International Journal of Computer Science and Engineering (IJCSE)
ISSN(P): 2278–9960; ISSN(E): 2278–9979
Vol. 10, Issue 1, Jan–Jun 2021; 11–20

International Academy of Science, Engineering and Technology
Connecting Researchers; Nurturing Innovations

SOFT COMPUTING: EXPERIMENTATION OF MULTI-CLASSIFIER-BASED CYBER-ATTACK DETECTION SYSTEM

Ismaila W. Oladimeji[1], Ismaila Folasade. M[2] & Olajide Anthony T[3]

[1]Research Scholar, Department of Computer Science and Engineering, Ladoke Akintola University of Technology, Ogbomoso, Nigeria

[2]Research Scholar, Department of Computer Science Osun State Polytechnic, Iree, Nigeria

[3]Research Scholar, Department of Computer Science, Kwara State Polytechnic, Ilorin, Nigeria

ABSTRACT

The World Wide Web is used by hackers to send malicious attack in form of phishing, e-mail spoofing and malware infection to people. With the speed of cyber activity and high volume of data used, the protection of cyber space cannot be handled by any physical device or by human intervention alone. It needs considerable automation to detect threats and to make intelligent real-time decisions. It is difficult to develop software with conventional algorithms to effectively protect against the dynamically evolving attacks. It can be tackled by applying bio inspired computing methods of artificial intelligence to the software. The purpose of this study is to explore the possibilities of artificial intelligence based algorithms in addressing the cybercrime issues.

The algorithms include Logistic Regression (LR), Support Vector Machine (SVM) and Counter Propagation Neural network (CPNN) and their ensemble. 700 dataset were gotten from a renowned database. The dataset were subjected to features extraction and transformation. The outputs of the experimentation showed that sensitivity produced by LR, SVM and CPNN are 65, 72.5 and 78% respectively. The results of specificity of LR, SVM and CPNN are 57.0, 66.5 and 63.5% respectively while the results of accuracy produced by LR, SVM and CPNN are 75.8, 88.3 and 87.5% respectively. However, the results produced by ensemble of the three algorithms are 70.4, 81.7 and 91.6% for sensitivity, specificity and accuracy respectively

KEYWORDS: *Cybercrime, Logistic Regression, Support Vector Machine, Counter Propagation Neural Network*

Article History

Received: *30 Jul 2020* **|** ***Revised:*** *08 Jan 2021* **|** ***Accepted:*** *19 Jan 2021*

INTRODUCTION

Cybercrimes also includes criminal activities performed by the use of computers like virus attacks, financial crimes, sale of illegal articles, pornography, online gambling, e-mail spamming, cyber phishing, cyber stalking, unauthorized access to computer system, theft of information contained in the electronic form, e-mail bombing, physically damaging the computer system, etc. (Kandpal and Singh, 2013). A cyber attack is an attack initiated from a computer against a website, computer system or individual computer (collectively, a computer) that compromises the confidentiality, integrity or availability of the computer or information stored on it. Cyber attacks take many forms, including: Gaining, or attempting to gain,

unauthorized access to a computer system or its data. Unwanted disruption or denial of service attacks, including the take down of entire web sites; Installation of viruses or malicious code (malware) on a computer system; Unauthorized use of a computer system for processing or storing data; Changes to the characteristics of a computer system's hardware, firmware or software without the owner's knowledge, instruction or consent and Inappropriate use of computer systems by employees or former employees (Smith, 2002).

Intrusion detection is the process of monitoring the events occurring in a computer system or network and analysing them for signs of possible *incidents*, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices. An *intrusion detection system* (IDS) is software that automates the intrusion detection process. An *intrusion prevention system* (IPS) is software that has all the capabilities of an intrusion detection system and can also attempt to stop possible incidents.

IDS Detection Methodologies

An Intrusion Detection System or IDS is a network security technology originally built for spotting vulnerabilities that exploit against a targeted application or a computer system. It is the process of monitoring the events occurring in a computer system or in a network and analyzing them for possible incidents indications, which are violations or impending threats of destruction of computer security strategies, suitably used policies, or common security practices.

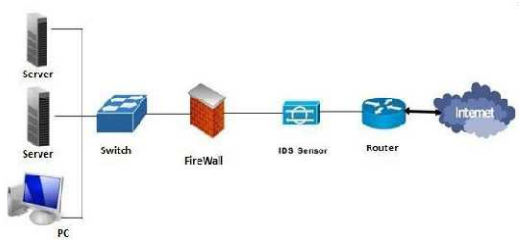

Figure 1: Intrusion Detection System.

IDPS technologies use many methodologies to detect incidents including signature-based, anomaly-based, and stateful protocol analysis, respectively. Most IDPS technologies use multiple detection methodologies, either separately or integrated, to provide more broad and accurate detection.

- **Signature-Based Detection** A *signature* is a pattern that corresponds to a known threat.

Signature-based detection is the process of comparing signatures against observed events to identify possible incidents. Sample includes a telnet attempt with a username of "root", which is a violation of an organization's security policy. Signature-based detection is very effective at detecting known threats but largely ineffective at detecting previously unknown threats, threats disguised by the use of evasion techniques, and many variants of known threats.

- **Anomaly-Based Detection** This is the process of comparing definitions of what activity is considered normal against observed events to identify significant deviations. An IDPS using anomaly-based detection has *profiles* that represent the normal behavior of such things as users, hosts, network connections, or applications. The major benefit of anomaly-based detection methods is that they can be very effective at detecting previously unknown threats. Anomaly-based IDPS products often produce many false positives because of benign activity that deviates significantly from profiles, especially in more diverse or dynamic environments.

- **Stateful Protocol Analysis** This is the process of comparing predetermined profiles of generally accepted definitions of benign protocol activity for each protocol state against observed events to identify deviations. Unlike anomaly-based detection, which uses host or network-specific profiles, stateful protocol analysis relies on vendor-developed universal profiles that specify how particular protocols should and should not be used. The "stateful" in stateful protocol analysis means that the IDPS is capable of understanding and tracking the state of network, transport, and application protocols that have a notion of state. The primary drawback to stateful protocol analysis methods is that they are very resource-intensive because of the complexity of the analysis and the overhead involved in performing state tracking for many simultaneous sessions. Also this method cannot detect attacks that do not violate the characteristics of generally acceptable protocol behaviour, such as performing many benign actions in a short period of time to cause a denial of service (Scarfone and Mell, 2007).

Types of Web Attacks

The different types of Web attacks covered in this section are the following:

• ***Cross-Site Scripting (XSS)*** attack is an application-layer hacking method used for hacking Web applications. This type of attack occurs when a dynamic Web page gets malicious data from the attacker and executes it on the user's system.

• **Cross-*Site Request Forgery (CSRF)*** In CSRF Web attacks, an attacker forces the victim to submit the attacker's form data to the victim's Web server. The attacker creates the host form, containing malicious information, and sends it to the authenticated user. The user fills in the form and sends it to the server. Because the data is coming from a trusted user, the Web server accepts the data.

• ***Code Injection*** A code injection attack is similar to an SQL injection attack. In this attack, when a user sends any application to the server, an attacker hacks the application and adds malicious code, such as shell commands or PHP scripts. When the server receives the request, it executes that application. The main goal of this attack is to bypass or modify the original program in order to execute arbitrary code and gain access to restricted Web sites or databases, including those with personal information such as credit card numbers and passwords.

• ***Parameter Tampering*** is a type of Web attack that occurs when an attacker changes or modifies the parameters of a URL. Parameter tampering takes advantage of programmers who rely on hidden or fixed fields, such as a hidden tag in a form or a parameter in a URL, as the only security measure to protect the user's data. It is very easy for an attacker to modify these parameters.

• ***Cookie Poisoning*** Web applications use cookies to store information such as user IDs, passwords, account numbers, and time stamps, all on the user's local machine. In a cookie poisoning attack, the attacker modifies the contents of a cookie to steal personal information about a user or defraud Web sites.

• ***Cookie Snooping*** Cookie snooping is when an attacker steals a victim's cookies, possibly using a local proxy, and uses them to log on as the victim. Using strongly encrypted cookies and embedding the source IP address in the cookie can prevent this. Cookie mechanisms can be fully integrated with SSL functionality for added security.

• ***Authentication Hijacking*** is a key component of the authentication, authorization, and accounting (AAA) services that most Web applications use. As such, authentication is the first line of defence for verifying and tracking the

legitimate use of a Web application. One of the main problems with authentication is that every Web application performs authentication in a different way. Enforcing a consistent authentication policy among multiple and disparate applications can prove challenging. Authentication hijacking can lead to theft of services, session hijacking, user impersonation, disclosure of sensitive information, and privilege escalation. An attacker is able to use weak authentication methods to assume the identity of another user, and is able to view and modify data as the user.

• ***Log Tampering*** Web applications maintain logs to track the usage patterns of an application, including user login, administrator login, resources accessed, error conditions, and other application-specific information. These logs are used for proof of transactions, fulfilment of legal record retention requirements, marketing analysis, and forensic incident analysis. The integrity and availability of logs is especially important when non-repudiation is required.

• ***Directory Traversal Attack***, also known as a forceful browsing attack, occurs when an attacker is able to browse for directories and files outside normal application access. This exposes the directory structure of an application, and often the underlying Web server and operating system.

• ***Impersonation Attack*** An impersonation attack is when an attacker spoofs Web applications by pretending to be a legitimate user. In this case, the attacker enters the session through a common port as a normal user, so the firewall does not detect it. Servers can be vulnerable to this attack due to poor session management coding.

Review of Related Work

According to Wijesinghe, *et al.* (2016) introduced a sophisticated cyber-crime defence system which involves intelligent agents that are based on artificial intelligence. Basically, an intelligent agent is a software component which can be emerged in an environment, take decisions, and has the ability of noticing and representing. Kirda and Kruegel (2005) developed Anti-Phish, a mechanism that aims at preventing Internet users against any form of phishing attack. The system tracks information considered sensitive and quickly provide warning against divulging such information to any website that is considered un-trusted. While Kolter and Maloof in 2006 explained the machine learning and data mining approaches for classifying and detecting malicious URLs anytime they appear in the wild. The authors were able to collate "*1,971 benign and 1,651 malicious"* executable and used *n*-grams of byte codes as a training example. After considering the most useful and relevant grams for prediction including Naïve Bayes, decision trees, support vector machines, and boosting, they arrived at conclusion that boosted decision trees performed best of all other approaches under the ROC curve of 0.996. Also, Alnajim and Munro (2009) proposed anti-phishing approach for detecting phishing website. This approach assists Internet users to differentiate between legitimate and phishing websites. It provides useful information to the end user to quickly recognize either a fake or genuine site. This approach is adjudged to be one of the best approaches for recognizing if a site is either of the two classifications. It was learnt from the work of Joshi et al. (2008) in which a mechanism for analysing feedbacks from the servers against the submitted credentials was also proposed that the main objective is to identify any forged website firstly submitting random credentials before the real credentials in a login process of a website. It is however observed that the technology is basically meant for a website that supports HTTP with both userID and passwords as credentials.

Kaur et al. (2012) constructed an efficient cybercrime detection system which is adaptive to the behaviour changes by combining the data mining techniques. The proposed system is a two stage cybercrime detection system which is based on the analysis of the user data in first stage and in second stage detects the false alarm. For this a two stage fraud detection system which combines decision tree classification and K-means clustering techniques is used. The accuracy of

the proposed work is 94.67 % and it efficiently detects the false rate anomalies. Ma, *et al.* in 2009 used the lexical and host-based features to detect malicious websites. Their approach could sift through numerous features and recognize the important URL metadata and components without demanding any domain expertise. They succeeded in evaluating up to 30,000 instances with good and promising results, specifically a very high classification rate of 95% - 99% and a low false positive rate. Ma, *et al.* (2011) adopted online algorithms so as to handle many URLs whose features evolve over a period of time. They developed a system to gather up-to-date URL features which was paired with a real-time feed of labelled URLs from a large mail provider. They reported a successful classification rate of 99% using confidence-weighted learning on a balanced dataset. However, apart from researchers findings, numerous proprieties based IDS were developed which includes (i) Emsa Web Monitor is a small Web monitoring program that monitors the uptime status of several Web sites, (ii) KeepNI checks the vital services of a Web site at an interval chosen by the user, (iii) eMailTrackerPro analyses e-mail headers and provides the IP address of the machine that sent the e-mail.

MATERIALS

This section gives a brief explanation of the mechanisms and algorithms used for the classification of web attacks/intrusion. This includes; Principal Component Analysis (used for feature extraction); Counter-propagation Neural Networks (CPNN), Logistic Regression (LR) and Support Vector Machine (SVM) used for classification.

Principal Component Analysis (PCA)

PCA is a widely used statistical technique for unsupervised dimension reduction. PCA is a useful statistical technique that has found application in fields such as face recognition and image compression, and is a common technique for finding patterns in data of high dimension. The main basis of PCA-based dimension reduction is that PCA picks up the dimensions with the largest variances. Principal component analysis (PCA) has been called one of the most valuable results from applied linear algebra. PCA is used abundantly in all forms of analysis - from neuroscience to computer graphics - because it is a simple, non-parametric method of extracting relevant information from confusing data sets. With minimal additional effort PCA provides a roadmap for how to reduce a complex data set to a lower dimension to reveal the sometimes hidden, simplified dynamics that often underlie it. For more information see Smith (2002), Jon (2003).

CPNN

The counter-propagation network is a supervised learning algorithm that combines the Grossberg learning rule with the SOFM. With a facial image fed into the CPN after some learning process, the Facial Expression Map was used to determine the unique emotional category for the image that is fed in. During learning, pairs of the input vector $\boldsymbol{X}$ and output vector $\boldsymbol{Y}$ were presented to the input and interpolation layers, respectively. These vectors propagate through the network in a counter flow manner to yield the competition weight vectors and interpolation weight vectors. Once these weight vectors become stable, the learning process is completed.

Logistic Regression

Logistic regression is used to obtain odds ratio in the presence of more than one explanatory variable. The procedure is quite similar to multiple linear regression, with the exception that the response variable is binomial. The result is the impact of each variable on the odds ratio of the observed event of interest. The main advantage is to avoid confounding effects by analyzing the association of all variables together. A logistic regression will model the chance of an outcome based on individual characteristics. Because chance is a ratio, what will be actually modeled is the logarithm of the chance given by

$$\text{Log}\,(\pi/(1-\pi)) = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \ldots\ldots\ldots + \beta_m X_m \quad (1)$$

Where π indicates the probability of an event (e.g., death in the previous example), and β_i are the regression coefficients associated with the reference group and the x_i explanatory variables. At this point, an important concept must to be highlighted. The reference group, represented by β_0, is constituted by those individuals presenting the reference level of each and every variable $x_{1\ldots m}$. (Sperande, 2018).

Support Vector Machine

A Support Vector Machine (SVM) is the most popular tool for dealing with a variety of machine-learning tasks, including classification. SVMs are associated with maximizing the margin between two classes. The concerned optimization problem is a convex optimization guaranteeing a globally optimal solution. The weight vector associated with SVM is obtained by a linear combination of some of the boundary and noisy vectors. Further, when the data are not linearly separable, tuning the coefficient of the regularization term becomes crucial. Even though SVMs have popularized the kernel trick, in most of the practical applications that are high-dimensional, linear SVMs are popularly used. The text examines applications to social and information networks.

RESEARCH METHOD

This section discusses the work flow of the multi-classifier-based intrusion detection system (as shown in figure 2) which is designed in stages including (i) Data source (ii) Feature extraction (iii) Pre-processing (iv) Classification (v) Evaluation.

Data Source The source of the dataset used was from United States (UCI) Machine Learning Repository at https://archive.ics.uci.edu/ml/datasets/URL+Reputation. The features extracted for classifications are thirteen in number based on each URL.

Feature Extraction With Principal component analysis (PCA), the objective of reducing the dimensions of a d-dimensional dataset used by projecting it onto a (k)-dimensional subspace with the aim of increasing the computational efficiency and accuracy.

Pre Processing In the dataset, features of an URL are tagged and coded as a set of binary attributes with each tallies to one of the likely value. When distributing a categorical value across dual binary attributes.

System Evaluation Different methods were employed for the performance evaluation including sensitivity, specificity and accuracy.

$$\text{Sensitivity} = \frac{\text{TP}}{\text{TP+FN}} \text{ X } 100\% \,, \quad (2)$$

$$Specitivity = \frac{TN}{FP+TN} \times 100\% \quad (3)$$

$$\text{Accuracy} = \frac{\text{TP+TN}}{\text{TP+FP+FN+TN}} \text{ X } 100\% \,, \quad (4)$$

Where TN (true negatives) is the number of correctly classified non- attacks; FP (false positives) is the number of falsely classified malicious; TP (true positives) is the number of successfully classified malicious and; FN (false negatives) is the number of non-correctly classified non-attacks.

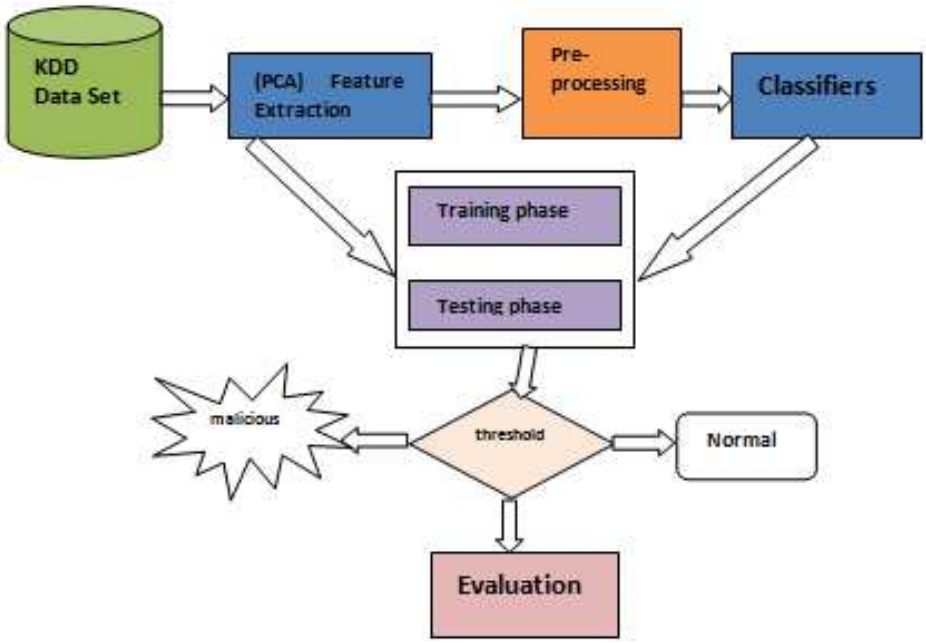

Figure 2: Work Flow of Multi-Classifier-Based IDS.

RESULT AND DISCUSSION

The system is a web based application, it classifies a URL as malicious or legitimate based on certain predefined features or covariates. Based on the predefined criteria, if anyone of the features is found in the URL, the system classifies the URL as malicious else it is classified as legitimate and the malicious and legitimate updated in the database. 1's and 0's are representations of results of each parameter from all the nine parameters that determined the legitimacy of the current URL. The table in appendix A shows the outputs of individual classifiers and the ensemble. The three supervised learning algorithms employed are LR, SVM and CPNN are tested against 700 URLs individually and ensemble. Then their results are analyzed using performance evaluation metrics.

The outputs of the experimentation showed that sensitivity produced by LR, SVM and CPNN are 65, 72.5 and 78% respectively. The results of specificity of LR, SVM and CPNN are 72.0, 79.5 and 83.4% respectively while the results of accuracy produced by LR, SVM and CPNN are 75.8, 88.3 and 90.5% respectively. However, the results produced by ensemble of the three algorithms are 86.4, 89.7 and 93.8% for sensitivity, specificity and accuracy respectively.

CONCLUSIONS

The main contribution of this work is to experiment an ensemble cyber-attack detection system by using supervised machine learning techniques namely Logistic Regression, Support Vector Machine and Counter Propagation Neural Network in order to better identify anomalies and to reduce false positive rate in network attacks. The data set features were reduced using PCA and finally classified by the three ensemble learning algorithms, The outputs of the experiments are satisfactory with an average accuracy rate of 93.8%. The experimented system is useful in different areas with more flexibility and good attack taxonomy.

REFERENCES

1. *L. I. Smith. A tutorial on Principal Components Analysis, February 26, 2002.*
2. *M. Kaur, S. Vashisht, Kumar S. (2012). "Adaptive Algorithm for Cyber Crime Detection", International Journal of Computer Science and Information Technologies (IJCSIT), Vol. 3 (3), 4381 – 4384.*
3. *K. Scarfone, P. Mell (2007). Guide to Intrusion Detection and Prevention Systems (IDPS), Computer Security Division, Information Technology Laboratory, National Institute Of Standards and Technology, Gaithersburg, Special Publication 800-94.*
4. *D. Halder, Jaishankar, K "Cyber crime and the Victimization of Women: Laws, Rights, and Regulations" Hershey, PA, USA: IGI Global. ISBN 978-1-60960-830-9*
5. *V. Kandpal and R. K. Singh, (2013)"Latest Face of Cybercrime and Its Prevention in India", International Journal of Basic and Applied Sciences, Vol. 2, pp. 150- 156.*
6. *E. Kirda, & Kruegel, C. (2005). Protecting users against phishing attacks with AntiPhish. 29th Annual International Computer Software and Applications Conference (COMPSAC'05) (pp. 1-8). Edinburgh, UK:IEEE.*
7. *J. Z. Kolter, & Maloof, A. M. (2006). Learning to detect and classify malicious executables in the wild. Journal of Machine Learning Research, 7, 2721-2744.*
8. *A. Alnajim, & Munro, M. (2009). An Anti-Phishing Approach that Uses Training Intervention for Phishing Websites Detection. 2009 Sixth International Conference on Information Technology: New Generations. Las Vegas, NV, USA.*
9. *Y. Joshi, Saklikar, S., Das, D., & Saha, S. (2008). PhishGuard: A browser plug-in for protection from phishing. 2008 2nd International Conference on Internet Multimedia Services Architecture and Applications. Bangalore, India: IEEE.*
10. *J. Ma, Saul, L. K., Savage, S & Voelker, G. M "Beyond blacklists: learning to detect malicious web sites from suspicious URLs," in Proceedings of the 15th ACM SIGKDD international conference on Knowledge discovery and data mining. ACM, 2009, pp. 1245–1254.*
11. *J. Ma, Saul, L., Savage, S., & Voelker, G. (2011). Learning to Detect Malicious URLs. ACM Transactions on Intelligent Systems and Technology, Vol. 2, No. 3, Article 30, Publication date: April 2011., 1-24.*
12. *L. S. Wijesinghe, L. De Silva, G. Abhayaratne, P. Krithika, S. Priyashan, D. Dhammearatchi* (2016). Combating Cyber Crime Using Artificial Agent Systems, International Journal of Scientific and Research Publications, Volume 6, Issue 4.*
13. *M. Kaur, Sheveta Vashisht, Kumar Saurabh ().Adaptive Algorithm for Cyber Crime*
14. *Detection, (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3 (3), 2012, 4381 – 4384.*
15. *S. Jyothsna, Mohan1, Nilina T. Prospects of Artificial Intelligence in Tackling Cyber Crimes, International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064*

16. *Akbar S.*, Srinivasa T. and Hussain M. (2016). A Hybrid Scheme based on Big Data Analytics using Intrusion Detection System. Indian Journal of Science and Technology, Vol 9(33).*
17. *S. Jon (2003). A Tutorial on Principal Component Analysis Derivation, Discussion and Singular Value Decomposition | jonshlens@ucsd.edu 25 March 2003.*
18. *S. Sperande (2018). Understanding logistic regression analysis |Request PDF. Available from: https://www.researchgate.net/publication/260810482Understanding_ logistic_ regression_analysis*
19. *Computer Hacking Forensic Investigator Investigating Network Intrusions and Cybercrime ((CHFIINIC)): EC-Council | Press, 2010 EC-Council, Vol 4, ISBN-13: 978-1-4354-8352-1. USA.*