FRAUDULENT DETECTION MODEL USING MACHINE LEARNING TECHNIQUES USING UNSTRUCTURED SUPPLEMENTARY SERVICE DATA

AKINJE AYORINDE OLUGBENGA

A project report submitted in fulfilment of the
requirements for the award of the degree of
Master of Science (Information Security)

School of Computing
Faculty of Engineering
Universiti Teknologi Malaysia

JANUARY 2021

ACKNOWLEDGEMENT

I would like to express heartfelt gratitude to my supervisor Dr. Fuad A.Ghaleb for his constant support during the entire window of this project report. I appreciate his willingness to give a helping hand whenever it is required even when it was late at night or on weekends sometimes. Without his continued support and interest, this project report would not have been the same as presented here.

I express profound gratitude and appreciation to my parents and siblings for providing their support and continuous encouragement throughout my time of studying. This accomplishment would not have been possible without them.

I'm also indebted to the Petroleum Technology Development Fund (PTDF for their financial assistance throughout my study. Special thanks to UTM for providing an enabling environment to complete this study.

My sincere appreciation also extends to all my colleagues and others who have assisted on various occasions. Their views and tips are useful indeed.

My friends with their encouragements and supports, Jemimah Joshua who isn't privileged to witness the completion of this, due to her demise, and to all those who were supportive in a way or the other toward this. Thank you……!

ABSTRACT

The increase in mobile phones accessibility and technological advancement in almost every corner of the world has shaped how banks offer financial service. Such services were extended to low-end customers without a smartphone providing Alternative Banking Channels (ABCs) service, rendering regular financial service same as those on smartphones. One of the services of this ABC's is Unstructured Supplementary Service Data (USSD), two-way communication between mobile phones and applications, which is used to render financial services all from the bank accounts linked for this USSD service. However, fraudsters have taken advantage of innocent customers and their security vulnerabilities on this channel resulting to high impart of fraud cases, there is still not an implemented fraud detection model to detect these fraud activities. Existing fraud detection models in USSD are in the abstract level and without implementation. Some of the existing studies uses Bayesian's algorithm for detecting the fraudulent transection. However, Bayesian uses a probabilistic model to predict its output which is influenced by prior history and has a long-term memory which results in low accuracy. This study aims at investigating the design of Fraud detection model using machine learning techniques for Unstructured Supplementary Service Data based on short-term memory. Statistical features were derived by aggregating customers activities were derived using a short window size to improve the model performance using selected machine learning classifiers. To achieve this aim, the research framework consists of two phases, the first phase was data pre-processing and feature derivation. The second phase is model construction and model evaluation. Feature selection was used to select the best set of features for training the model. Many classifiers were trained to investigate their detection accuracy performance. Results of each classifier were tabulated and compared against each other. The results demonstrated that the proposed Fraudulent detection model using machine learning techniques for Unstructured Supplementary Service Data achieve its best performance with Random forest having the best result of 100% across all its performance measure, KNeighbors was second in performance measure having an average of 99% across all its performance measure while Gradient boosting was third in its performance measure, the achieved accuracy is 91.94%, the precession is 86%, the recall is 100% and f1 score is 92.54%. The result validates that with the right feature derived and appropriate machine learning algorithm the proposed model offers the best accuracy in fraud detection. The proposed fraud detection model can help in detection the USSD based frauds for low-end customers who don't have smartphones.

ABSTRAK

Peningkatan aksesibilitas telefon bimbit dan kemajuan teknologi di hampir setiap pelosok dunia, telah membentuk bagaimana bank menawarkan perkhidmatan kewangan, memperluas perkhidmatan mereka bahkan kepada pelanggan kelas bawah tanpa telefon pintar yang menyediakan perkhidmatan Saluran Perbankan Alternatif (ABC), menjadikan perkhidmatan kewangan biasa sama seperti yang terdapat pada telefon pintar, salah satu perkhidmatan ABC ini adalah Unstructured Supplementary Service Data (USSD), komunikasi dua hala antara telefon bimbit dan aplikasi, yang digunakan untuk memberikan perkhidmatan kewangan semua dari akaun bank yang dihubungkan untuk ini Perkhidmatan USSD, penipu telah memanfaatkan pelanggan yang tidak bersalah dan kerentanan keselamatannya di saluran ini menyebabkan banyaknya kes penipuan, masih belum ada model pengesanan penipuan yang dilaksanakan untuk mengesan kegiatan penipuan ini. Penyelidikan yang dilakukan untuk menangani pengesanan penipuan di USSD secara abstrak dan tanpa pelaksanaan, penulis mencadangkan model pengesanan penipuan yang akan menggunakan Bayesian algorithm untuk pengiraan dan analisis data tetapi algoritma ini mempunyai beberapa kekurangan Tujuan kajian ini adalah untuk menyiasat model pengesanan Penipuan menggunakan teknik pembelajaran mesin untuk Unstructured Supplementary Service Data. Ciri statistik diperoleh dengan mengagregatkan aktiviti pelanggan yang diperoleh untuk meningkatkan prestasi model menggunakan pengelasan pembelajaran mesin terpilih, untuk mencapainya, kerangka kajian berada dalam fasa, fasa pertama adalah pemrosesan data dan turunan fitur dan fasa kedua adalah pembuatan model akhirnya penilaian model Hasil dari setiap pengklasifikasi ditabulasi dan bersaing satu sama lain, pemilihan fitur digunakan untuk memilih set fitur terbaik untuk model. Hasil kajian menunjukkan bahawa model pengesanan Penipuan yang dicadangkan menggunakan teknik pembelajaran mesin untuk 1Unstructured Supplementary Service Data mencapai prestasi terbaik dengan Random forest yang mempunyai hasil terbaik 100% di seluruh ukuran prestasinya, KNeighbours berada di tempat kedua ukuran prestasi yang mempunyai rata-rata 99% di seluruh ukuran prestasinya sementara Gradient boosting berada di tempat ketiga dalam ukuran prestasinya, ketepatan adalah 91.94%, precession 86%, recall adalah 100% dan f1-score adalah 92.54% . Hasilnya mengesahkan bahawa dengan ciri yang tepat diperoleh model yang dicadangkan menawarkan ketepatan terbaik dalam pengesanan penipuan.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

ANN	-	Artificial neural network
EM	-	Expectation-Maximization
FDS	-	Fraud Detection Systems
FDM	-	Fraud detection model
GSM	-	Global Mobile Communicative System
HHT	-	Hierarchical Hypothesis Testing
PCA	-	Principle Component Analysis
RF	-	Random Forest
SVM	-	Support Vector Machines
TPR	-	True Positive Rate
TNR	-	True Negative Rate
USSD	-	Unstructured Supplementary Service Data

CHAPTER 1

INTRODUCTION

1.1 Overview

Making payment these days has never been so easy, with a click, dialing codes from our mobile phones to perform a financial transaction that would have required going into a bank to carry out or physical cash payment but with every transaction comes the same question how secure is the channel, will this transaction be without any security issue. With mobile phones reaching almost every village in Africa, coupling with the recent technological advancement that has shaped the telecommunication industries enabling them to provide improved services for their customers across each level of income classes, with these improved technologies and services in telecommunication sectors, the banks have taken benefit of this to expand their mode of operation beyond the usual face to face banking service and payment methods, e-payment and mobile banking have been introduced and adopted by every bank not just locally but globally.

Banks have taken the advantage of mobile phone banking to reach low-end customers those without smartphones (H. Gupta Ranjan & J. Lakshmi K. K., 2017) producing Alternative Banking Channels (ABCs) service, offering various financial services, from cash withdrawal, transfers, deposits, to paying for electricity bills, phone bills, phone top-ups, traveling expenses, and television cable subscriptions which can be utilized from anywhere and at any time (OKO I.A, 2019), one of the services of this ABC’s is Unstructured supplementary service data (USSD) a Global Mobile Communicative System (GSM) capability that enables high speed, two-way communication between mobile phones and applications (Globitel, 2019), which can be used for payment of utility bills, phone top-ups, transferring money to friends and family bank account all from the account linked for this USSD service, fraudsters have taken advantage of innocent customers on this channel to carry out fraudulent activities, with no feasible measures in detect the fraudulent activities.

This study covers fraud detection in USSD, developing and designing an accurate fraud detection using machine learning techniques, and evaluating each technique to adopt a preferred technique for its fraud detection model, after evaluating their respective results.

1.2 Problem Background

Banks in Africa have taken advantage of mobile phone banking to reach low-end customers without smartphones (H. Gupta Ranjan & J. Lakshmi K. K., 2017) adopting services like Unstructured supplementary service data (USSD) for mobile banking services to reach more customers without physical bank branches in their rural areas.

We've all enjoy these electronic channel services like paying for services, banks transactions, and other e-services from our mobile phones with just dialing codes ending with the hash sign (#) to make transactions, it has made life easier for us all, but it comes along with its challenges and shortcomings, the same questions come on our mind each time the services is utilized "How secure it is", fraud has been the major challenges these e-service systems had to battle with since its inception, fraudsters take advantage of innocent users on these platforms to maximize the vulnerabilities in the system for their financial gain.

Current measures to control its security flaws and threats are preventives measures such as short authentications PINs, encryption channels, this preventive measure has several disadvantages and drawbacks at the client end, the communication channel, and vulnerabilities in its security policy (Nyamtiga et al, 2013).

PIN characters entered by users are not masked and uses only 4-digit numerals while most times customers prefer to use digits that are easy to remember such as 1111,1234,0000 this can be easily be guessed or brute-forced when a customer phone falls into the wrong hand, solving this will resolve in modifying the USSD framework which will renew the USSD concept to rewriting the protocol and authentication gateway to increase its number from 4 to minimum of 8 password authentication characters which can then enforce the inclusion of alphabets and other characters that is required to meet the requirement for a strong password.

The service relies on the A5 algorithm commonly used for encryption in GSM encryption channel which has been reverse engineered (A. Biryukov and A. Shamir, 1999) (E. Barkan. E. Biham and N. Keller, 2003) and leaving USSD data traveling through the communication channel vulnerable to attacks because messages are not encrypted on the GSM backbone (M. Toorani and A. Beheshti, 2008) especially on low-end phones which most of the customers use. Encryption and decryption on the phone are not supported with the current USSD implementations, there is no room for cryptography application unless the USSD implementation on the particular phone requires encrypting the responses before sending data, so secure communication channel relies on manufacturers incorporating enhanced security features in existing USSD technology, which would rely on the interventions of mobile phones and gateways manufacturers.

Encryption security flaws of the GSM technology have been addressed in higher generations above the 2G systems; i.e. UMTS, EDGE, 3G, 4G and above, 3GPP has replaced the weak crypto proprietary algorithms (COMP128, A5/1, A5/2) with stronger encryption algorithm, (Nyamtiga et al, 2013), this provides services providers a better preferred secure channel of higher GSM generations to handle the mobile transactions instead of 2G, but this has been available to customers only in urban areas while those in remote areas still have to perform their transaction on the only option available to them which is on the 2G network. Detection of the fraud before it happens is another method to reduce the vulnerabilities of the system, but for now, they only exist in abstract forms without implementation yet.

Right features are very important in fraud detection models, as right features derived from transaction data contribute to the model classification, Insufficient features have been a major issue in the USSD fraud detection model, which has been major attributes to its low detection accuracy, raw features such as time, location and amount of transaction in its transactional dataset have left out important features that need to be considered to help uncover fraud patterns. When fraud detection models don’t consider a set of features from analyzing periodic features this will often contribute to its poor accuracy as important patterns are not detected due to this.

Adaptation of credit card fraud detection models would have solved the USSD fraudulent issues but they are two entirely complete different systems, mode of transaction and operation are completely different when compared against each other, to complete a credit card transaction requires the cards details such as card number, expiry date, card verification value (CVV) and one-time password, token or PIN to complete a credit card transaction, while on the other hand a USSD transaction just requires dialing some assigned codes provided by the banks or service providers follow each step on the menu-driven prompt messages that follow corresponding to the type of service you are performing and completing it with customers authentication PIN, with these comparing both datasets against each there is a huge difference in their features so this will prevent credit card fraud detection model from being compactible when applying to USSD fraud detection.

Currently, there is no fraud detection mechanism in the USSD service to detect its fraudulent transactions, to mitigate all these drawbacks in the USSD service, detecting the fraud before it happens will be of great benefit. Scenario leading to the problem with USSD mobile banking is, but not limited to, network downtime, phishing users’ personal information such as PINs and passwords over the phone, agent-related fraud, SIM swap – phone numbers can easily port to another sim without demanding for identification cards to verify ownership of the numbers.

Meanwhile, few types of research have been done towards fraud detection in USSD services so few papers are addressing this issue. The research that was done to address fraud detection in USSD is still abstract and without implementation, the author (Vukeya K. E., 2014) proposed a fraud detection model that uses Bayesian's algorithm for data calculations and analysis but this algorithm has several drawbacks. However, Bayesian predicts based on prior history not posterior this means its fraud detection is based on the history of the customer's transactions when the user changes the pattern of a transaction, this will result in high false alarms, giving no room for detecting new attacks because it's based on prior probability causing poor detection.

The issues in the current model which contributed to its poor detection accuracy as shown in Figure 1.1, first flaw in its fraud detection model is inadequate and inadequate features, which has contributed to its poor detection accuracy due to features not rightly represented. Second is its ineffective model design, which has not helped to detect its fraudulent activities across the fraud detection model, all of which have contributed to the poor detection of USSD fraud detection model.

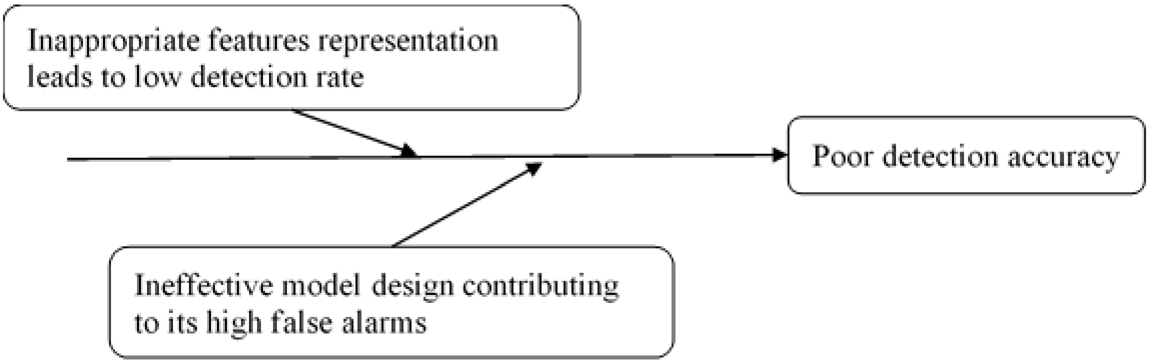
Inappropriate features representation leads to low detection rate
Poor detection accuracy
Ineffective model design contributing to its high false alarms

Figure 1.1 Issues with the USSD fraud detection model.

Customer spending is not constant they tend to change based on their needs, festive periods shopping this change in spending pattern is known as concept drift. And several authors have dealt with in various ways using different techniques for fraud detection models to cope with the change users spending habit, (Yu S. & Abraham Z, 2017) proposed hierarchical hypothesis testing (HHT) framework that can detect and also adapt to various concept drift types (e.g., recurrent or irregular, gradual or abrupt), (Mao Huiying et al, 2018) propose a dynamic-risk features approach as model inputs to address concept drift, measuring the variations in the probability distribution of the risk of certain entity profiles due to concept drift, (Somasundaram A. & Reddy S, 2019) proposes a transaction window bagging (TWB) model, parallel and incremental learning as an approach to address concept drift in credit card fraud detection model.

1.3 Problem Statement

The prevention mechanism in place has not prevented fraudulent transactions, due to its drawbacks such as short authentication PINs of 4 digits and easy to guess, sim cloning, theft of phones so there is a need for other means of fraud mitigation in USSD mobile banking service. Meanwhile, few types of research have been done towards fraud detection in USSD services so few papers are addressing this issue. The research that was done to address fraud detection in USSD is in abstract and without implementation, the author proposed a fraud detection model that will use Bayesian's algorithm for data calculations and analysis but this algorithm has several drawbacks. However, Bayesian uses a probabilistic model to predict its output which is influenced by prior history and not posterior this means fraud detection will be based on the history of the customer's transactions (long-term memory) so if the user changes his pattern of the transaction this will result in high false alarms, and this gives no room for detecting new attacks because it uses calculation on prior probability. Also, in classification tasks, big data set is needed to make reliable estimations of the probability of each class, Naïve Bayesian classification algorithm works well with a small data set but precision and recall will be very low. Representing the right features is very important in the case of fraud detection models, if the right feature are not considered from analyzing periodic features this will often contribute to its poor accuracy as important patterns are not detected and this has contributed to the drawbacks in the existing model.

1.4 Research Aim

To investigate a USSD fraud detection model with deriving features to improve its performance accuracy using machine learning techniques.

1.4.1 Research Objectives

The objectives of the study are:

To derive new representative features for the USSD fraud detection model to improve the detection accuracy by statistical aggregation of customers' transactions using short time window size.

To investigate a Machine learning classifier to improve the accuracy of the USSD fraud detection model based on the features derived in (a).

1.5 Research Questions

(a) What are the representative features present in the dataset which can improve the detection accuracy?

(b) How do derived features improve a fraud detection model accuracy?

1.6 Scope of the Study

To achieve the stated objective, the scope of this study is limited to the following:

(a) USSD fraud detection only. no further action was taken after the detection.

(b) PaySim dataset was sourced from Kaggle https://www.kaggle.com/ntnu-testimon/paysim1

(c) Python 3.6 is used to develop the model

REFERENCES

A. Biryukov and A. Shamir. (1999). Real time cryptanalysis of the alleged A5/1 on a PC. 34.

Abdallah, A. M. (2016). Fraud detection system: A survey. . *Journal of Network and Computer Applications, 68.*, 90-113.

Africa Mobile Money. (2019). *Mobile Money Africa*. Retrieved from Mobile Money Africa website: https://mobilemoneyafrica.com/blog/nigeria-ussd-transactions-grew-by-35-hits-n261m

Aisha Abdallah, M. A. (2016). Fraud detection system: A survey. *Journal of Network and Computer Applications*, 90-113.

Aleem, A. &.-B. (2011). Internet auction fraud: The evolving nature of online auctions criminality and the mitigating framework to address the threat. *International Journal of Law, Crime and Justice, 39(3),* 140-160.

Alexopoulos, P. K. (2007). Towards a Generic Fraud Ontology in e-Government. *In ICE-B*, 269-276.

Behdad, M. B. (2012). Nature-inspired techniques in the context of fraud detection . *IEEE Trans. Syst. Man Cybern. Part C (Appl. Rev.) 42 (6),* 1273–1290.

Bolton, R. J. (2002). Unsupervised profiling methods for fraud detection. *Credit scoring and credit control VII,,* 235-255.

Botchey F. E. et al. (2020). Money Fraud Prediction—A Cross-Case Analysis on the Efficiency of Support Vector Machines, Gradient Boosted Decision Trees, and Naïve Bayes Algorithms. I. *Information, 11(8), ,* 383.

Busuulwa, B. (2016). *Mobile money fraud, crime rate increase in Uganda*. Retrieved from theeastafrican.co.ke: www.theeastafrican.co.ke/business/Mobile-money-fraud-and-crime-rate-increase-in-Uganda-/2560-3415786-quaydf/index.html/

CFCA. (2019). *COMMUNICATIONS FRAUD CONTROL ASSOCIATION*. Retrieved from COMMUNICATIONS FRAUD CONTROL ASSOCIATION: https://cfca.org/sites/default/files/Fraud%20Loss%20Survey_2019_Press%20 Release.pdf

Chang, Y. C. (2017). Mining the Networks of Telecommunication Fraud Groups using Social Network Analysis. *In Proceedings of the 2017 IEEE/ACM International*

Conference on Advances in Social Networks Analysis and Mining (pp. 1128-1131). ACM/IEEE.

Chatain, P. Z. (2011). Protecting Mobile Money against Financial Crimes: Global Policy Challenges and Solutions. New York, NY.: World Bank Publications.

Chen, S. G. (2013). A novel approach to uncover health care frauds through spectral analysis. *IEEE International Conference on Healthc. Informatics.* (pp. 499–504). IEEE.

Dallas Justice . (2018, November 4). Retrieved from Dallas Justice website: https://www.dallasjustice.com/consumer-insurance-fraud-crime-involving-submission-of-insurance-claim

Deloitte. (2015, 6 June 2017 6). *Deloitte.* Retrieved from Deloitte: https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/financial-services/Banking/lu-mobile-money-payment-industry-marketing-distribution.

Domingues, R. B. (2016). An application of unsupervised fraud detection to Passenger Name Records. *46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshop (DSN-W)* (pp. 54-59). IEEE.

Dong Fei, S. M. (2009). Combating online in-auction fraud: Clues techniques and challenges. *Computer Science Review, vol. 3.4*, 245-258.

E. Barkan. E. Biham and N. Keller. (2003). *Instant ciphertext-only cryptanalysis of GSM encrypted communication, in Advances in Cryptology.* Springer.

EC3, T. M. (2019). *EUROPOL.* Retrieved from EUROPOL: https://www.europol.europa.eu/publications-documents/cyber-telecom-crime-report-2019

Finance, U. K. (2019). Fraud the facts 2019. . *Computer Fraud & Security, 2019(4),*.

FTC. (2018). *FEDERAL TRADE COMMISSION·*. Retrieved december 23, 2019, from FEDERAL TRADE COMMISSION website: https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2018/consumer_sentinel_network_data_book_2018_0.pdf

G. T. Krugel. (2007). *Mobile Banking Technology Options.* Retrieved from FinMark Trust.

Ganguly, S. &. (2018). Online detection of shill bidding fraud based on machine learning techniques. *In International Conference on Industrial, Engineering and Other Applications of Applied Intelligent Systems* (pp. 303-314). Springer.

Globitel. (2019, December 22). *Globitel.* Retrieved from Globitel website: http://www.globitel.com/ussd-gateway/

Gupta, P. a. (2015). Corporate frauds in India–Perceptions and emerging issues. *Journal of Financial Crime, Vol. 22 No. 1,*, 79-103.

H. Gupta Ranjan & J. Lakshmi K. K. (2017). USSD—Architecture analysis, security threats, issues and enhancements. *International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions)(ICTUS)* (pp. 798-802). IEEE.

H.Lookman Sithic, T. (2013). Survey of Insurance Fraud Detection Using Data Mining Techniques. *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, 62-65.

Hand, D. J. (2012). Overcoming selectivity bias in evaluating new fraud detection systems for revolving credit operations. *International Journal of Forecasting, 28(1)*, 216-223.

IC3. (2014). *Internet Crime Complain Center Internet Crime Report, 2001-2013,* . Retrieved from Internet Crime Complain Center Internet Crime: [online] Available: http://www.ic3.gov/media/annualreports.aspx

ICE. (2020, JULY 27). *FBI's Internet Crime Complaint Center (IC3)*. Retrieved from https://www.fbi.gov/news/pressrel/press-releases/fbi-releases-the-internet-crime-complaint-center-2018-internet-crime-report

InfoGile, T. (2007). *Mobile Banking: The Futures.* Retrieved from InfoGile Technologies website: http:// www.infogile.com/pdf/ Mobile _ Banking .pdf

Insurance Informative Institute. (2019, May 20). Retrieved from Insurance Informative Institute website: https://www.iii.org/article/background-on-insurance-fraud

Jain, V. (2017). Perspective analysis of telecommunication fraud detection using data stream analytics and neural network classification based data mining. *International Journal of Information Technology*, , 303-310.

Jia-Zhi D. U. et al. (2018). L-SVM: A radius-margin-based SVM algorithm with LogDet regularization. . *Expert Systems with Applications 102.*, 113-125.

John, A. (2013). Data mining application for cybercredit fraud detection systems. *Lecture note in Engineering and computer science*, 1537-1542.

Jyothsna V., R. P. (2011). A review of anomaly based intrusion detection systems. *Int. J. computer Appl.*, 26-35.

K. Randhawa C. K. Loo M. Seera C. P. Lim and A. K. Nandi. (2018). Credit Card Fraud Detection Using AdaBoost and Majority Voting. *IEEE Access*, 14277-14284. doi:10.1109/ACCESS.2018.2806420.

Kelvin chikomo, M. K. (2006). *Security of Mobile Banking.*

KOVALESKI, D. (2019, December 21). *Financial Regulations News.* Retrieved from Financial Regulations News website: https://financialregnews.com/banking-industry-suffered-2-2-billion-fraud-losses-2016/

Kruger, P. J. (2012). Cellphone banking at the bottom of the pyramid. *Doctoral dissertation, Stellenbosch: Stellenbosch University*.

Lakshmi, K. K. (2017). USSD—Architecture analysis, security threats, issues and enhancements. *International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions)(ICTUS)* (pp. 798-802). IEEE.

Lakshmi, K. K. (2019). UPI Based Mobile Banking Applications–Security Analysis and Enhancements. *Amity International Conference on Artificial Intelligence (AICAI)* (pp. 1-6). IEEE.

Laleh, N. &. (2009). A taxonomy of frauds and fraud detection techniques. *In International Conference on Information Systems, Technology and Management* (pp. 256-267). Berlin, Heidelberg: Springer.

Li, J. H.-Y. (2008). A survey on statistical methods for health care fraud detection. *Health Care Manag. Sci. 11 (3),*, 275-287.

Liu, Q. W. (2012). *Supervised Learning Encyl.Sci Learn*.

Lopez-Rojas & E. Elmir A. & Axelsson S. (2016). PaySim: A financial mobile money simulator for fraud detection. *28th European Modeling and Simulation Symposium, EMSS,* (pp. 249-255). Larnaca: Dime University of Genoa.

Lopez-Rojas E. A. et al. (2018). Analysis of fraud controls using the PaySim financial simulator. *International Journal of Simulation and Process Modelling, 13(4),* , 377-386.

Lovro Subelj, S. F. (2011). An expert system for detecting automobile insurance fraud using social network analysis. *Expert Systems with Applications*, 1039-1052.

M. Toorani and A. Beheshti. (2008). Solutions to the GSM security weaknesses. *The Second International Conference on Next Generation Mobile Applications, Services and Technologies, NGMAST'08.* IEEE.

Navanshu Khare and Saad Yunus Sait. (2018). "Credit card fraud detection using machine learning models and collating machine learning models." 118.20. *International Journal of Pure and Applied Mathematics*, 825-838.

NIBSS. (2018). *About NIBSS: Nigeria Inter-Bank Settlement System Plc (NIBSS). was incorporated in 1993 and is owned by all licensed banks including the Central Bank of Nigeria (CBN).* Retrieved from Nigeria Inter-Bank Settlement System Plc (NIBSS) website: https://nibss-plc.com.ng/

Nyamtiga, B. W. (2013). Security Perspectives for USSD versus SMS in conducting mobile transactions: A case study of Tanzania. *international journal of technology enhancements and emerging engineering research, 1(3), .,* 38-43.

Nyamtiga, B. W. (2013). Security Perspectives for USSD versus SMS in conducting mobile transactions: A case study of Tanzania. *International journal of technology enhancements and emerging engineering research, 1(3),* 38-43.

OKO I.A. (2019). Electronic Fraud and Financial Performance of Quoted Commercial Banks in Nigeria. *International Journal of Advanced Academic Research*, 15-35.

Pambudi Bayu Nur et al. (2019). Improving Money Laundering Detection Using Optimized Support Vector Machine. *019 International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)* (pp. 273-278). IEEE.

Patidar, R. &. (2011). Credit card fraud detection using neural network. *International Journal of Soft Computing and Engineering (IJSCE)*, 32-38.

Patil Suraj Varsha Nemade and Piyush Kumar Soni. (2018). Predictive modelling for credit card fraud detection using data analytics. *Procedia computer science 132.*, 385-395.

PwC. (2020). *PwC's Global Economic Crime and Fraud Survey 2020 : Fighting fraud A never-ending battle.* Retrieved from Pwc.com/fraudsurvey: https://www.pwc.com/gx/en/forensics/gecs-2020/pdf/global-economic-crime-and-fraud-survey-2020.pdf

Raghavendra Patidar & Lokesh Sharma. (2011). Credit Card Fraud Detection Using Neural Network. *International Journal of Soft Computing and Engineering (IJSCE)*, 32-39.

RGA. (2019). *RGA 2017 Global Claims Fraud Survey*. Retrieved from Reinsurance Group of America Web site: https://rgare.com/knowledge-center/media/research/rga-2017-global-claims-fraud-survey

Sanganagouda, J. (2011). USSD-A Potential Communication Technology that can Ouster SMS Dependency. *International Journal of Research and Reviews in Computer Science, 2(2),*, 295.

Sanusi, Z. M. (2015). Fraud schemes in the banking institutions: prevention measures to avoid severe financial loss. *Procedia Economics and Finance, 28,* (pp. 107-113.). Wadham College, Oxford: Elsevier.

Sasirekha, M. T. (2012). An Integrated Intrusion Detection System for Credit Card Fraud Detection. *In Advances in Computing and Information Technology*, 55-60.

Schreyer Marco et al. (2019). Detection of accounting anomalies in the latent space using adversarial autoencoder neural networks.

Sherly, K. K. (2010). BOAT adaptive credit card fraud detection system. *n 2010 IEEE International Conference on Computational Intelligence and Computing Research* (pp. 1-7). IEEE.

Subudhi, S. &. (2016). Use of fuzzy clustering and support vector machine for detecting fraud in mobile telecommunication networks. *IJSN, 11(1/2)*, 3-11.

Taskin, E. (2012). GSM MSC/VLR Unstructured Supplementary Service Data (USSD) Service.

Tennyson, S. (2001). Claims Auditing in Automobile Insurance.

U. K Finance, ". t. (2019, December 21). *U K finance Org.* Retrieved from U K finance Org website: https://www.ukfinance.org.uk/system/files/Fraud%20The%20Facts%202019%20-%20FINAL%20ONLINE.pdf

Vukeya K. E., &. K. (2014). A Model of Fraud Detection in Mobile Transaction via Unstructured Supplementary Service Data. *Southern African Telecommunication Networks and Applications Conference (SATNAC).* Port Elizabeth, Eastern Cape, South Africa: Research Gate.

Vukeya, K. E. (2014). A Model of Fraud Detection in Mobile Transaction via Unstructured Supplementary Service Data. *Southern African Telecommunication Networks and Applications Conference (SATNAC)* . Port Elizabeth, Eastern Cape, South Africa: Research Gate .

Wells, J. T. (2011). *Financial statement fraud casebook: baking the ledgers and cooking the books.* John Wiley & Sons.

Xenopoulos & Peter. (2017). Introducing DeepBalance: Random deep belief network ensembles to address class imbalance. *IEEE International Conference on Big Data (Big Data).* (pp. 3684-3689). IEEE.

Yufeng Kou, C.-T. L.-P. (2004). Survey of Fraud Detection Techniques. *Proceedings of the 2004 IEEE International Conference on Networking, Sensing & Control* (pp. 749-754). Taipei, Taiwan, : IEEE.