International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 6 | ISSN : 2456-3307

Network Security and Detection in Cloud Based Environment Systems

Ankita Bung
Assistant Professor, Department of CSE, MGIT College, Hyderabad, India

ABSTRACT

Technology transformation is wide and vast keyword found in the Domain of the network of data transmission, irrespective of the network system, whether virtual or any other classical network system. Technology have its own significance the way we look forward, in the same aspect of cloud which we call as the hot cake in the Industry of Information technology; More or less is a typical word to understand what really it stands for to put forward the glimpse of Information Technology. If we will consider he classical and today world parallel distributed and virtual network is typical for us to provide the best way we use having lot feature. IN the dictionary word we can call as network means security which is mandatory, hence we can go for the best intrusion mechanism, which involves the robust and hinder free, hacker free counter measure to defend the penetration mechanism.

Keywords : Network Security, Cloud Computing, Intrusion Detection, Attack Graph, Zombie Detection

I. INTRODUCTION

In the Domain of Networking, Given that the IEEE 802.15.4 devices are typically severely constrained in terms of their communication and computational resources, the implementation of such solutions is likely to impose a significant performance overhead. Currently, not many wireless sensor network overhead statistics are available when security is employed in such networks. Sensor network application developers and network administrators always need these overhead statistics in choosing the security option that best suites the security for a particular threat environment. For evaluating these security overheads on wireless sensor networks, we will simulate IEEE 802.15.4 media access control layer and secure data exchange once the devices exchange link keys with the PAN coordinator. We will measure communication costs that are incurred after employing these security features under different inputs to wireless sensor network model. Cloud computing is a technology which works only on the internet; central remote servers are used to maintain data and applications.

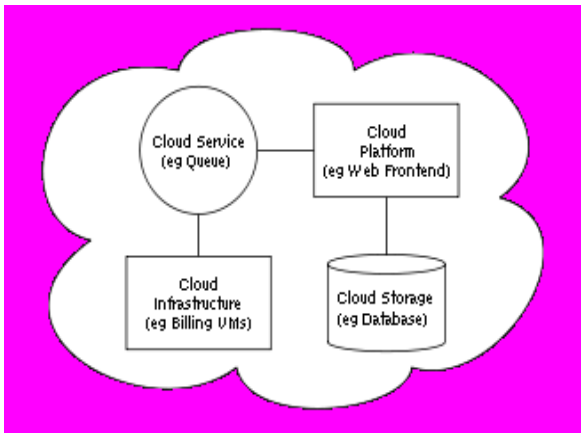

Figure 1.1. Infrastructure as Cloud in the Network Model

Cloud computing allows the users to use applications without installing software's. The users can access the internet and send messages anywhere in the world. Cloud computing allows more efficient computing by centralized storage, memory, processing and bandwidth. The best example is Google mail. For this, the users need not install any software or a server to use a Google mail account. The user can access internet, through which he sends messages. Therefore the servers and email software are all present on the cloud i.e. internet and these software's and servers are

managed by the cloud service provider i.e. Google. Cloud computing is divided in to three layers, infrastructure, software and platform. Refer to the paragraph below for further information.

II. Related Work

The client sends a request to the server for getting a service. In the "conventional client server" system, the client communicates with the end server directly, due to which traffic congestion or data loss etc. might take place. So to overcome this issue we have implemented a proxy server, which extends the functionality of the main cloud server and is the mediator between your web browser and the end server. Initially, your web browser sends a request to the proxy server, after which the proxy server forwards the request to the end server. The end server then gives acknowledgment to the proxy server. Finally, the proxy server replies to the browser. Therefore, there is no direct communication between the user and the end server. So, HTTP request is originated from the intermediate proxy server.

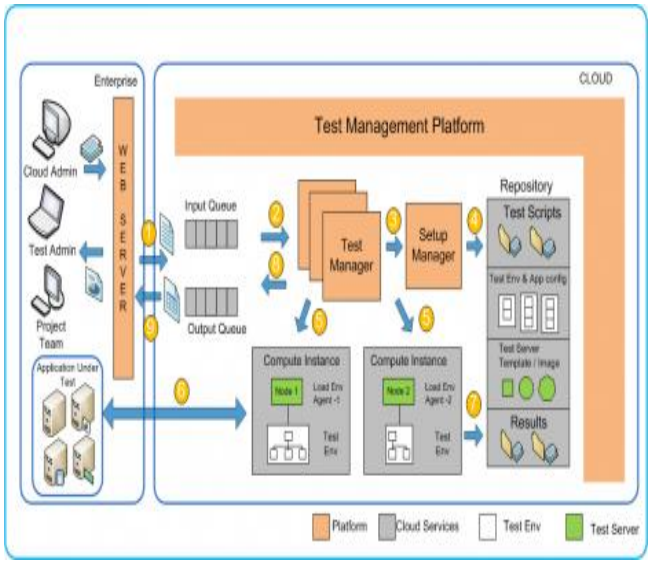

Fig.2.1 Mac Based ACK Confirmation in the NODE

As a result the client computer's IP address will be in hidden state and illegitimate users cannot access the client computer's IP address. This type of proxy server is also known as anonymous proxy server.

III. Methodology

In today's world if the cloud system develops, then the core cloud computing technologies will elaborate. Web applications and services and virtualization IAAS offerings are the cloud computing technologies. The below two are the best examples of vulnerabilities in cloud computing technology that are related to our research. The possibility that an intruder gets away successfully from a virtualized environment lies in virtualization's very nature. Virtual machine escape is an exploit; an attacker can execute arbitrary code on a virtual machine. So in this case the operating system executes within itself to break out and interact directly with the hypervisor. As a result, an attacker can gain access to the host operating system and all other virtual machines running on that host. In this case we can imagine that this type of vulnerability is a high risk in cloud systems.

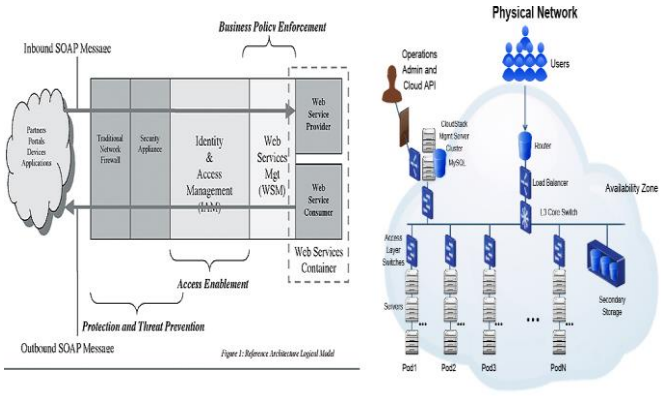

Fig.3.1 Architecture Model for Node Based Intrusion

Storage service is a database. When the node receives a request or an acknowledgment, then the analyzer system will compare the node information in the storage service.

Algorithm

Feistel Networks – the fundamental building block is the *F* function : a key-dependent mapping of an input string onto an output string.

An *F* function is always non-linear and possibly non-surjective.

$$F : \{0,1\}^{n/2} \times \{0,1\}^{N} \mapsto \{0,1\}^{n/2}$$

where *n* is the block size of the Feistel Network, and *F* is a function taking *n*/2 bits of the block and *N* bits of a key as input, and producing an output of length *n*/2 bits. A successful *chosen-key attack* against Twofish requires choosing 160 bits of a pair of keys, and needs 2^{34} work, 2^{32} chosen-plaintext queries, and 2^{12} adaptive

chosen-plaintext queries so that 10 rounds Twofish can be broken.The *meet-in-the-middle attack* on standard Twofish requires 4 rounds, 256 known plaintexts, 2^{225} memory and 2^{232} work.The successful *differential attack* on standard Twofish can break 5 rounds with 2^{232} work and 2^{41} chosen-plaintext queries.

Knowledge service we used audit information for the communication system and the logging system for evaluating the knowledge service. Moreover, we are free to delete and modify rules at will in a knowledge service.
Behavior service it compares recent user actions to the usual behavior. It is divided into two types i.e. user behavior and node behavior.

3.1 Analysis of Behavior

User behavior is nothing but analyzing the user's behavior. By using this method we can identify expected behavior or a severe behavior deviation. Node behavior Refer to the concept "Anomaly based IDS "for further information. Event auditor has two components for detecting an intrusion in the network as data is exchanged between the nodes and environment states. In the first component, when the data is exchanged between the nodes, audit information about the communication between the nodes is being captured. Therefore, audit data captures only the node information, but not network data.

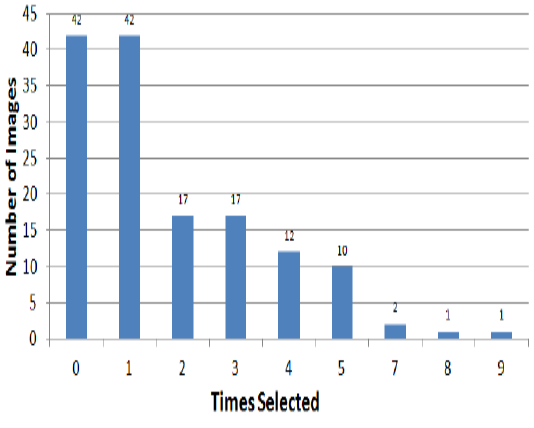

Figure 3.1.1. Comparison of the Peak of the Images

The second component is logging system, for each event in the node, a log entry is created and they have action types such as error, alert or warning. By using this approach we can easily find ongoing intrusions .A proxy server can be the other way around: a server which receives and queues requests, makes format changes and packet divisions etc. for information from just one single information carrying server. The network administrator cannot monitor all the clients, so it will depend on the IDS which gives the alerts to the remaining "cloud server". In this case we can hide the data from the intruders. In cloud computing, there is more possibility to hack the data. We are providing a security mechanism called IDS.

IV.Conclusion and Future Work

Technologically providing security, we have implemented IDS. It is more secure beyond passwords, digital signatures, and confidentiality. IDS cannot substitute any of those mentioned mechanisms. But it can enhance a system where those mechanisms are not enough. For data efficiency, we have implemented a proxy server. The proxy server extends the functionality for a single server. Hence proxy servers are more efficient than a single server. For system performance, we have implemented a grid system.

V. REFERENCES

[1]. Cloud Security Alliance, "Top Threats to Cloud Computing v1.0," https://cloudsecurityalliance.org/topthreats/csathreats. v1.0.pdf, Mar. 2010.

[2]. 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," ACM Comm., vol. 53, no. 4, pp. 50-58, Apr. 2010.

[3]. B. Joshi, A. Vijayan, and B. Joshi, "Securing Cloud Computing Environment Against DDoS Attacks," Proc. IEEE Int'l Conf. Computer Comm. and Informatics (ICCCI '12), Jan. 2012.

[4]. H. Takabi, J.B. Joshi, and G. Ahn, "Security and Privacy Challenges in Cloud Computing Environments," IEEE Security and Privacy, vol. 8, no. 6, pp. 24-31, Dec. 2010.

[5]. "Open vSwitch Project," http://openvswitch.org, May 2012. 6Z. Duan, P. Chen, F. Sanchez, Y. Dong, M. Stephenson, and J. Barker, "Detecting Spam Zombies by Monitoring Outgoing Messages," IEEE Trans. Dependable and Secure Computing, vol. 9,no. 2, pp. 198-210, Apr. 2012.

[6]. G. Gu, P. Porras, V. Yegneswaran, M. Fong, and W. Lee, "BotHunter: Detecting Malware

Infection through IDS-driven Dialog Correlation," Proc. 16th USENIX Security Symp. (SS ’07), pp. 12:1-12:16, Aug. 2007.
[7]. G. Gu, J. Zhang, and W. Lee, "BotSniffer: Detecting Botnet Command and Control Channels in Network Traffic," Proc. 15th Ann. Network and Distributed Sytem Security Symp. (NDSS ’08), Feb. 2008.
[8]. O. Sheyner, J. Haines, S. Jha, R. Lippmann, and J.M. Wing, "Automated Generation and Analysis of Attack Graphs," Proc. IEEE Symp. Security and Privacy, pp. 273-284, 2002,
[9]. "NuSMV: A New Symbolic Model Checker," http://afrodite.itc. it:1024/nusmv. Aug. 2012.
[10]. P. Ammann, D. Wijesekera, and S. Kaushik, "Scalable, graphbased network vulnerability analysis," Proc. 9th ACM Conf. Computer and Comm. Security (CCS ’02), pp. 217-224, 2002.
[11]. X. Ou, S. Govindavajhala, and A.W. Appel, "MulVAL: A Logic- Based Network Security Analyzer," Proc. 14th USENIX Security Symp., pp. 113-128, 2005.
[12]. R. Sadoddin and A. Ghorbani, "Alert Correlation Survey: Framework and Techniques," Proc. ACM Int’l Conf. Privacy, Security and Trust: Bridge the Gap between PST Technologies and Business Services(PST ’06), pp. 37:1-37:10, 2006.
[13]. L. Wang, A. Liu, and S. Jajodia, "Using Attack Graphs for Correlating, Hypothesizing, and Predicting Intrusion Alerts," Computer Comm., vol. 29, no. 15, pp. 2917-2933, Sept. 2006.
[14]. S. Roschke, F. Cheng, and C. Meinel, "A New Alert Correlation Algorithm Based on Attack Graph," Proc. Fourth Int’l Conf. Computational Intelligence in Security for Information Systems, pp. 58-67, 2011.
[15]. A. Roy, D.S. Kim, and K. Trivedi, "Scalable Optimal Countermeasure Selection Using Implicit Enumeration on Attack Countermeasure Trees," Proc. IEEE Int’l Conf. Dependable Systems Networks (DSN ’12), June 2012.
[16]. N. Poolsappasit, R. Dewri, and I. Ray, "Dynamic Security Risk Management Using Bayesian Attack Graphs," IEEE Trans. Dependable and Secure Computing, vol. 9, no. 1, pp. 61-74, Feb. 2012.
[17]. Open Networking Fundation, "Software-Defined Networking: The New Norm for Networks," ONF White Paper, Apr. 2012.
[18]. "Openflow," http://www.openflow.org/wp/learnmore/, 2012.
[19]. N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner, "OpenFlow: Enabling Innovation in Campus Networks," SIGCOMM Computer Comm. Rev., vol. 38, no. 2, pp. 69-74, Mar. 2008.
[20]. E. Keller, J. Szefer, J. Rexford, and R.B. Lee, "NoHype: Virtualized Cloud Infrastructure without the Virtualization," Proc. 37th ACM Ann. Int’l Symp. Computer Architecture (ISCA ’10), pp. 350-361, June 2010.

Author Details:

Name: Ankita Bung Department of CSE, Assistant Professor, MGIT College, Hyderabad.