Communications on Applied Electronics (CAE) – ISSN : 2394-4714
Foundation of Computer Science FCS, New York, USA
Volume 7– No. 35, April 2021 – www.caeaccess.org

A Fog-based Cyber Security Risk Management System using Bayesian Games

Akinwunmi D.A.
ICT Application Center,
Adekunle Ajasin University,
Akungba-Akoko, Nigeria

Gabriel A.J.
Dept. of Cyber Security
Federal University of Technology,
Akure, Nigeria

Oluwadare S.A.
Dept. Computer Science
Federal University of Tech. Akure,
Nigeria

Akinyede R.O.
Dept. of Information Systems Federal University of Technology,
Akure, Nigeria

Alese B.K.
Dept. of Cyber Security, Federal University of Technology,
Akure, Nigeria

ABSTRACT

Cyber security is among the most complex and rapidly evolving issues in the society today and has been the focus of most present day organizations. Cyber security risk management is the process of reducing potentially harmful and uncertain events that poses as threat to cyber security. One of the prominent cyber security risk management techniques is the Game Theoretic Approach (GTA). The objective of this research is to develop a cyber-security risk management system using a game theoretic approach in the concept of Fog computing which will encourage proactive management of cyber risks and enhances cyber operational effectiveness and efficiency. In this research, a Cyber Security Risk Management System was developed using Bayesian Game. The algorithm was formulated such that PyQt4 framework serves as a shield to the Fog server. The algorithm checks the server's CPU utilization, memory utilization, running threads and all logs to the console. The algorithm with the help of Snort performs inline packet inspection and logs any malicious packet to the console and also to a database on the server. The algorithm regularly checks the cached content on the server, reports the size at every point in time and also monitor-connected clients. The algorithm was implemented in Linux Ubuntu Desktop 14 environment using Python programming language. Nmap was used to probe a remote node for its vulnerabilities and Snort was used as a Network-Based Intrusion Detection System (NIDS). Experimental results on Adekunle Ajasin University's network demonstrate the ability of the system to manage cyber risks in the network. Obtained data on the proposed Cyber Security Risk Management System, formed the basis for the evaluation. The model developed will be useful for managing security risks in a computer network environment.

General Terms

Cloud Computing, Security, Computer Network, Communications

Keywords

Fog Computing, Cyber Security, Fog Computing, Game Theory, Risk Management

1. INTRODUCTION

Human beings have grown to depend on the Internet on a continual basis and have incorporated it into their lives. As a result of this dependence upon the Internet, hackers have also made the Internet a potential attack platform [1]. In recent times cyber-attacks have become more frequent and complex, while attackers also have become more professional. Attackers have taken the advantage of the openness and extent of cyberspace to launch attacks and misuse vulnerable systems as tools for an attack. A big challenge is that the dynamic nature of the Internet offer benefits to both an attacker and a defender making many cyber-battles to be won by the party that uses cutting-edge technologies to greater advantage [2-3].

Cyber risk is risk associated with cyber activities. Cyber security is the preservation of confidentiality, integrity and availability of information in the cyberspace. A cyber-attack is an attack in cyberspace directed against one or more systems with the aim of damaging the security of the system thereby compromising the confidentiality, integrity and availability of the system. Risk management is the process of identifying risks, assessing risks, and taking steps to reduce risks to an acceptable level [4-6]. Game theory is the methodology of using mathematical tools to model and analyze situations of interactive decision- making. Cyber security when viewed from game theoretic approach attempts to design a defence against a sophisticated attacker who plans in anticipation of a complex defence [7]. Game theoretic approaches have been introduced as a useful tool to handle tricky network and cyber-attacks [8]. However, game theory has not been fully applied in a Fog-based environment.

The need for a system that is able to manage cyber-security risks efficiently and adequately address the short falls of traditional methods gave birth to the development of the proposed Game Theoretic model for Cyber-Security Risk Management in the concept of Fog computing. This research paper laid emphasis on Bayesian game approach because games are useful in understanding risks posed by an intelligent attacker trying to attack a system.

The remainder of this paper is organized in a way that, section 2 contains review of related existing research works. The design of the new system is reported in section 3, while section 4 contains a vivid description of the experiment's set up. Then section 5 presents results and findings of the experiment conducted. Section 6 presents performance evaluation of the system. Section 7 contains the conclusion.

2. RELATED WORKS

Several related research works have been carried out in the research community, some of them are highlighted in this section.

The authors in [9], proposed a Deterministic Stochastic Game-theoretic Modelling (DSGM) method for analyzing the security of computer network as a non-zero sum stochastic game. The research was motivated by the existing techniques lack of capability to provide analytical tool and algorithm whose solutions can serve as basis for decision making as well as to predict attackers' behavior. The objective of the research is to propose a deterministic stochastic game modelling strategies for both attacker and defender in a network environment. The interaction between an attacker and a defender is presented as two-player non-zero deterministic game whose model is constructed using a saddle point solution (non-linear program) to compute the value of the game. The probability of possible attack on a network given available attacker strategy or best-response strategies for the attacker and the defender was demonstrated. The contribution of their research lies in the fact that the authors presented a non-zero, Deterministic Stochastic Game-theoretic Modeling (DSGM) method for analyzing the security of computer networks. Moreover, through the security game, the defender can gain a deeper understanding of the attacker's strategies and potentials but could not predict how attackers exploit vulnerabilities nor analyze attacker's behavior.

The authors in [10], proposed a system for modeling attacker-defender interaction as a zero-sum stochastic game. The research was motivated by the existing techniques lack of capability to predict attackers set of moves and possible counter-measures. The objective of the research was to propose a quantitative method for analyzing network security using stochastic game modeling technique. State games are encoded using a binary scheme in order to properly capture components of the underlying network environment. The model involves reducing each state game into a min and max linear programming problem for both the defender and attacker. Game costs, rewards and outcomes were modeled to closely match real world measurements. The use of a combination of the pivotal algorithm and a custom stochastic algorithm to compute the optimal (best-response) strategies for the players at each state was also proposed. A major contribution of the research is the development of a two-player zero-sum stochastic game model of the interaction between malicious users and network administrators, which introduces a hypothetical network of a typical scenario to show the applicability of the model within that scenario. However, the limitation of the work is that the model could not predict how attackers exploit vulnerabilities nor analyses attacker's behavior.

In [11], an Attack Tree Based Comprehensive Framework for the Risk and Security Assessment of VANET using the Concepts of Game Theory and Fuzzy Logic is presented. Vehicular Ad-hoc Network (VANET) faces a lot of research challenges in terms of security because the existing risk and security analysis approach of VANET fails to work well as it is purely based on the ideological beliefs and it does not reflect any realistic conditions. The research objective was to explore and discuss the usage of game theory and fuzzy logic in analysis of the attack and defense equilibrium. The authors used game theory and fuzzy logic in carrying out analysis of the attack and defense equilibrium. The limitation of their approach is that, it did not conduct the assessment of the assets so as to come up with a comparative analysis of the risk.

The paper in [12], presented a game theoretic framework for cyber-threats I formation sharing among different organizations, so as to maximize the discovery rate of vulnerabilities, at a minimum cost. Despite its advantages, there are costs and risks associated with cyber threats information sharing. When a firm shares its vulnerabilities with others there is a risk that these vulnerabilities are leaked to the public or to attackers resulting in loss of reputation, market share and revenue. The authors used game theory to investigate when multiple self-interested firms can invest in vulnerability discovery and share their cyber-threat information, especially in a public cloud domain. However, the work is limited to two users only and there is no consideration of heterogeneous vulnerabilities, heterogeneous players and incomplete information. Furthermore, the theoretical predictions of the game model were not compared with real data on cyber-threat information sharing.

The ArtivleArticle [13], presented a game theoretic and trust model to moving assets in the cloud based. This is important especially as there is increase in organizations' and individuals' reliance on external parties to store, maintain and protect their critical assets. The use of public clouds offers advantage in terms of flexibility, scalability and cost effectiveness. However, the security challenges remain unresolved since a malicious cloud provider can carry out internal attacks. The authors used game theory to assess the risk involved in moving critical assets of an IT system to a public cloud adopting a user perspective to model costs and benefits functions of the user and attacker. However, their work only covered few assets, the model could be extended to cover more assets, more actions and even more players. This will allow for a more comprehensive picture of the overall risks so as to make the model more realistic.

The research work in [14], proposed a game theoretic attack defense tree model using Vehicular Ad-hoc Networks (VANETs) for accessing risk priority of SSL SYN attacks. VANETs are prone to several types of attacks due to their decentralized nature and mobility. Most importantly, the involvement of traffic and human beings makes the security of VANETs highly imperative. Their research was motivated by the need to have a mechanism that can access and analyse the risk priority of an attacker's way of attacking and defender's way of defending. The authors designed a risk priority assessment model of SSL SYN attack using attack- defense tree model in VANETs and used the Attack-defense tree model to analyze the approaches used by attackers to achieve SSL SYN attack. The limitation of the research work is that, only SSL SYN attack is considered in the attack-defense tree model. Other types of attacks in VANETs were not considered, thus, the neglects of other areas where security is a concern.

The authors in [15], presented a novel approach for the risk assessment of coordinated cyber-physical attacks against power grids and considered the finite budget owned by the attacker and defender, which will have vital influence on the risk assessment. The authors formulated a two-player zero-sum stochastic game between the attacker and defender in which each player seeks to maximize its respective minimum rewards under the opponent's optimal strategy. In order to quantify their rewards, the optimal load shedding technology is introduced to determine the minimum cost of shed load. Using these quantified rewards as input, the attacker and defender's Nash equilibrium strategies about its budget allocation are derived by solving the proposed stochastic game. At the Nash equilibrium of the game, the attack and defense strategies can be used to assess the risk for various states of the power grid, and the optimal defense budget allocation is formulated in terms of the corresponding risk. The game framework is tested on the IEEE 9-bus system as a proof of concept. Also, the risk sensitivity analysis to the attack/defense budget variation is presented. However, the work only considered coordinated cyber-physical attacks against power grids. In real life scenarios, unorganized attacks can result into great consequences.

The paper in [16], proposed a game theoretic approach to cyber security risk management. Information Technology (IT) systems are now ubiquitous in all aspects of the society. Armed with an ability to create IT incident effects via cyberspace, criminals can steal and extort money or information, terrorists can disrupt society or cause loss of life, and the effectiveness of a military can as well be degraded. The research is motivated by the need to minimize the system's cyber security risk. The research objective was to use game theory approach to model the attacker's response to any defensive measures, since for every action a defender makes to improve a system's security, a sophisticated attacker will make a corresponding adjustment to select the next most promising attack. The authors applied a software-based method called the Cyber Security Game (CSG) to identify and reduce a system's cyber risk as well as determine the most cost-effective defense methods to protect an ICT system The risk score is calculated by using a mission impact model to compute the consequences of cyber incidents and combining that with the likelihood that attacks will succeed. The likelihood of attacks succeeding is computed by applying a threat model to a system topology model and defender model. The research established how CSG can be used to prescriptively identify which defense methods is best used and where they should be used as well as determine whether the set of defense methods achieve that target. The performance of CSG, however, is only as good as the models it has to work with. If they are incorrect then its output will be incorrect.

In [17], the authors proposed middleware architecture to solve IoT issues, and discuss the generic concept of using fog computing along with cloud in order to achieve a higher security level because the existing traditional security approaches are not suitable to solve IoT challenges and require fundamental changes. The authors designed the security middleware to act as a smart gateway to pre-process data at the edge of the network. Depending on the received information, data might either be processed and stored locally on fog or sent to the cloud for further processing. In the model, IoT constrained devices communicate through the proposed middleware, which provide access to more computing power and enhanced capability to perform secure communications. The research established that the model is effective to handle some of the most relevant IoT security challenges. However, the model was neither implemented nor analyzed on actual test-beds and real world scenarios to test its feasibility, practicality and performance.

The work in [18], proposed a fog computing security mechanism based on human nervous system. When users in fog computing open their resources, their devices are easily intercepted and attacked because they are accessed through wireless network. The authors introduced credible third party to supervise the behavior of users and use evolutionary game theory to protect the security of user cooperation. MATLAB simulation was used to test the effect of the dynamics game evolution and parameters on the final stability state of the game were conducted. The MATLAB simulation results show that the proposed mechanism can reduce the number of attack behaviors effectively and increase the profits of users. However, the work did not develop a specific technological method to discover the malicious behavior of users based on the credible third party.

Our current paper was therefore towards addressing some of the challenges or limitations of existing related research works as highlighted. Our work also considered the implementation of the game theoretic approach to cyber security risk management framework..

3. THE PROPOSED FOG-BASED SYSTEM CYBERSECURITY RISK MANAGEMENT SYSTEM

The conceptual diagram of cyber-security risk management system is presented in Figure 1, which comprises of four phases. The first phase is the risk assessment, which comprises risk analysis and risk evaluation. Under the risk analysis we have two steps: the first step in cyber risk analysis is the identification of threats and the second step is identification of vulnerabilities. Studying the system or the infrastructure for weaknesses identifies these risks. Once the risk has been identified, Risk evaluation is to analyze and prioritize the risks. The prioritization of risks is according to the impact that a risky event would have on the system or infrastructure. The second phase is the risk reporting that gives a comprehensive report of all results obtained in the assessment sub-process. What follows after prioritizing the risks is the allocation of resources to mitigate the risk or the consequence of the risk, which is the third phase. If a risk falls below an acceptable threshold, the risk is left untreated and accepted as it is. Otherwise, risks that do not fall into the acceptable category can be controlled by introducing countermeasures to reduce the risks down to a tolerable level or reject the risks and use workarounds to avoid the identified problems. In addition, the risks could be transferred to other parties. After the mitigation of the risk, the fourth phase is to monitor the effectiveness of the protection measures used against the risk.

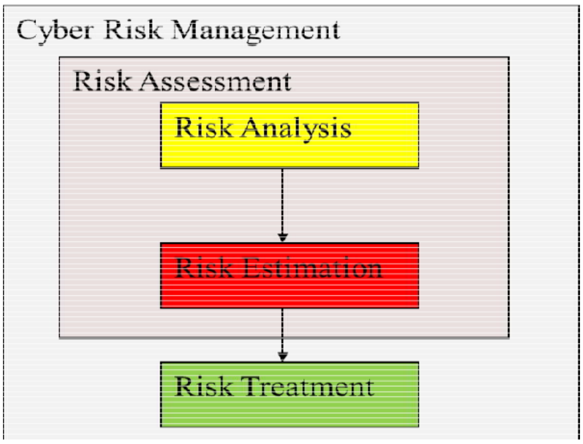


Figure 1: Architecture of a typical Cyber Security Risk Management System [19]

4. SETUP FOR THE EXPERIMENTS

The hardware components used in the development of the proposed system are: HP Speare laptop with Intel ch Laptop with Intel core i3 processor and 4 gigabytes of RAM. Other characteristics of the experiment environment includes, Linux Ubuntu Operating System running to represent the Fog server which handled the Snort in Network-Based Intrusion Detection System (NIDS) mode. Kali Linux 2016 was used the computer system designated as the attacking computer, kali was chosen for its attacking applications that are preinstalled in Kali OS. The development environment is further characterized by Python 2.7 programming language, with the following python libraries; System (sys), Process Utility (psutil), Matplotlib, OpenCVand PyQt4 (QtGui, QtCore, QtNetwork, QtSql) as the framework.

Third party softwares used in the experiments includes, “Squid3”, which designates the primary application. It is a caching application that intercepts Hyper Text Transfer Protocol (HTTP) request and sends the request on their behalf. It stores the return data in its cache in order to serve the subsequent request without going through the hops again to the Internet to get the requested information. The Squid application runs inside the Ubuntu machine. Similarly, “Snort”, an Intrusion Detection System (IDS), was tuned and used as the Network-Based IDS (NIDS). In the experiment, Snort runs as an NIDS that sniffs the entire network for any malicious traffic like “Ping Sweep”, or even “Port Scan”. Snort was deployed to run on the Ubuntu machine.

Network Mapper (Nmap), a vulnerability assessment application, was preinstalled in the Kali machine..

4.1 Test Bed Setup

The research was conducted using the campus network of Adekunle Ajasin University, Akungba-Akoko, Nigeria as the test bed. In the Experimental setup, three computers with the above hardware configuration were connected. The first computer runs the Server Application (defence) while the second computer runs the Client Application and the third computer is the Kali Linux OS. Two of the computers are connected together on a LAN while the third computer is connected to the Internet (Attacker). Figure 2 is the network topology used. The topology is a full mesh topology with three sections; the Campus Network, the Data Centre and the Demilitarized Zone (DMZ).

The Algorithm was implemented on Adekunle Ajasin University’s network for fast access to Data Centre (DC) data. The bandwidth of the University’s Internet connection is 40 megabytes per second (Mbps), speed test was performed before the Fog test, the speed test before the Fog test shows the time taken and also the hops taken to reach the server. Fog server was given a Domain Name System (DNS) record of aauafog.net.

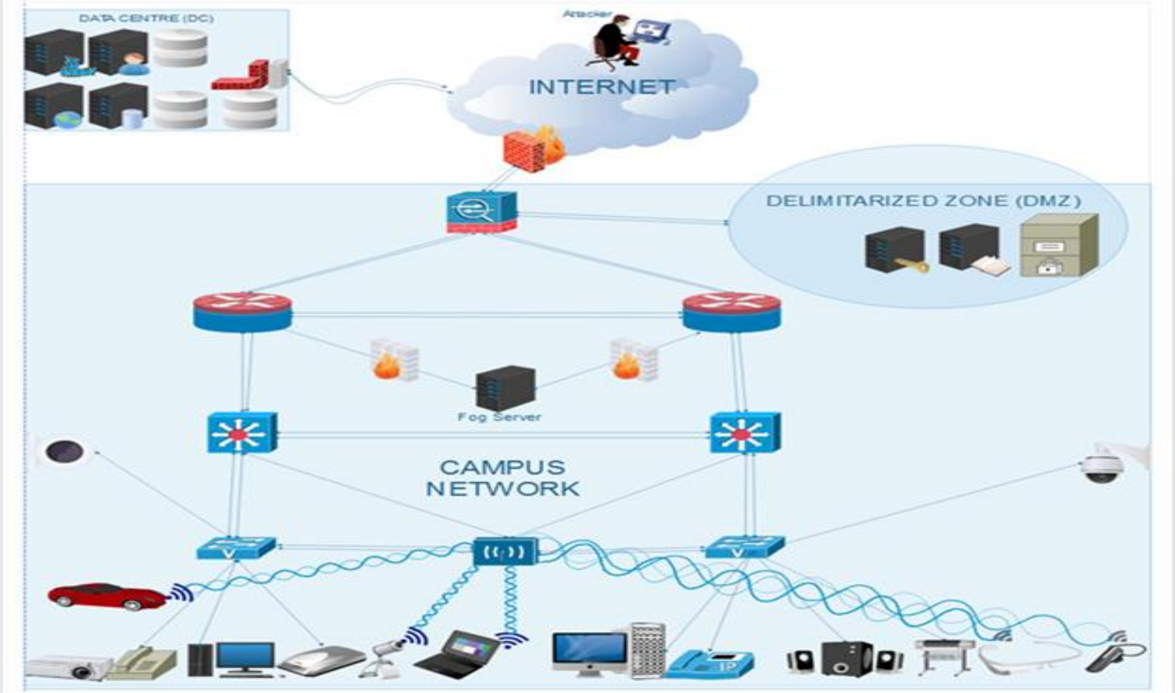


Figure 2: Network Topology used for the Experiment

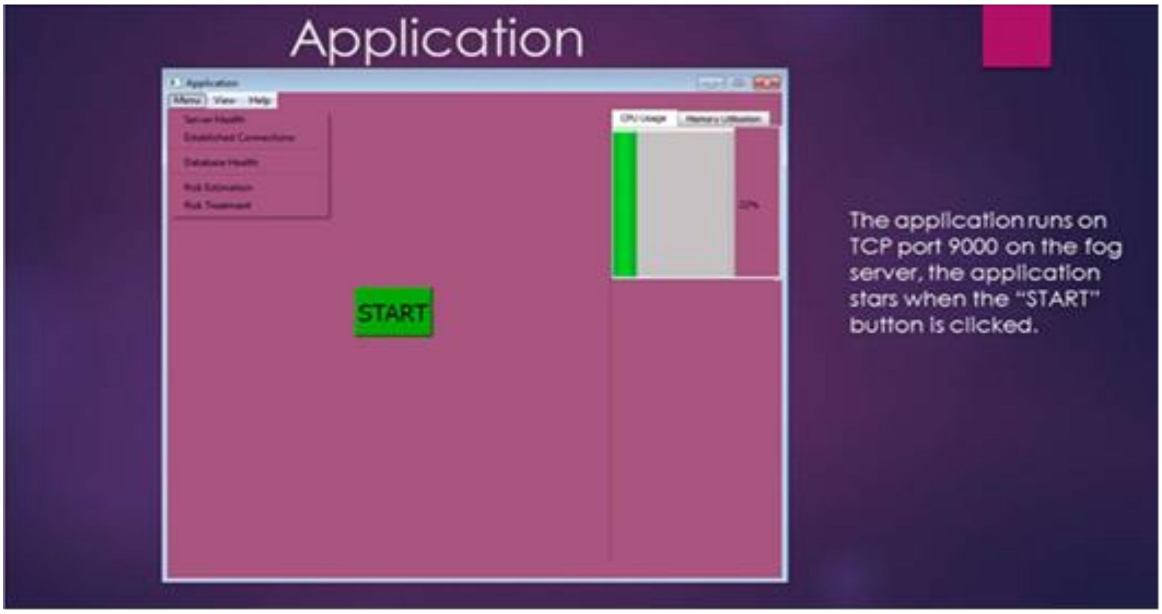
4.2 System Implementation, Results and Discussions

An application was developed to simulate our ideas. Once the application is launched, the user activates the system by first signing up. If the registration or sign up is is successful, the user is expected to login into the system. Login information (username and password) is authenticated and error returned if failed. If the login is successful, it takes the user to the main application for the game. This is captured in the diagram on figure 3.

The risk estimation module presented in Figure 4 computes the likelihood, impact and the associated risks. In figure 4, the likelihood was calculated by selecting a particular threat-source and applies appropriate defence strategies. The likelihood is described as High, Medium, and Low using scale, 0.70-1.00, 0.30-0.69, 0.00-0.29 respectively. The impact is measured by either loss or degradation of integrity, availability and confidentiality. Impact is estimated by computing the significance of integrity, availability and confidentiality and the resulting consequences for each of the security goals, determine the likelihood and the risk involved. This is presented in figure 4. In this figure46, it shows the likelihood estimations which consist of threat, defense strategy and the risk involved. In addition, the impact estimations consist of the confidentiality, integrity and the availability. These three factors determine the impact involved. For example, if the degree of confidentiality, integrity and availability are 4.0, 4.0 and 4.0 respectively, then the impact is 12.0, the likelihood is 0.0036 and the risk is 0.0432 as depicted in figure 4.

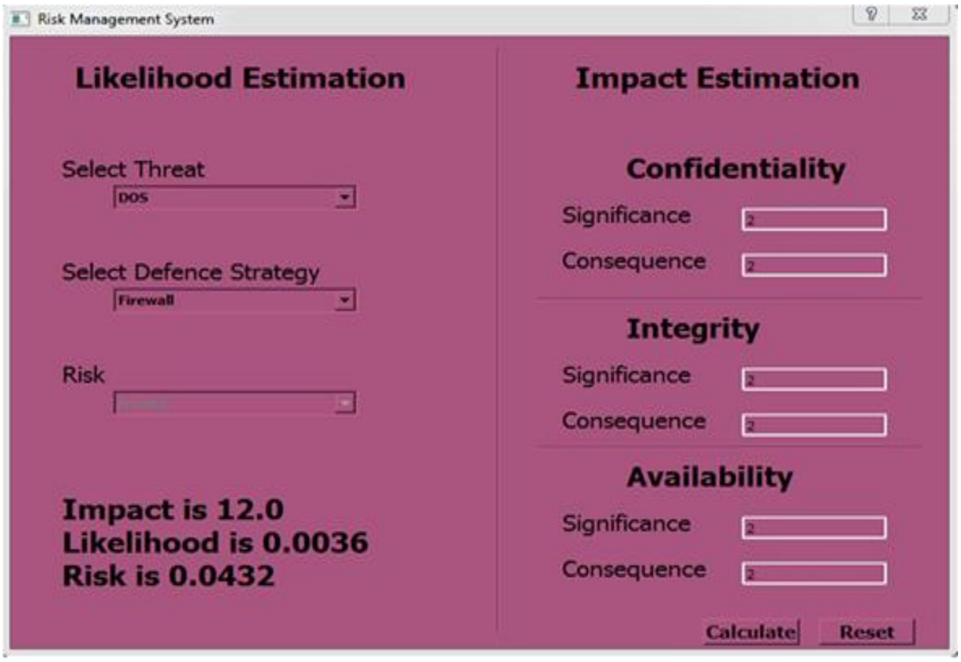
Figure 5 shows the results of the mechanism for the risk treatment. The mechanism for selection is based on High, Medium or Low. Risk that fall below the threshold is accepted. Otherwise, the risk is rejected, avoided or transferred to other parties. Figure 5, reveals the risk levels and the strategy proposed for each level. In this experiment, three strategies were used based on the level of risk involved. For example, between 0.0003 – 0.0005 can be handled by the administrator while that of 0.0006 and above are handled by the Snort application.

Risk estimation for a period of three (3) months was carried out. As shown in Figure 5, we observed that the number of risk handled by the administrator is almost linear between January and February. However, between mid- January and March the number of risk treated by the administrator is almost constant. On the risk treated by firewall, from our result, we observed that the number of risk treatment seems to be higher than that of the administrator. On the risk treatment by the Snort, between January 1 and January 9, nearly all the risks under this range were treated but from January 10 to March 19 most risk group under this level were not treated except in February 19 to February 27 and March 7


Application

The application runs on TCP port 9000 on the fog server, the application stars when the "START" button is clicked.

Figure 3: The Game-Theoretic Assessment Application's Interface



Risk Management System

Likelihood Estimation

Select Threat: DOS

Select Defence Strategy: Firewall

Risk

Impact is 12.0
Likelihood is 0.0036
Risk is 0.0432

Impact Estimation

Confidentiality
Significance: 2
Consequence: 2

Integrity
Significance: 2
Consequence: 2

Availability
Significance: 2
Consequence: 2

Figure 4: The Risk Estimation Module

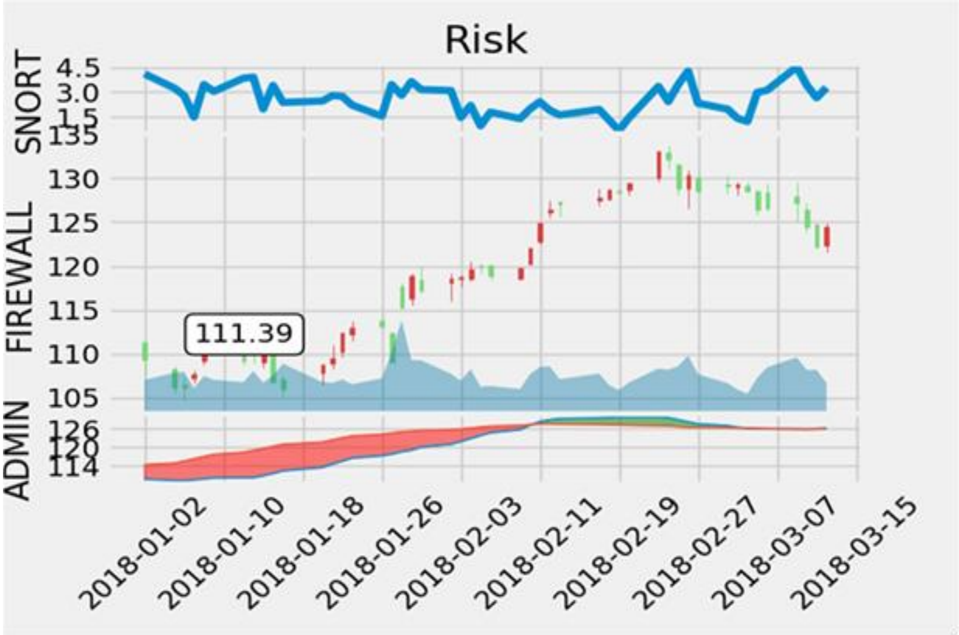


Figure 5: Mechanism for Risk Treatment Handling

5. PERFORMANCE EVALUATION OF THE PROPOSED SYSTEM

The performance of the proposed model was evaluated based on results obtained from case study of cyber-risk management in Adekunle Ajasin University Information and Communication Technology Application Centre’s network. Figure 6 shows the comparison of the average time taken for three (3) months from the University network to the host (HT) with our proposed cyber risk management system for cloud and also the Fog computing facilities.

Figure 7 shows the comparison of the average hop taken for three (3) months from the University network to the host (HT) with the proposed cyber risk management system for cloud and fog computing facilities.

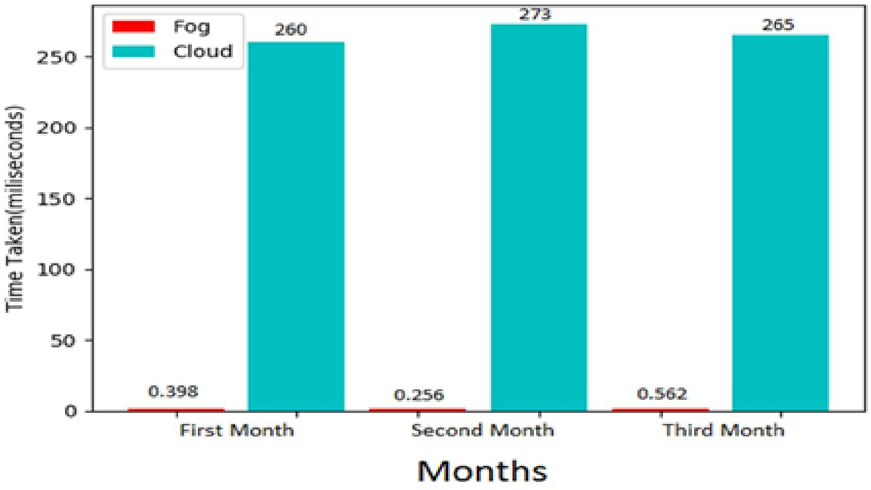


Figure 6: The Average Time taken for three (3) Months

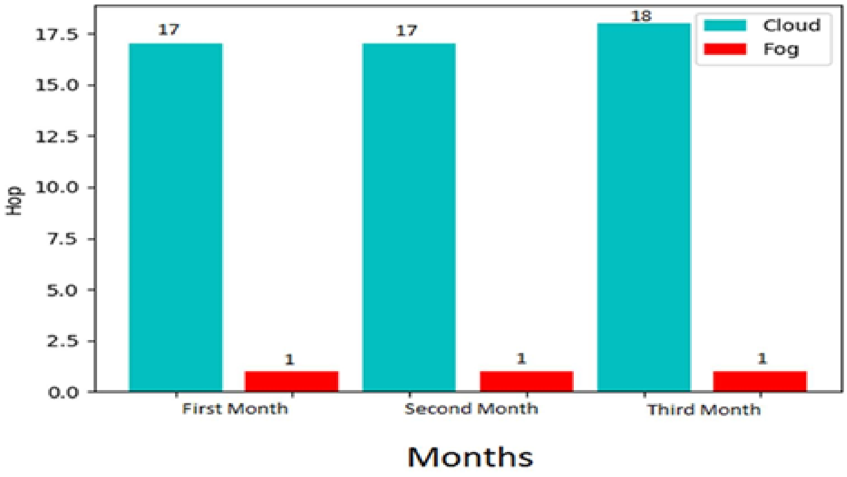


Figure 7: The Average Hop taken for three (3) Months

6. CONCLUSION AND RECOMMENDATION

This paper addresses the implementation and evaluation of Fog-based Game Theoretic Approach to Cyber Security Risk Management. The cyber risk management architecture presents game theoretic models that seeks to automate the interaction between the attacker and the defender, through the analysis of incoming packets in the network. The introduction of Fog computing has brought more cyber risks because, fog allows lightweight cloud-like facility at the proximity of mobile users. Fog also serves mobile users with a direct short-fat connection as compared to the long-thin mobile cloud connection. Therefore, fixing the issues through traditional cyber security approaches of detection and response to new vulnerabilities and threats is a challenge. The failure of many of the present cyber security paradigm points to the need for a new and better approach. One of the prominent risk management techniques to tackle this challenge is the use of Game Theoretic Approach (GTA). This research opens up a solution of using a game theoretic approach to manage cyber risks in the concept of Fog computing so as to enhance cyber operational effectiveness and efficiency. The solution is approached using Bayesian Game. The evaluation obtained from the results shows the adequacy and practicality of the system for cyber risk management in the Fog-based environment.

Future works would consider the use of privacy preserving schemes for ensuring data privacy.

7. ACKNOWLEDGMENTS

Our thanks to the management of the School of Computing at the Federal University of Technology, Akure-Nigeria, as well as those at the Adekunle Ajasin University Akungba-Akoko, Nigeria, for providing the enabling environment for this research, and for allowing us carry out our experiments on their networks.

8. REFERENCES

[1] Gabriel A. J., Adetunmbi A. O., Obaila P. 2020. A Two-Layer Image-Steganography System for Covert Communication over Enterprise Network. In: Gervasi O. et al. (eds). Lecture Notes in Computer Science, vol 12254 pp. 459-470. Springer Nature Switzerland. https://doi.org/10.1007/978-3-030-58817-5_34

[2] Lewis, J. A. 2002. Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. Center for Strategic and International Studies (CSIS).

[3] Alese B. K., Gabriel A. J., Ayodele T. and Akinsowon O. A. 2016 "Cost-Benefit Analysis of Cyber-Security Systems". Proceedings of the World Congress on Engineering and Computer Science 2016. Vol I, WCECS 2016, October 19-21, 2016, San Francisco.

[4] Alese, B.K., Gabriel A. J., Olukayode O. and Daramola O.A. 2014. Modelling of Risk Management Procedures for Cybercrime Control Systems; The 2014 International Conference of Information Security and Internet Engineering; World Congress on Engineering, ISBN 978-988-19252-7-7; 505-509.

[5] Stoneburner, G., Goguen, A. and Feringa, A. 2002. Risk Management Guide for Information Technology Systems—NIST Special Publication 800-30. Technical Report, National Institute of Standards and Technology, (July).

[6] Gabriel, A.J., Darwish, A. and Hassanien, A.E., 2021. Cyber Security in the Age of COVID-19. *Digital Transformation and Emerging Technologies for Fighting COVID-19 Pandemic: Innovative Approaches*, pp.275-295. Springer. DOI:10.1007/978-3-030-63307-3_18

[7] Gueye, A. 2011. A Game Theoretical Approach to Communication Security. University of California, Berkeley, PhD Thesis.

[8] Roy, S., Ellis, C., Shiva, S., Dasgupta, D., Shandilya, V. and Wu, Q. 2010. A Survey of Game Theory as Applied to Network Security. Proc. of the 43rd Hawaii International Conference System Sciences (HICSS), Hawaii..

[9] Alese, B. K., Iwasokun, G. B. and Haruna, D. I. 2013. DGM Approach to Network Attacker and Defender Strategies. In 'Information Security' A Conference Proceedings on International Conference for Internet World Congress on Internet Security Technologies and Secured Transactions ICITST.

[10] Ibidunmoye, E.O., Alese, B. K. and Ogundele, O. S. 2013. Modeling Attacker-Defender Interaction as a Zero- Sum Stochastic Game. Journal of Computer Sciences and Applications, 1(2), 27–32.

[11] Garg, S. and Aujla, G. S. 2014. An Attack Tree Based Comprehensive Framework for the Risk and Security Assessment of VANET using the Concepts of Game Theory and Fuzzy Logic. Journal of Emerging Technologies In Web Intelligence, 6(2).

[12] Kamhoua, C., Martin, A., Tosh, D. K., Kwiat, K. A., Heitzenrater, C., and Sengupta, S. 2015. Cyber-threats Information Sharing in Cloud Computing : A game Theoretic Approach, 382–389. DOI: 10.1109/CSCloud.2015.80.

[13] Maghrabi, L. 2015. Moving Assets to the Cloud : A Game Theoretic Approach Based on Trust.

[14] Garg, S. and Aujla, G. S. 2016. Accessing Risk Priority of SSL SYN Attack using Game Theoretic Attack Defense Tree Model for VANETs, 729–734.

[15] Wei, L., Sarwat, A., and Saad, W. 2016. Risk Assessment of Coordinated Cyber-Physical Attacks Against Power Grids : A Stochastic Game Approach, 1.

[16] Musman, S. and Turner, A. 2017. A game theoretic approach to cyber security risk management. Journal of Defense Modeling and Simulation: Applications, Methodology, Technology, (Special). DOI: 10.1177/1548512917699724.

[17] Razouk, W., Sgandurra, D. and Sakurai, K. 2017. A New Security Middleware Architecture, Based on Fog Computing and Cloud To Support IoT Constrained Devices. In IML '17: International Conference on Internet of Things and Machine Learning, October 17–18, 2017, Liverpool, United Kingdom. ACM, New York, NY, USA, Article 143, 8 pages. DOI: 10.1145/3109761.3158413.

[18] Sun, Y., Lin, F .and Zhang, N. 2018. "A security mechanism based on evolutionary game in fog computing" Saudi Journal of Biological Sciences 25 (2018) 237–241.

[19] Netland, L. 2008. Assessing and Mitigating Risks in Computer Systems, PhD Thesis at the University of Bergen, Norway.