Scientific Research Publishing

Int. J. Communications, Network and System Sciences, 2022, 15, 167-180
https://www.scirp.org/journal/ijcns
ISSN Online: 1913-3723
ISSN Print: 1913-3715

Analysis of Global System for Mobile Communication (GSM) Subscription Fraud Detection System

E. N. Ekwonwune[1], U. C. Chukwuebuka[1], A. E. Duroha[2], A. N. Duru[3]

[1]Department of Computer Science, Imo State University, Owerri, Nigeria
[2]Department of Computer Science, Gregory University, Abia, Nigeria
[3]Department of Computer Science, Federal University of Technology, Owerri, Nigeria
Email: ekwonwuneemmanuel@yahoo.com

How to cite this paper: Ekwonwune, E.N., Chukwuebuka, U.C., Duroha, A.E. and Duru, A.N. (2022) Analysis of Global System for Mobile Communication (GSM) Subscription Fraud Detection System. *Int. J. Communications, Network and System Sciences*, **15**, 167-180.
https://doi.org/10.4236/ijcns.2022.1510012

Received: September 15, 2022
Accepted: October 28, 2022
Published: October 31, 2022

Abstract

This work is concerned with GSM subscription fraud detection system using some network techniques. Fraud is a hitch around the globe with huge loss of income. Fraud has an effect on the credibility and performance of telecommunication companies. The most difficult problem that faces the industry is the fact that fraud is dynamic, which means that whenever fraudsters feel that they will be detected, they devise other ways to circumvent security measures. In such cases, the perpetrators' intention is to completely avoid or at least reduce the charges for using the services. Subscription fraud is one of the major types of telecommunication fraud in which a customer obtains an account without intention to pay the bill. Thus at the level of a phone number, all transactions from the number will be fraudulent. In such cases abnormal usage occurs throughout the active period of the account; which is usually used for call selling or intensive self usage. This provides a means for illegal high profit business for fraudsters requiring minimal investment and relatively low risk of getting caught. A system to prevent subscription fraud in GSM telecommunications with high impact on long distance carriers is proposed to detect fraud. The system employs adaptive flexible techniques using advanced data analysis like Artificial Neural Networks (ANN). This study aims at developing a fraud detection model occurrence in GSM Network. The paper also gives analysis of the fraud detection Systems, fraud detection and prevention, fraud prevention methods etc. Fraud affects us all and is of particular concern to those who manage large government and business organisations where the potential losses are greatest. The operation of a mobile network is complex, and fraudsters invest a lot of energy to find and exploit every weakness of the system. A typical example would be subscription fraud,

where a fraudster acquires a subscription to the mobile network under a false identity; and start reselling the use of his phone to unscrupulous customers (typically for international calls to distant foreign countries) at rate less than the regular tariff.

Keywords

GSM, Fraud, Mobile, Fraud Detection, Communication System, Mobile Telecommunication

1. Introduction

Following the exponential growth in the telecommunications sector in the end of the last decades, telecommunication operators face a new challenge: fraud. It is not only a risk, but a highly organized global business, that affects operators all over the world. In order to realize the severity of this problem, Communication Fraud Control Association (CFCA) published some statistics stating that the annual global fraud losses in the telecoms sector are now between US$54 Billion and $60 Billion, an increase of 52% since 2003. Global System for Mobile communication (GSM) fraud, has identified itself as the single biggest cause of revenue loss for telecom carriers with the increasing number of mobile phone users, Global mobile phone fraud is also set to rise. Known fraud scenarios are: subscription fraud, dial through fraud, free phone fraud, handset theft and roaming fraud. The Cambridge Advanced learners Dictionary defines fraud as "the crime of obtaining money by deceiving people", while the concise Oxford Dictionary defines it as a "criminal deception by the use of false representations to gain an unjust advantage". GSM fraud can simply be described as any activity by which service is obtained without intention of paying. Using the definitions, fraud can only be detected once it has occurred. In subscription fraud, the typical behaviour of fraudsters is to abuse service by making significant usage of telecom services (for example, calling, messaging, internet, etc) before the bill is served. Customers' applications are sometimes rejected by the company at the time of application if they find that it is risky to entertain customers who are likely to have bad dept. The followings are known types of fraud scenarios: neural network models of subscription fraud were proposed by [1] at the time of application.

1.1. Statement of the Problem

Currently, due to the development of new technologies, traditional fraudulent activities, such as money laundering, have been joined by new kind of fraud like GSM fraud and computer intrusion. Fraud is increasing dramatically each year resulting in loss of a large amount of money worldwide.

The following problems have been identified as likely causes of increase in subscription fraud.

1) The use of GSM lines without proper registration of SIM card.
2) Call roaming, that is making calls outside home system.
3) Signing up GSM telecom service, using false or stolen identification.
4) No standard fraud detection system to checkmate fraudsters.

1.2. Aim and Objectives of Study

The study is aimed at developing a fraud detection model occurrence in GSM Network.

The objectives used to achieve the aim are as following:-

1) To develop an architecture for the detection of GSM telecom fraud with an alarm system.
2) To develop a software for the detection of GSM telecom fraud.

1.3. Significance of the Study

If fraud is properly handled using artificial neural network, there are more beneficial to both the subscriber and service provider. The benefits are:

1) Prevention of revenue loss.
2) Detection of untrustworthy dealers.
3) Reduction of widespread costs by subscription fraud.
4) Identification of fraudsters, when the use of a service that is not properly registered.

2. Theoretical Framework

Many definitions in the literature exist, where the intention of the subscriber plays a central role. Johnson defines fraud as any transmission of voice data across a telecommunications network, where the intent of the sender is to avoid or reduce legitimate call charges [2]. In similar vein, fraud was defined as obtaining unbuildable services and nude-served fees. Hoath considers fraud as attractive from fraudster's point of view, since detection risk is low, no special equipment is needed, and product in question is easily converted to cash as cited. Although the term fraud has particular meaning in legislation, this established term is used broadly to mean, misuse, dishonest intention or improper conduct without implying any legal consequences. Fraud is a problem for all businesses, it is generally internal or external or a combination (collusion). Increased innovation in telecoms fuels more fraud; also increased competition provides more avenues of attack and increased mobility also means fraudsters are harder to track down when internationally organized. In survey conducted by communication control fraud association (CFCA), including 123 operators in more than 30 countries, the survey estimated the global fraud loss as in the following [3]:

1) 72$ - 80$ billion (USD) annually (34% increase from 2005).
2) Approx. 4.5% of telecom revenue.
3) 91% global fraud losses increased or stay the same.

4) Top 3 fraud types:
5) 22$ billion—subscription fraud.
6) 15$ billion—compromise private branch exchange (PBX).
7) 4.5$ billion—premium rate service (PRS) fraud.

2.1. The Genesis of Fraud in Telecommunication (GSM) Services

Fraud exists in every operator in every country throughout the world. There are no exceptions. Committing fraud does not need highly complex equipment or skills. Fraudsters are normally lazy people. Fraudulent application for service is the first step in achieving illegal access to network services, Fraudsters prey on operator's weaknesses in their controls and procedures. In a recent survey 85% of the communications operators surveyed stated that global fraud losses have increased. All operators will suffer from some internal fraud at some point irrespective of whether they believe their employees are all honest and trustworthy "Top 5" Countries where fraud was concentrated were Pakistan, Philippines, Cuba, India and Bangladesh.

[4] proposed on a geographic basis, operators in Middle East and Africa suffered most, experiencing more than 20% losses, while Asia close behind at just below 20% and Central America and Latina America at more than 15%. Western Europe ranked lowest in losses at about 7%, while by Central and Eastern Europe 8% and North America just about at the average of [3], so Is fraud different here (Palestine) than other countries? The answers may be no, or yes:

1) NO: A subscription fraud is a subscription fraud where ever in the world.
2) YES: Local culture and sales offerings, method of activation etc.

No one really knows how much fraud is costing the industry with estimates varying considerably thus:

a) Unpaid bills and defaulting customers are costing mobile operators around US$26 billion every year with around 5% of total billings being written off annually

b) The Communications Fraud Control Association, estimated that annual global fraud losses in the telecoms sector *i.e.* between $54 billion and $60 billion, an increase of 52 percent from previous years.

c) The CFCA also estimated that global annual losses to fraud account for 5 percent of the total telecom sector revenue with mobile operators seen as more vulnerable than fixed line.

d) 47.3% of global fraud losses are from Subscription/Identity Document (ID) Theft and Private Branch Exchange PBX/Voicemail.

Fraud losses continue to impact virtually every business enterprise, despite significant advances in fraud detection technology, fraud losses continue to pose a significant problem to many finance, insurance, health care, internet merchants, brokerage and securities, and many others in the telecom industry. We can only estimate the cost because operators are reluctant to admit to fraud or are not actively looking for fraudulent accounts in the bad debt [5], also the business driv-

er is for subscriber growth and market share, therefore, the fact that huge number of the new customers could actually be fraudsters is not taken into consideration. Responsibility for chasing unpaid bills is spread across a variety of departments which could include billing, IT, fraud, credit management, customer service, collections and the finance departments. This often results in an ineffective ability to collect debts and a1so does not help identify fraud as skills are not present in all business areas to identify fraudsters as opposed to bad debtors in [6]

2.1.1. Subscription Fraud

It is considered as one of the most commonly suffered frauds by operators and accounts for most of their secondary losses; it is airtime related, looks for weaknesses and exploits them. The Subscription fraud result looks like bad debt and is often misinterpreted as bad debt. It is estimated that 70% of fraud losses relate to subscription fraud which is over $28 billion a year (78 million dollars a day!) [7]

2.1.2. Identity Thefts

Identity theft is one of the fastest growing crimes in certain countries, not just related to telecom but all types of financial service. Fraudsters may assume the identity of another "genuine person" in order to obtain service, they can also create identities which are even harder to detect once established. Generally fraudsters are using details that are guaranteed to pass credit checks, customer profiling and validation, they obtain information from any source of computer records, paper records, (steal it, pay for it, simply just find it!). It is often the case that fraudulent accounts will initially look like and behave like operator best customer and, in certain countries they pay people to "use" their identities to obtain telecom services as in [8].

2.1.3. Roaming Fraud

Roaming is an act of a cellular customer to automatically make and receive voice calls, send and receive data, or access other services when travelling outside the geographical coverage area of the home network, by means of using a visited network. Roaming is technically supported by mobility management, authentication and billing procedures. Establishing roaming between network operators is based on—and the commercial terms are contained in—Roaming Agreements. If the visited network is in the same country as the home network, this is known as National Roaming. If the visited network is outside the home country, this is known as International Roaming (the term Global Roaming has also been used). If the visited network operates on a different technical standard than the home network, this is known as Inter-standard roaming. GSM Roaming, which involves roaming between GSM networks, offers the convenience of a single number, a single bill and a single phone with worldwide access to over 218 countries. The convenience of GSM Roaming has been a key driver behind the global success of the GSM Platform.

The roaming fraud principle is that the home network is responsible for its customers (and their cellular identities) when roaming on another network irrespective of the fraud type. The visited network will only be liable if the roaming agreement has not been complied with Call Details Records – CDR's or fraud alerts not sent on time. The abuse of roaming facilities to make free calls has been a major issue for a number of operators with reported losses being in millions [9]. Roaming subscription fraud has been the major problem across the GSM world (SIM card) is simply taken to another market. Satellite roaming problems also occur in the delivery of information. Also prepaid roaming fraud increases as operators are not prepared for it, and sometimes not even looking at prepaid Test Access Path (TAP) files.

2.1.4. Direct Inward System Access (DISA) Fraud

Most businesses of Telephone Systems have a feature called Direct Inward System Access or DISA for short. This feature allows authorized users to dial a special number into one's telephone system and then either dial extension numbers directly or outside numbers utilizing one's company's less expensive long distance trunks and services. Risk increases due to a lack of understanding of risks by the customer, they "trust" or rely on the PBX provider to provide the required security settings to prevent fraud. Recent victims have included telecom Operators, financial institutions, anyone who is normally involved in making high numbers of IDD calls. Recall it will not be the telecom provider that is defrauded; it will be the customer whose PBX is abused who suffers the loss.

2.1.5. Phone Thefts

Mobile phone theft has risen 190% in recent years. In the UK a handset is stolen every 12 seconds; phone jacking is costing UK consumers $M780 every year. Fraudsters now develop sophisticated techniques to pass off stolen handsets as legitimate. Evidence of new techniques being developed to conceal stolen phones has been uncovered where the UK Police suspect crooks are taking stolen handsets, illegally changing their IMEI (International Mobile Station Equipment Identity) numbers and then giving them fake interiors complete with counterfeit IMEI labels of their own production plants. Incidents of mobile phone theft/Snatching are also on the rise worldwide, cases involving mobile phone thefts top the list of crimes reported in Bangalore [10].

2.1.6. Voicemail Fraud

Voice-mail (also known as voicemail, voice message or voice bank) is a computer based system that allows users and subscribers to exchange personal voice messages; to select and deliver voice information; and to process transactions relating to individuals, organizations, products and services, using an ordinary telephone. The term is also used more broadly to denote any system of conveying a stored telecommunications voice messages, including using an answering machine. If one's does not change the default password on one's voice mailbox, one's company, could be in for a big—and expensive—surprise. The Federal

Communications Commission (FCC) has become aware of a form of fraud that allows hackers to use a consumer's or business's voice mail system and the default password to accept and collect calls without the knowledge or permission of the consumer. A hacker calls into a voice mail system and searches for voice mailboxes that still have the default passwords active or have passwords with easily-guessed combinations, like 1-2-3-4. (Hackers know common default passwords and are able to try out the common ones until they can break into the phone system.) The hacker then uses the password to access the phone system and makes international calls. There is also another twist to this scam. A hacker breaks into voice mailboxes that have remote notification systems that forward calls or messages to the mailbox owner. The hacker programs the remote notification service to forward to an international number. The hacker is then able to make international calls.

2.1.7. Some Factors Leading to Telecom Fraud

1) How the technology is actually installed and configured, default settings.
2) How the technology, products and services are sold /offered.
3) Inherent weaknesses in procedures and working practices.
4) Lack of management control, supervision and monitoring.
5) Lack of knowledge and experience of personnel.
6) Rush to market—no product or service fraud risk evaluation.

2.1.8. Fraudsters and Their Location

1) Fraud has and can be committed by any type of person in society, whatever the social status, nationality, or position/role within the business If they have the driver (initiative, desire, commitment, purpose etc) they will find the way and means to commit fraud, no one is exempted.

2) Bernard Ebbers, the former Chief Executive Officer (CEO) of Wor1dCom. was sentenced to 25 years in Jail for orchestrating an $11 billion fraud.

3) Bernard Maddoff, non executive chairman at NASDAQ stock exchange, commited the largest financial fraud in history, with losses estimated at $65 billion based on a "Ponzi Scheme"—a pyramidal build up. Leading to inevitable collapse. He has been convicted and sentenced to 150 years in prison.

Company managers were named as the biggest perpetrators in a recent fraud survey as they are often not being watched; they are trusted and have access to more information and systems than other employees under them.

External fraudsters can work from anywhere as they often have people working for them whilst they control the fraud activities centrally. Often they will pay for personal details, identity documents, or pay other people to obtain subscriptions for them in their name to avoid detection. "The end justifies the means". Roaming frauds are committed outside of the home network with either the fraudster or their contacts being in another country running the fraud; they cross international boundaries, and operate globally. Hackers can work from anywhere there is internet access, unlimited opportunities provided by technology.

Internal frauds committed from inside the company often with outside collusion and influence are far easier to commit from within [11].

2.1.9. Reasons for Committing Fraud

1) Incentive—What does the fraudster expect to receive for committing the crime, easy money with minimal risk?

2) Opportunity—Can the fraudster successfully commit the crime and get away with it. Lack of adequate supervision of activities, weak Internal controls, no accountability, and ineffective audits present opportunities for the fraudster.

3) Rationalization—Fraudsters believe they can commit their crimes and their actions are justified. They do not live by the same acceptable norms and standards of society. They commit fraud simply because they can and do not care about their victims.

4) Capability—The fraudster must have the requisite education, skills, knowledge, expertise and experience to be capable of effectively committing the fraud.

2.2. Fraud Prevention and Detection

The biggest revenue leakage area in the telecom industry is fraud. Global telecommunications fraud losses are estimated in the tens of billions of dollars every year. The history of telecommunications crime, including several types of fraudulent activities, was reviewed by some authors have emphasized the importance of distinguishing between fraud prevention and fraud detection. Fraud prevention describes measures to avoid fraud to occur in the first place. In contrast, fraud detection involves identifying fraud as quick as possible once it has been committed. In [12], the authors distinguished six different fraud scenarios: Subscription fraud, which is defined as the use of telephone services with no intention of paying, is probably the most significant and prevalent worldwide telecom fraud Subscription fraud can be subdivided into two categories: (a) for profit, *i.e.* mainly for selling long distance calls and (b) for personal usage. Subscription fraud can be committed upon fixed and mobile telephones, and it is usually difficult to distinguish from bad debt, particularly if the fraud is for personal usage. Both subscription fraud and bad debt are major problems to telecoms in developing and third world countries. Two strategies have been proposed for detecting subscription fraud: examining account applications and tracking customer behavior [13]. Other efforts have focused on formalizing and predicting the deceiving intention of fraudsters. The detection of fraud in mobile telecommunications was investigated in the European project ASPeCT (Advance Security for Personal Communications Technologies) [14]. The ASPeCT fraud detection tool is based on investigating sequences of call detail records (CDRs), which contain the details of each mobile phone call attempt for billing purposes. The information produced for billing also contains usage behaviour information valuable for fraud detection. A differential analysis is performed to identify a fraudster through profiling the behaviour of a user. The analysis of user profiles are based on comparison of recent and longer-term behaviour histories derived from the

toll ticket data. Alarms are activated when the usage pattern of a mobile phone changes significantly over a short period of time. The ASPeCT fraud detection tool utilizes a rule-based system for identifying certain frauds, and neural networks (NNs) to deal with novel or abnormal instances or scenarios. In [8], the author used customer data, in addition to CDRs, to discover rules for identifying subscription fraud. A fraud detection algorithm has two components: 1) a summary of the activity on an account that can be kept current and 2) rules that are applied to account summaries to identify accounts with fraudulent activity. A popular approach is to reduce the CDRs for an account to several statistics that are computed for each period, e.g. average call duration, and compare them to thresholds. The authors developed a method for choosing account-specific thresholds rather than universal thresholds. Their procedure takes daily traffic summaries for a set of accounts that experienced at least 30 days of fraud-free traffic activity followed by a period of fraud. This method was applied to cellular cloning, in which fraudulent usage is superimposed upon the legitimate usage of an account. For each account a set of rules that distinguish fraud from non-fraud was developed. The superset of the rules for all accounts was then pruned by keeping only those that cover many accounts, with possibly different thresholds for different accounts.

2.2.1. Fraud Prevention

Fraud prevention describes measures to avoid fraud to occur in the first place.

Fraud is a generic category of crime which involves an individual or group of individuals dishonestly obtaining property or some financial advantage by means of deception. Perpetrators of fraud may seek to gain money, property, time or information and the means used are as varied as are the opportunities which arise. Offenders may be individuals or employees or managers of organisations in both the public and private sectors, while their victims may be their employers as well as individual consumers of any age and gender. Put simply, fraud affects us all and is of particular concern to those who manage large government and business organisations where the potential losses are greatest. Strategies used to prevent and to control fraud are astoundingly diverse, varying from the most general policy statements designed to ensure the efficient conduct of business organisations, to highly specific information offered to enable people to avoid personal victimisation. Fraud prevention involves a complex and sensitive process of balancing an organisations diverse interests and limited resources. Some solutions may be totally effective in terms of reducing fraud but may have the consequence of stifling commerce and making everyday business transactions so unwieldy and costly to manage that one would be willing to use them. Fraud prevention should, therefore, aim to maximise crime reduction without imposing unrealistic burdens on legitimate business activity. Hp Central View portfolio provides solutions to help operators and content providers stop fraudsters early-even before activation-and drastically reduce their revenue losses. The Hp Central View subscription fraud prevention solution is designed to identify sub-

scription fraud attempts and provide evidence that enables operators to intervene in the activation process as early and rapidly as possible-and ultimately mitigate subscription fraud before activation. The subscription fraud prevention solution incorporates the learning's from the extensive Hp communications, media and entertainment (CME) fraud and revenue assurance implementations, successfully proven in all corners of the globe and currently protecting hundreds of millions of customers. Solution features includes:

1) Enhanced Data Input and Cleansing—The subscription prevention solution analyzes inputs from wide-reaching sources, including activations historic fraudulent customer data, bad debt data and more so that the crime does not go undetected. The data is cleansed of impurities that create "noise" in the subsequent match process. This cleansing greatly enhances the efficacy of the matching and is achieved by applying extensive and easily modifiable rules.

2) Identity Matching—The cornerstone of the solution's processing compares the incoming activation data with historical information on previous customers whose connections were terminated due to non-payment of bills, and it triggers a match event. The matching is enhanced with "fuzzy techniques," so that relevant variations of data are considered. Similar to the cleansing rules, the matching and analysis rules are configurable through a graphical user interface (GUI).

3) Dictionary Management—To enable better matching, the solution has a dictionary functionary that contains various valid values for a given field (e.g.; Name) or a group of fields (e.g.; Name, ID, City). For example, a name may be listed as "Bill" in one data source and as "William" in other sources; or "Edward" may be "Edouard" or "Eduardo", depending on counting of origin.

4) Evidence Generator—As a complement to the identity matching module, the evidence generator module applies intelligent techniques to the customer data to identify anomalies requiring analysis (for example: the number of activations with the same passport number within a time window). The anomalies are evaluated according to business determined criteria. Those exceeding the defined thresholds trigger an evidence event.

5) Reports and Display—The solution reports are designed to enable rapid investigation and resolution of the generated subscription fraud cases. Information about the new customer is presented side-by-side with its suspected match to a previous fraudulent customer. The results are prioritized and colour coding helps users to readily identify the most severe findings.

With its modular and pre-integrated structure, the Hp Central View portfolio evolves with an operator's needs and growth. A service provider can choose to focus only on select areas or start with critical areas and progress to other business challenges as circumstances and available resources mandate.

2.2.2. Fraud Detection

Fraud detection refers to the attempt to detect illegitimate usage of a communication network by identifying fraud as quickly as possible once it has been com-

mitted. Talking to employees of international companies about fraud detection, many of them answer "We have a very good internal control system. Fraud is not possible here." This is a common range of thought. What is meant with internal control will depend on who is asked. Generally speaking, internal control implies a system of well designed processes and procedures for the purpose of fraud prevention and deterring. Are internal control systems sufficient as a fraud detection mechanism? Apparently not, since over one third of the fraud cases in the surveys are discovered by chance. Internal controls can be split into two groups: active and passive internal control systems. Active internal controls are signatures, passwords, segregation of duties etc., these can be compared with fences [9]. They may appear insurmountable at first sight, but like all fences, they have their weakness to be defeated by clever fraud perpetrators. Equally like a fence, once evaded, there is little or no continuing value in preventing or deterring fraud. The author Passive internal controls operate at a different level. Instead of *preventing* fraud, like active controls attempt to, the emphasis here is on *deterring*. Passive internal control systems induce a state of mind in the would-be perpetrator that strongly motivates him "not to go there". Examples of passive control systems are surprise audits, customized controls and audit trails. Passive control systems, when turned active if a company feels the need to do so (they suspect fraud), mainly make use of reporting tools, like providing different numbers and statistics for manual analysis. Neither active nor passive control systems are best. They complement each other and should both be prevalent.

2.2.3. Supervised Versus Unsupervised Learning

After clarifying the terms, machine learning and data mining, it is worth looking at the literature using these techniques for the purpose of fraud detection. The machine learning and artificial intelligence solutions that are explored may be classified into two categories: "supervised" and "unsupervised" learning. In supervised learning, samples of both fraudulent and non-fraudulent records are used. This means that all the records available are labeled as "fraudulent" or "non-fraudulent". After building a model using these training data, new cases can be classified as fraudulent or legal. Of course, one needs to be confident about the true classes of the training data, as this is the foundation of the model. Another practical issue is the availability of such information. Furthermore, this method is only able to detect frauds of a type which has previously occurred.

In contrast, unsupervised methods don't make use of labeled records. These methods seek for accounts, customers, suppliers, etc. that behave 'unusual' in order to output suspicion scores, rules or visual anomalies, depending on the method. Whether supervised or unsupervised methods are used, note that the output gives us only an indication of fraud likelihood. No stand alone statistical analysis can assure that a particular object is a fraudulent one. It can only indicate that this object is more likely to be fraudulent than other objects. In what follows we give an overview of the explored data mining techniques for fraud detection, divided into supervised and unsupervised techniques. This overview

takes only data mining tools, and no reporting tools or traditional data analysis techniques, into account. Furthermore, it is restricted to mentioning the technique used, without elaborating on the practical decisions the authors made.

2.2.4. Unsupervised Methods of Fraud Detection

The use of unsupervised learning for fraud detection is not explored as intensively as the use of supervised learning. The authors are monitoring behaviour over time by means of Peer Group Analysis [15]. Peer Group Analysis detects individual objects that begin to behave in a way different from objects to which they had previously been similar. Another tool developed for behavioural fraud detection is Break Point Analysis. Unlike Peer Group Analysis, Break Point Analysis operates on the account level. A break point is an observation where anomalous behaviour for a particular account is detected. Both the tools are applied on spending behaviour in credit card accounts. Also in [16], the authors focus on behavioural changes for the purpose of fraud detection and present three-level-profiling. As the Break Point Analysis from the three-level-profiling method operates at the account level and it points any significant deviation from an account's normal behavior as a potential fraud. In order to do this, 'normal' profiles are created (on three levels), based on data without fraudulent records. In this respect, we better use the term semi-supervised instead of unsupervised. To test the method, the three-level-profiling is applied in the area of telecommunication fraud. In the same field, also use behaviour profiling for the purpose of fraud detection. However, using a recurrent neural network for prototyping calling behaviour, unsupervised learning is applied (in contrast to semi-supervised learning). Two time spans are considered at constructing the profiles, leading to a current behaviour profile (CBP) and a behaviour profile history (BPH) of each account. In a next step the Hollinger distance is used to compare the two probability distributions and to give a suspicion score on the calls. A brief paper of [17] the author combines human pattern recognition skills with automated data algorithms. In their work, information is presented visually by domain-specific interfaces. The idea is that the human visual system is dynamic and can easily adapt to ever-changing techniques used by fraudsters. On the other hand have machines the advantage of far greater computational capacity, suited for routine repetitive tasks. With the authors most important studies concerning unsupervised learning in fraud detection are quoted. Although this list may not be exhaustive, it is clear that research in unsupervised learning with respect to fraud detection is due for catching up.

3. Summary and Conclusions

Fraud is a generic category of crime which involves an individual or group of individuals dishonestly obtaining property or some financial advantages by means of deception. Perpetrators of fraud may seek to gain money, property, time or information and the means used are as varied as the opportunities which arise. Offenders may be individuals or employees or managers of organisations in both

the public and private sectors, while their victims may be their employers as well as individual consumers of any age and gender. Put simply, fraud affects us all and is of particular concern to those who manage large government and business organisations where the potential losses are greatest.

The operation of a mobile network is complex, and fraudsters invest a lot of energy to find and exploit every weakness of the system. A typical example would be subscription fraud, where a fraudster acquires a subscription to the mobile network under a false identity; and start reselling the use of his phone to unscrupulous customers (typically for international calls to distant foreign countries) at rate less than the regular tariff. The fraudster accumulates a large number of expensive calls, but disappears before the bill can be collected. The issue of a sure security is very important; this project has also developed application software that will give a high level security for GMS subscription in mobile phone. Using a high level standard model coded in Java programming Language, which when used can solve in a very high percentage the problems of security in GSM subscription.

As GSM telecommunication gains more grounds, so also fraudsters develop more ways of breaking into the system; making the devices face a new range of security threats. This study has demonstrated that Neural Network can be employed to improve the GSM telecommunication fraud detection using neural network parameter and give the best recommendation to the user on suitable parameter for fraud detection.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Estévez, P.A., Held, C.M. and Perez, C.A. (2006) Subscription Fraud Prevention in Telecommunications Using Fuzzy Rules and Neural Networks. *Expert Systems with Applications*, **31**, 337-344. https://doi.org/10.1016/j.eswa.2005.09.028

[2] Hollmén, J. (2000) User Profiling and Classification for Fraud Detection in Mobile Communications Networks. Helsinki University of Technology, Helsinki.

[3] Otero, J.F. (2005) Revenue Assurance and Fraud. Caribbean Telecoms Briefing. Vol. 6, 234-267.

[4] Levi, M., Burrows, J., Fleming, M., Hopkins, M. and Matthews, K. (2007) The Nature, Extend and Economic Impact of Fraud in the UK. Report of the Association of Chief Police Officers, Economic Crime Portfolio.

[5] Jans, M., Lybaret, N. and Vanhoof, K. (2009) A Framework for Internal Fraud Risk Reduction at IT Integrating Business Processes: The IFR^2 Framework. *The International Journal of Digital Accounting Research*, **9**, 1-29. https://doi.org/10.4192/1577-8517-v9_1

[6] Kurtiz, N. (2002) Practical Vision, Securing a Mobile Telecommunication Network from Internal Fraud. *International Journal of Telecommunication Network*, **12**, 543-547.

[7] Abidogu, O.A. (2005). Data Mining, Fraud Detection and Mobile Telecommunication: Call Pattern Analysis with Unpublished Neural Network. Doctoral Dissertation, University of the Western Cape, Cape Town.

[8] Shelton, R. (2003) The Global Battle against Telecommunication Fraud. Sweden University, Vol. 1, 3-56.

[9] Doe, S.K. (2008) GSM Roaming Fraud, Fraud in International Roaming and Fraud Prevention. *International Journal of Fraud Prevention*, **6**, 45-67.

[10] Nelsson, O. (2009) Subscription Fraud in Telecommunication Using Detection Tree Learning. Maker ere University. Vol. 2, 20-26.

[11] Smith, R.G. (2010) Revenue Mobile Telephone Crime. Australasian Institute of Criminology, 345-359.

[12] Kumar, M., Garfinkel, T., Boneh, D. and Winograd, T. (2007) Reducing Shoulder-Surfing by Using Gaze-Based Password Entry. *Proceedings of the* 3*rd Symposium on Usable Privacy and Security*, Pittsburgh, 18-20 July 2007, 13-19. https://doi.org/10.1145/1280680.1280683

[13] Gagnier, M. (2009) The Rise and Fall of Burnard L. Maoff. *Blombirg Business Week. International Journal*, **6**, 23-28.

[14] Robert, R. and Dabija, D. (2009) Telecom Fraud Management Training Course Praesidium. *Qtel.*, **5**, 122-127.

[15] Kumar, R. (2010) Fraud Management System-Selection and Retuning. Naughthan University, 56-71.

[16] Allen, L. (2010) Fraud and Social Engineering in Community Bank: Information Security Trends and Strategies. http://www.larsonallen.com/Advisory_Services/Fraud_and_Social_Engineering_in_Community_Banks.aspx

[17] KROLL (2010) The Downturn and Fraud, Your Sector May Even Be Better off. *International Journal of Downturn and Fraud*, **12**, 345-354.