through the Network.

Below are the parameters that can be adjusted to suited different data types and sizes

Hidden layers: this defines the number of hidden layers to be implemented on the network before the training process is started

Training cycles: This is number of cycles the training data is passed through the network.

Learning rate**:** This define the rate at which the learning process is adopted by the Network

Momentum: This defines the lag between the training cycles.

In our study we have used *RapidMiner* on all the three stages of the study i.e. Network building, Network Training and the Network Testing

Network building: - All the components required for the Network build are assembled and connected using the *drag and drop* functionality of *RapidMiner* and their relationship defined using the *xml* language.

Network Training: - After the network is built a *Training data input* connector is defined to point to the database where the training is located. This data is fetched and passed through the Network for training

Network Testing: - The *Testing data* connector is defined to point to the database where the testing data is located. This data is passed to an already trained Network for testing.

3.3.2 Database Design:

The database consisted of four major tables, two containing voice data and two containing SMS data, which are organized into two schemas i.e.

- Training schema: - this will hold both SMS and Voice Neural network training data
- Test schema: - This will hold both SMS and Voice Neural network testing data

For this study the transformed call records consisted of real time data from one of the telecom companies were loaded to the database

The major reason for storing the data in form of tables is to speed up the data access during the processing phase. Depending with the scale i.e. number of expected records different database software can be used i.e.

For small scale deployment MS access or excel spread sheet can be used to store the data. For medium to large scale deployments more advance RDBMS software e.g. MS sqlsever, Mysql and Oracle can be used in addition the database can run on a wide range of operating systems ranging from Windows, Linux,IBM AIX,HP UX etc as the data storage is independent to the operating system used

Below are the tables' layout and the indexes' as used in the study

The tables are not joined as and hence no foreign keys were needed on the tables

Table 1: Voice_test Tables

INDEX NAME	COLUMN NAME	COLUMN DATA TYPE
idx_voice_test_on	Orgn_number	Number (20)
idx_voice_test_dn	dest_number	Number (20)
idx_voice_test_fn	first_name	Varchar2 (40)
idx_voice_test_fl	known_status	Varchar2 (40)

Table 2: Voice_train Table

INDEX NAME	COLUMN NAME	COLUMN DATA TYPE
idx_voice_trn_on	Orgn_number	Number (20)
idx_voice_trn_dn	dest_number	Number (20)
idx_voice_trn_fn	first_name	Varchar2 (40)
idx_voice_trn_fl	known_status	Varchar2 (40)

Table 3: SMS_train Table

INDEX NAME	COLUMN NAME	COLUMN DATA TYPE
idx_SMS_trn_on	Orgn_number	Number (20)
idx_SMS_trn_dn	dest_number	Number (20)
idx_SMS_trn_fn	first_name	Varchar2 (40)
idx_SMS_trn_fl	known_status	Varchar2 (40)

Table 4: SMS_test Table

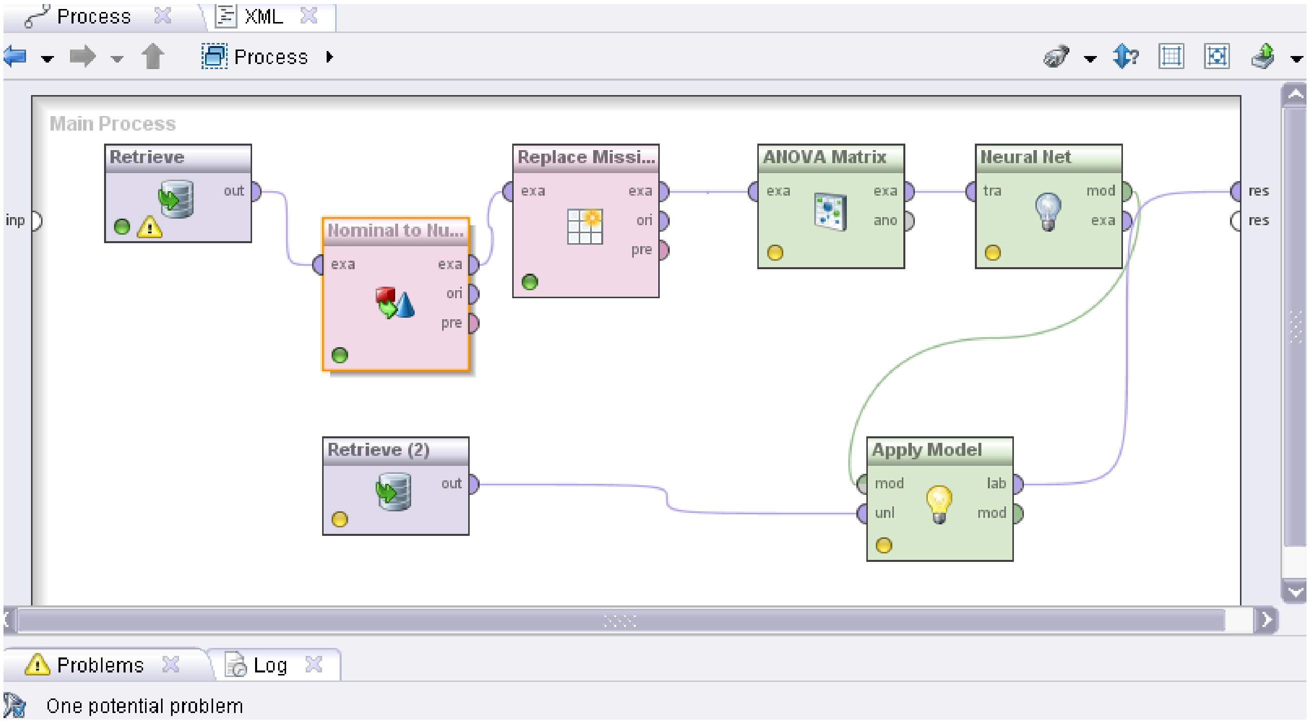
INDEX NAME	COLUMN NAME	COLUMN DATA TYPE
idx_SMS_test_on	Orgn_number	Number (20)
idx_SMS_test_dn	dest_number	Number (20)
idx_SMS_test_fn	first_name	Varchar2 (40)
idx_SMS_test_fl	known_status	Varchar2 (40)

3.3.3 Internal Communications Design

This represents the Artificial Neural network engine which does the actual data processing.

The neural network is build using an out of box software 'Rapid Miner' which runs on the Ms Windows platform

Below are the major components:



One potential problem

Figure 14: Internal Communication.

Training data input: This function provide the input on the training data to the network

Nominal converter: This function converts invalid inputs to readable values

Replace Missing: This function replaces the missing values with predified once if any

ANOVA Matrix function: This smoothens the data before feeding it to the network

Neural Net: This is the actual function that does the training

Test Data Input: This function provides the input for both Testing and the actual CDR data

Apply mode Function: This function applies the model to the data

3.5.4 External Interfaces Design

We have one major external interface that links the system to the network sub system that populates the call and SMS records

The interface runs an ETL job as below

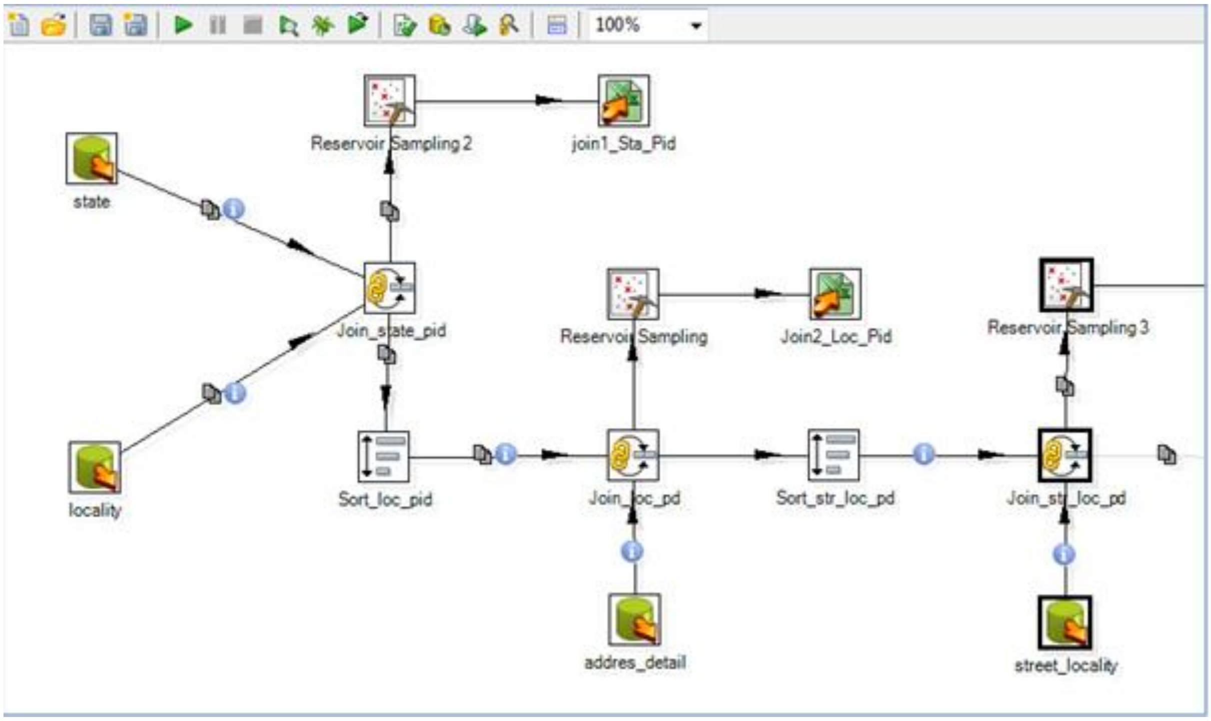


Figure 15: External Communication.

3.5.5 System Hardware Design

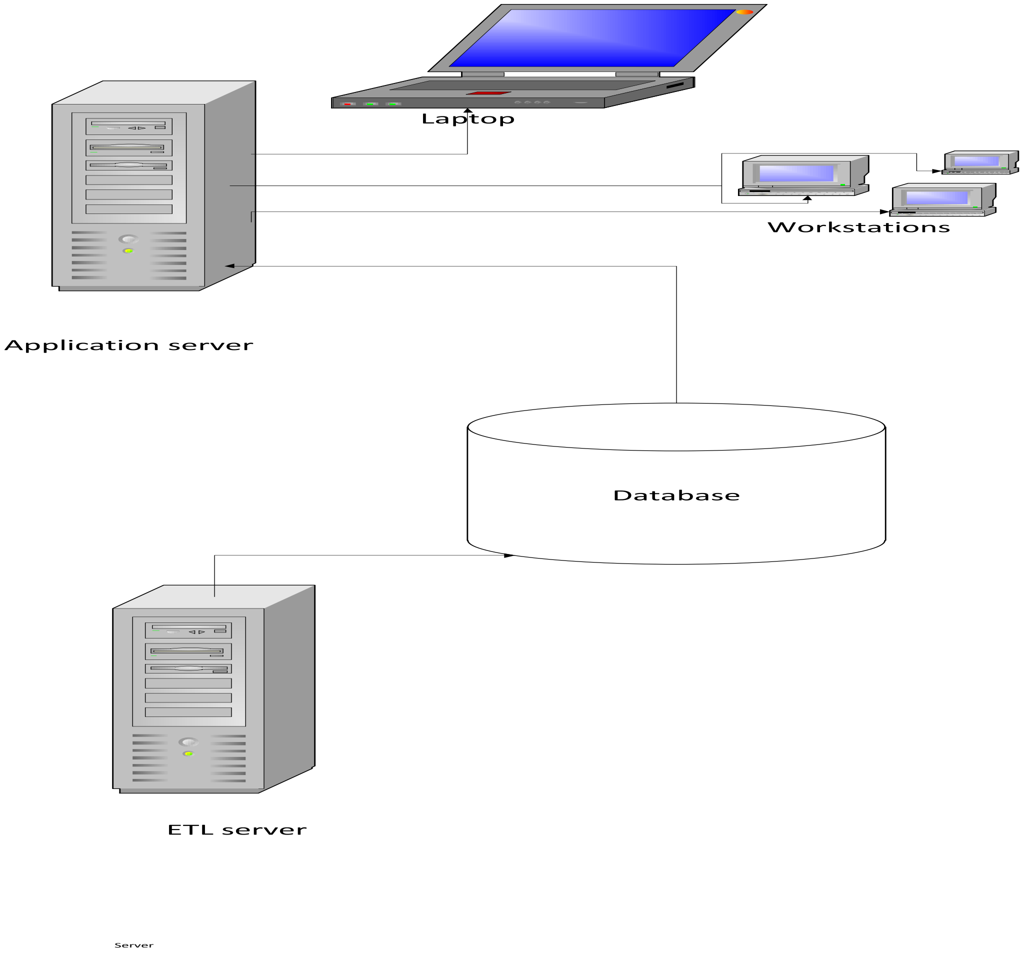


Figure 16: Hardware Architecture.

Application Server: Performs the Neural Network Application logic

ETL server: Performs data loading to the database from the raw CDRs

Database: This is the processed data storage

3.6 Implementation:

The fraud detection algorithm is run on three months data since there is usually an anticipated lag between the occurrences of fraud activities and user reports to the carrier, we use the list that contains numbers inserted with the same months by the service provider.

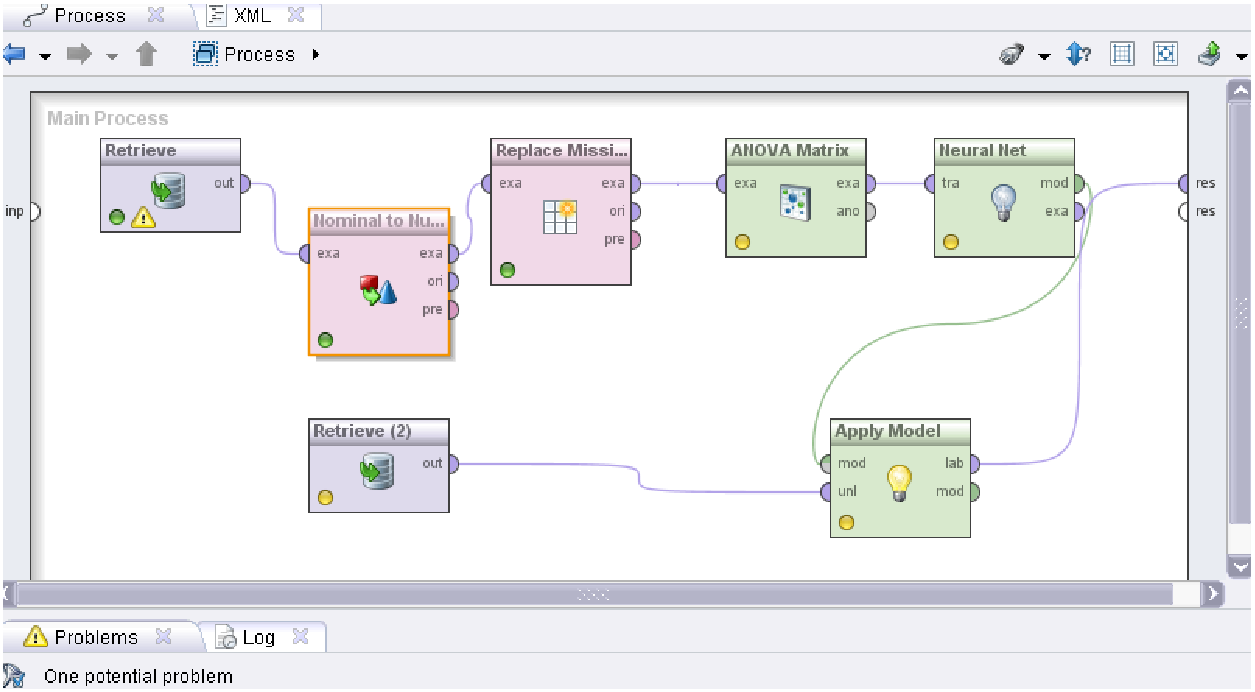
To assess the severity and impact of fraud activities, we measured the number of victims and fraud calls attracted by each fraud number. To ensure a fair comparison and to capture the real impact of fraud activities, we counted the number of victims and fraud calls of a fraud number only within a 4-week time window prior to its first report time. For true detections and missed detections, we consider the first report time as the time when the fraud numbers were inserted into the list. For new detections, we treated the time of the first online post regarding a fraud number as its first report time.

To make the network learn, supervised learning technique was used, which is used to infer the mapping implied by the data and the cost function is related to the mismatch between mapping and the data.

In a complete integrated system the engine should be placed on the network subsystem where all the traffic from the base stations is combined

3.6.3 Network Building:

Step 1: The network is built by assembling all the function as shown in Figure 17



One potential problem

Figure 17: Network Build.

Training data input: This function provide the input on the training data to the network. It reads the database where the training data is stored

Nominal converter: This function converts invalid inputs to readable values. Neural Network will only work with nominal values, so this function converts all non-nominal values to nominal values so as to be used in the training phase

Replace Missing: This function replaces the missing values with predefined once if any missing is found in the training data to avoid errors

ANOVA Matrix function: This smoothens the data before feeding it to the network

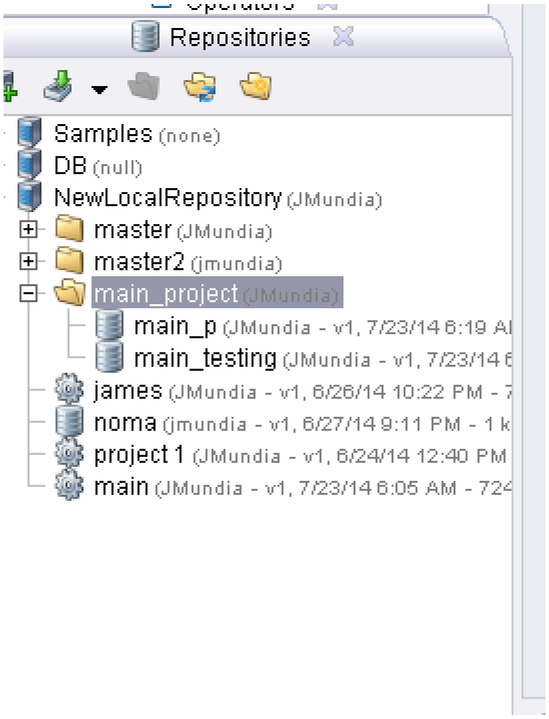
Neural Net: This is the actual function that does the training, Based on the attributed of a record and the outcome the algorithm build a logical neural network that is adjusted accordingly as more training data is passed through the network

Test Data Input: This function that reads the testing data stored in the database and then passes it through the network for classification

Apply mode Function: This is a control function that applies the build Network model to the data retrieved for both testing and training databases

Step 2: Select the location where the data is located (the database can be on different location):

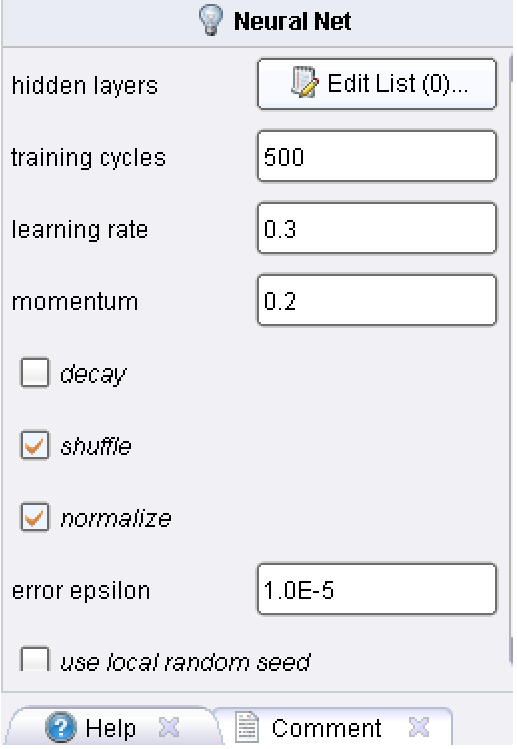
After the components are assembled and relationships defined, select the location on the data from the *repository* tab



```
Repositories
Samples (none)
DB (null)
NewLocalRepository (JMundia)
  master (JMundia)
  master2 (jmundia)
  main_project (JMundia)
    main_p (JMundia - v1, 7/23/14 6:19 AI
    main_testing (JMundia - v1, 7/23/14 6
  james (JMundia - v1, 6/26/14 10:22 PM - 7
  noma (jmundia - v1, 6/27/14 9:11 PM - 1 k
  project 1 (JMundia - v1, 6/24/14 12:40 PM
  main (JMundia - v1, 7/23/14 6:05 AM - 724
```

Figure 18: Data Source Selection.

Step 3: Adjust parameters for the network training: During the Network building below parameters can be adjusted accordingly depending with the type of data that need to be trained



Neural Net

hidden layers: Edit List (0)...

training cycles: 500

learning rate: 0.3

momentum: 0.2

☐ *decay*

☑ *shuffle*

☑ *normalize*

error epsilon: 1.0E-5

☐ *use local random seed*

Figure 19: Adjustable Parameter.

Hidden layers: this defines the number of hidden layers to be implemented on the network before the training process is started. The number of the hidden layers is determined by the nature of data used in the training process

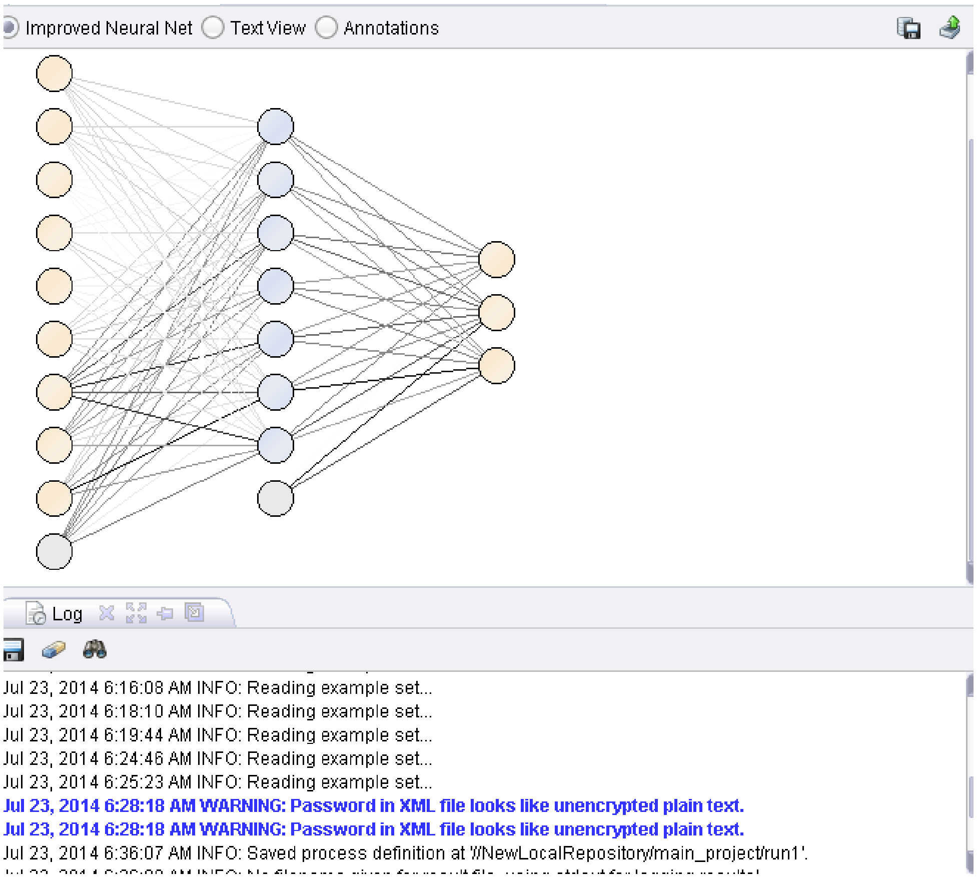
Training cycles: This is number of cycles the training data is passed through the network. The more the cycles the accuracy the more the accuracy but more time is consumed during the training process.

Learning rate: This defines the rate at which the learning process is adopted by the Network. It ranges from 0.1 to 1 with 0.1 being the slowest and 1 being the highest. This parameter affects the speed of the learning process but does not affect the classification accuracy

Momentum: This defines the lag between the training cycles .This parameter affects the speed of the learning process but does not affect the classification accuracy.

Complete network with the hidden layers:

The below shows the the complete Neural Network idicating the hidden layers



```
Jul 23, 2014 6:16:08 AM INFO: Reading example set...
Jul 23, 2014 6:18:10 AM INFO: Reading example set...
Jul 23, 2014 6:19:44 AM INFO: Reading example set...
Jul 23, 2014 6:24:46 AM INFO: Reading example set...
Jul 23, 2014 6:25:23 AM INFO: Reading example set...
Jul 23, 2014 6:28:18 AM WARNING: Password in XML file looks like unencrypted plain text.
Jul 23, 2014 6:28:18 AM WARNING: Password in XML file looks like unencrypted plain text.
Jul 23, 2014 6:36:07 AM INFO: Saved process definition at '//NewLocalRepository/main_project/run1'.
```

Figure 20: Hidden Layers.

Chapter 4: RESULTS AND DISCUSSION

In this chapter describes in details the data used to train and test the Network, experimentation process and the results obtained from the experiments

4.1 Datasets

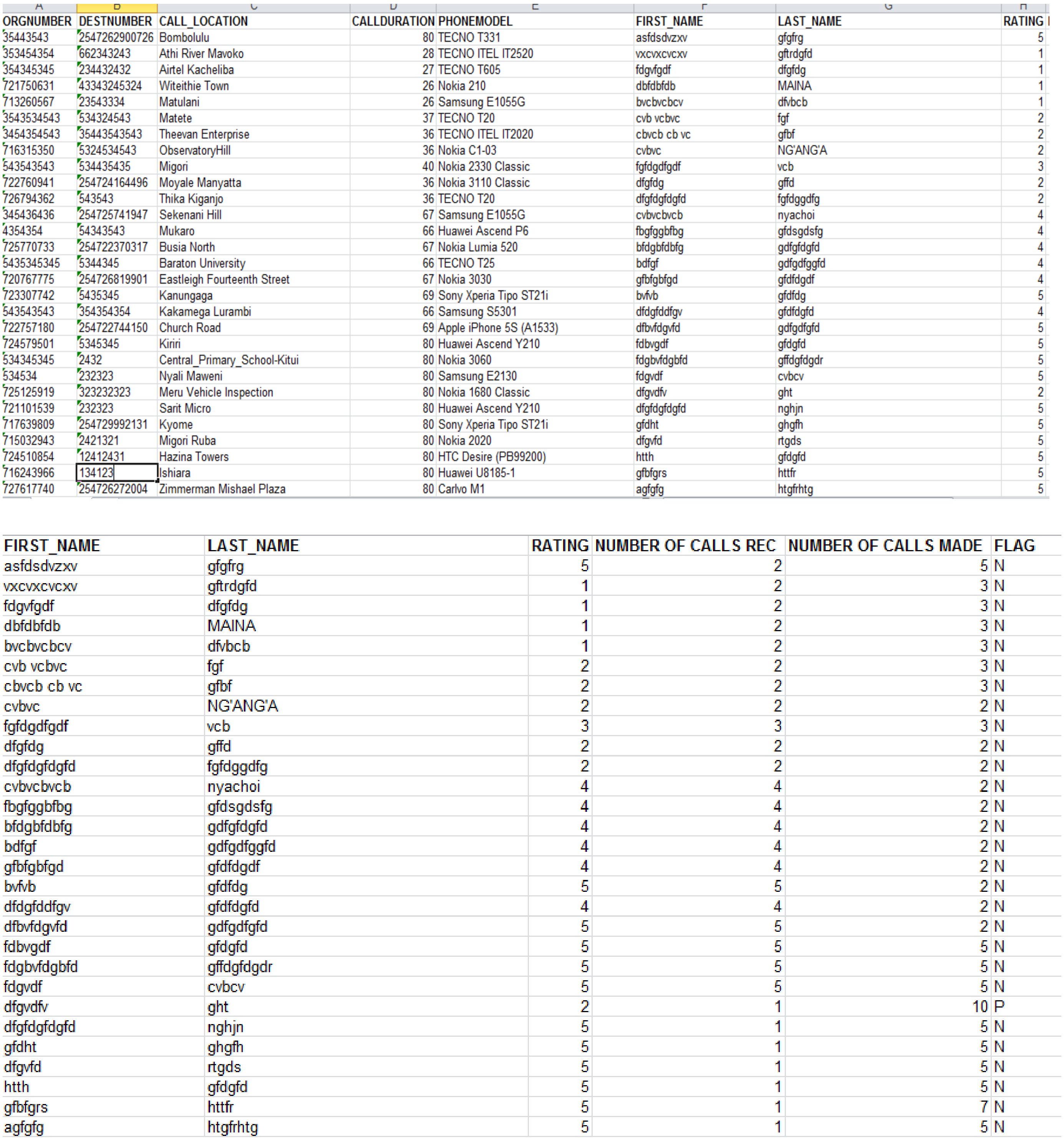
In the study, actual data obtained from a service provider's network, consisting of a complete set of voice calls and SMS details collected at the MSCs of the UMTS network under study was used. Theses phone calls are initiated by mobile users in the cellular network (i.e., domestic users) to international terminating numbers or domestic users to domestic users.

We emphasize here that no customer private information was used in our analysis and we have anonymized all customer identities. In particular, the anonymization process keeps the area code intact and only anonymizes the remaining 7 digits in the originating numbers. More importantly, the location of the two numbers is also preserved after anonymization. In addition to protecting users' privacy, this type of anonymization enabled us to study the relationship among phone numbers that participate in the same fraud activities. Similarly, to adhere to the confidentiality under which we had access to the data, in places, we only presented normalized views of our results while retaining the scientifically relevant magnitudes.

4.2 Inputs

The data is input from the raw CDRs (customer data records) generated by the network and inserted into the *voice_train* and *SMS_train* tables.

Below is a sample of training data



ORGNUMBER	DESTNUMBER	CALL_LOCATION	CALLDURATION	PHONEMODEL	FIRST_NAME	LAST_NAME	RATING
35443543	2547262900726	Bombolulu	80	TECNO T331	asfdsdvzxv	gfgfrg	5
353454354	662343243	Athi River Mavoko	28	TECNO ITEL IT2520	vxcvxcvcxv	gftrdgfd	1
354345345	234432432	Airtel Kacheliba	27	TECNO T605	fdgvfgdf	dfgfdg	1
721750631	43343245324	Witeithie Town	26	Nokia 210	dbfdbfdb	MAINA	1
713260567	23543334	Matulani	26	Samsung E1055G	bvcbvcbcv	dfvbcb	1
3543534543	534324543	Matete	37	TECNO T20	cvb vcbvc	fgf	2
3454354543	35443543543	Theevan Enterprise	36	TECNO ITEL IT2020	cbvcb cb vc	gfbf	2
716315350	5324534543	ObservatoryHill	36	Nokia C1-03	cvbvc	NG'ANG'A	2
543543543	534435435	Migori	40	Nokia 2330 Classic	fgfdgdfgdf	vcb	3
722760941	254724164496	Moyale Manyatta	36	Nokia 3110 Classic	dfgfdg	gffd	2
726794362	543543	Thika Kiganjo	36	TECNO T20	dfgfdgfdgfd	fgfdggdfg	2
345436436	254725741947	Sekenani Hill	67	Samsung E1055G	cvbvcbvcb	nyachoi	4
4354354	54343543	Mukaro	66	Huawei Ascend P6	fbgfggbfbg	gfdsgdsfg	4
725770733	254722370317	Busia North	67	Nokia Lumia 520	bfdgbfdbfg	gdfgfdgfd	4
5435345345	5344345	Baraton University	66	TECNO T25	bdfgf	gdfgdfggfd	4
720767775	254726819901	Eastleigh Fourteenth Street	67	Nokia 3030	gfbfgbfgd	gfdfdgdf	4
723307742	5435345	Kanungaga	69	Sony Xperia Tipo ST21i	bvfvb	gfdfdg	5
543543543	354354354	Kakamega Lurambi	66	Samsung S5301	dfdgfddfgv	gfdfdgfd	4
722757180	254722744150	Church Road	69	Apple iPhone 5S (A1533)	dfbvfdgvfd	gdfgdfgfd	5
724579501	5345345	Kiriri	80	Huawei Ascend Y210	fdbvgdf	gfdgfd	5
534345345	2432	Central_Primary_School-Kitui	80	Nokia 3060	fdgbvfdgbfd	gffdgfdgdr	5
534534	232323	Nyali Maweni	80	Samsung E2130	fdgvdf	cvbcv	5
725125919	323232323	Meru Vehicle Inspection	80	Nokia 1680 Classic	dfgvdfv	ght	2
721101539	232323	Sarit Micro	80	Huawei Ascend Y210	dfgfdgfdgfd	nghjn	5
717639809	254729992131	Kyome	80	Sony Xperia Tipo ST21i	gfdht	ghgfh	5
715032943	2421321	Migori Ruba	80	Nokia 2020	dfgvfd	rtgds	5
724510854	12412431	Hazina Towers	80	HTC Desire (PB99200)	htth	gfdgfd	5
716243966	134123	Ishiara	80	Huawei U8185-1	gfbfgrs	httfr	5
727617740	254726272004	Zimmerman Mishael Plaza	80	Carlvo M1	agfgfg	htgfrhtg	5

FIRST_NAME	LAST_NAME	RATING	NUMBER OF CALLS REC	NUMBER OF CALLS MADE	FLAG
asfdsdvzxv	gfgfrg	5	2	5	N
vxcvxcvcxv	gftrdgfd	1	2	3	N
fdgvfgdf	dfgfdg	1	2	3	N
dbfdbfdb	MAINA	1	2	3	N
bvcbvcbcv	dfvbcb	1	2	3	N
cvb vcbvc	fgf	2	2	3	N
cbvcb cb vc	gfbf	2	2	3	N
cvbvc	NG'ANG'A	2	2	2	N
fgfdgdfgdf	vcb	3	3	3	N
dfgfdg	gffd	2	2	2	N
dfgfdgfdgfd	fgfdggdfg	2	2	2	N
cvbvcbvcb	nyachoi	4	4	2	N
fbgfggbfbg	gfdsgdsfg	4	4	2	N
bfdgbfdbfg	gdfgfdgfd	4	4	2	N
bdfgf	gdfgdfggfd	4	4	2	N
gfbfgbfgd	gfdfdgdf	4	4	2	N
bvfvb	gfdfdg	5	5	2	N
dfdgfddfgv	gfdfdgfd	4	4	2	N
dfbvfdgvfd	gdfgdfgfd	5	5	2	N
fdbvgdf	gfdgfd	5	5	5	N
fdgbvfdgbfd	gffdgfdgdr	5	5	5	N
fdgvdf	cvbcv	5	5	5	N
dfgvdfv	ght	2	1	10	P
dfgfdgfdgfd	nghjn	5	1	5	N
gfdht	ghgfh	5	1	5	N
dfgvfd	rtgds	5	1	5	N
htth	gfdgfd	5	1	5	N
gfbfgrs	httfr	5	1	7	N
agfgfg	htgfrhtg	5	1	5	N

Figure 21: Training Data.

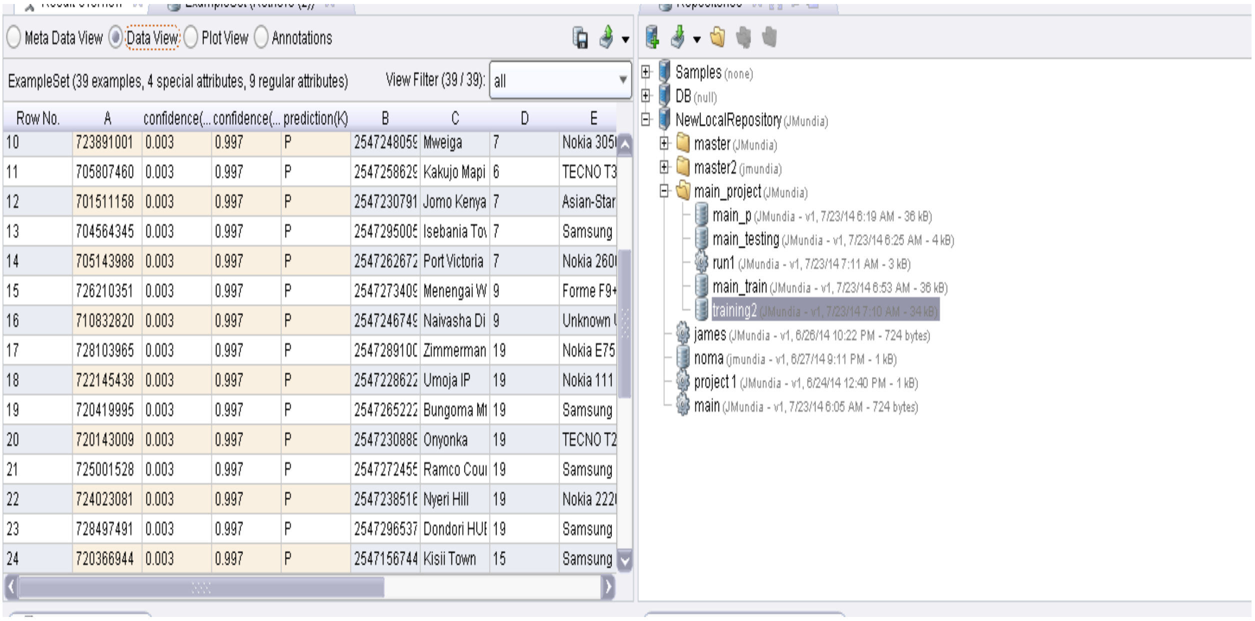
4.3 Outputs

The output is a representation of two feeds:

Test data output: this represents the accuracy of the neural network after the training data is passed on the network

Actual fraud rent output: This provides the actual output of the fraud rent activities

Below is a sample



○ Meta Data View ● Data View ○ Plot View ○ Annotations

ExampleSet (39 examples, 4 special attributes, 9 regular attributes)   View Filter (39 / 39): all

Row No.	A	confidence(...	confidence(...	prediction(K)	B	C	D	E
10	723891001	0.003	0.997	P	254724805§	Mweiga	7	Nokia 305(
11	705807460	0.003	0.997	P	254725862§	Kakujo Mapi	6	TECNO T3
12	701511158	0.003	0.997	P	2547230791	Jomo Kenya	7	Asian-Star
13	704564345	0.003	0.997	P	254729500§	Isebania To\	7	Samsung
14	705143988	0.003	0.997	P	254726267‡	Port Victoria	7	Nokia 260(
15	726210351	0.003	0.997	P	254727340§	Menengai W	9	Forme F9+
16	710832820	0.003	0.997	P	254724674§	Naivasha Di	9	Unknown (
17	728103965	0.003	0.997	P	254728910(	Zimmerman	19	Nokia E75
18	722145438	0.003	0.997	P	254722862‡	Umoja IP	19	Nokia 111
19	720419995	0.003	0.997	P	254726522‡	Bungoma Mi	19	Samsung
20	720143009	0.003	0.997	P	254723088§	Onyonka	19	TECNO T2
21	725001528	0.003	0.997	P	254727245§	Ramco Coui	19	Samsung
22	724023081	0.003	0.997	P	254723851§	Nyeri Hill	19	Nokia 222(
23	728497491	0.003	0.997	P	2547296537	Dondori HUI	19	Samsung
24	720366944	0.003	0.997	P	2547156744	Kisii Town	15	Samsung

Samples (none)
DB (null)
NewLocalRepository (JMundia)
master (JMundia)
master2 (jmundia)
main_project (JMundia)
main_p (JMundia - v1, 7/23/14 6:19 AM - 36 kB)
main_testing (JMundia - v1, 7/23/14 6:25 AM - 4 kB)
run1 (JMundia - v1, 7/23/14 7:11 AM - 3 kB)
main_train (JMundia - v1, 7/23/14 6:53 AM - 36 kB)
training2 (JMundia - v1, 7/23/14 7:10 AM - 34 kB)
james (JMundia - v1, 6/26/14 10:22 PM - 724 bytes)
noma (jmundia - v1, 6/27/14 9:11 PM - 1 kB)
project 1 (JMundia - v1, 6/24/14 12:40 PM - 1 kB)
main (JMundia - v1, 7/23/14 6:05 AM - 724 bytes)

Figure 22: Network Output.

4.4 Training:

Training is done by passing data that the outcome is known. Algorithm is used as a straight forward application of optimization theory and statistical estimation. Gradient Descent Algorithm and Least Mean Square Algorithm have been used in this study. There is use of learning algorithm to make the network learn and there is training algorithm to train the network. Learning rate (µ) is an important consideration to change the weights at each step. If µ is small it will take long time to converge and if it is very large error surface may bounce out of control i.e. lead to divergence.

Below is the training exercise where the data with a FLAG of positive (P) or Negative (N) is input to train the network

This is a phase where the training data is passed to the network to learn the fraudrent patents

Retrieve: This represent the training data source

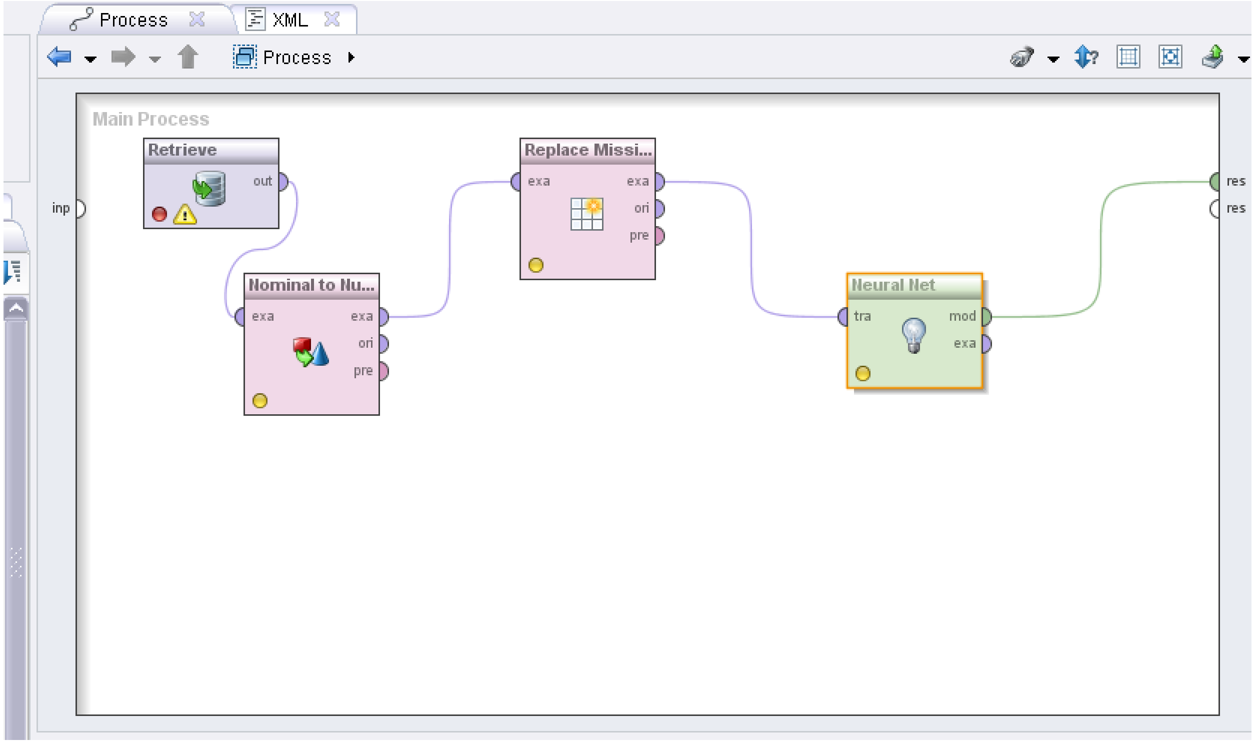


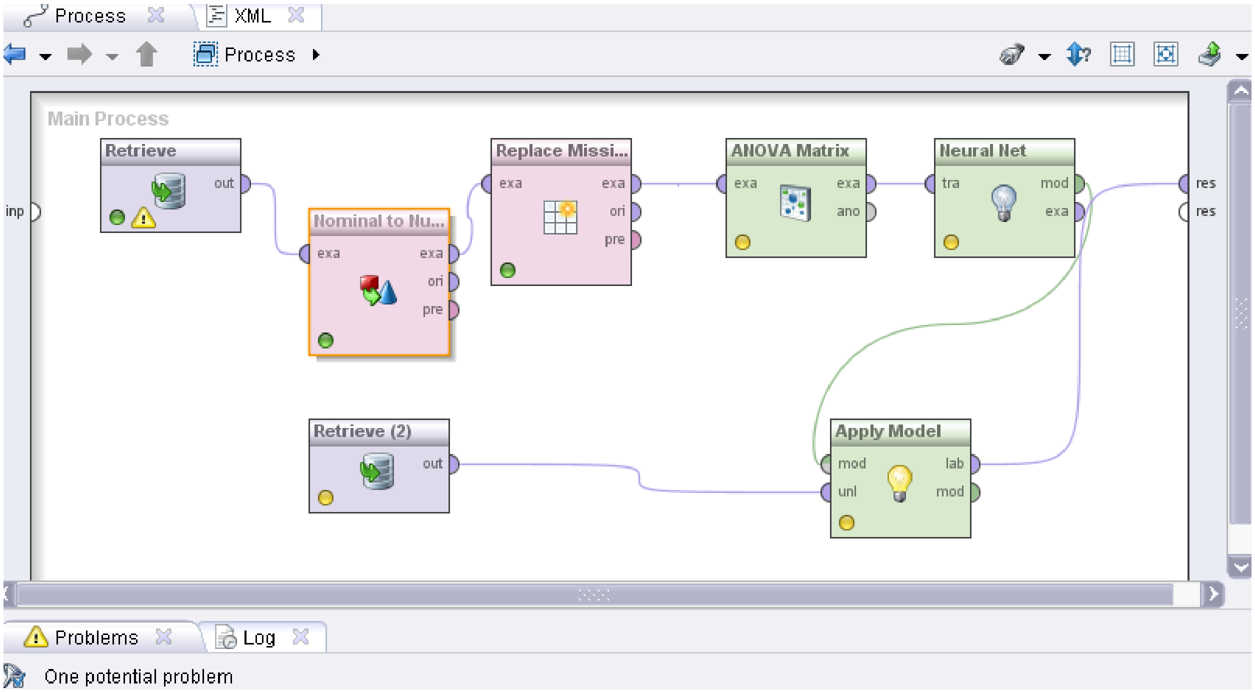
Figure 23: Training Process.

4.5 Testing:

This is the phase where the test data is passed through the network for verification and accuracy determination.

Retrieve: This defines the training used in the Network

Retrieve (2): This defines the test data passed through the Network. The classification is then done and the results compared to the real values.



One potential problem

Figure 24: Testing Process. Source

4.6 Experimentation:

The experiment was carried out by training the Network using 15 datasets captured within one week’s interval for three months (March 2014, April 2014 and May 2014).Testing was carried out using 3 datasets also captured in the same duration as the training data. Training data was be used to training the Network while Testing data was be used to measure the efficiency on the network i.e. Accuracy in classifying new instances

Table 5 show the description of each Training data set

Table 5: Training dataset

Training Data set	Description	Size (No. of records)
Training Data Set 1	Captured in the 1st week of March 2014	10000
Training Data Set 2	Captured in the 2nd week of March 2014	10000
Training Data Set 3	Captured in the 3rd week of March 2014	10000
Training Data Set 4	Captured in the 4th week of March 2014	10000
Training Data Set 5	Captured in the 1st week of April 2014	10000
Training Data Set 6	Captured in the 2nd week of April 2014	10000
Training Data Set 7	Captured in the 3rd week of April 2014	10000
Training Data Set 8	Captured in the 4th week of April 2014	10000
Training Data Set 9	Captured in the 1st week of May 2014	10000
Training Data Set 10	Captured in the 2nd week of May 2014	10000
Training Data Set 11	Captured in the 3rd week of May 2014	10000
Training Data Set 12	Captured in the 4th week of May 2014	10000
Training Data Set 13	Captured in the 4th week of May 2014	1000
Training Data Set 14	Captured in the 4th week of May 2014	100000
Training Data Set 15	Captured in the 4th week of May 2014	500000

Testing was done using 3 data sets described below in table 3

Table 6: Testing Dataset

Training Data set	Description	Size (No. of records)
Testing Data Set 1	Captured in the 4th week of March 2014	500
Testing Data Set 2	Captured in the 4th week of April 2014	500
Testing Data Set 3	Captured in the 4th week of May 2014	500

The two aims of the experiment were:-

- Determine the dependency of training data age in classifying new cases
- Determine the dependency of training data size in classifying new cases

4.6.1 Experimentation procedure:

A total 15 experiments was carried out with each experiment following the below steps:-

i) On the already built Network pass the training data set by selecting the database location (*Retrieve 1*)

ii) Set the parameter to be used in the training process

iii) Train the Network

iv) Pass the Test data on the already trained network (Retrieve 2)

v) Evaluate the results

vi) Calculate the Accuracy of the experiment

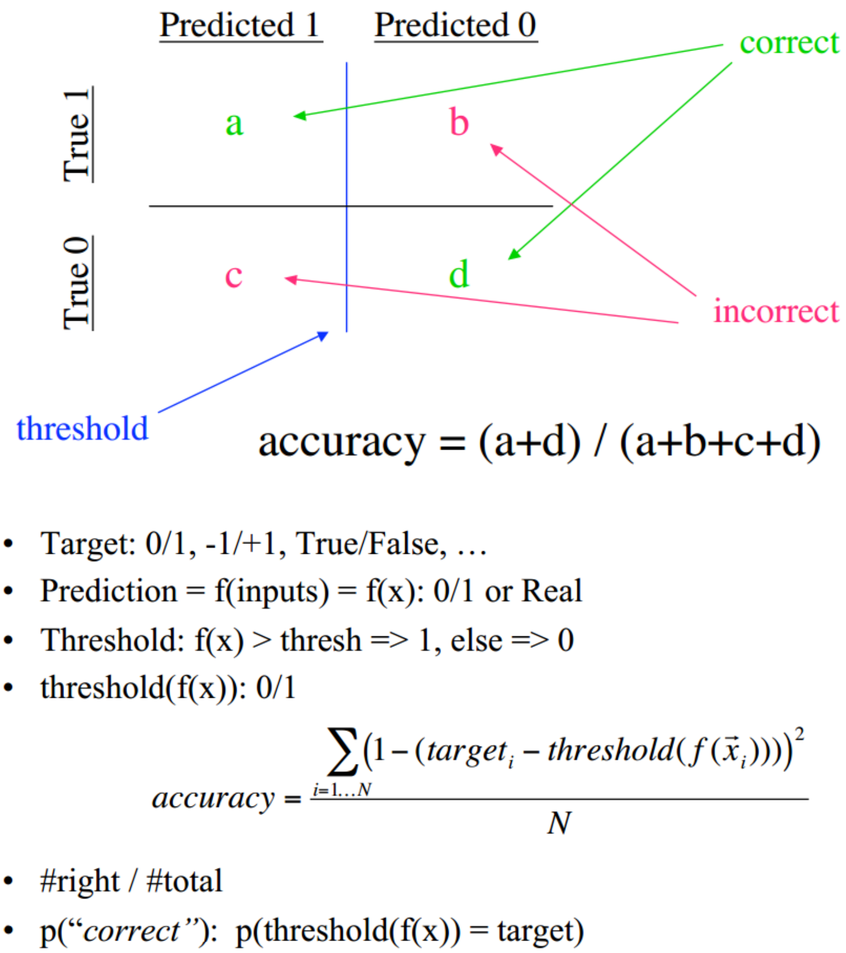
Below is tabulated description for each experiment carried out

Table 7: Experiments Description

			Parameters used			
Experiment	**Training Data set used**	**Test Data set Used**	**Hidden layers**	**Training cycles**	**Learning rate**	**Momentum**
experiment 1	Training Data Set 1	Testing Data Set 1	1	500	0.3	0.2
experiment 2	Training Data Set 2	Testing Data Set 1	1	500	0.3	0.2
experiment 3	Training Data Set 3	Testing Data Set 1	1	500	0.3	0.2
experiment 4	Training Data Set 4	Testing Data Set 1	1	500	0.3	0.2
experiment 5	Training Data Set 5	Testing Data Set 2	1	500	0.3	0.2
experiment 6	Training Data Set 6	Testing Data Set 2	1	500	0.3	0.2
experiment 7	Training Data Set 7	Testing Data Set 2	1	500	0.3	0.2
experiment 8	Training Data Set 8	Testing Data Set 2	1	500	0.3	0.2
experiment 9	Training Data Set 9	Testing Data Set 3	1	500	0.3	0.2
experiment 10	Training Data Set 10	Testing Data Set 3	1	500	0.3	0.2
experiment 11	Training Data Set 11	Testing Data Set 3	1	500	0.3	0.2
experiment 12	Training Data Set 12	Testing Data Set 3	1	500	0.3	0.2
experiment 13	Training Data Set 13	Testing Data Set 3	1	500	0.3	0.2
experiment 14	Training Data Set 14	Testing Data Set 3	1	500	0.3	0.2
experiment 15	Training Data Set 15	Testing Data Set 3	1	500	0.3	0.2

4.7 Accuracy computation:

This is a measure of how close to the actual value or classification and every classification will lie in any of the below four sections



accuracy = (a+d) / (a+b+c+d)

- Target: 0/1, -1/+1, True/False, …
- Prediction = f(inputs) = f(x): 0/1 or Real
- Threshold: f(x) > thresh => 1, else => 0
- threshold(f(x)): 0/1

$$accuracy = \frac{\sum_{i=1\ldots N}\left(1-(target_i - threshold(f(\vec{x}_i)))\right)^2}{N}$$

- #right / #total
- p("*correct*"): p(threshold(f(x)) = target)

Simplified by the formula:

% Error = (YV – AV) x 100 ÷ AV

%accuracy = 100-%Error

Where: YV is the measured Value & AV is the Accepted Value

4.8 Results:

Below are the results for the experiments grouped by the month the data was captured and the aim of the experiment.

4.8.1 Results for the experiments 1, 2, 3 and 4

These are the results for the experiments carried out with data captured in the Month of March 2014 (beginning from 3rd March to 29th march). The Aim of these experiments was to evaluate the effect of training data age in detecting the current fraud-rent calls.

Each training dataset contained 10,000 records and a testing dataset of 500 records was used in every experiment

Training set: 10000 records

Test set: 500 records

Table 8: Results for the experiments 1,2, 3 and 4

RUN	% categorized as Fraudrent (+ve)	% categorized as non fraudrent (-ve)	% False positive	%False Negative	%True Positive	%True Negative	%Accuracy
Experiment 1 (Training data 4 weeks old)	7.45	92.55	31.45	25.36	68.55	74.64	71.59
Experiment 2 (Training data 3 weeks old)	5.56	94.44	16.78	2.48	83.22	97.52	90.37
Experiment 3 (Training data 2 weeks old)	4.42	95.58	17.76	11.04	82.24	88.96	85.56
Experiment 4 (Training data up to date)	5.78	94.22	7.26	9.23	92.74	90.77	91.77

4.8.2 Results for the experiments 5, 6, 7 and 8

These are the results for the experiments carried out with data captured in the Month of April 2014 (beginning from 3rd April to 30th April). The Aim of these experiments was to evaluate the effect of training data age in detecting the current fraud-rent calls.

Each training dataset contained 10,000 records and a testing dataset of 500 records was used in every experiment

Training set: 10000 records

Test set: 500 records

Table 9: Results for the experiments 5, 6, 7 and 8

RUN	% categorized as Fraud rent (+ve)	% categorized as non-fraud rent (-ve)	% False positive	%False Negative	%True Positive	%True Negative	%accuracy
Experiment 5 (Training data 4 weeks old)	12.56	87.44	25.23	25.36	74.77	74.64	74.70
Experiment 6 (Training data 3 weeks old)	10.45	89.55	22.36	16.26	77.64	83.74	80.69
Experiment 7 (Training data 2 weeks old)	13.67	86.33	16.26	5.62	83.74	94.38	89.06
Experiment 8 (Training data up to date)	12.57	87.43	4.23	4.26	95.77	95.74	95.77

4.8.3 Results for the experiments 9, 10, 11 and 12

These are the results for the experiments carried out with data captured in the Month of April 2014 (beginning from 2nd May to 29th May). The Aim of these experiments was to evaluate the effect of training data age in detecting the current frauderent calls.

Each training dataset contained 10,000 records and a testing dataset of 500 records was used in every experiment

Training set: 10000 records

Test set: 500 records

Table 10: Results for the experiments 9, 10, 11 and 12

RUN	**% categorized as Fraud rent (+ve)**	**% categorized as non-fraud rent (-ve)**	**% False positive**	**%False Negative**	**%True Positive**	**%True Negative**	**%Accuracy**
Experiment 9 (Training data 4 weeks old)	3.58	96.42	16.58	8.25	83.42	91.75	87.58
Experiment 10 (Training data 3 weeks old)	4.26	95.74	13.59	6.89	86.41	93.11	89.76
Experiment 11 (Training data 2 weeks old)	3.56	96.44	12.96	4.23	87.04	95.77	91.04
Experiment 12 (Training data up to date)	2.39	97.61	5.24	4.26	94.76	95.74	95.25

4.8.4 Results for the experiments 13, 14, 15 and 12

This run was carried out with data captured in the Month of April 2014 (beginning from 2nd May to 29th May). The experiment was to evaluate the accuracy of the Neural network in detecting fraud-rent call while using training data of a constant age set but different training dataset sizes (1000 records,10000 records,100000 records and 500000 records)

Each training data set call records are 1 day old and the same testing data set of 500 records is used in every experiment

The Aim of this was to evaluate the effect of training data size in detecting the current fraud-rent calls.

Table 11: Results for the experiments 13, 14, 15 and 12

RUN	% categorized as Fraud rent (+ve)	% categorized as non-fraud rent (-ve)	% False positive	%False Negative	%True Positive	%True Negative	%Accuracy
Experiment 13 (1000 size training set)	4.18	95.82	22.58	11.25	77.42	88.75	83.08
Experiment 12 (10000 size training set)	2.39	97.61	5.24	4.26	94.76	95.74	95.25
Experiment 14 (100000 size training set)	3.27	96.73	10.96	4.23	94.94	95.77	95.45
Experiment 15 (500000 size training set)	1.39	98.61	10.25	3.76	94.92	96.24	95.99

4.9 Discussion:

In section we will analysis the factors affecting the classification accuracy and the call records attributes influence in classification process

4.9.1 Training Dataset Age Analysis

The accuracy of the network is highly affected by the time gap between the training and the testing data, as per the results the accuracy of the network is highly improved when more recent data is used to train the network.

Below is the summarized accuracy result for the time variant training datasets

Table 12: Accuracy Summary.

Training dataset	% Accuracy
Training data 4 weeks old	77.96
Training data 3 weeks old	86.94
Training data 2 weeks old	88.55
Training data up to date	94.23

From the analysis above, Training data older than one week will result to a more than 10% prediction error which is way on the high side

This is can majorly be attributed to the below:

Changing patterns of the fraudsters: - past treads and patterns become absolute and inaccurate to be used to predict current fraud rent activities

Data inaccuracy: - This is caused by the changes that happen on the data i.e. Phone number changes, Location change, rating changes. As a result the accuracy on the prediction will highly reduce

***Environmental changes:* -** These are changes that happen in the telecommunication industry i.e. phone models, Promotions offered the provides etc. . This will highly affect the calling patterns hence invalidating the results if the time gap between training and testing is very wide

As a result the training of the network should happen at least one a week to achieve more than 90 % accuracy levels which lies on the acceptable range

4.9.2 Training Size Analysis

Based on the result on table 5, the training size is has a major effect on the classification

The bigger the training set the more the accuracy. But as the training set grows, the accuracy tends to be constant.

From the above analysis the optimum size would be 100000 as the increasing the size above this value does not translate to increased accuracy

4.9.3 Attribute Influences Analysis:

Below is a table representing the average weights associated with each attribute by the Neural Network

Table 13: Attribute Influence Summary.

Attribute	weight allocated
Orgn number	8.96
Dest number	2.36
Call_location	9.25
Call duration	5.26
Phone model	6.25
First_name	3.39

Last_name	4.25
Rating	7.25
Number of calls received in minute	2.69
Number of calls made in a minute	4.26
Flag status	5.23
MSIDN age	6.36

The attributes can be categorized into two:

Attributes influenced by the caller: - these are attributes that are majorly in the control by the call initiator e.g. Call location, Rating MSIDN age

Attributes influenced by the receiver: - these are attributes that are majorly in the control by the call terminator e.g. Number of calls received

Call location and the call origin number had the highest influence with an average weight of 9.25 and 8.96 respectively

Destination Number (MISDN) and Number of calls received in a minute had the lowest influence to the Network

Based on the above observation, the major influencers on the call classification are the attributes that are solely dependent on the call originator

Chapter 5: CONCLUSION

5.1 Achievements:

The main objective of the study was to test and evaluate the performance of Artificial Neural Networks in detecting mobile fraud. This was achieved by building the Network using *RapidMiner* tool then training the network using data captured in three months and finally testing the Network by passing actual classified data from the service provider. From the study, Neural Network can be used to classify call and SMS records and detect fraud-rent ones. The advantage in the utilization of a neural network in the mobile phone fraud detection was the flexibility that the network provided. A neural network was capable of analyzing the data from the network, even if the data was incomplete or distorted. Similarly, the network possessed the ability to conduct an analysis with data in a non-linear fashion. Both of these characteristics were important in a networked environment where the information which was received was subject to the random failings of the system. Further, because some attacks may have been conducted against the network in a coordinated assault by multiple attackers, the ability to process data from a number of sources in a non-linear fashion was important.

The inherent speed of neural networks was another benefit of this approach. Because the output of a neural network is expressed in the form of a probability the neural network provided a predictive capability to the detection of instances of mobile phone fraud.

However, the most important advantage of neural networks in fraud detection was the ability of the neural network to "learn" the characteristics of the fraud and identify instances that are unlike any which have been observed before by the network. A neural network might be trained to recognize known suspicious events with a high degree of accuracy. While this would be a very valuable ability, since attackers often emulate the "successes" of others, the network would also gain the ability to apply this knowledge to identify instances of attacks which did not match the exact characteristics of previous fraud-rent activity.

The other objective was to establishing the mobile phone fraud patterns and the calls’ attributes influence in fraud detection which was achieved by evaluating the weight assigned by the Network on each call/SMS record attribute. It was noted that some on the attributes had more weight compare to others and this helped curve out the fraud-rent patterns

From the analysis it was noted that Training data age is very key in determining the accuracy on the results and using the most recent data is paramount in achieving accurate result. From the experiments it was clear that a Network that was trained using older data was less accurate in classifying new fraud case. In addition, an adequate training set size is required to achieve an acceptable level of accuracy. As we found out from the experiments that training the Network using a certain number of records reduced the accuracy drastically

5.2 Challenges

Due to the limited information in a call record, it was difficult to dig deep on a more detailed analysis probably based on other factors like SIM card swapping. We used call features such as call duration, call time, location etc. However, some of them exhibit significant difference between fraud numbers and legitimate numbers. If more call attributes or features like user calling history can be used, this can highly improve detection accuracy

The other challenge of using Artificial Neural Network related to the training requirements of the Neural Network. Because the ability of the artificial Neural Network to identify indications of a fraud is completely dependent on the accurate training, this demanded a very high computation resource especially for experimental cases that involved huge number of records. For example the training exercise that involved 500000 records run for 3 days. The training routine requires a very large amount of resource to ensure that the results are statistically accurate and are completed on time.

5.3 Future works

In our study, we managed to use only one hidden Neural Network layer due to the computation resource limitation. It would be a good study in future to evaluate the performance on the Neural Network while using more than one hidden layer. This may have an improved accuracy in comparison to a single layered network

Also in our study we used 12 attribute for a call or SMS record, In future more attributes can be used to define a call record and study how these attributes affect the classification accuracy. In addition more study can be done on the effect of increasing the number of training cycles i.e. passing the same training dataset multiple times

Combination of the Neural Network with other classifier to classify same set of data can be another area of study in future.

REFERENCES

[1] Admob A. 2013, *The insider's guide to mobile Web/marketing in Kenya*

Available at: *ttp://www.ihub.co.ke/ihubresearch/uploads/2012/july/1343053407_819_604.pdf*

[2] Bbc, 2012. *Over 5 billion mobile phone connections worldwide, Article 10569081*

Available at: *http://www.bbc.co.uk/news/10569081.*

[3] Business Monitor International, May 2013

Available at: *http://euwifo.ch/press/2013_23/pressemitteilung_int_english.pdf*

[4] Jacob B., et al., 2005. *Introduction to Grid Computing.*

Available at: *http://www.vldb2005.org/program/paper/tue/p169-metwally.pdf*

[5] Jimmy M., et al., 1998. *An Approach to Rules based Fraud Management inEmerging Converged Networks*

Available at: *http://eprints.wit.ie/619/1/2003_ITSRS_McGibney_Hearne_final.pdf*

[6] Jose C., 2000 *Neural Networks and Adaptive Systems*

Available at: *http://eu.wiley.com/WileyCDA/WileyTitle/productCd-0471351679.html*

[7] Michael M. 2013. *Understanding Mobile Networks Work,* Article 2021961

Available at: *http://www.quepublishing.com/articles/article.aspx?p=2021961*

[8] Simon H. et al., 1994. *Neural Networks, New York: Macmillan*

Available at *http://conferences.sigcomm.org/imc/2007/papers/imc170.pdf*

[9] Haykin, et al., 2007. Computational methods for dynamic graphs. *Journal of Isolating and Analyzing Fraud Activities in a Large Cellular Network via Voice Call Graph Analysis*

Available at: *http://networking.cs.umn.edu/newsite/sites/default/files/isolating-fraud-cellular-networks.pdf*

APPENDICES

HTML code for the network:

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<process version="5.1.006">
 <context>
  <input/>
  <output/>
  <macros/>
 </context>
 <operator activated="true" class="process" compatibility="5.1.006" expanded="true" name="Process">
  <process expanded="true" height="325" width="681">
   <operator activated="true" class="retrieve" compatibility="5.1.006" expanded="true" height="60" name="Retrieve" width="90" x="45" y="30">
    <parameter key="repository_entry" value="//NewLocalRepository/main_project/main_p"/>
   </operator>
   <operator activated="true" class="retrieve" compatibility="5.1.006" expanded="true" height="60" name="Retrieve (2)" width="90" x="179" y="210">
    <parameter key="repository_entry" value="main_testing"/>
   </operator>
```

```
    <operator activated="true" class="nominal_to_numerical" compatibility="5.1.006" expanded="true" height="94" name="Nominal to Numerical" width="90" x="179" y="75"/>

    <operator activated="true" class="replace_missing_values" compatibility="5.1.006" expanded="true" height="94" name="Replace Missing Values" width="90" x="296" y="30">

      <list key="columns"/>

    </operator>

    <operator activated="true" class="anova_matrix" compatibility="5.1.006" expanded="true" height="76" name="ANOVA Matrix" width="90" x="447" y="30"/>

    <operator activated="true" class="neural_net" compatibility="5.1.006" expanded="true" height="76" name="Neural Net" width="90" x="581" y="30">

      <list key="hidden_layers"/>

    </operator>

    <operator activated="true" class="apply_model" compatibility="5.1.006" expanded="true" height="76" name="Apply Model" width="90" x="514" y="210">

      <list key="application_parameters"/>

    </operator>

    <connect from_op="Retrieve" from_port="output" to_op="Nominal to Numerical" to_port="example set input"/>

    <connect from_op="Retrieve (2)" from_port="output" to_op="Apply Model" to_port="unlabelled data"/>

    <connect from_op="Nominal to Numerical" from_port="example set output" to_op="Replace Missing Values" to_port="example set input"/>
    <connect from_op="Replace Missing Values" from_port="example set output" to_op="ANOVA Matrix" to_port="example set"/>
    <connect from_op="ANOVA Matrix" from_port="example set" to_op="Neural Net" to_port="training set"/>
    <connect from_op="Neural Net" from_port="model" to_op="Apply Model" to_port="model"/>
    <connect from_op="Apply Model" from_port="labelled data" to_port="result 1"/>
    <portSpacing port="source_input 1" spacing="18"/>
    <portSpacing port="sink_result 1" spacing="0"/>
    <portSpacing port="sink_result 2" spacing="0"/>
  </process>
 </operator>
</process>
```