Enhanced Decentralized Control and Attack Analysis Model for Virtual Network System

Kolan.Saritha*1, K.Ramesh Babu*2

PG Scholar, Dept of CSE, MRECW, Dist: secunderabad, Telangana state, India

Associate Professor & HOD, Dept of CSE, MRECW, Dist: secunderabad, Telangana state, India

ABSTRACT

Technologically Network Security is always looping whole like the matter of Physics Black Hole. If we consider the these days demanding Technology which called as cloud computing in turn we call as virtualization, where Network is Most Primary Component leads us to a high level research to provide the best of security mechanism and minimizing the vulnerability. Network Security in the cloud environment is typically involve the first task as Detection of vulnerability which may lead the hacker to explore some more new technical flip-flop. Hence, in this paper we try to put forward some of the countermeasure as “prevention is better than cure” where we put the multi hop based counter vulnerability and making the Node to node acknowledgement with the intention of making the system enable with same intrusion mechanism.

KEYWORDS: Network security, cloud computing, intrusion detection, IDS.

I.INTRODUCTION

Networks are becoming increasingly popular with many potential applications including general engineering, health, military, environment science, etc. They consist of large number of tiny sensor nodes with limited energy, memory, bandwidth, and processing power. Sensor nodes can be randomly deployed in inhospitable places. A WSN is self-organized with collaboration between nodes. Base station, which is usually a powerful computer with more computational resources, energy, and storage, is present and receives aggregated data from the sensors. IAAS: An organization or a company which provides a service. Those services may include much essential functionality such as computer networking, information storage, servers and virtualization. SAAS: This is also provided by an organization. They provide software, in which you can use these services. An example is Face book. Vulnerability is a prominent factor of risk. ISO 27005 defines risk as “the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm of the organization”.

II.RELATEDWORK

Nowadays everyone has to accept the fact that the percentage of intruders is
increasing day by day as technology advances. But at the same time we have a lot of chances to keep the data in security. We have a lot of free software on the internet to protect data from intruders such as antivirus software etc. Coming to this thesis, Intrusion Detection System (IDS) is the tool for monitoring traffic in the network. Whenever it identifies vulnerabilities in the network, it sends a report to the system or network administrator. IDS are like an alarm on your computer. It makes it possible to block the unauthorized persons from accessing data.

IDS and IPS both are software but they have different terminologies. IDS control the Intrusion Detection process while IPS has all the features from IDS as well as tools to prevent the attacks from intruders. The intrusion detection system is classified into two methods namely, behavior analysis and knowledge analysis. Behavior analysis method is done by comparing the previous behavior with the present one. It detects the intrusion by using heuristic/anomaly. Knowledge analysis method detects intrusions by using signatures/patterns. We are free to delete and modify rules at will in a knowledge based system. We refer to the next section “Signature/pattern & heuristic/anomaly” for further information. How to detect: The two IDS tools which we are going to discuss related to the project are signature/pattern Based IDS and Heuristic/anomaly based IDS.

III. PROPOSED METHODOLOGY

Intrusion detection system service helps to increase the security in the cloud system by using two methods i.e. behavior based and knowledge based service. We refer to the previous section for further information. The audited data is sent to the IDS service core, which analyzes the behavior using artificial intelligence to detect deviations. It has two sub systems namely analyzer and alert systems. Analyzer system the analyzer gets audit data and examines whether a heuristic in the database is being broken, after which it sends the outcome to the IDS service. For these outcomes, IDS estimates the attack probability and if probability ratio is high then it alerts the other nodes. Alert system in the cloud system if any one node is harmed by the intruder then alert system will alert the remaining nodes in the network regarding the attack.

![Fig.2.1 Ideal Frame Structure of Access period](image)
Fig.3.1 Architecture Diagram of Cloud Based Intrusion at Each Node

Vulnerability is cloud specific if it is prevalent in established state-of-the-art cloud offerings. Even though cloud computing is a new system in the market, in spite of this fact, currently thousands of cloud offerings are in the market. So we are going to discuss two important vulnerabilities that are related to our project. The two main vulnerabilities are injection vulnerabilities and weak authentication schemes. Injection vulnerabilities are attack techniques, in which the attacker exploits by editing the services or by user inputs to perform, execute and oppose the user's aim.

- The below three examples are injection vulnerabilities. Vulnerability is cloud specific if it is intrinsic to or prevalent in a core cloud computing technology.

Authentication Mechanism: The main root cause of weaknesses in current authentication mechanism is usernames and passwords, because the users are using the same passwords in different websites and weak passwords. Session hijacking is an attack technique. A user does not have permission to access the system, but he gains the services in the system. The attackers steal a magic cookie that can be used to authenticate a client to a remote server. The fact is that these types of attacks are most common in websites because the web applications run over HTTP from a web server to a web browser. Therefore, HTTP cookies are used to maintain a session on so many websites. So in this case the attacker can steal cookies easily by using an intermediate system and they can access the user's web account. Session hijacking produces anomalies in the network traffic. Therefore, by using IDS we can detect the attack.

IV.ANALYSIS

The main cloud server is connected to all the proxy servers and it maintains the index of the data information by all the proxy servers.

Fig.3.1.1 Illustration of Node Probability
At first, the user sends the request to the main cloud server about the “hi.doc” file. Then the main cloud server will forward the request to the exact proxy. The proxy server gives back the information to the main cloud server. Finally, the proxy server will send the file to the user. In this case the main cloud server can handle multiple user requests. The proxy server helps to decrease the acknowledgment time and gives the reply to the users in a proper manner.

V. CONCLUSION AND FUTURE ENHANCEMENT

Everything starts with an idea, and then we have to analyze the idea step by step. Based on the implementation procedure we will get results. Data encryption is provided by exchanging link keys between each device. The signature payload plays a big role on performance of the network. I have developed model of key exchange integrated into the sensing function of beacon enabled IEEE 802.15.4 cluster. The results show important impact of the ratio of the event sensing reliability and key update threshold on the clusters energy consumption.

VI. REFERENCES


AUTHORS PROFILE:

NAME: Kolan.Saritha, PG Scholar, Dept of CSE, MRECW, Dist: secunderabad, Telangana state, India, sarithakolan@gmail.com.
NAME: K. Ramesh Babu, Associate Professor & HOD, Dept of CSE, MRECW, Maisammaguda, Secunderabad, Telangana State, India, krubabu@gmail.com