Available online ***www.jsaer.com***

***Journal of Scientific and Engineering Research*, 2020, 7(5):131-136**

Research Article

ISSN: 2394-2630
CODEN(USA): JSERBR

Cybercrime Reporting, Analytics and Tracking using Deep Learning Algorithm for Reconnaissance and Recovery: A Case Study of Nigeria

Jovworie Tanshi*, Nkolika O. Nwazor

Centre for Information and Telecommunications Engineering, University of Port Harcourt, Rivers State Nigeria
*Corresponding author: t.jovworie@tcomhq.com

Abstract The Cybercrime reporting system is a platform that gives cybercrime victims the opportunity to report a failed or successful cyber-attack on them. This system relies on deep learning to analyze the details of the report in other to give relevant law enforcement agencies the information they need to make more informed decisions. This will help reduce the number of cyber criminals in the society and increase the recovery rate of stolen funds due to cybercrimes. The front end of the Reporting system is a basic form that require the user to provide a well detailed information about the perpetuated or attempted crime. The designed system was implemented using HTML, CSS and Javascript for the form and PHP for submission of complaint to the database. Python programing language was used to implement the Deep Learning algorithm for analyzing the validity of a report and also cross reference information on multiple databases that will help the system provide substantial information about the source of the crime.

Keywords Cybercrime, Cyber Security, Deep learning, Encryption, Two Factor Authentication

Introduction

As the number of cyber criminals are growing, the number of their victims keep increasing as well. Much work has been done in creating awareness on data privacy, use of strong password, multi-factor authentication techniques etc. However, the number of Cybercriminals that are being convicted is very insignificant compared to the number of victims. Information Technology based Private and Government organizations both in Nigeria and abroad have being doing a great job in creating awareness on how users can stay safe on the internet. However, with all the awareness that is being created, hundreds of millions of users still fall victims of these cyber-attacks. Now, the question that comes to mind is; who are these cyber criminals and where are they?

According to the work in [1], the worldwide expense of cybercrime has now come to as much as $600 billion which is about 0.8 percent of worldwide Gross Domestic Product (GDP). More stressing than that figure might be the huge development from 2014, when a similar examination demonstrated the expense was distinctly as much as $445 billion [1].

The security challenges of internet banking have increased with the increase in the use of internet banking platforms by the general populace. Of all the various authentication techniques, OTP (one-time password) is regarded as one of the most effective methods of implementing two factor authentication, and it is now widely used on online banking platforms. However, attack methods that can detour OTP have been developed that additional security for OTP is now required [2].

Cyber security is the term for the techniques deployed to maintain a strategic distance from or decrease in unauthorized access to information, PCs (personal computers) or cell phones. Cyber security covers shielding, secrecy and protection, additionally it also entails the accessibility and integrity of information, the two of which are crucial for quality assurance. Security bridges can happen when we use paper records, send data utilizing fax machines and even verbally. Be that as it may, the results of security ruptures with advanced data are conceivably unquestionably progressively serious, as data can be circulated all the more effectively and to a far more extensive group of audience [3].

In other to mitigate the operations carried out by these Cyber Criminals different authentication processes have been put in place such as encouraging internet users to use Alpha-numeric and special character based passwords. This has its own issues, as hackers can physically eavesdrop on users or use password sniffing tools to obtain their passwords. This gave rise to the introduction of Two-Factor Authentication (2FA) and Multifactor Authentication (MFA) that can be used to validate the identity of the user before providing access or completing an operation. Popular examples of 2FA and MFA techniques is the use of One-Time-Password (OTP) and Hardware token devices in conjunction with password and Personal Identification Number (PIN). OTPs that are passed over SMS and email are vulnerable to social engineering attacks. OTPs are also indirectly susceptible to man in the middle (MITM) and man in the browser (MITB) attacks [4]. The work in [5] proposed the introduction of a push to approve application to enable the user accept or decline a request for approval of a transaction.

For cyber criminals, the expression "crime doesn't pay" is ludicrous. Cybercrime has expanded immensely, and the reasons are self-evident: It is profoundly rewarding and far less risky, contrasted with the good old bank heist. Until essential measures are taken to increase the risk and lower the value of cybercrimes, we won't be able to stop the culprits. Until we secure the Internet, cyber criminals will keep on pulling off high-value, low-risk offenses [6].

Data framework compromise and cyber security incidents are becoming increasingly costly. Canadian lender Desjardins Group recently realized it had spent C$70 million ($53 million) during a breach earlier in the year that exposed personal information of 2.9 million users. A manufacturer Norsk Hydro disclosed that the final bill for its crippling cyberattack could be as high as $75 million. British Airways and Marriott have also included $100 million each onto the final cost of their incidents after falling foul of GDPR [7].

In 2016 took cybercrimes escalated. There were reports of it being used to influence votes during general elections. In Nigeria, several organizations suffered cyberattacks, some had to pay ransom for their data to be released [6]. The federal government also estimated the annual cost of cybercrime in Nigeria to be about 0.08% of the country’s Gross Domestic Products (GDP), which represents about N127 billion. Also, as predicted in the annual cyber security forecast, 2016 saw a rise in the number of sophisticated phishing attacks; these occurred on the platforms of various Nigerian financial institutions and utility companies [8].

The FBI also reported an increased interest in cyber security hacking competitions and also efforts by the regulatory bodies in setting up committees responsible for implementing and monitoring the cybercrime act [8].

In February 2020 a hacker group in Romania that has been on the FBI’s watch list since 2007 was apprehended in Romania. This a significantly lengthy period for a crime that doesn’t leave physical trails behind.

In Nigeria, the operation of tracking down active cyber criminals by the police force is not very effective and most times uses a double standard. Aside the common advance free fraud and basic money swindling, law enforcement agents are not really involved in tracking down cyber criminals that use phishing, brute force attacks and credential theft to perpetrate crimes on the internet. Also, law enforcement agents and Information Technology Agencies don’t have a comprehensive record of perpetuated internet crimes as majority of the victims rarely report these case. Even the few that are reported are not properly documented.

With a significant rise in internet penetration in Nigeria to about 47.1 % in 2018 by Statistica combined with youth unemployment rate of about 45% in 2017 by the Nigerian Bureau of Statistics, some Nigerian youths have chosen a negative way of getting riches through different types of cybercrime. The Nigerian government loses 128 billion naira yearly to this menace as reported by the Nigerians Communications Commission Cyber Security standpoint in 2017. Aside from the economic destruction cybercrime does to the nation, it has additionally created a bad picture for Nigerians in the Diaspora. Furthermore, the rate at which the EFCC reports cases on cyber related crimes has soared [9].

In 2019 Internet Crime Report, the Federal Bureau of Investigation (FBI) received 23,775 Business Email Compromise (BEC)/Email Account Compromise (EAC) reports with adjusted losses of over $1.7 billion. BEC/EAC is a new trick focusing on the two organizations and individuals performing a transfer of funds [8]. The fraud is frequently carried out when a subject compromises legitimate business email accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds [8]. BEC/EAC is continually advancing as criminals get increasingly updated. In 2013, BEC/EAC tricks routinely started with the hacking or spoofing of the email accounts of chief executive officers or chief financial officers, and fraudulent emails were sent requesting wire payments to be sent to fraudulent locations. Throughout the years, the misrepresentation changed to incorporate trade off of individual messages, bargain of seller messages, parodied legal counselor email accounts, demands for W-2 data, the focusing on the real estate sector, and fraudulent solicitations for large amounts of gift cards [10].

In 2019, the FBI observed an increase in the number of BEC/EAC reports related to the diversion of payroll funds. In this type of scheme, a company's human resources or payroll department receives an email impersonating an employee requesting to update their direct deposit information for the current pay period. The new direct deposit information generally links to a pre-paid card account [10].

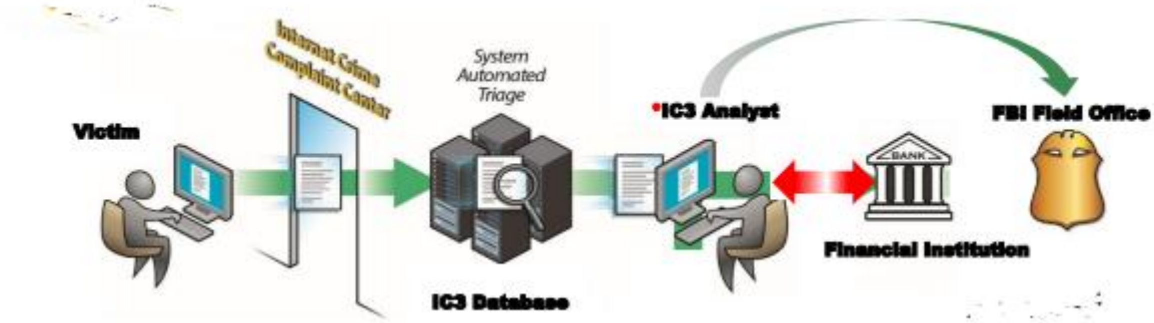

Figure 1: United States FBI's Cybercrime Reporting System
Source: Federal Bureau of Investigations, 2019

Analysis of the Existing System

In Nigeria, the activities of cybercriminals are not properly handled by the law enforcement agencies. There is no central point for submitting cybercrime complaints. The cases submitted by some victims are not properly documented. This makes it very difficult for to really follow up with the perpetrators of the crime.

Most Nigerian law enforcement officers even lack the requisite knowledge of the basic use of computers and internet security standards. This makes it extremely difficult for them to comprehend the complexity of cybercrimes as they cut deep, ranging from basic SMS based fraud to advanced phishing and brute force attacks. In summary, there is actually no infrastructure in place to give Nigerians the opportunity to provide detailed information about a cybercrime or an attempted cybercrime.

Design of the Proposed System

In other to handle these lapses in addressing the issue of cybercrime, the Federal Government of Nigeria should set up an Internet Crime Complaint Center where victims of cybercrime can directly report incidents by providing detailed information about how they were compromised. When the information is received, an artificial intelligent system known as the Report Analyzer will first examine the content of the report to determine if it is valid or a duplicate report. If the report submitted by the user is invalid or a duplicate of a valid report, the information will be discarded. However, if the information provided appears to be valid, it will be feed into the deep learning and analytics system, where more information will be gathered about the victim, criminal and the crime.

In a situation where an illegal website may be involved, the system may track the ownership of the website, using information that may be available via various regulatory bodies and law enforcement agencies such as International Consortium of Assigned Names and Numbers (ICANN) and Nigerian Communications Commission (NCC).

The deep learning algorithm can also track the IP address which the cyber-criminal may have used. Although with the advent of VPN that effectively reroutes traffic and IP addresses, it may not be easy to achieve that easily. However, most cyber-criminals have patterns, make mistakes such as giving away useful information that will expose their identity. A system that relies on analytics, deep/machine learning, coupled with artificial neural networks and other supporting smart technologies will be able to trigger some red flags or provide indicators that can be used to locate these cyber-criminals.

Figure 1 shows the structure of the cybercrime reporting system.

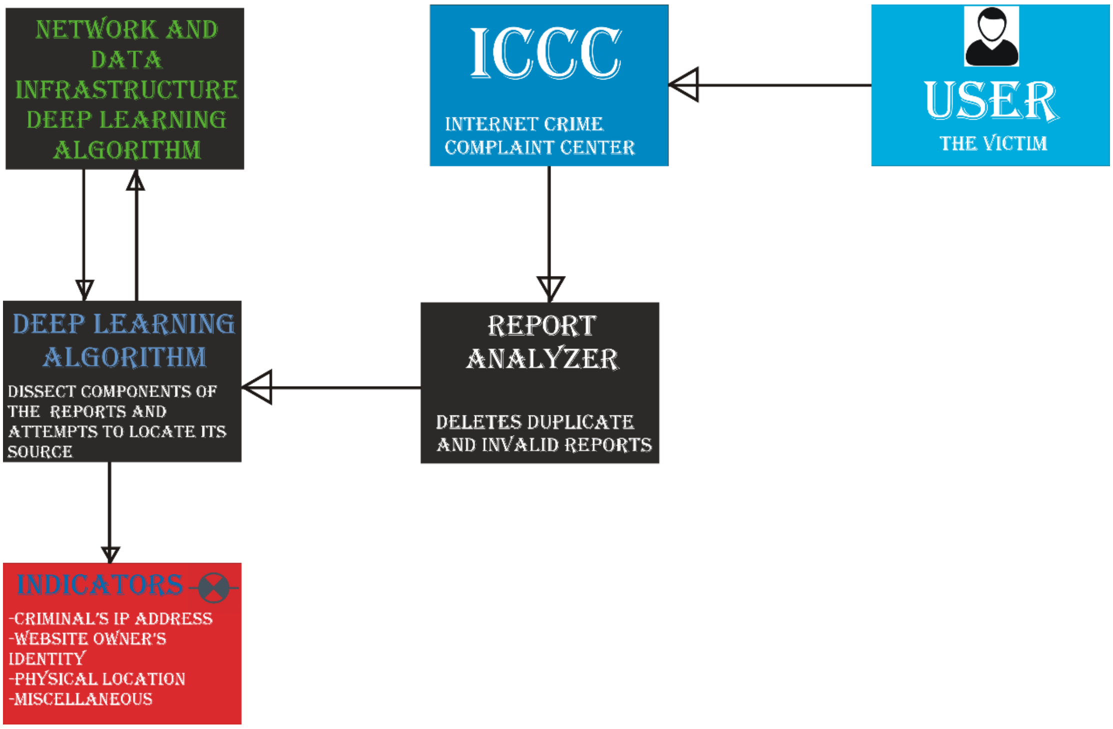
NETWORK AND DATA INFRASTRUCTURE DEEP LEARNING ALGORITHM
ICCC
INTERNET CRIME COMPLAINT CENTER
USER
THE VICTIM
DEEP LEARNING ALGORITHM
DISSECT COMPONENTS OF THE REPORTS AND ATTEMPTS TO LOCATE ITS SOURCE
REPORT ANALYZER
DELETES DUPLICATE AND INVALID REPORTS
INDICATORS
-CRIMINAL'S IP ADDRESS
-WEBSITE OWNER'S IDENTITY
-PHYSICAL LOCATION
-MISCELLANEOUS

Figure 1: Structure of the Cybercrime Reporting System

In other to achieve this design;

a) Some policies regarding ICT and Digital privacy must be put in place to give the government and the parastatals involved the power to act.
b) This system will require a high level of harnessing of data from telecommunication companies, banking and finance sectors and literarily the entire backbone of the countries data infrastructure. The key agencies that will be involved include: Nigerian Identity Management Commission (NIMC), Central Bank of Nigeria (CBN), the Nigerian Military and Police Force
c) The center will also have a direct information exchange with the ICCCs of other countries in other to adequately perform. This is very important because most cybercrimes may be committed outside the shores of the victim's country.

Description of the Components of the Proposed System

The cyber reporter system relies on the following parameters to function;

a. **User generated content:** This is the report from the victim of the crime. It contains a detailed description of the asset that was stolen from the user and the method that was deployed. For example, if a user's credentials were stolen using a phishing website, the user can submit the link of the website and the description of the credentials that were stolen (e.g. username & password, credit card details, contact information and other personal information). User can also state the medium through which the phishing link was sent, the time it was sent and the time the credentials were submitted.
b. **Analyzer:** The job of the analyzer algorithm is to inspect, the records submitted and determine its validity. For example, if the supposed phishing link reported is not an existing website address or an address that has been inactive before the timeline of the supposedly time of theft, the analyzer will flag such a report as invalid and discard it. If a reporter provides the phone number(s) that made/received the call or phishing text, and the timeline of the call or text does not match any records on the telecommunications database, the report will also be discarded.

c. **Deep learning Algorithm:** After a report has been flagged as valid, it is then forwarded to the deep learning algorithm section of the platform for further analysis. At this stage, the purpose of this analysis is to identify the culprit behind the attack. Identification entails collecting the name, IP address, MAC Address, physical location, bank account details, domain WHOIS data and other relevant information that can be used to profile the attacker.

d. **Database Chain:** In other for the deep learning algorithm to work, the system has to be linked with multiple state own and private sector database. These databases may range from police, telecommunications, financial institutions, identity management institutions, cloud based service providers. Cross referencing the cybercrime reports with these chains of databases will supply some form of pattern that can be used to identify the culprit and also determine the nature of the crime and also the appropriate agent to monitor it.

e. **Law Enforcement Agencies' Interface:** Due to the fact that a single agency may not be able to address all the various forms of cybercrimes, there is a need to collaborate with relevant agencies such as the Economic and Financial Crimes Commission (EFCC), Central Bank of Nigeria (CBN), Nigerian Police Force (NPF) and the Nigerian Security Agency (NSA). These organizations are mandated to carry out arrests and asset retrieval depending on the severity of crime and their mandate. The deep learning algorithm will help determine who gets the analysis of the report suggestions on the next point of action.

Conclusion

The security challenges involved in cyberspace has been an issue for the past three decades. The increase of cybercriminals has exponentially increased the rate of cybercrimes. Although safety measures are being suggested on a regular basis to internet users, it is high time a different approach is deployed to actually bring the fight to the attackers instead of just defending ourselves from them. Thus, we need a system that will help us to not just gather eyewitness/victim's reports on cybercrimes to better educate users on current trends, but also use this data to effectively profile and apprehend cybercriminals. This will also increase the recovery rates of stolen assets of cybercrime victims.

References

[1]. Lynette Lau, “Cybercrime ‘pandemic’ may have cost the world $600 billion last year 2018”. Available online: https://www.cnbc.com/2018/02/22/cybercrime-pandemic-may-have-cost-the-world-600-billion-last-year.html [Accessed: September 2, 2019].

[2]. Yoo, C., Kang, B. T., & Kim, H. K. (2015). Case study of the vulnerability of OTP implemented in internet banking systems of South Korea. Multimedia Tools and Applications, 74(10), 3289–3303. Available online: https://doi.org/10.1007/s11042-014-1888-3 [Accessed: September 8, 2019].

[3]. Cavelty, M. D. Cyber-security. (2017, May). Available online: https://www.researchgate.net/publication/256018865_Cyber-Security [Accessed: September 2, 2019].

[4]. Rakesh Thatha, Limitations of two factor authentication (2FA) technology. Published on Computer Weekly: 25 Sep 2012. Available online: https://www.computerweekly.com/tip/Limitations-of-two-factor-authentication-2FA-technology [Accessed: September 5, 2019]

[5]. Tanshi J. and Nwazor N.O, (2020). Standalone Two Factor Authentication System using Push to Approve. International Journal of Engineering and Science Inventions, 9 (3), 16-21. Available online: ijesi.org/v9i3(series-1).html

[6]. Roger A. Grimes, 2012. ANALYSIS; Why Internet crime goes unpunished. Available online: https://www.csoonline.com/article/2618598/why-internet-crime-goes-unpunished.html

[7]. Dan Swinhoe, 2019. What is the cost of a data breach? Available online: https://www.csoonline.com/article/3434601/what-is-the-cost-of-a-data-breach.html

[8]. Tope Aladenusi, 2017. 2017 Nigeria Cybersecurity Outlook. Available online: https://www2.deloitte.com/ng/en/pages/risk/articles/2017-nigeria-cybersecurity-outlook.html#

[9]. Obarafor Victor, 2019. Cyber Crime in Nigeria, some causes, effects, and solutions.

https://www.researchgate.net/publication/335790484_Cyber_Crime_in_Nigeria_some_causes_effects_and_solutions_by_Obarafor_Victor

[10]. Federal Bureau of Investigation, 2019. 2019 INTERNET CRIME REPORT.