

Network Traffic Analysis for Enhanced Protection in Critical Information Infrastructure

Ibitoye Akinfolo Akinrinnola, Aremu Idris Abiodun, Odesanya Oluwafunsho Idowu

Computer Science Department, School of Technology, Lagos State Polytechnic, Ikorodu Lagos, Nigeria

Email address:

aremu.i@mylaspotech.edu.ng (A. I. Abiodun), mideeanddee@hotmail.com (I. A. Akinrinnola)

To cite this article:

Ibitoye Akinfolo Akinrinnola, Aremu Idris Abiodun, Odesanya Oluwafunsho Idowu. Network Traffic Analysis for Enhanced Protection in Critical Information Infrastructure. *Mathematics and Computer Science*. Vol. 6, No. 5, 2021, pp. 71-76. doi: 10.11648/j.mcs.20210605.11

Received: April 25, 2021; **Accepted:** July 23, 2021; **Published:** October 28, 2021

Abstract: Owing to the surfacing of new technologies which can abet easier and faster processing of data, there has been a increasing need for most organization to develop an online system. Most of these systems are developed using php programming language. This paper shows that most of these web-based systems are vulnerable to different types of attacks resulting from the disregard to security appraise during the development of the system. Security of information asset which are painstaking to any organization is one of the most important tasks which need to be safeguard regularly. Critical information infrastructure protection (CIIP) had become a lingering area of interest in the modern days of information dissemination, from the inauguration of internet to the modern elevated-profile dispersed denial-of-service assail against critical systems. Critical systems rely deeply on information communication; the interruptions of the information communication can obstruct the operation of critical systems. The western nations have advanced CIIP elucidation in place, but these elucidations are not always suitable for growing countries, where exceptional contest and necessities have to be addressed. Meanwhile, the western worlds are familiarizes with unmatched improvement of their information infrastructures. However, the lack of national CIIP efforts creates a situation for developing nations to become launch pads for cyber-attacks. In this paper, I have proposed a Network Traffic Analyzer that will analyze source codes of web based critical infrastructures and detect vulnerability in the codes for better security from attacks.

Keywords: Critical Information Infrastructure Protection, Information Security, Vulnerabilities, Network Analyzer

1. Introduction

Dependability and smooth operation of system control are highly depend on the spectrum of inter-reliant of national and international software based dominant in solving national security [1, 2]. The present society involved the best suite to manage the information infrastructure in any organization for safety of attacks or treat from third party.

Critical information infrastructure (CII) supports countless underpinnings of the critical infrastructure (CI), when some of the emerging technologies were embraced and implemented, connection to other infrastructures / organizations became easier and made them interconnected and co-dependent [3]. Information systems does not only exposed to failures or malicious attack, they're also likely to attractive targets for malicious attacks [4-6]. The CI conveys a spread of services to individuals, and society as a whole, depending on the extent of the information dissemination in

the organisation. Any damage to or interruption of the CI causes ripples across the technical and therefore the societal systems – a principle that has held true within the past and even more. Attacking infrastructure, therefore, encompasses a ‘force multiplier’ effect, allowing even a comparatively small attack to realize a far greater impact. For this reason, CI structures and networks have historically proven to be appealing targets for a full array of actors (OCIPEP, 2003). Driven by a growing concern for the potential vulnerability of networked societies along with an increasing number of disruptions within the cyber-domain, many countries have taken steps to raised understand the vulnerabilities of and threats to their information infrastructure, and have proposed measures for the protection of those assets Critical Infrastructure Protection (CIP)/Critical Information Infrastructure Protection (CIIP)). Critical infrastructures (CI) are at center of any advanced civilized country [7, 8].

These organizations comprise: insurance sectors, financial

infrastructure (e.g. aircraft, railways, and mass transit), public services (e.g., emergency services, enforcement, and fire services), energy, and health care. Critical Information Infrastructure Protection (CIIP) could be a convoluted but focal topic for any nations. Nations at large critically depend upon Critical Infrastructure (CI) services like energy supply, telecommunications, financial systems, the middle, and governmental services [9, 10].

Critical Infrastructures (CI): can be referred to as those substructures/organizations that are vital for the upkeep of relevant functions such as economy, security, medical and general care of the members of a society, and thus the interruption or destruction of which will have a serious consequences on such society”.

A network traffic analyzer is sometimes a combination of related hardware and or software (computer program), or at other times an unconnected hardware component, which an organization can install on either a computer or network to increase their defense or protection against malicious activity or hackers. It is sometimes referred to as protocol analyzer or packet analyzer.

Network analyzers can be an alternative firewall, or anti-malware tracking programs. It also can act as an intrusion detection device.

Network analysis is the technique involved in getting network traffic and scrutinizing it thoroughly to find out the kind of activities that is going on a particular network [11, 12]. The network analyzer translates the data packets of known rules and presents the deciphered network traffic in a format that is understandable.

A sniffer could also be a program that monitors data traveling over a network. Unauthorized sniffers are dangerous to network security because they're difficult to detect and should be inserted almost anywhere, which makes them a favorite weapon of hackers.

Traditional network analyzers were mainly highly expensive devoted hardware systems which are highly complicated in usage [13]. But at present, emergence of newer technology has given room for network analyzers which are just software. This makes it easier and cheaper for professionals who may require it to effectively detect faults in a network. It also brings the potential of network analysis.

2. Literature Review

Malware Detection and Framework Analysis for Windows based API was design by [14], the work "Windows API based ", came up with a proposal for malware detection method that is based on mining applicable Application Programming Interface (API) calls from sub classes of malware. In their work, the related APIs were extracted from each defined malware group and additionally distinguished using DCFS Document Class-wise Frequency feature Selection criteria to categorize the executable as hateful or gentle. They concentrated on the Windows API calls, therefore it will be limited to the detection of Windows PE malware.

A highly automated Web based applications methods for protecting against SQL injection which has abstract and applied benefits over most existing methodologies was proposed [15]. This was achieved by the use of auditing to analyze the communications to prevent malicious access and on the other hand Signature based method is used to decrease the time taken to detect attacks. Besides, observed evaluation is completed on wide range of web applications & WASP (wireless application service provider) which automates the task very easily.

Phishing attacks and their mode of operations was also design by [16]. They claimed this kind of attacks has been on the increase lately and is affecting both industry and individuals. Phishing has impacts such as reduced confidence on the internet, financial loss, and difficulties in investigation of fraud related incidents in the banking industries. Their paper deliberates the efficiency of several anti-Phishing tools against phishing attack. Their study further shows that these tools are good in cases where the threats are known beforehand. Their methodology was named "Anti-Phishing design using mutual authentication”.

Analyses of some very undesirable opinions, created in the past few years, about Critical Information Infrastructure Protection (CIIP) and Cyber Security in Africa continent [17]. The work approached the expressed undesirable views that Africa can become the vehicle or podium from where cyber-attacks could be thrown towards the rest of the world. The paper reviewed the motives for such adverse views and then proposes some steps which Africa needs to take in other to fight such impressions and to protect it against cyber-attacks. Most of their proposals are based on sensitizing the end users and giving safety procedures on measures organizations needs to follow in the development of their platforms.

This paper intends to shift attention on the incident response stage, preparing first the rules, regulations, techniques, procedures, skills and tools to avoid having to approach the issue only after an incident. It is intended to attempt defense of cybercrime even from the attempt stage as damages may be too grave once an attack is successful.

It will basically test the source code itself for vulnerability and in turn help the developer of the web-based application to take corrective actions on areas where vulnerabilities are detected.

3. Methodology

Figure 1 shows the general network analyzer of the proposed system. The application comprises of both the client Front end and the server. In other for the client to perform any of the functions defined, the client must first connect to the server using the local host.

The web application will be deployed on a web server and accessible through a web-based user interface by the client. The HTTP server (e.g. Apache or Microsoft IIS) accepts HTTP requests send by the client (normally by a web browser such as Mozilla Firefox or Microsoft Internet Explorer) and hands back a HTTP response with the result of the request.

When a HTTP request is sent by the client it is parsed by the HTTP server (step 1 in figure 1).

The HTTP server extracts the file name that is being requested and the parameters send (for example GET or POST parameters). When it detects a request for a dynamic file (in example a PHP script) it fetches the source code from the file system (step 2 in figure 1) and passes it along with the parameters to the scripting language interpreter (step 3 in figure 1). The interpreter executes the source code and

handles external resources like databases (step 4 and 5 in figure 1) or files. It then creates the result (normally a HTML file) and sends it back to the Network analyzer which does all the analysis and sends it to the client where the result is displayed in the web browser.

The analyzer: The analyzer itself scans through an entire web application and breaks each part into tokens that can be processed as units.

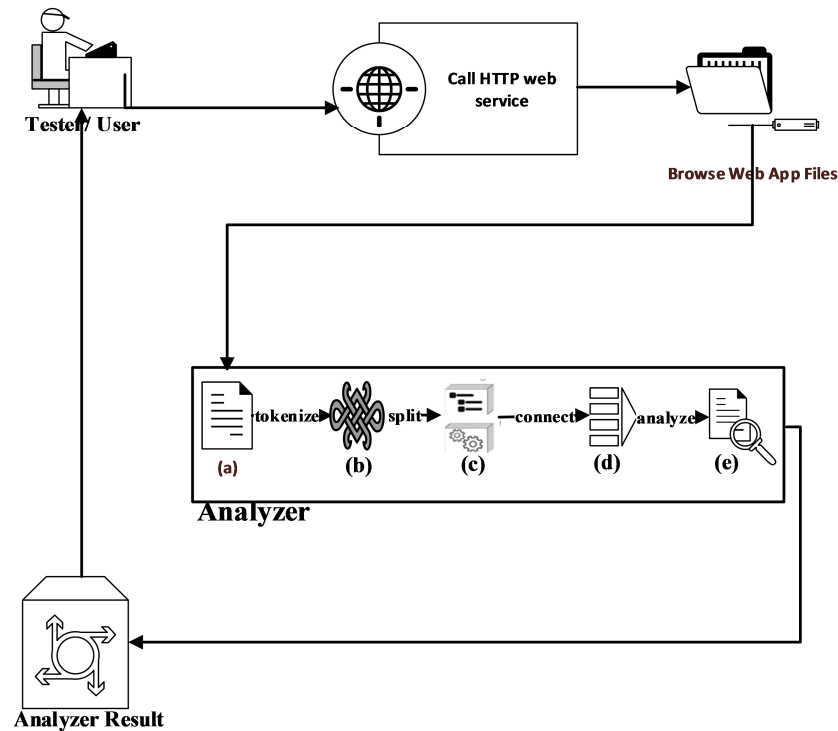


Figure 1. Architecture of the Network Analyzer.

4. Results

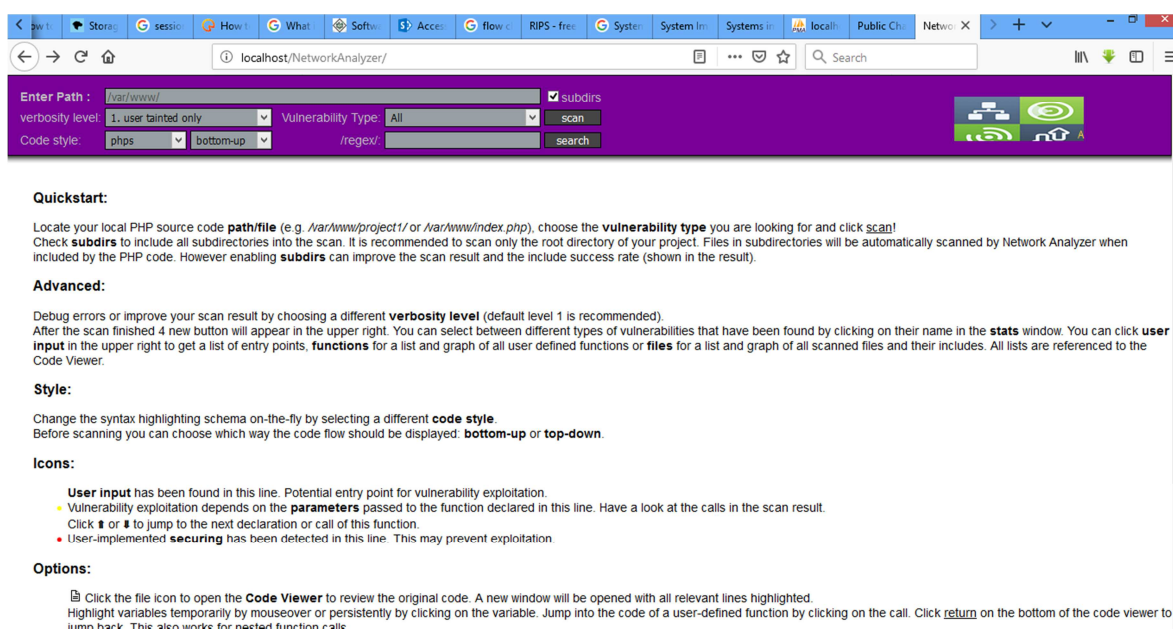


Figure 2. Shows the home page of the analyzer which contains a detailed guide on the usage of the analyzer for users intending to use the application.

It also contains fields where the user can specify the path of the source code to analyze on the local host, the extent of analysis required, type of vulnerability to search for, an option to analyze sub directories and a button (Scan) to perform analysis once criteria are all set.

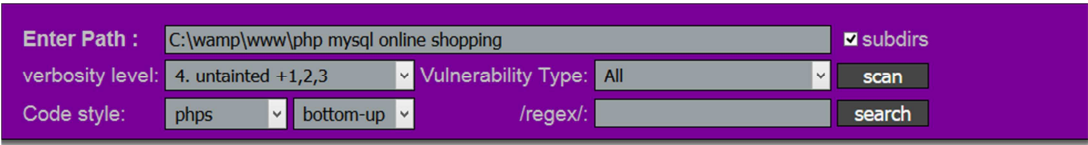


Figure 3. Select Path and criteria to analyze.

Figure 3 above further explains the path of the application, the verbosity level, the kind of vulnerable detected that may prone to attacks upper, Figure 4 explained earlier where all criteria for the analysis are set. This will determine the kind of result that will be displayed by the application after input has been processed.

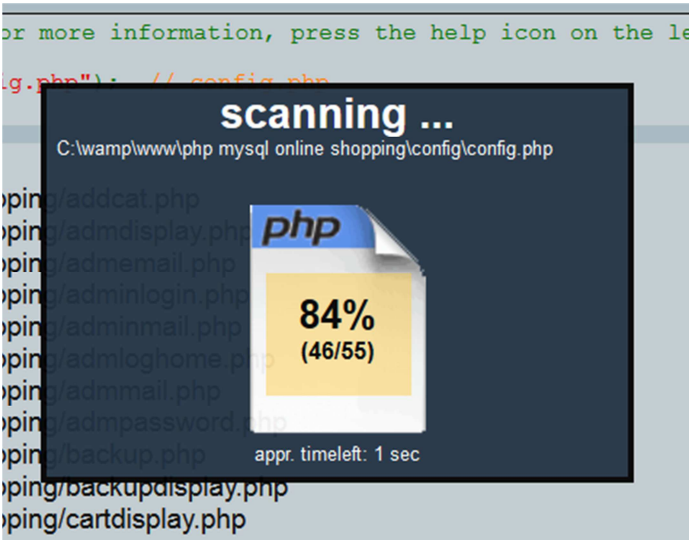


Figure 4. Analyzer in progress.

Figure 4 above shows the output of application during the process of analyzing the source code which has been inputted into the system.

Figure 5 above is the result of the analysis itself at a glance. This is generated by the system after it has successfully completed the analysis on the input in Figure 4. The result contains the different types of vulnerabilities detected, the sum of the vulnerabilities in total, total number of files analyzed, the amount of time it took to analyze the input, etc.

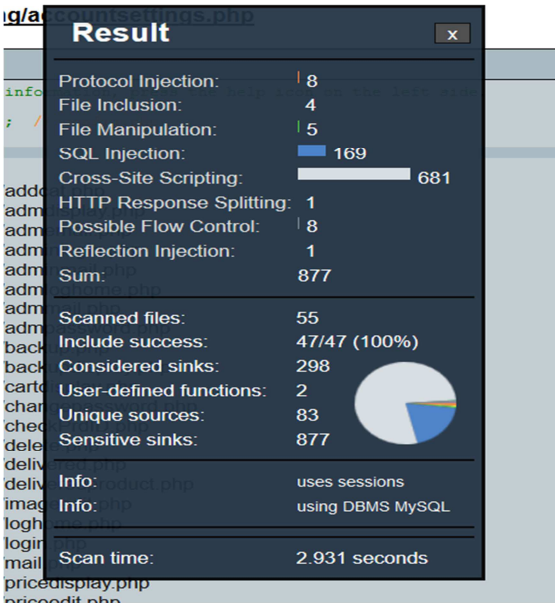


Figure 5. Analyzer Result.

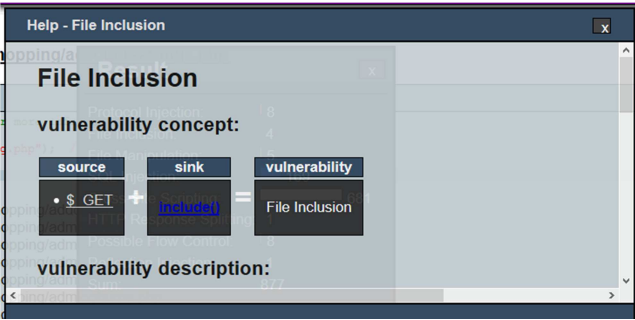


Figure 6. Sample Vulnerability Concept.

Figure 6 above shows one of the types of the result by clicking on one of the vulnerability type detected in Figure 4 earlier and explains the concept of formation for the vulnerability type.

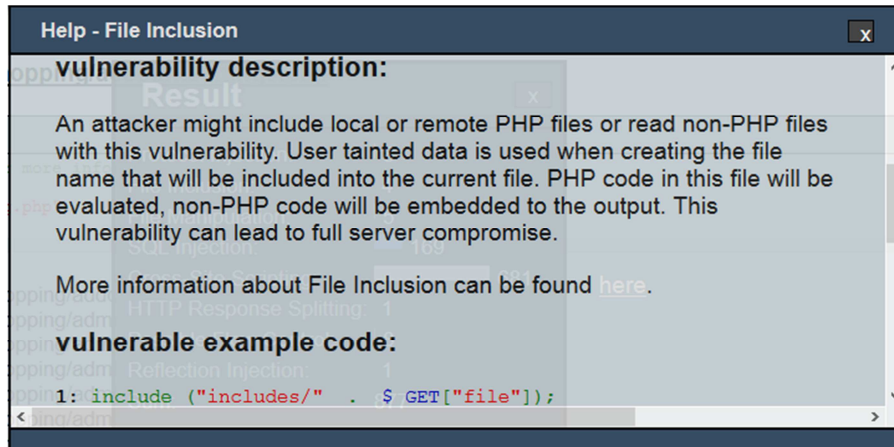


Figure 7. Sample Vulnerability description.

Figure 7 above shows a scenario where a user is coming across a vulnerability type for the first time or does have much information about it. By clicking on Help the user is presented with a short description (explanation) of the vulnerability and an example code as shown above.

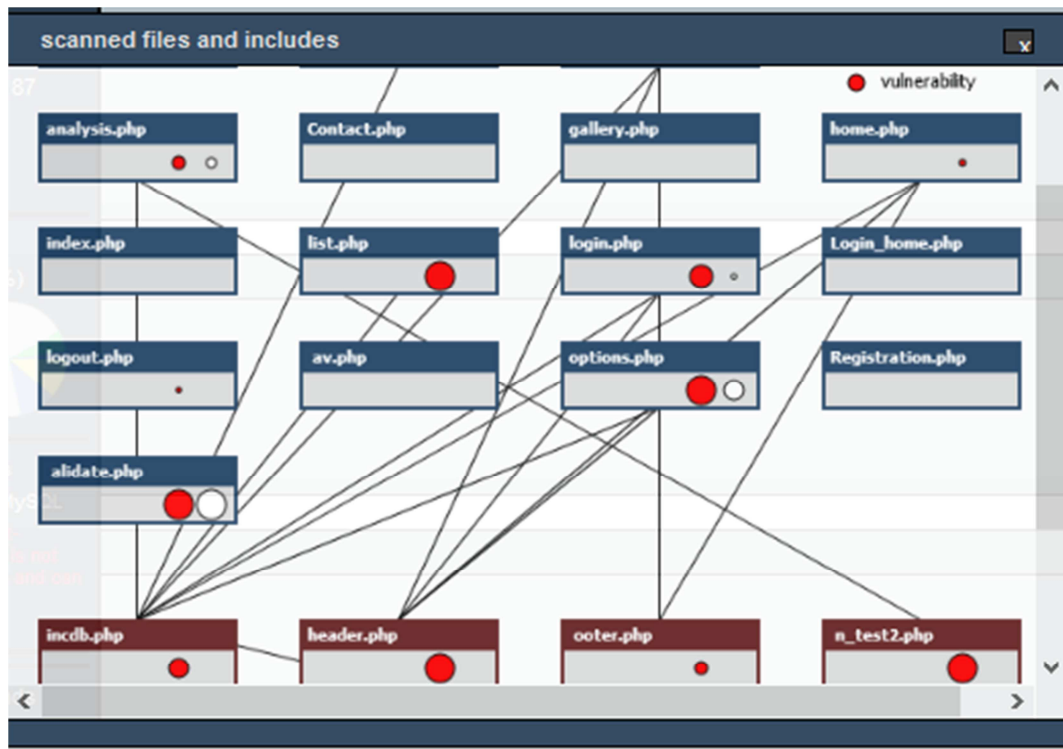


Figure 8. Sample Vulnerability Mapping.

Figure 8 above shows the mapping of files/modules analyzed in the source code and shows how they are interconnected to one another including which of those unit of codes has vulnerabilities and how it can in turn affect the entire software.

5. Conclusion

This paper has enhanced Critical Information Infrastructure Protection using the concept of Network analysis to implement an intelligent system which automate

vulnerabilities detection in web based applications which are specifically designed for vital societal functions (Such as health, security and education etc) and in turn prevents the system or its information from being accessed by unauthorized users.

References

- [1] Chala, D. G. (2019). *College of Social Sciences* (Doctoral dissertation, Addis Ababa University).

- [2] Dyer, S. K. (2020). *Human error and interactions with technology in safety-critical workplaces: Learning from the aviation industry* (Doctoral dissertation, University of Illinois at Urbana-Champaign).
- [3] Rogan, K. (2019). *Anti-Intelligence: A Marxist Critique of the Smart City* (Doctoral dissertation, MA Thesis in the Program of Theories of Urban Practice, Parsons School of Design, The New School, 2019: https://www.academia.edu/39125907/Antiintelligence_A_Marxist_critique_of_the_smart_city).
- [4] Turner, H., White, J., Camelio, J. A., Williams, C., Amos, B., & Parker, R. (2015). Bad parts: Are our manufacturing systems at risk of silent cyber attacks? *IEEE Security & Privacy*, 13 (3), 40-47.
- [5] Kimani, K., Oduol, V., & Langat, K. (2019). Cyber security challenges for IoT-based smart grid networks. *International Journal of Critical Infrastructure Protection*, 25, 36-49.
- [6] Murugesan, S. (2019). The cybersecurity renaissance: security threats, risks, and safeguards. *IEEE ICNL*, 14 (1), 33-40.
- [7] Lewis, T. G. (2019). *Critical infrastructure protection in homeland security: defending a networked nation*. John Wiley & Sons.
- [8] Arnold, N. R., Mahoney, W. R., Derrick, D. C., Ligon, G. S., & Harms, M. M. (2015). Feasibility of a Cyber Attack on National Critical Infrastructure by a Non-State Violent Extremist Organization. *Journal of Information Warfare*, 14 (1), 84-100.
- [9] Steele, W., Hussey, K., & Dovers, S. (2017). What's critical about critical infrastructure?. *Urban Policy and Research*, 35 (1), 74-86.
- [10] Garschagen, M., & Sandholz, S. (2018). The role of minimum supply and social vulnerability assessment for governing critical infrastructure failure: current gaps and future agenda. *Natural Hazards and Earth System Sciences*, 18 (4), 1233-1246.
- [11] Marchetti, M., Pierazzi, F., Colajanni, M., & Guido, A. (2016). Analysis of high volumes of network traffic for advanced persistent threat detection. *Computer Networks*, 109, 127-141.
- [12] Zhang, C., Patras, P., & Haddadi, H. (2019). Deep learning in mobile and wireless networking: A survey. *IEEE Communications surveys & tutorials*, 21 (3), 2224-2287.
- [13] Casilari-Perez, E., & Garcia-Lagos, F. (2019). A comprehensive study on the use of artificial neural networks in wearable fall detection systems. *Expert Systems with Applications*, 138, 112811.
- [14] Veeramani, R., & Rai, N. (2012, January). Windows api based malware detection and framework analysis. In *International conference on networks and cyber security* (Vol. 25).
- [15] Uwagbole, S. O., Buchanan, W. J., & Fan, L. (2017, May). Applied machine learning predictive analytics to SQL injection attack detection and prevention. In *2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)* (pp. 1087-1090). IEEE.
- [16] Avireddy, S., Perumal, V., Gowraj, N., Kannan, R. S., Thinakaran, P., Ganapathi, S.,... & Prabhu, S. (2012, June). Random: An application specific randomized encryption algorithm to prevent SQL injection. In *2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications* (pp. 1327-1333). IEEE.
- [17] Kritzing, E., Look, M., & Mwim, E. N. (2018, October). Cyber Safety Awareness and Culture Planning in South Africa. In *International Symposium on Cyberspace Safety and Security* (pp. 317-326). Springer, Cham.