PATTERNS OF INTERNET SECURITY IN NIGERIA: AN ANALYSIS OF DATA MINING, FRAUD DETECTION AND MOBILE TELECOMMUNICATIONS IN UNSUPERVISED NEURAL NETWORKS

BY

OMOTERE TOPE

N.C.E., B.A. (Ed)

Published Online By:
EgoBooster Books
www.omotere.tk

ISBN: 978-1-105-40587-7

Published By:

EgoBooster Books, Ogun State, Nigeria.

Identification No: 42
File No: 2012122218

Project Classification: ***Computer Science*****.**

www.omotere.tk

Office: EgoBooster, Shop 5, Kikelomo Shopping Complex, Ojuri B/S, Ijagun, Ijebu-Ode, Ogun State.

NIGERIA: 08077447220, 08074472654
INTERNATIONAL: +234 807 744 7220

ABOUT THE AUTHOR

Omotere Tope attended Adeniran Ogunsanya College of Education, Otto- Ijanikin, Lagos (N.C.E. in Christian Religious Studies/ History) and holds a B.A. (Ed) in History and Diplomatic Studies from Tai Solarin University of Education, Ijagun, Ijebu-Ode, Ogun State. He has undergone training at the United States Institute of Peace (Online Training Program) with a certificate of course completion in *Conflict Analysis*.

He conducts researches (both online and offline) to produce academic works that students can use for their long essays, theses and dissertations. With access to his online project database www.omotere.tk, students in Colleges of Education, Polytechnics and Universities can download full texts of related works prepared by him and other researchers. This will enable them to read literature reviews, check for empirical evidences from data analysis and understand the methodology used.

Contact

Email: omoteretope@gmail.com
Tel: 08077447220, 08074472654.
Facebook: www.facebook.com/omoteretope
Blog: www.egoboosterbooks.wordpress.com
Website: www.omotere.tk
Webstore: www.stores.lulu.com/EgoBoosterBooks

PATTERNS OF INTERNET SECURITY IN NIGERIA: AN ANALYSIS OF DATA MINING, FRAUD DETECTION AND MOBILE TELECOMMUNICATIONS IN UNSUPERVISED NEURAL NETWORKS

ABSTRACT

Data mining has become one of the key features of many security initiatives developed by the Nigerian government to monitor both mobile and internet activities in the country. Attempts are being made to track the data of the so called "yahoo boys" who are taking advantage of e-commerce system available on the internet to defraud unsuspected victims who are mostly foreigners. Some target the telecom companies such as MTN, GLO, AIRTEL, ETISALAT, MULTILINKS, STARCOMMS and VISAFONE to defraud them in terms of free browsing, free international calls and free text messaging. While others target credit card companies to hack into their customers database and steal vital information that could make them buy goods/services through the credit cards. Some even go further to defraud individuals through the use of social media such as facebook, tafoo, myspace, and yahoo chat. Unfortunately, few studies have been conducted on the implication of these criminal activities on national security especially in this era of global terrorism. This study therefore examines the correlation between data mining and internet security in Nigeria, analyse the importance of data mining to Call Pattern in Mobile Telecommunication Networks and evaluate the impact of data mining and fraud detection on unsupervised Neural Networks. The target population for the study consists of two hundred undergraduate students (100 males and 100 females) from Lagos State University, Ojo. Data was analyzed using step wise regression analysis. The research contends that there is a correlation between data mining and fraud detection in unsupervised neural networks in that the former helps in improving security in the country.

TABLE OF CONTENT

CHAPTER ONE

INTRODUCTION

1.1 Background to the Study

Data mining has become one of the key features of many security initiatives developed by the Nigerian government to monitor both mobile and internet activities in the country. Scholars have noted that data mining is used as a means for detecting fraud, assessing risk, and product retailing, data mining involves the use of data analysis tools to discover previously unknown, valid patterns and relationships in large data sets (G. A. Barreto, 2003, M. Collins, 1999 and P. Hoath, 1998). In the context of national security, data mining can be a potential means to identify terrorist activities, fraudulent activities such as money transfers and communications, and to identify and track group activities, such as through travel and immigration records. In Nigeria, many terrorist networks have sprouted in many parts of the country, MEND, Boko Haram and MASSOB to mention just but a few, have been unleashing terror to the Nigerian public. The government is extremely concern in curtailing the activities of these extremist as well as other crime

perpetrators ranging from mobile phone theft, cult activities, drug trafficking, gang related offences, fraud, kidnapping for ransom, organized crime and others.

Focusing on subscribers' use of internet and mobile telecommunications, which is the main concern of this research, telecommunication fraud occurs whenever a perpetrator uses deception to receive telephony services free of charge or at a reduced rate (P. Barson, e al., 1996). It is a worldwide problem with substantial annual revenue losses for many companies. Globally, telecommunications fraud is estimated at about 55 billion US dollars . In the United States of America, telecommunication fraud is generally considered to deprive network operators of approximately 2 percent of their revenue. However, as noted by (P. Barson, e al., 1996), it is difficult to provide precise estimates since some fraud may never be detected, and the operators are reluctant to reveal figures on fraud losses. The situation can significantly be worse for mobile operators in Africa for, as a result of fraud, they become liable for large hard currency payments to foreign network operators. Thus, telecommunication fraud is a significant problem which needs to be addressed, detected and prevented in the strongest possible manner. Popular examples of fraud

Huge amounts of data are being collected by the Nigerian government especially through the Nigerian Communications Commission (NCC) as a result of the increased use of mobile telecommunications and registration of Sim cards. Insight into information and knowledge derived from these databases can give operators a competitive edge in terms of customer care and retention, marketing and fraud detection. One of the strategies for fraud detection checks for signs of questionable changes in user behavior. Although the intentions of the mobile phone users cannot be observed, their intentions are reflected in the call data which define usage patterns. Over a period of time, an individual phone generates a large pattern of use. While call data are recorded for subscribers for billing purposes, we are making no prior assumptions about the data indicative of fraudulent call patterns, i.e. the calls made for billing purpose are unlabeled.

Efficient fraud detection and analysis systems can save telecommunication operators a lot of money and also help restore subscribers' confidence in the security of their transactions. Automated fraud detection systems enable operators to respond to fraud by detection, service denial and prosecutions against fraudulent users. The huge volume

of call activity as well as data usage on internet within a network means that fraud detection and analysis is a challenging problem.

In general, the more advanced a service, the more it is vulnerable to fraud. In the future, operators will need to adapt rapidly to keep pace with new challenges posed by fraudulent users. In addition, the number of actors involved in the provision of a service is likely to increase, making the possibilities for fraud to expand beyond the simple case of subscribers trying to defraud an operator. While conventional approaches to fraud detection and analysis such as rule-based systems based on thresholds for particular parameters may be sufficient to cope with some current types of fraud, they are less able to cope with the myriad of new possibilities. In addition, fraudsters can change their tactics fairly easily to avoid detection; for instance, systems based on thresholds can be fooled by keeping the call duration below that of the detection threshold.

Detecting criminals and solving crime is not an easy task at all and have been a prerogative of the law enforcement agencies, the initiative of crime fighting is solely the responsibility of law enforcement agencies concern, however with the increasing sophistication in technology, computer system are now being used in tracking criminals and their

activities and computer data analysts have started helping the law enforcement officers and detectives to speed up the process of solving crimes. Fraud in telecommunications networks can be characterized by fraud scenarios, which essentially describe how the fraudster gained the illegitimate access to the network. Detection methodologies designed for one specific scenario are likely to miss plenty of the others. For example, velocity trap and overlapping calls detection methodologies are solely aimed at detecting cloned instances of mobile phones and do not catch any of the subscription fraud cases.

Therefore, there is need for the consideration of dynamic and adaptive fraud detection and analysis approaches; artificial intelligence techniques order the promise to effectively address some of these challenges. Further analysis is thus, required to be able to isolate fraudulent usage. An unsupervised learning algorithm can analyse and cluster call patterns for each subscriber in order to facilitate the fraud detection process. This research investigates the unsupervised learning potentials of two neural networks for the profiling of calls made by users over a period of time in a mobile telecommunication network. It also intends to provide a comparative analysis and application of Self-Organizing Maps (SOM) and Long Short-Term Memory (LSTM) recurrent

neural networks algorithms to user call data records in order to conduct a descriptive data mining on users call patterns.

1.2 Statement of the Problem

Technology has integrated nations and the world has become a global village. The economy of most nations in the world is accessible through the aid of electronic via the internet. Since the Electronic market is opened to everybody it also includes eavesdroppers and criminals. False pretence, finds a fertile ground in this situation. Some perpetrators of this crime usually referred to in Nigeria as "yahoo boys" are taking advantage of e-commerce system available on the internet to defraud unsuspected victims who are mostly foreigners thousands and sometimes millions of dollars. They fraudulently represent themselves as having particular goods to sell or that they are involved in a loan scheme project. These criminally minded individuals usually have discussion with their victims via the internet and mobile phones. Patterns of fraudulent activities vary. Some target the telecom companies such as MTN, GLO, AIRTEL, ETISALAT, MULTILINKS, STARCOMMS and VISAFONE to defraud them in terms of free browsing, free international calls and free text messaging. While others target credit card companies to hack into their customers database

and steal vital information that could make them buy goods/services through the credit cards. Some even go further to defraud individuals through the use of social media such as facebook, tafoo, myspace, and yahoo chat. Unfortunately, few studies have been conducted on the implication of these criminal activities on national security especially in this era of global terrorism.

1.3 Objectives of the Study

The primary aim of this study is to analysis the importance of data mining to internet security, fraud detection and mobile telecommunications in unsupervised neural networks in Nigeria. This general aim is expressed in the following specific objectives which are to:

i. Examine the correlation between data mining and internet security in Nigeria

ii. Analyse the importance of data mining to Call Pattern in Mobile Telecommunication Networks

iii. Discuss the relationship between data mining and fraud detection in Nigeria

iv. Evaluate the impact of data mining and fraud detection on unsupervised Neural Networks

1.4 Research Questions

i. Is there any correlation between data mining and internet security in Nigeria?

ii. Does data mining have any significant impact on Call Pattern in Mobile Telecommunication Networks?

iii. Is there any relationship between data mining and fraud detection in Nigeria?

iv. How does data mining and fraud detection affect fraudsters in unsupervised Neural Networks?

1.5 Research Hypotheses

Ho^1 There is no significant difference between data mining and internet security in Nigeria

Ho^2 There is no significant relationship difference between data mining and Call Pattern in Mobile Telecommunication Networks

Ho^3 There is no significant difference between data mining and fraud detection in Nigeria

Ho^4 There is no significant difference between data mining and fraud detection in unsupervised Neural Networks

1.6 Scope of the Study

This study centers on the importance of data mining to internet security, fraud detection and mobile telecommunications in unsupervised neural networks in Nigeria. It touches on the correlation between data mining and internet security; importance of data mining to Call Pattern in Mobile Telecommunication Networks; relationship between data mining and fraud detection; and, the impact of data mining and fraud detection on unsupervised Neural Networks. However, it does not cover such areas as the use of data mining in fighting terrorism or other cyber security issues. It mainly examines how data mining could be used to improve upon internet security and in detecting fraud in telecommunication networks.

1.7 Limitation of the Study

There are several limitations inherent in this study. The findings, interpretations, and subsequent discussion derived from this study are considered with the knowledge of the limitations described here. Due to

the sensitive nature of some of the topic, some respondents may not be comfortable responding accurately. Rates of fraudulent activities may therefore be difficult to establish because of response bias. Moreover, the study used a subgroup of internet users as well as GSM users who are undergraduates. These students may be different from the general population of internet and GSM users in Nigeria who are not in the formal school system. This may limit the generalization of the study.

1.8 Definition of Terms

Cyber attack refers to the use of deliberate actions—perhaps over an extended period of time—to alter, disrupt, deceive, degrade, or destroy adversary computer systems or networks or the information and/or programs resident in or transiting these systems or networks.

Data mining involves the use of sophisticated data analysis tools to discover previously unknown, valid patterns and relationships in large data sets. These tools can include statistical models, mathematical algorithms, and machine learning methods (algorithms that improve their performance automatically through experience, such as neural networks or decision trees).

Internet security is a branch of computer security specifically related to the Internet. Its objective is to establish rules and measures to use against attacks over the Internet. The Internet represents an insecure channel for exchanging information leading to a high risk of intrusion or fraud, such as phishing. Different methods have been used to protect the transfer of data, including encryption.

Neural Network consists of an interconnected group of artificial neurons, and it processes information using a connectionist approach to computation.

Telecommunication Fraud: fraud as any transmission of voice or data across a telecommunications network where the intent of the sender is to avoid or reduce legitimate call charges.

BUY THE COMPLETE PROJECT

CALL

08077447220

08074472654

PRICE

NIGERIA: N3000
INTERNATIONAL: $40

OFFICE

5, Kikelomo Shopping Complex, Ijagun, Ijebu-Ode, Ogun State, Nigeria.

PAYMENT OPTIONS

NIGERIA
Cash Deposit

Bank: Guaranty Trust Bank
Account Name: Omotere Tope
Account No: 0050329679
AMOUNT: N3000

NIGERIA
Cash Deposit

Bank: Intercontinental Bank Plc.
Account Name: Omotere Tope
Account No: 1014785737
AMOUNT: N3000

INTERNATIONAL

Section [A]
Payment: Western Union Money Transfer
Send to: Omotere Tope
Location: Lagos State, Nigeria.
Amount: $40

Section [B]
Sender's Full Name:
Location of Sender (Where Money Was Sent From):
Money Transfer Control Number (MTCN):
Test Question and Answer (if applicable):

Send details of payment to: +2348077447220 omoteretope@gmail.com