Development of Software for Power System and Cybercrime Monitoring

Anumaka, M. C
Department of Electrical Engineering, Faculty of Engineering,
Imo State University,Owerri, Nigeria.

Abstract

As the world becomes a global community through the advancement and complexity of power systems triggered the Internet and digital revolutions, which generated the tremendous benefits of the mankind are being challenged because of the formidable menace of energy theft and cybercrime. This project focuses on the development of a software system that will aid electric energy theft and cybercrime monitoring by using artificial intelligent (AI) as a tool of Support Vector Machines (SVMs). The data was obtained from Interpalse, which is an international social network for cultural exchange and practices. The obtained data was analyzed using LIBSVM.NET, which is a library for implementing the support vector machine (a type of machine learning algorithm) in the .NET framework. The C $ programming algorithm was also deployed. The results show that AI, which is Support Vector Machines (SVM) is an efficient and effective means for dictation and monitoring cyber-crime activities in the cybercafé. Implementation of this project work will ensure drastic reduction and final elimination of energy theft and cybercrime.

Keywords - *Cybercrime, Monitoring, Support vector machine, Artificial intelligence.*

I. INTRODUCTION

The advent of digital technology gave birth to modern communication hardware, internet services and powerful computer systems necessary to process data. The society is increasingly relying on the electric power system, Internet and other information Technology (IT) tools to carry out personal communication, research, conduct of business and medical activities among other numerous benefits. This study focuses on the development of a system for monitoring electrical energy and cybercrime. The cyberspace has provided a safe anchorage for internet platform, which has transformed the entire world into a global community, as well as creating geometric growth and accelerated windows of opportunities for national and international communications (Bola and Ogunlade, 2012: Hunter, 2003: Balkin*et al* 2006: McQuade, 2006). The power system and cyberspace have also removed economic barriers hitherto faced by many nations of the world. People from different areas of human endeavour can freely interact, access and utilize the invaluable benefits offered by the electric power and Internet platform.

Cybercafes, also called Internet cafes are public places that provide commercial paid or metered access to the Internet (Oluwafemi and Adepoju, 2016; Adepoju, 2008; Mohammed 2008; Hendrix, 2013; Sodiq; 2012; Ramaswamy, 2012).

These benefits and developments are analogous to Lenz's law. They have led to an enormous gain in productivity, efficiency in data processing as well as communication. The benefits turn-around to created harmful escape routes that have led to energy theft, cybercrimes and other internet crimes. Cybercrime is defined as any crime that involves computers and networks, including crimes that do not rely heavily on computers' (Casey, 2014). Cybercrime is growing as internet continues to penetrate every sector of our society. The cybercrimes include those crimes that affect computer networks and devices such as computing viruses, malware and malicious codes as well as those crimes that are facilitated by computer networks or devices like fraud, identity theft, cyber stalking, information warfare and phishing scams. The destructive routes may totally destroy the economy and organization. Lakshmi and Ishwarya (2015) Maitanmi*et al* (2013) noted that the growth of the Internet and its wide acceptance has given rise to rapid insecurity threats globally. Cybercrime is a worldwide problem that is costing countries billions of dollars (Parthiban and Raghavan, 2014). Lakshmi (2015) remarked that a sat 2003, the United States and South-Korea have the highest cyber- attacks of 35.4% and12.8%respectively.

Nigeria has a total population of 60 million from the last census carried out in 2006. Recent statistics revealed that 39.6% African users of internet are actually Nigerians, and that about 28.9% have access to the internet (Hassan, 2012). Therefore, it is not a surprise that Nigeria has a very high rate of internet crime (Okeshola and Adeta, 2013). In their

research investigations, Ewepu (2016); Iroegbu (2016) found out that Nigeria loses N127bn annually to cybercrime. Presently, cybercrimes are performed by people of all ages ranging from young to old, but in most instances the young.

In their research investigations, Utulu (2008) Batool and Mahood (2010), Bola and Ogunlade (20012) Otukenefor and Kari (2008) revealed that cybercafés have grown in popularity, and in Africa and most developing countries, Internet access is largely through these cybercafés. Like other information Technology (IT), systems cybercafés are prone to abuse.

The alarming growth of the internet and its wide acceptance has led to increase in security threats. In Nigeria today, different internets assisted crimes (Cybercrimes) are committed daily in various forms such as scams, fraudulent electronic mails, pornography, identify theft, hacking, cyber harassment, spamming, Automated Teller Machine spoofing, piracy and phishing. Cybercrime is a threat against various institutions and people who are connected to the internet either through their computers or mobile technologies.

The exponential increase in cybercrime in the society has become a strong issue that should not be overlooked. The internet users are not aware of the security risks they are exposed to. They have relied on the cybercafe managers to provide adequate security (Mohammed, 2008). The impact of this kind of crime can be felt on the lives of individuals. Thus, the national economy and international reputation of the country are under threat. Therefore, it becomes imperative to develop a dependable system for monitoring and detecting cybercrimes (Otukenefor and Kari, 2008 Adogbeje, 2008). This is the thrust of this research project.

II. REVIEW OF PREVIOUS STUDIES

Many researchers have focused on different aspects of the cybercafé, including their security, cybercrimes, management, use and effect of usage.

Omodunbi*et al* (2016) investigated on cybercrimes in Nigeria. The authors described types of cybercrimes in Nigeria, analysed their causes as well detection, and found out that the majority of cybercrimes are carried out by youths in our society through phishing. They recommended that the Government should make the welfare and wellbeing of citizens paramount through provision of good paying jobs and provision of basic amenities.

Another study by Wada and Adolaja (2012) specifically assessed cybercrime in Nigeria and its impact on the banking institutions in Nigeria, and well as the existing policy framework.

Utulu (2008) focused on the development of cybercafé security policy in Nigeria. The author argued that enhancement of cyber security will boost social security. He recommended that such policy should be integrated into the National Information Policy.

A study carried out by Onojaefe and Leaning (2008) noted that the security of the cybercafé does not solely depend on technological infrastructure. They argued that security measures and technological mechanism, are also based on social and soft components of management.

Obuh (2008) and Garuba (2008) investigated in the malware detection and prevention in their respective research. Other aspect of cybercrimes in different literatures include a research by Low (2014) Tiemo and Charles-Iyoha (2008) Rauniar (2008) Sommer (2004) Igun (2008) Emiri (2008).

On the management of cybercafés, Mohammed (2008) concentrated on the management of infrastructures, Otokunefor and Kar (2008) dwelt on operational issues, controversies, and challenges of cybercrimes.

The Treaties of the Council of Europe (2001), noted that cyber-crime involves 'action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data.

Oyelunde and Adewami (2008) noted that computer is used to commit cybercrime. When crimes are committed through computer networks like the internet, they are said to be cybercrimes.

In his opinion, Casey (2014) also note that refers cybercrimes as 'any crime that involves computers and networks, including crimes that do not rely heavily on computers' Research from Collier, (2014) and Bazelon *et al*, (2006) described the role of computers and the internet in the promotion of crime, Lewis (2004) found out that cybercrime include computer related and content-based species.

III. METHODOLOGY

This research adopted a system development methodology, which is a framework used to structure, plan, and control the process of developing an

information system. Object-oriented analysis and design methodology (OOADM) were also utilized. OOADM is a popular technical approach to analyzing and designing of an application, system, applying the object-oriented paradigm and visual modeling throughout the development life cycle. It fosters better stakeholder communication, product quality, emphasizes modularity and re-usability, with the goal of satisfying the "open closed principle". The primary tasks in object-oriented analysis (OOA) include: to find the objects, organize the objects, describe how the objects interact, define the behavior of the objects and define the internals of the objects.

Support Vector Machines (SVMs): SVMs are categorization methods that plot class examples (e.g., messages) to points in space with the objective to maximize the margin around a hyperplane separating the classes. In the application of ScalaNLP's built-in SVM solver, which implements the Pegasus maximization algorithm, the optimizer runs stochastic sub gradient descent on the primal objective using the batches. The ScalaNLP SVM interface does not allow users to change kernel parameters.

A. System Design

The systems design involves:

- **Conceptual design:** what the system should do
- **Logical design:** what the system should look like to the user
- **Physical design:** how the system should be built

Structured design tools: organization of programs and program modules (structure chart) and processing logic specification in each module (pseudo code)

Architectural Design: The architectural design of the system emphasizes the design of the system logical design of the system and focused on the abstract representation of the data flows, outputs and inputs of the system. This can be achieved through modeling, using graphical model of the actual system. Logical design involves entity-relationship (ER) diagrams architecture that describes the structure, behavior and more views of that system.

Physical Design: The physical design relates to the actual input and output processes of the system. This is explained in terms of how data is input into a system, how it is verified/authenticated, how it is processed, and how it is displayed. In physical design, the following requirements about the system are decided.

- Input requirement,
- Output requirements,
- Storage requirements,
- Processing requirements,
- System control and backup or recovery.
- Actually, the physical portion of system design can generally be broken down into three sub-tasks:
- User Interface Design
- Data Design
- Process Design

IV. RESULTS AND DISCUSSION

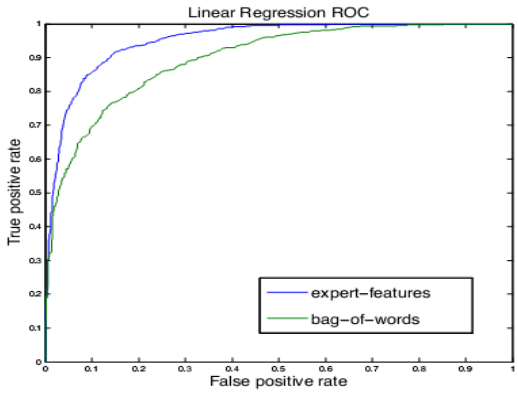

Figure 4.1: Linear Regression Curves

Linear regression ROC curves for classier using bag-of-words and bag-of-words with "expert" features Our initial results using the Pegasos SVM solver included in ScalaNLP were lower than expected. The classifier trained on the bag-of-words feature set (29 messages) yielded a 77% mean accuracy over 10-fold cross-validation. The addition of expert features actually decreased this accuracy to 51%. Table 4 provides a list of top features for the bag-of-words and expert feature models.

The lists include a number of words, such as "Nigerian prince", "send the money fast" and "do not disclose details of this transaction" which should ideally not be highly weighted.

While we did not remove stop words for this project, this is left for future consideration.

Our results with LIBSVMs RBF kernel were consistently better than any of the other classifers we tested. We evaluated the classifier's performance on five pairs of bag-of-words and expert feature data sets ranging in size from 20 to 35 messages. Our mean accuracy over the bag-of-words datasets was 85.73% and 98.41% for the bag-of-words with expert features. We observed a slight decrease in performance on the bag-of-words data sets as the data size grew, but do not have a hypothesis as to why this occurred. Figure 4.1 shows the AUCs and ROC curves for the 50k data sets, making clear the significantly greater AUC resulting

from the addition of expert features. As expected, however, both the ScalaNLP and LIBSVM implementations took substantially longer to train.

Table 4.3 Training dataset

Text	IsSpam
Go until jurong point, crazy	-2
Free entry in 2 a wkly comp to win FA Cup	-2
Hello	0
,000	-2
00,000.00	-2
diplomatic courier	-2
Hi	0
Barrister	-2
Barr	-2
foreign payment department	-2
Hi how are you	0
I love you	0
courier service	-2
charlessoludo	-2
Lagos	-2
remain blessed	-2
You	0
I am now rich	-2
thinking of relocating	-2
refused to pay me	-2
travel down to Nigeria	-2
Morning	0
my compensation	-2
directed to meet	-2
I contacted him	-2
those that are yet to receive their payments	-2
Afternoon	0
David Mark	-2
Sanusi Lamido	-2
David Koffi	-2
Evening	0
Living	0
Working	0
OkonjoIweala	-2
fund is with them	-2
nobody will find out	-2
off the books	-2
Police	0
Army	0
Prince	-2
god bless	-2
wire the money	-2
Stop	0
travel agent	-2
Confidential	-2
render advice	-2
Fff	0
credit card	-2
God-fearing	-2

The Splash screens

This is the first screen displayed on startup which shows the student information and initializes all modules of theproject.

Figure 4.2 The Splash screen

Spam Detected Page

This page is displayed when spam is detected by the SVM classifier. It covers the entire screen preventing the user from further continuing his or her activities.

To continue using the system, the admin must input his or her username and password. The dataset used to train the SVM is shown in fig 4.6, it shows an accuracy of 55% and correctly classifies the last sentence as spam.

Figure 4.3: Spam detected page

Figure 4.4 Admin log in details on detection

Fig 4.5 Admin password entry on detection

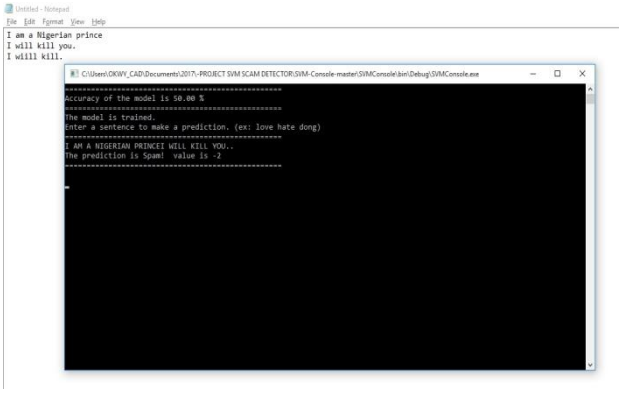

Figure 4.6 The trained dataset information

V. CONCLUSION

There have been several attempts to monitor and detect energy theft and network attacks (cybercrimes) using various techniques, all to no avail. Emphases have always been on cybercrime laws without detection and monitoring cybercrime. A paradigm shift was made from mere cyber-attack to the monitoring/identification of the workstation and cyber-criminal, who hitherto appeared to be anonymous. Electric energy theft and cybercrime is a menace that should be eradicated or reduced to a very minimum level for our great nation to break even. Several prominent cybercrimes and causes have been discussed in this research. The study shows that majority of the crimes conducted and carried out by the youths in our society. Implementation of this research will eliminate energy theft and cybercrimes in the society.

VI. RECOMMENDATIONS

a. It is recommended that the Government and corporate organizations should sponsor mass-production of this dependable cybercrime monitoring system, which can be applicable in towns, Local Government Areas and related environments.

b. All cyber stations should be implored to and implement the new monitoring software for security checks against cyber threats, and should permit cyber police access to check threats as to detect and apprehend criminals.
c. Cyber security education should be introduced at all levels of education to enlighten citizens and prospective ones on possible threats they are likely to face as they use the Internet.

REFERENCES

[1] Adegbeji, O. B (2008). "Computer Security in Cyberfafes", In Security and Software for Cybercafes,E.E.Adomi, Ed. Hershey PA. IGI Global, pp. 18-29.
[2] Balkin, J., Grimmelmann, J., Katz, E., Kozlovski, K., Wagman, S. &Zarsky, T. (2006). (eds) Cybercrime: Digital Cops in a Networked Environment, New York.
[3] Batool, S.H and Mahmood, K "Entertainment, communication r academics use? A Survey of Internet Café users in Lahore, Pakistan," Inf. Dev, vol 26, no. 2. Pp 141-147, 2010.
[4] Bazelon, D.L, Choi, Y.J and Conaty, J.F (2006), 'Computer Crimes', 43 American Criminal Law Review, 259.
[5] Bola, O. O and Ogunlade,O.O (2012) "Accessibility and Utilization of Intent Service by Graduate Students in University of Lagos Nigeria", Eur Res.,vol. 25. No 7.pp 1092-1098,
[6] Casey, E (2004), "Digital Evidence and Computer Crime". St. Louis, MO: Elsevier Press.
[7] Colliers, D (2004), 'Criminal Law and the Internet', in Buys, R, (ed.) Cyberlaw @ SA (2' Ed.), Pretoria: Van Schaik Publishers.
[8] Council of Europe Convention on Cybercrime, (2001) ETS No. 185, 2001.
[9] Emiri, O.T (2008), "Prevention of cybercafes". In Security and Software for Cybercafe E.E. Adomi, Ed. Hershey PA: IGI Global, 2008, pp. 2.53-269
[10] Ewepu G, (2016) "Nigeria losesN127bn annually to cyber-crime" – NASA available at:http://www.vanguardngr.com/2016/04/nigeria-loses-n127bn-annually-cyber-crime-nsa/Retrieved Jun 29, 2017.
[11] Gencer, S.I and Koo, M (2012) "Internet Abuse among Teenagers and its Relations to Internet Usage Patterns and Demographics", *Educ. Technnol. Soc.*, vol 15, no. 2. Pp. 25-36, 2012.
[12] Hassan, A.B. Lass F.D. and Makinde J. (2012) Cybercrime in Nigeria Case, Effects and the Way Out, ARPN Journal of Science and Technology, vol 2(7), 626-631.
[13] Hendrix,R.C (2013) "A Guide to Starting an Internet Café Business", 2013.
[14] Iroegbu, E (2016) "Cyber-security: Nigeria lose over N127bn annually through Cybercrime," available at: http://www.thisdaylivecom/index.php/rertieved Jun. 9, 2016.
[15] Igun, S.E (2008) "Cybercrime control in developing countries cybercafes" In Security and Software for Cybercafe E.E. Adomi, Ed. Hershey PA: IGI Global, 2008, pp. 283-294.
[16] Laskshmi P. and Ishwaeya M. (2015),"Cyber Crime Prevention" Communication Engineering, vol. 4(3).
[17] Lewis, B.C (2004), 'Prevention of Computer Crime Amidst International Anarchy', 41 American JournaL of Crimina1 Law Review, 1353.
[18] Lininger, R and Dean, R (2005), "Phishing, Cutting Identity Theft Line" Toronto, Wiley.
[19] Low, C, (2014)"Understanding Wireless Attacks and Detection". Available at http://www.sans.org/reading/click/528Accessed on 10-04-2017.
[20] Maitanmi, O. Ogunlere, S. and Ayinde (2013) "Impact of Cyber Crimes" International Journal of Engineering and Science (1)JES, vol. 2(4), 45-51.
[21] Mbaskei, M.O. (2008) "Cybercrime: Effect on Youth Development"http://www.i-genius.org
[22] McQuade, S. (2006)"Understanding and Managing Cybercrime" Boston: Allyn & Bacon.
[23] Mohammed, L.A. (2008)"Cybercafé Systems Security", In *Security and Software for Cybercafes*, E.E. Adomi, Ed. Hershey PA: IGI Global, 2008, pp. 1-17.
[24] Okeshola F.B and Adeta A.K, (2013) "The Nature, Causes and Consequences of Cyber Crime in Tertiary Institutions in Zaria-Kaduna State, Nigeria" American International Journal of Contemporary Research, vol. 3(9), 98-114.
[25] Oluwafemi,O, and Adepoju, S.A. (2016) "cybercafés in Nigeria: Course to Internet?", Internal Conference on Information and Communication Technology and its Applications" Federal University of Technology Mina, Nigeria, 117-123.
[26] Omodunbi, B.A, Odiase, P.O, Olaniyan, O. M and Esan (2016) "Cybercrime in Nigeria: Analysis, Detection and Prevention" , FUOYE Journal of Engineering and Technology, vol.1, Issue 1, 37-42.
[27] Otokunefor, H.O.C and Kari, H. K (2008). "Issues, Controversies, and Problems of Cybercafes Located in a University Campus", In Security and Software for Cybercafe E.E. Adomi, Ed. Hershey PA: IGI Global, 2008, pp. 62-83.
[28] Oyelude,A. A and Adewumi, C.O.B (2008) "Cybercafe Physical and Electronic Security Issues. Issues in security and software for cybercafes E.E Adomi Ed Hershey PA: IGI Global Pg 84-89
[29] Onojaefe D. Learning M (2008). Managing cybercafes: achieving mutual benefit through partnership Issues in security and software for cybercafes E.E Adomi Ed Hershey PA: IGI Global Pg 95-111
[30] Obuh, A.O (2008). Viruses and Virus protection in cybercafes, Issues in security and software for cybercafes E.E Adomi Ed Hershey PA: IGI Global Pg 70-185
[31] Utulu S.C.A (2008) Enhancing social security in Nigeria in security and software for cybercafes", In Securociity and Software for Cybercafes. E.E Adomi Ed Hershey PA: IGI Global Pg 30-39
[32] Rangaswamy, N (2008) "Telecenters and Internet Cafes the case of ICTs in Small Business", Asian J. Comm.,vol. 18, no. 4, pp. 46-61.
[33] Rauniar D (2008) "Cybercafes of Nepal: Passage to cyber crime."In Security and Software for Cybercafe E.E. Adomi, Ed. Hershey PA: IGI Global, 2008, pp. 253-269.
[34] Sodiq.K. A, (2012) "Assessment of the Management of Information and Communication Technology (ICT) Infrastructure of Selected Cybercafes in Lagos State", in Journal of Education and Social Research.Vol. 2, no. 9, 2012, pp. 181-188.
[35] Sommer. P (2004) 'The Future for the Policing of Cybercrime'., Computer Fraud and Security,8.
[36] Tiemo, P. A. and Charles- Iyoha,C.U"Cybercafes and Cybercrimes in Nigeria", Ed. Hershey PA IGI Global 2008, pp. 295-306.
[37] Utulu,S.C.A (2008)"Enhancing Social Security through Appropriate Cyber Security Policy and Nigeria" In Security and Softwae for Cybercafes,E.S. Adomi, Ed. Hershey PA: IGI Global, 2008, pp. 30.
[38] Wada,, F, and Odulaja, G.O, (2012)"Electronic Banking and Cyber Crimes in Nigeria: A Theoretical Policy Perspective on causation "African journal of Computing & ICT, 69-82.