Malware Detection in Cloud Environment (MDCE)

https://doi.org/10.3991/ijim.v11i2.6575

Mahmoud M. El-Khouly
Helwan University, Cairo, Egypt
melkhouly@yahoo.com

M. Samir Abou El-Seoud
The British University in Egypt (BUE), Cairo, Egypt
selseoud@yahoo.com

Abstract—Since cloud computing technology is growing day by day, it comes with many security problems, especially from threats such as malware. As more services migrate to the cloud architecture, the cloud will become a more appealing target for cyber criminals. In this paper, we present the current threats to the cloud environment, and the proposed detection systems for malware in the cloud environment. We then present a multiple detection system that is aimed at combating the spread of malware by cloud environment.

Keywords—Malware, Security, Cloud Environment

1 Introduction

The National Institute of Standards and Technology (NIST) (http://www.nist.gov/itl/cloud) defined five essential characteristics of cloud computing, namely: on-demand self-service, broad network access, resource pooling, rapid elasticity or expansion, and measured service. Also, cloud computing is described as a dynamic and often easily extended platform to provide transparent virtualized resources to users through the Internet. Cloud computing architecture consists of three layers: (i) Software as a service (SaaS); (ii) Platform as a service (PaaS) and (iii) Infrastructure as a service (IaaS). The clouds are also viewed as five component architectures that comprise (clients, applications, platforms, infrastructure and servers). The current clouds are deployed in one of four deployment models: (a) public clouds in which the physical infrastructure is owned and managed by the service provider. (b) community clouds in which the physical infrastructure is owned and managed by a consortium of organizations. (c) Private clouds in which the infrastructure is owned and managed by a specific organization. And(d) Hybrid clouds that include combinations of the previous three models.

There are new concepts introduced by the clouds, such as, resource sharing and centralized shared data, create new security challenges. The direct access or indirect usage of cloud infrastructure amplify cloud vulnerabilities and threats. As clouds become more popular, security concerns grow bigger. Clouds are more sensitive to

Distributed Denial of Service (DDoS) attacks due to the availability of resources and the elasticity of the architecture. Many researchers provide surveys that cover specific areas of cloud security concerns and proposed solutions. This survey is categorized in threats, vulnerabilities, attacks, and other security and privacy issues that face the cloud [1] [2].

Recent product releases, such as Apple's I Cloud [3], and established products, such as Dropbox [4], have proven that remote storage and excellent access to data across multiple devices are common features for consumers. In the future, we will see an increase in the dependence of cloud computing as consumers increasingly move to mobile platforms for their computing needs.

In this paper, we review previous work on malware detection, both conventional and in the presence of storage in order to determine the best approach for detection in the cloud. We also argue the benefits of distributing detection throughout the cloud and present a new approach to coordinate detection across the cloud.

1.1 Cloud Security Categories

We can categories the cloud security according to (Network, access control, and data) as shown in figure 1.

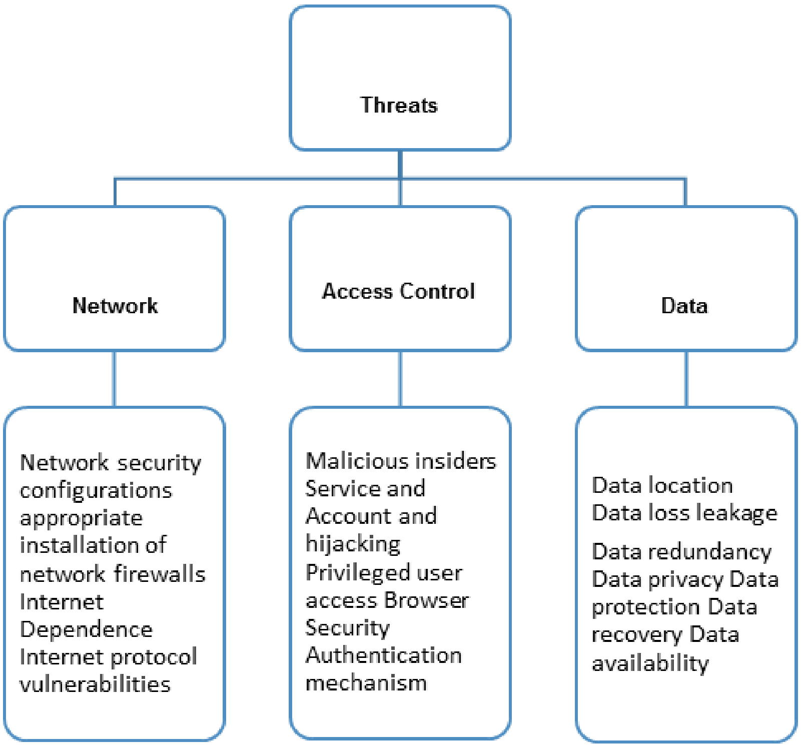
Threats
Network
Access Control
Data
Network security configurations appropriate installation of network firewalls Internet Dependence Internet protocol vulnerabilities
Malicious insiders Service and Account and hijacking Privileged user access Browser Security Authentication mechanism
Data location Data loss leakage
Data redundancy Data privacy Data protection Data recovery Data availability

Fig. 1. Cloud Security Categories [5]

The rest of this paper is organized as follow: Section II, provides background to the research area, specifically: cloud technologies, security in the cloud, malware detection and detection in the cloud. Section III, presents the proposed model. Section IV, focusses on remarks of malware detection at the hyper visor level. Finally, section V, summarizes the points raised in this paper.

2 Background

A hybrid system of two detection methods:

2.1 Static analysis: Signature Optimizing Pattern Matching

There are several new viruses detected; therefore, it becomes necessary to add their signatures to a library. To this end, a failure comparisons increase, which would negatively affect the efficiency of the signature matching procedure. Based on the virus characteristic of self-replicating and seasoning, this system proposed optimizing policy focus on Signature library; one common feature of virus is that it will scan targeted files and inject the malicious code into the normal files. So lots of replicas coexist within one system. So when any virus is detected by signature match, this virus signature is temporarily stored, so the other replicas do not need to match against the other large amount of signatures in the actual signature library. So this pre-comparison with already-detected viruses will reduce the signature matching times. [6]

2.2 Heuristic Detection Method

Antivirus software often used one or several techniques proactively detect malware. This method is dependent on analysing suspicious file's characteristics and behaviour to determine whether it is indeed a malware, Heuristic analyser (or simply, a heuristic), i.e. a technology in virus detection, which cannot be detected by antivirus databases. It allows detecting objects, which are suspected as being infected by unknown or new modification of known viruses. Files which are found by the heuristic analyser are considered to be probably infected. [7]

An analyser usually begins by scanning the code for a suspicious attributes (commands) characteristic of malicious programs. This method is called static analysis. For example, many malicious programs search for executable programs, open the files found and modify them. A heuristic examines an application's code and increases its "auspiciousness counter" for that application if it encounters a suspicious command. If the value of the counter after examining the entire code of the application exceeds a predefined threshold, the object is considered to be probably infected.

3 Proposed System

Our paper proposes a malware detection system to be built on cloud environment, a cloud computing which is a new service and an information delivery model that utilizes existing technologies. The proposal of this work is to find the optimal solutions to the problems of anti-viruses and improve performance and find possible alternatives for a better working environment without problems with high efficiency and flexibility. We used the best traditional methods and modern to detect virus systems, for unknown and already detected viruses through the signatures and the Heuristic. We connect these processes and initial database to cloud computing environment to be lighter weight and processing speed and performance; we used a file transfer protocol (FTP) for connect between the database & the internal processes of the detection system is located on the host in cloud computing; We used the technique of detected in real time (RTP) to detect any suspicious attack on real time for working, In addition sending notifications to the user in the end -host if there an attack or suspecting files, Thus the user is using the action required for Eliminate or fix. In case finding cases of suspecting or unknown this virus added to the database.

Figure (2), shows the simple outline of operations in our system in cloud computing.

4 Remarks of the System

Our project includes two types of protection built in remote-server protection; make sure that it has a backup system by File Transfer Protocol (ftp); FTP is normally used to transfer files between computers on a network. Cloud FTP enables files to be transferred to Storage Clouds, for transforming data and process to the cloud [8].

This process saves the latest malware protection in a local cache on your computer so that it protects your PC even when you aren't connected to the cloud.

In view of different detection, methods must be combined to determine whether a file is secure to open, access, or execute. Several variables may impact this process, to be more powerful and safe at malware Known and unknown to continuous update of the database of viruses and automatically.

Thus, in today’s antivirus programs, static analysis is used in combination with dynamic analysis. The idea behind this combined approach is to emulate the execution of an application in a secure virtual environment; the following figure shows the detection rates for viruses of this system and Interface scan.

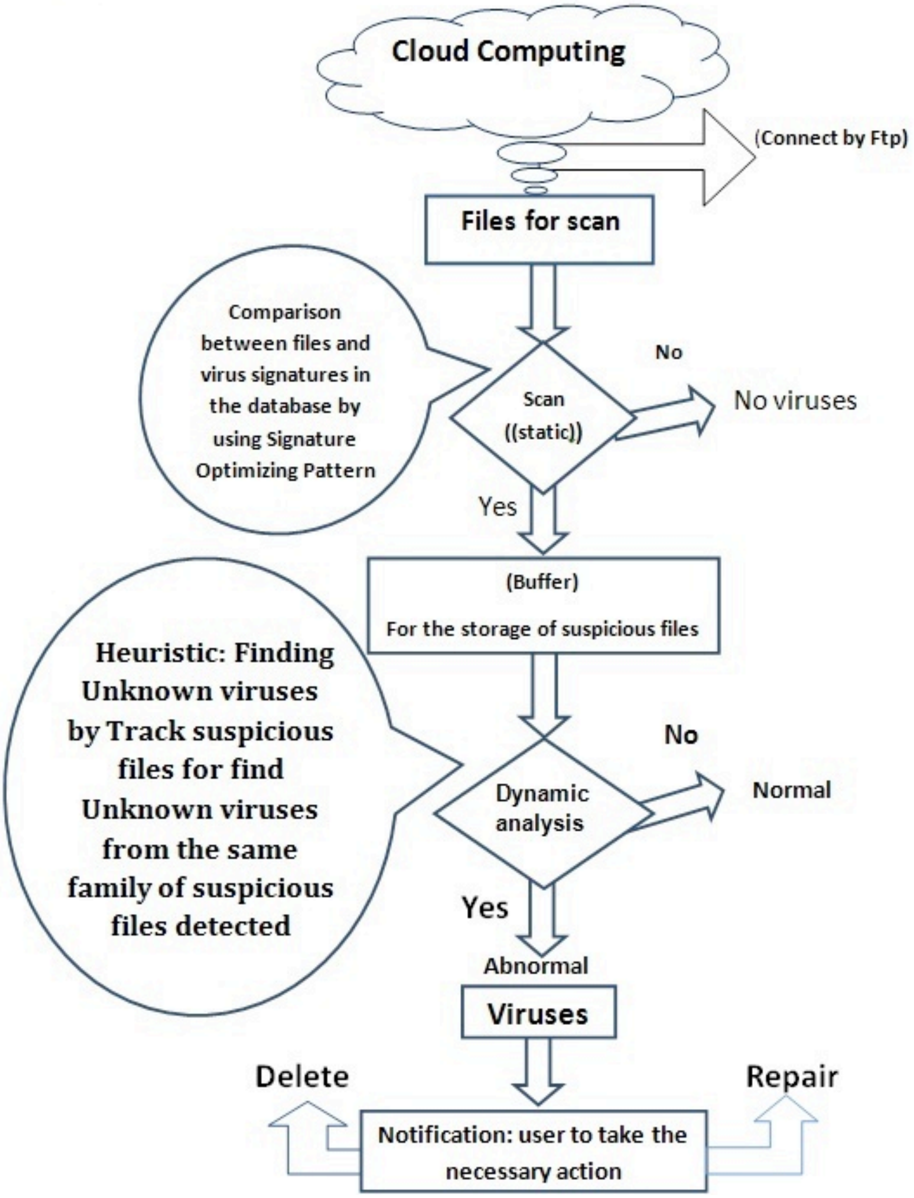
Cloud Computing
(Connect by Ftp)
Files for scan
Comparison between files and virus signatures in the database by using Signature Optimizing Pattern
Scan ((static))
No
No viruses
Yes
(Buffer)
For the storage of suspicious files
Heuristic: Finding Unknown viruses by Track suspicious files for find Unknown viruses from the same family of suspicious files detected
Dynamic analysis
No
Normal
Yes
Abnormal
Viruses
Delete
Repair
Notification: user to take the necessary action

Fig. 2. Simple outline shows the processes used in this system [9]

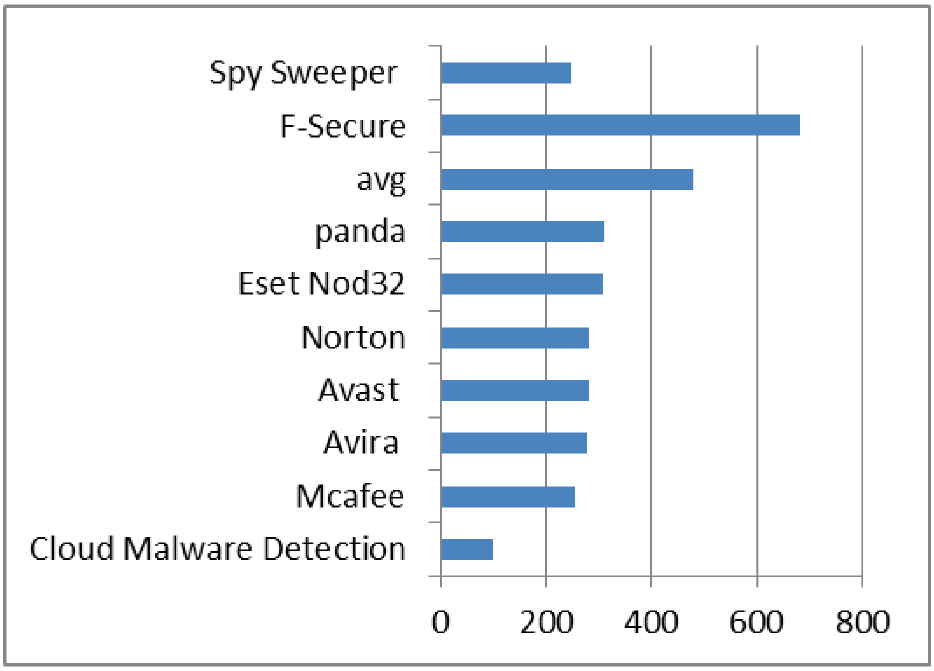

Fig. 3. Size (MB) of each installed anti-virus software - has been download updates after installation to being included in the results. [9]

5 Conclusion

A system for combined malware detection systems and cloud computing environments has been introduced, all running binaries and malware are intercepted by submitting to one or more analysis engines. A complete check against a signature database to detect yet unknown exploits or malware. In the future, we will see an increase in the dependence of cloud computing as consumers increasingly move to mobile platforms for their computing needs. Thus, in today's antivirus programs, static analysis is used in combination with dynamic analysis. The idea behind this combined approach is to emulate the execution of an application in a secure virtual environment; the following figure shows the detection rates for viruses of this system and Interface scan.

In this system, we have used traditional detection techniques as per static signatures and dynamic detection technology. Then, we have chosen for safer system methods as well as speed and modern to rival existing anti-virus. The proposal of this work is to find the best solutions to the problems of anti-viruses and improve performance and find possible alternatives for a better working environment without problems with high efficiency and flexibility. We used the optimal traditional methods and modern to detect virus systems, for unknown and already detected viruses through the signatures and the Heuristic.

6 References

[1] Cyril1, B. Rex , DR. S. Britto Ramesh Kumar, Cloud Computing Data Security Issues, Challenges, Architecture and Methods- A Survey, International Research Journal of Engineering and Technology (IRJET), Volume: 02 Issue: 04 | July 2015

[2] Ruchi U. Samudre, Prof. Vaishali R. Patel, Department of Information Technology SVM Institute of Technology Bharuch 392-001,

[3] Subashini, S., V. Kavitha s.l "A survey of security issues in service delivery models of cloud computing." ScienceDirect, Journal of Network and Computer Applications, pp. (1-11) January (2011).

[4] Shirlei Aparecida de Chaves, Rafael Brundo Uriarte and Carlos Becker Westphall "Toward an Architecture for Monitoring Private Clouds." S.l. IEEE December (2011).

[5] Rola Motawie, Mahmoud M. El-Khouly, Maged Hussien Wafy, "Addressing Security Issues in Cloud Computing", European Journal of Scientific Research, Volume 138 Issue 2, 2016.

[6] Carlin, S., & Curran, K. "Cloud computing security. International Journal of Ambient Computing and Intelligence," 3, 14-19, (2011). https://doi.org/10.4018/jaci.2011010102

[7] Petty, C., & Tudor, B. "Gartner says worldwide cloud services market to surpass $68 billion in 2010." [Online] http://www.gartner.com/it/page.jsp?id=1389313

[8] Gujarat, India, A Survey on Secure Access and Storage of Data in Cloud Computing, International Journal of Engineering Technology Science and Research IJETS R www.ijetsr.com ISSN 2394 – 3386 Volume 2, Special Issue September 2015

[9] Safaa Salam Hatem, Maged H. wafy, Mahmoud M. El-Khouly, "Malware Detection in Cloud Computing", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 5, No. 4, 2014.

7 Authors

Mahmoud El-Khouly, Head of Information Technology, Faculty of Computers and Information, Helwan university, Egypt, (e-mail: elkhouly@fci.helwan.edu.eg).

Samir Abou-Elsoud, Basic Science Coordinator, Faculty of Informatics and Computer Science, The British University in Egypt, (e-mail: samir.elseoud@bue.edu.eg)

This article is a revised version of a paper presented at the BUE International Conference on Sustainable Vital Technologies in Engineering and Informatics, held Nov 07, 2016 - Nov 09, 2016 , in Cairo, Egypt. Article submitted 21 December 2016. Published as resubmitted by the authors 03 March 2017.