International Journal of Applied Engineering Research ISSN 0973-4562 Volume 15, Number 7 (2020) pp. 628-630

Analysis and Detection of Malware Using Intrusion Detection Technique for a Private Cloud

Bhagya Roy[1] and Dr. Joby P P[2]

[1]*Dept. Computer Science and Technology, St. Joseph's College of Engineering and Technology, Palai, Kerala, India.*

[2]*Dept. Computer Science and Technology, St. Joseph's College of Engineering and Technology, Palai, Kerala, India.*

Abstract

Network security is one of the most promising sectors of today's world. For the easy access and storage most of the data's are not being kept in the computer but instead it is kept in a place called "Cloud". Cloud doesn't require computer memory and can be accessed from anywhere. Security is the main concern when we are using cloud. Files and folder which are getting uploaded and downloaded from the cloud should be free from malware. So the analysis and also detection plays a very important role. Intrusion Detection System (IDS) is used to study about malware and is being used along with a private cloud.

Keywords: Cloud, Security, Intrusion Detection

I. INTRODUCTION

Cloud computing is one among the emerging technologies which provide performance enhancement and also make use of technology smartly. In cloud nothing is stored in the computer; instead it is stored in a place called "cloud". Most of the organizations are using cloud for their storage because it provides unlimited storage, so no worries about running out of storage. Organization uses mainly three services models including SaaS (Software as a Service), IaaS (Infrastructure as a Service) and PaaS (Platform as a Service) and deployment models including public, private, hybrid and community cloud. The advantages of cloud computing are cost-efficient, easy to maintain, backup and recovery etc.

Rather than having many advantages, cloud computing also has disadvantages. Before one get registered to a cloud, one should be aware that we are surrending all our sensitive information to a third party server provider of a cloud. This is obviously a serious risk. This can be avoided for a extend by choosing a trustworthy service provider. Threats and attackers are the other issues in cloud. Since data is stored in cloud, it is vulnerable to external attack or threats. A public cloud is the most used deployment model but for accessing some features, paid versions should be taken which might be practically not possible. So, here a private cloud which is created for a small organization is described. A private cloud can act as a 'protective fence' built between an organization and attackers.

II. WHAT IS PRIVATE CLOUD?

Basically there are four types of cloud including public, private, hybrid and community cloud. Private clouds are models developed for and by IT department of a particular organization behind their own firewall. It involves secure and distinct cloud based environment. This model is similar to Local Area Network (LAN).But it has a virtual environment that discard many security issues and provide security.

Some key properties of private cloud are described below:

- No outside resources is needed to determine the private cloud
- Support for protocols and linguistic transparency
- Enable information exchange audit
- Inter-cloud service exchange
- Higher reliability and performance
- Customizable and great control over hardware performance
- Cost and energy efficiency

Data encryption and security should be done for secure computing. This is generally done at the IP layer level using IPsec or at DTLS (protocol layer).The files and folders that are getting uploaded or downloaded to and from cloud should be free from malware. Malware are set of instructions that run on a computer and make it do something that an attacker wants to do.

III. MALWARE DETECTION METHODS

One of the significant challenges within the development of secure cloud is related to correct identification and detection of malware. This is due to the reality that, within the majority of cases, malware is the first factor of initiation for large scale. Distributed Denial of Service (DDoS) attacks, phisphy and email spamming etc. are some examples. There is huge effort made to study about the behaviour of certain malware in Internet. Generally they are termed as intrusion Detection System (IDS). IDS are a system that alert when some suspicious activity had generated in the network traffic. It scans a network for any unusual activity. Sometimes false alarms can

also be generated. So the organization nee d to configure the IDS software when they first install them.

IDS can be classified into five types:

- Network intrusion Detection System
- Host intrusion Detection System
- Protocol intrusion Detection System
- Application intrusion Detection System
- Hybrid intrusion Detection System

IV. DETECTION METHODS OF IDS

There are two types of detection methods. First, Signature based method and second, Anomaly detection method.

A. Signature based method

Signature based detection detects the attack on the premise of the particular pattern like number of bytes (1‘s and 0‘s) within the network traffic. It also detect on the premise of already known malicious instruction sequence that is employed by malware. The detected pattern (signature) already exists in system but it is quite difficult to detect the new malware attack as their pattern isn‘t known.

This is the simplest form of detection. Most of the malware are in the form of PE (Portable Executable) format, which is the common form for windows operating system. Malware detection is generally software and is deployed at the desktop use. Whenever the scanning operation starts, it scans all the files and list out all the suspicious files, scanner check the hash value or file‘s‘ signature database. A signature database is a database in which signature values of all the known malwares are stored by using reverse engineering techniques with low false positive rates.

In signature based, the traffic is compared with the known signature present in the database of possible attacks. To detect an attack properly, the signature analysis and matching should be accurate. Sometimes if the detection has a small variation from the database then the system might not be able to correctly identify. For example, “I Love You” is a common virus that affects a computer. Instead of “I Love You” if it is “Love You” the system will fail to detect the threat.

Signature database must be maintained fully updated, almost on each day from the antivirus labs like McAfee, Symantic, TrendMicro and other security providers. If the signature isn‘t up to the point, chances are high that the IDS system will fail to detect a number of intrusion attacks. The opposite disadvantage is that they need little or no information about the previous request when processing the new one.

B. Anomaly detection method

Anomaly detection method is also known as outlier detection. This type of detection is generally developed for finding unknown threats using certain algorithms. They are generally used to reduce bank frauds. Medical problem or text errors. If any unexpected happening occurs in the data set, it can also be termed in the category.

It was developed to detect unknown malware because more and more new malware are developing rapidly. Anomaly IDS uses machine learning techniques to form a trust worthy activity model and anything coming in is compared thereupon that mode and is declared suspicious, if it is not found in model. Anomaly is more generalizes than signature based because it uses machine learning method and is also more trained. There are three types of anomaly detection techniques, unsupervised anomaly detection, supervised anomaly detection, semi-supervised anomaly detection.

A number of anomaly detection techniques are made but due to their complexity in statics measure they lack scalability. Many of the detection techniques require prior knowledge thus it make them unsuitable for cloud. One of the outstanding and famous machines learning classification method which can be used to design IDS is by Support Vector Machine (SVM). Mathematical tractability and geometric interpretation makes SVM more powerful When compared to traditional SVM, one class SVMs provide maximum separation between samples of known threats. Only some threats lie on the other side.

V. IMPLEMENTATION

The whole system is divided into two parts, cloud part and malware part. The whole cloud part is implemented using a private cloud and the malware part include analysis and detection of different malwares.

A. Private cloud

The private cloud is done using the help of OwnCloud built with the help of Ubuntu 16.04 and virtual box. At the time of installation the organization can set its own username and password and whenever the user login using virtual box the last login details will be shown. The advantage of using OwnCloud is that it is easy to develop and can be configured as our requirement. Files can be stored to cloud easily and also it can be stored to computer if needed. The IP of our OwnCloud is set static so that it can only be accessed through that particular IP address. Fig1 shows a typical login page of owncloud.

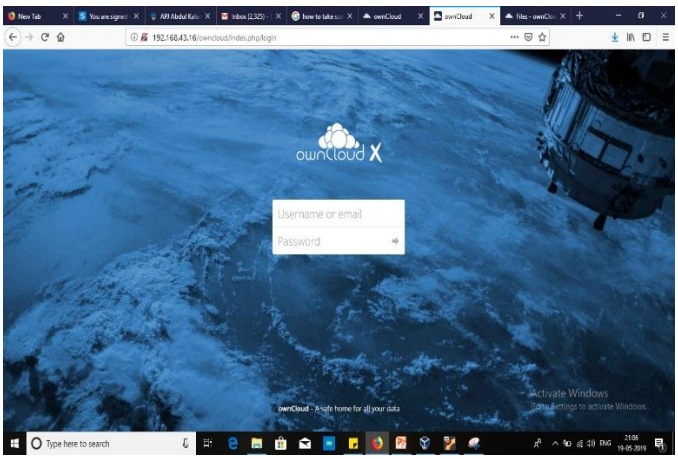

Fig. 1. OwnCloud Login Page.

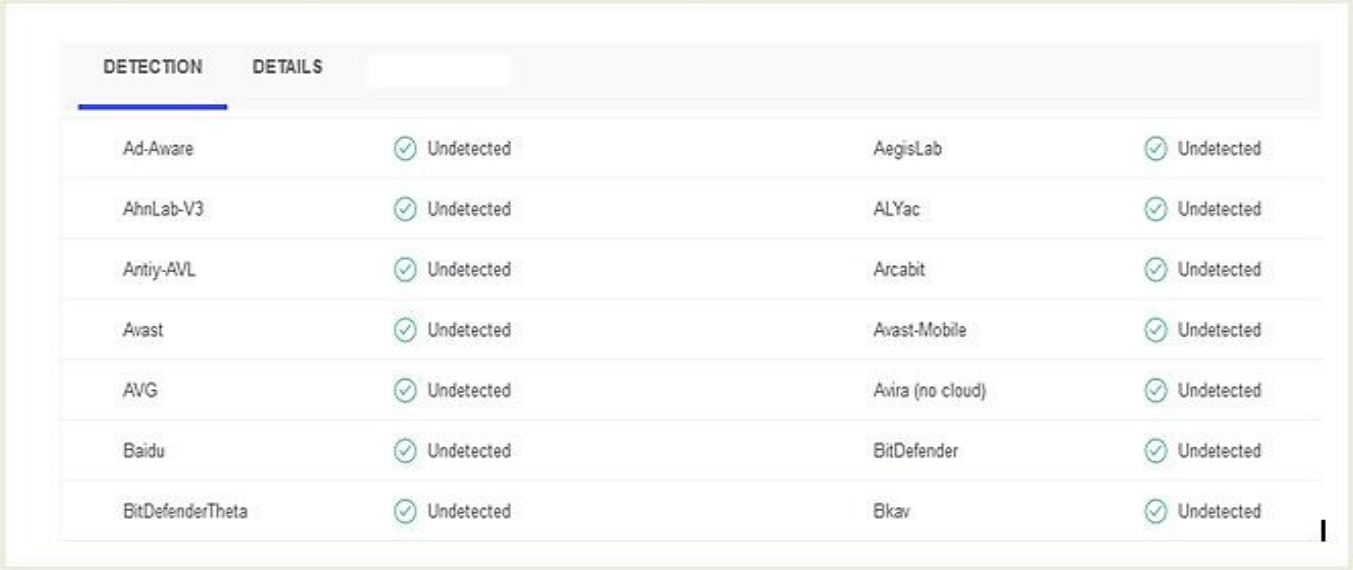

Fig. 2. Malware detection

B. Malware identification

The malware identification is done using Intrusion detection technique which is a combination of both signatures based and anomaly based. The main advantage is that both known and unknown malware can be detected. The process is a follows. Users logins to the private cloud and whenever he wants to upload a file to the cloud, he selects the file and before it get uploaded the scanning operation takes place with the help of cryptographical algorithm like MD5,SHA-1 and SHA-256. The analysis and detection is done using hash values (Signature detection) and SHA-1 and SHA-265 can be used for anomaly detection along with trained malware set. So, only after scanning the selected file, it can be uploaded to the cloud. Finally a complete report about the analysis and detection can be retrieved.

VI. CONCLUSION

Protecting cloud from malware is one of the main concern in cloud computing. The data which is carried to the cloud should be secure. So, a combination of signature and anomaly detection is used along with a private cloud. From the analysis it can be seen that malware detection is possible using this combination and it is not that much time consuming. It is also user friendly.

REFERENCES

[1] FarzadSabahi,"Cloud computing Security threats and responses "Communication Software and Networks(ICCSN)".2011 IEEE 3rd International Conference.

[2] DeyanChen,Hong Zhao," Data Security and Privacy Protection Issues in Cloud Computing, " 2012 IEEE International Conference on Computer and Electronics engineering.

[3] Arneja, Parminder Singh, and Sidharth Sachdev. "Detailed Analysis of Antivirus based Firewall and Concept of Private Cloud Antivirus based Firewall." International Journal of Computer Applications 111.4 (2015).

[4] M. R. Watson, N. u. h. Shirazi, A. K. Marnerides, A. Mauthe and D. Hutchison, "Malware Detection in Cloud Computing Infrastructures," in IEEE Transactions on Dependable and Secure Computing, vol. 13, no. 2, pp. 192-205, March-April 1 2016.

[5] Liu, Hui, and Yonghui Cao. "The research on search algorithms in the machine learning." networks 1.2 (2013).

[6] NesrineKaaniche,AymenBoudguiga, Maryline Laurent, "ID Based Cryptography for Secure Cloud Data Storage,"Cloud Computing (CLOUD), 2013 IEEE Sixth International Conference.