IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 2, February 2018

Monitoring Cyber Thread Behaviors in Cloud Environment using Honeypot Technique

M.Umamaheswar[1] and V.Arulmozhi[2]

M.Phil Research Scholar, Dept. of Computer Science, Tiruppur Kumaran College, Tirupur, Tamilnadu, India[1]

Associate Professor, Tiruppur Kumaran College, Tirupur, Tamilnadu, India[2]

Abstract: A cloud computing is one of the upgrading technology, it provide the data access mechanism through cloud provider. User can accomplish a useful and economical advance for information sharing between group members in the cloud. Cyber thread is one of the critical factors in cloud computing. To provide a safe transaction network faces the many issues. The safety critical systems that need to provide a high-level of confidence in their safety and functionalities under multiple operating in network. With the support of the SDN network play a major role. According to the cyber threads, cyber-physical systems testbed based on cloud computing and Software Defined Network (SDN) were used. And Cyber physical Monitoring System is proposed to monitor the attacks.

Keywords: Cloud Computing, Cyber thread, Security, SDN and Attack monitoring.

I. INTRODUCTION

Cloud computing is a very latest emerging innovations of the modernized internet and technological view with everyone from the White house to major online technological leaders like Amazon and Google using or offering cloud computing services it is presented by itself as an exciting and innovative method to cache and handling data on the internet. Aside subscribing functions, cache, software and other services online account, Cloud providers can greatly diminish costs for small/large businesses and startups through giving them access to advanced features that may be very expensive otherwise and far above their means to obtain or maintain [1].

Cyber-Physical Systems (CPS) is described as reframing technologies for managing interconnected systems between its physical assets and computational capabilities. With recent developments that have resulted in higher availability and affordability of sensors, data acquisition systems and computer networks, the competitive nature of today's industry forces more factories to move toward implementing high-tech methodologies. Consequently, high volume data has been arised by the ever growing use of sensors and networked machines which are known as Big Data [2]. In such an environment, CPS can be further developed for managing Big Data and leveraging the interconnectivity of machines to reach the goal of intelligent, resilient and self-adaptable machines. Furthermore, logistics and services connects with production, in the continuing industrialized practices, it would transform today's factories into an Industry 4.0 factory with significant economic potential. For instance, a joint report by the Fraunhofer Institute and the industry association Bitkom said that German gross value can be boosted by a cumulative 267 billion euros by 2025 after introducing Industry 4.0. Since initial stage of improvement of the CPU, it is essential to clearly define the structure and methodology of CPS as guidelines for its implementation in industry. To meet such a demand, a unified system framework has been designed for general applications. Furthermore, each system layer proposes parallel algorithms and technologies at each and every system to conspire with the unified structure and realize the desired functionalities of the overall system for enhanced equipment efficiency, reliability and product quality. Software-Defined Networking (SDN) is an emerging networking paradigm that gives hope to change the limitations of current network infrastructures [3]. SDN is being circulated to different networking system. It is the ability to program network performance in open way using languages, systems, computers that are ordinary.

A simplified view of this SDN is shown in Figure 1. First, it breaks the vertical integration by separating the network's control logic (the control plane) from the underlying routers and switches that forward the traffic (the data plane). Second, simple forwarding devices are converted by separated data planes and control, network switches and the control logic is resolved in a logically centralized controller (or network operating system1), simplifying policy enforcement and network (re)configuration and evolution [4]. It is important to emphasize that a logically centralized programmatic model does not postulate a physically centralized system. Cloud layer is a virtual processing of hardware resources using cloud computing and software defined network technology. It is segmented into two levels: control layer and datapath layer.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 2, February 2018

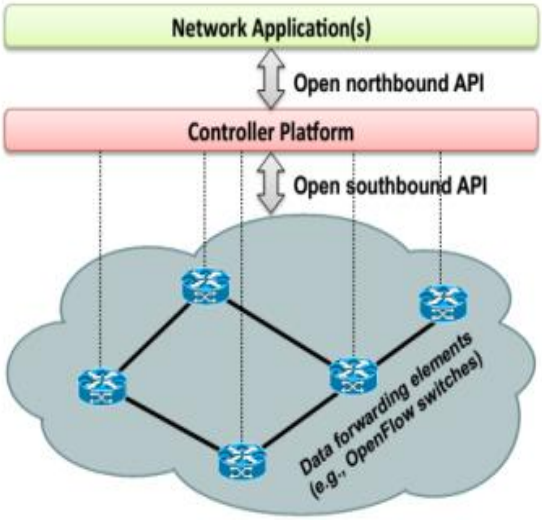

Fig 1. View of SDN

Control layer is composed principally of openflow controller and cloud controller which are responsible for the construction of SDN network using virtual machine and OpenvSwitch. In the datapath layer, OpenvSwitch can interact with the external network to realize the combination of the hybrid network. Finally, the OpenvSwitch introduces the dataflow of SDN network into real-world systems through interact with the external network interface.

II. LITERATURE REVIEW

The compound wireless experimentation is examined by Mahesh K. Marina [5], which has arrived as an alternative and complementary methodology to physical experimentation and simulation for wireless network evaluation. Specifically, our focus in this paper is on WHYNET, a flexible hybrid evaluation framework providing the capability to seamlessly integrate simulated, emulated and physical networks, thereby enabling several ways of actualizing a given target wireless network scenario each using physical (operational) and simulated elements in different combinations depending on the evaluation needs and available testbed resources. Using two novel and detailed case studies of WHYNET, we demonstrate the utility of the hybrid approach for realistic, scalable and cost-effective evaluation of heterogeneous wireless network scenarios and cross-layer protocol mechanisms.

Xinshu Dong et al [6] Emerging networking paradigm of Software-Defined Networking (SDN) is that provides unprecedented flexibility in dynamically reconfiguring an IP network. It enables various applications such as network management, qualIty of Service (QoS) optimization, and system resilience enhancement. The possibilities of applying SDN have been researched by Pilot studies on smart grid communications, while the specific benefits and risks that SDN may bring to the resilience of smart grids against accidental failures and malicious attacks remain largely unexplored. To embrace SDN will be unlikely by the power industry issues, since resilience is always a key consideration for critical infrastructures like power grids. In this position paper, we aim to provide an initial understanding of these issues, by investigating (1) how SDN can enhance the resilience of typical smart grids to malicious attacks, (2) SDN introduces additional risks and how to manage them, and (3) how to validate and evaluate SDN-based resilience solutions. Our goal is also to trigger more profound discussions on applying SDN to smart grids and inspire innovative SDN-based solutions for enhancing smart grid resilience.

Christof J. Budnik[7] Cyber-Physical Production Systems (CPPS) build a network of industrial automation components and systems to enable individualized products at mass production costs. Failures or vulnerabilities in CPPS can be life threatening and can cause physical damage while hiding the effects from monitors. Thus, software verification and validation methods need to analyze the dynamics and behavior of CPPS. In this work, we present a hybrid testbed used in Siemens Corporate Technology. The testbed combines a physical CPPS together with its virtual simulated counterpart, allowing us to verify the system using runtime monitoring, model-based testing, simulation and formal techniques. Their approach to model-based testing relies on a black-box view of the system. Once a formal model of the CPPS is defined, it becomes easier to generate test-cases that lead to particular configurations, by using model-checking techniques. Many questions still need to be addressed in order to effectively combine formal verification and simulation techniques. Nevertheless, having a realistic testbed will allow us to better characterize the problems, and create interesting benchmarks to drive the development of tools.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 2, February 2018

Varun Krishna Veeramachaneni [8], "Cloud computing" represents a relatively new computing model in the evolution of on-demand information technology services and products, that is built on decades of research in distributed computing, virtualization, utility computing, and more recently networking, web and software services. Service adapted architecture is involved by it and compressed information technology overhead for the end-user, great flexibility, and reduced total cost of ownership. Various categories of such security concerns are trust, architecture, identity management, software isolation, data protection, confidentiality and availability. All these security vulnerabilities point to various threats on the cloud such as authentication, misuse of cloud infrastructure, eavesdropping, network intrusion, denial of service attack, session hijacking. Further Cloud Forensic is an emerging challenge related to cloud security [9]. It investigates the key security issues of Cloud computing being faced today and the challenges and opportunities that it brings for business community. A brief information of what exactly cloud computing security-related issues are explained by this research paper, and discusses data security and privacy protection issues associated with cloud computing across all stages of data life cycle. It also displays current solutions for data security and privacy protection issues in cloud. and describes future research work.

III. PROBLEM STATEMENT

More standardized, networked and intelligentized nature of industry 4.0 has intensified critical infrastructures cyberthreats. According to cyber-physical systems (CPS) layered architecture and security requirements in industry 4.0, a cyber-physical systems testbed based on cloud computing and software defined network (SDN), or CPSTCS is proposed. The CPSTCS uses a network testbed based on cloud computing and SDN to recreate the cyber elements of cyber-physical systems and real-world physical devices for the physical components [10]. The CPSTCS helps assess cyberthreats against the cyber and physical dimensions of critical infrastructures.

IV. PROPOSED WORK

The interdependent quality of Industry 4.0–directed operations and the pace of artificial transformation mean that cyber attacks can have far more comprehensive effects than ever before, and manufacturers and their supply networks may not be prepared for the risks. For cyber risk to be adequately have to monitor the activity of the hackers. Cyber thread is one of the dangerous factors in cloud computing. To afford a safe contract network tackle many issues. The security critical systems that necessitate to provide a high-level of assurance in their safety and functionalities beneath multiple operating in network. With the support of the SDN network play a major role [11]. According to the cyber threads, cyber-physical systems testbed based on cloud computing and Software Defined Network (SDN) were used. And Cyber physical Monitoring System was proposed to monitor the attacks. The proposed methodologies were

A. SDN Interface

SDN is a innovative networking paradigm which key feature is the separation of the data plane and the control plane. In SDN, network switches are simple forwarding devices, whose forwarding rules can be dynamically configured by a central controller. In fact, the need to guarantee adequate levels of performance, scalability, and reliability would preclude such a solution. Instead, production-level SDN network designs resort to physically distributed control [12]. A well-defined programming interface between the switches and the SDN controller can realize the separation of the control plane and the data plane.

B. Configuring Network

This is a computer system, mostly connected to the Internet that is configured to trap attackers. Honeypots are similar in nature to darknet with more specific goals. Honeypots, in general, require more resources than darknet since the aim is to interact with the adversary. There are 3 major types of honeypots, namely low, medium and high interactive honeypots. Types are differentiated based on their interactivity level with the initiator of the communication. On one hand, a low-interactive honeypot is a simple solution configured to interact with the intruder at a basic level by emulating services (e.g., send ECHO Reply message to an ECHO Ping Request). Further, a medium-interactive honeypot is similar to low-interactive one but with further interactions and more emulated services for more data capturing and analysis (e.g., reply SYN ACK to a SYN request) [13, 14]. On the other hand, a high interactive honeypot is a computer system that do not emulate some services. Instead, it runs a complete vulnerable or non-patched operating system and applications such as an OS version on a virtual machine. Note that a collection of honeypots form a honeynet.

C. Monitoring

Running and operating a monitoring system might be a simple exercise. However, having the legal right to monitor network activities of users might be the issue. Many sources might have restrictions on monitoring the cyber space such as privacy and employment policies, terms-of-service agreement, state and provincial laws, etc. Any violation of these

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 2, February 2018

laws might lead to civil liability and even criminal sanctions [15]. It is noteworthy to mention that monitoring cyber activities today takes a big attraction as it produces exclusive insights for security operators, organizations, law enforcement agencies, governments and even adversaries. This helps to find the malicious activities, but also detect the strategy of the attack, its intention, its uniformity and coordination features.

D. Honeypot Deployment

Honeypot deployment depends on several factors such as the location of the sensor, configuration of the sensor, and most importantly, the type of the sensor (low, medium, high). First, a major factor in honeypot deployment is choosing the location. A good practice exercise recommends installing several honeypot in separate locations and separate from the production system to prevent liability issues [16, 17]. The more distributed are the sensors, the better are the extracted insights and the vision. Second, configuring a honeypot changes based on the need of the analysts. For instance, setting up a highly interactive honeypot with capabilities to detect botnet is less challenging than deploying a low-interactive honeypot to monitor solely scanning activities. In any case, the deployment of low-interactive honeypot is close to darknet deployment whereas deploying high-interactive honeypot must be done in a way to emulate the operation of a regular machine. Therefore, a practical way to deploy high-interactive honeypot is to run the trap on a Virtual Machine (VM) and run this service in a safe environment.

V. EXPERIMENTAL RESULT

The availability of effective evaluation platform is key to the development of high performance, reliable and energy efficient wireless network systems. However, the design of such platforms is challenging as they need to satisfy a conflicting set of requirements — viz., realism, controllability, scalability and cost-effectiveness — rising from the need to support varied experimentation needs and wide range of wireless networking and radio technologies. The two most common evaluation methodologies, physical experimentation and simulation, while offering a unique set of benefits, are insufficient in meeting those requirements. Physical experimentation is very practical, but difficult to manage and can be a costly approach for evaluation of futuristic radio technologies and large-scale or mobile scenarios. Simulation, on the other hand, allows controlled and flexible experimentation of large-scale wireless network scenarios, but usually at the expense of realism.

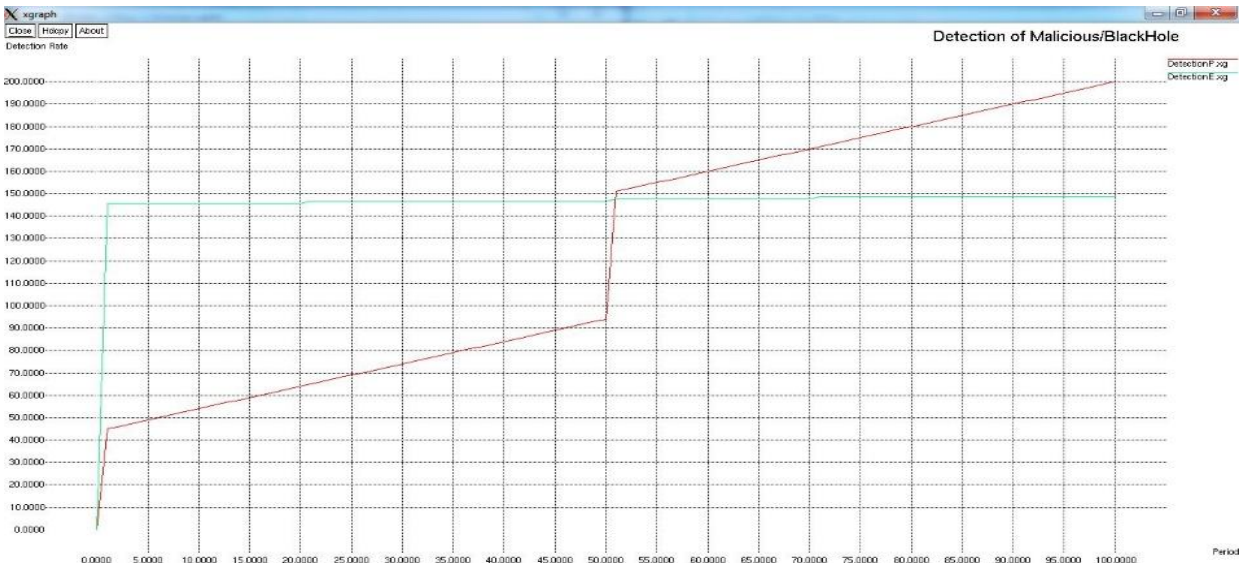

Fig 2. Malicious Detection

In this fig 2 it provide the detection of malicious activity for the security reason. This behavior in different ways, but it seems that the main motivation is fear of competitors stealing their ideas. To opposed this, we reconsidered security monitoring mechanisms from not only commercial solutions, but also open communities which are doing research in this field. In this analysis, we focus more on monitoring mechanisms which help us to cover security challenges

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 2, February 2018

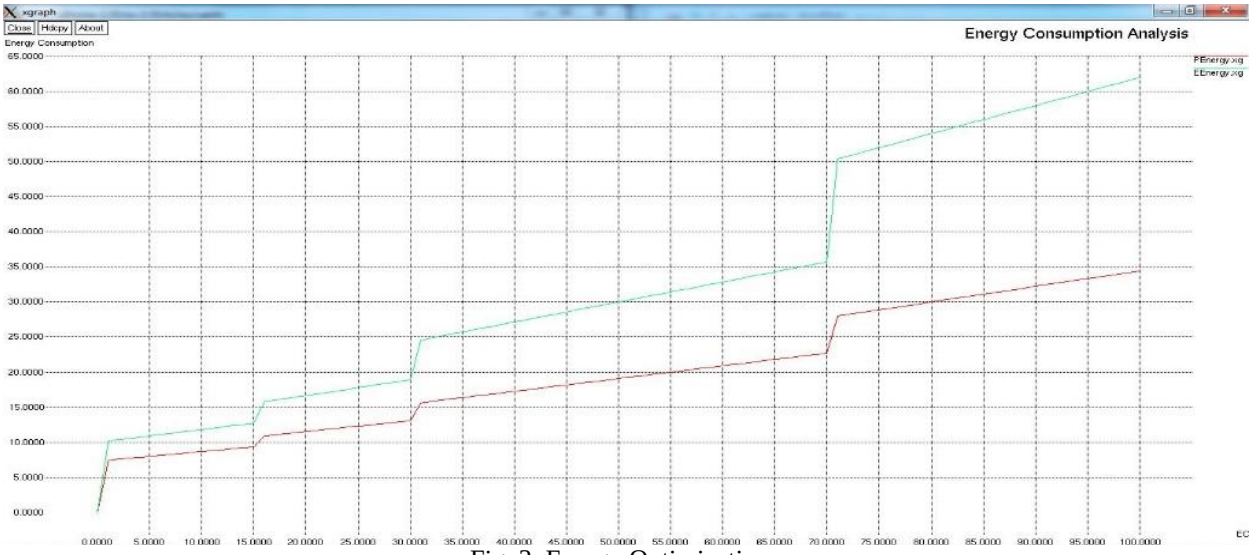

Fig 3. Energy Optimization

In figure 3 an energy optimization data replication scheme has been proposed for datacenter storage. Underutilized storage servers can be turned off to minimize energy consumption, although each data object must be kept by one of the replica servers to guarantee availability.

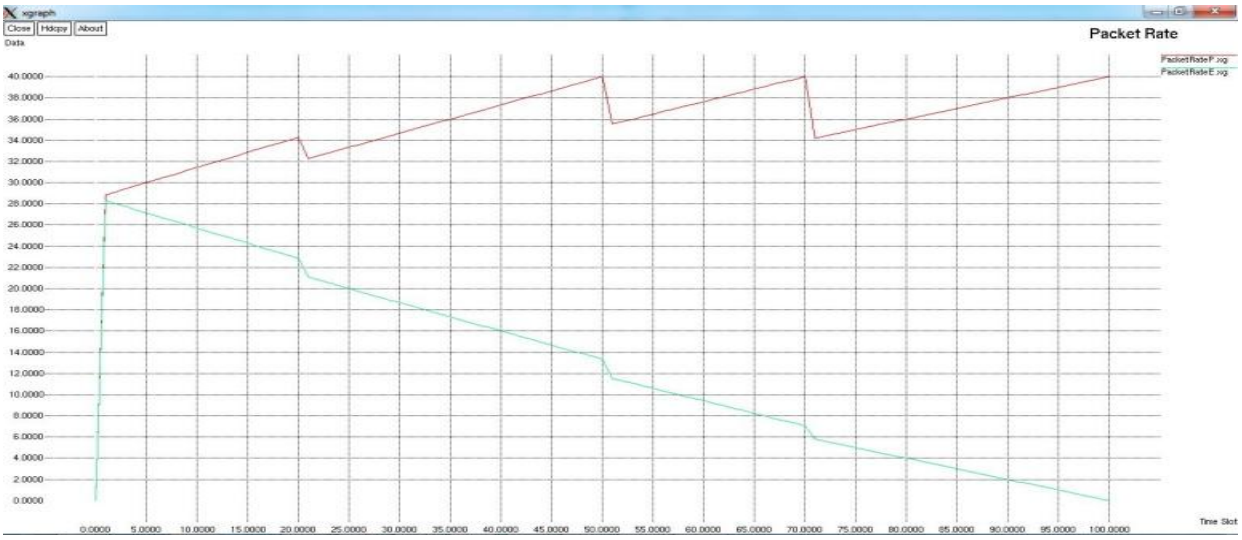

Fig 4. Delivered Packet Data

Cloud layer is a virtual processing of hardware resources using cloud computing and software defined network technology. It is segmented into two levels: control layer and datapath layer. Control layer is composed principally of openflow controller and cloud controller which are responsible for the construction of SDN network using virtual machine and OpenvSwitch. In the datapath layer, OpenvSwitch can interact with the external network to realize the combination of the hybrid network. Application layer provides a user portal for deploying applications, such as topological structure configuration, host management and traffic monitoring. It provides OpenvSwitch a packet matching function to achieve fine-grained division and forwarding for different business traffic. In other words, different business traffic has different forwarding strategies and forwarding path. Finally, the OpenvSwitch introduces the dataflow of SDN network into real-world systems through interact with the external network interface.

VI. CONCLUSION

With recent developments that have resulted in higher availability and affordability of sensors, data acquisition systems and computer networks, the competitive nature of today's industry forces more factories to move toward security issues. Cyber thread is one of the dangerous factors in cloud computing. To afford a safe contract network tackle many issues. The security critical systems that necessitate to provide a high-level of assurance in their safety and functionalities beneath multiple operating in network. With the support of the SDN network play a major role.

According to the cyber threads, cyber-physical systems testbed based on cloud computing and Software Defined Network (SDN) were used. And Cyber physical Monitoring System were proposed using honeypot technique to monitor the attacks.

REFERENCES

[1]. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia. "A View of Cloud computing," Comm. ACM, vol. 53, no. 4, pp. 50-58, Apr.2010.
[2]. Lee, L. Sha, and J. Stankovic. Cyber-physical systems: The next computing revolution. Proceedings of the 47th Design Automation Conference, 2010:731-736
[3]. SDxCentral. (2017). "What's Software-Defined Networking (SDN)?". [online] Available at: https://www.sdxcentral.com/sdn/definitions/what-the-definition-of-software-defined-networking-sdn/ [Accessed Feb. 2017].
[4]. Yan, Q., Yu, F.R., Gong, Q. and Li, J., 2016. Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A survey, some research issues, and challenges. IEEE Communications Surveys & Tutorials, 18(1), pp.602-622.
[5]. Mahesh K. Marina, "Utility of Hybrid Wireless Experimentation for Evaluation of Heterogeneous Wireless Architectures and Cross-Layer Protocols".
[6]. Xinshu Dong, Software-Defined Networking for Smart Grid Resilience: Opportunities and Challenges
[7]. Christof J. Budnik, "Testbed for Model-based Verification of Cyber-Physical Production Systems"
[8]. Varun Krishna Veeramachaneni, "Security Issues and Countermeasures in Cloud Computing Environment" IJESIT, 2015.
[9]. R. Gellman, "Privacy in the Clouds:Risks to Privacy and Confidentiality from Cloud Computing," 2009.
[10]. Haihui Gao, Yong Peng, Zhe Wen, "Cyber-Physical Systems Testbed Based on Cloud Computing and Software Defined Network"
[11]. Christos Siaterlis and Béla Genge,Cyber-Physical Testbeds. COMMUNICATIONS OF THE ACM,2014,57(6):64-73 R. (Raj) Rajkumar,
[12]. Yan, Qiao, et al. "Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A survey, some research issues, and challenges."
[13]. Provos, N. (2004, August). A Virtual Honeypot Framework. In USENIX Security Symposium (Vol. 173).
[14]. Provos, N., & Holz, T. (2007). Virtual honeypots: from botnet tracking to intrusion detection. Pearson Education
[15]. Khorshed, Md Tanzim, ABM Shawkat Ali, and Saleh A. Wasimi. "Controlling insiders activities in cloud computing using rule based learning." Trust, Security and Privacy in Computing and Communications (TrustCom),
[16]. Mokube, I., & Adams, M. (2007, March). Honeypots: concepts, approaches, and challenges. In Proceedings of the 45th annual southeast regional conference (pp. 321-326). ACM.
[17]. Spitzner, L. (2003). The honeynet project: Trapping the hackers. IEEE Security & Privacy, 1(2), 15- 23.