IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-6, Issue-11, Nov 2018 E-ISSN: 2347-2693

Malware Detection In Cloud Computing

Aswin Sadanandan[1*], T. Poovarasan[2], V. Kavitha[3], N. Reavthy[4]

[1,2]Master of computer applications, Hindusthan College of Arts and Science(Autonomous), Affliciated by Bharathiar University , Coimbatore, Tamil Nadu, India
[3,4]Hindusthan College of Arts and Science (Autonomous), Affliciated by Bharathiar University, Coimbatore, Tamil Nadu, India

[*]*Corresponding Author: aswinkp00@gmail.com, Tel.: +91 8903084687*

Available online at: www.ijcseonline.org

Accepted: 20/Nov/2018, Published: 30/Nov/2018

***Abstract*—** In recent years the usage of cloud computing were emerged in big aspects. Hence the security of this big systems were in danger due to the intrusion and stealing of personal data. Inspite there are many primitive measures and antivirus tools were used in the cloud but they are not much effective in nature of modern malwares. Inorder to withstand or recover quickly from difficult conditions the cloud has to react towards not only to the known threats, but also to prevent against the new objection. This paper includes in about an approach in detection of malwares in cloud infrastructure. This approach provides greater efficiency in detection of malwares enhanced forensics capabilities and improved deployability. In this paper we join together detection techniques, Behavioral Blocking and Heuristic Analysis or Pro-Active Defense. Using this mechanism we find that cloud-malware detection provides better detection against recent threats compared to a single antivirus engine and a 98% detection rate across the cloud environment.

***Keyword*—** Cloud computing,threats,antivirus,security,deployability,resilience,malware.

I. INTRODUCTION

Security may be the most important aspect in cloud computing. The cloud services are distinguished within the private,public and industrial domains, many of these services are most necessary in the field of cloud computing, hence security and flexibility are more important. This facilities provides cloud services more reliable to more and more user of the technology. Instead of increasing the use of cloud computing technology. It pays way for more security risks. The cloud services can be secured by using latest security tools, but we can't make sure that all data are secured over some-where in the internet. The possibilities are that the security attacks can occurs when the user's accessing the its data. The malware can be accessed by the end users. The intruder is able to access the organization's computer and control it in some way to view and access the resources.

- **Challenges in cloud computing :**

As per the recent report ,discuss about the top 10 security concern pertain to cloud computing which include- data breaches, Hijacking of accounts, Insider threat, Malware injection, abusing cloud services,insecure APIs, DDoS attacks, Insufficient Due Diligence, shared vulnerabilities, and data loss.

In this paper we proposed a new model for the detection functionality that were performed by the antivirus software.

- **Intrusion detection system (IDS) :**

An intrusion detection system (IDS) is a device or software application that monitors a network or systems for malicious activity or policy violations. Any malicious activity or violation is typically reported either to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system combines outputs from multiple sources, and uses alarm filtering techniques to distinguish malicious activity from false alarms.

While there are several types of IDS, ranging in scope from single computers to large networks,[1]. the most common classifications are network intrusion detection systems (NIDS) and host-based intrusion detection systems (HIDS). A system that monitors important operating system files is an example of a HIDS, while a system that analyzes incoming network traffic is an example of a NIDS. It is also possible to classify IDS by detection approach: the most well-known variants are signature-based detection (recognizing bad patterns, such as malware) and anomaly-based detection (detecting deviations from a model of "good" traffic, which often relies on machine learning). Some IDS have the ability to respond to detected intrusions. Systems with response capabilities are typically referred to as an intrusion prevention system.

- **N-version protection** :

Second, the identification of malicious and unwanted software should be determined by multiple, heterogeneous

detection engines in parallel. Similar to the idea of N-version programming, we propose the notion of N-version protection and suggest that malware detection systems should leverage the detection capabilities of multiple, heterogeneous detection engines to more effectively determine malicious and unwanted files.

II. CLOUD COMPUTING ATTACKS

A. Denial of Service (DoS) attacks:

Some security professionals have argued that the cloud is more vulnerable to DoS attacks, because it is shared by many users, which makes DoS attacks much more damaging. When the Cloud Computing operating system notices the high workload on the flooded service, it will start to provide more computational power (more virtual machines, more service instances) to cope with the additional workload. Thus, the server hardware boundaries for maximum workload to process do no longer hold. In that sense, the Cloud system is trying to work against the attacker (by providing more computational power), but actually—to some extent—even supports the attacker by enabling him to do most possible damage on a service's availability, starting from a single flooding attack entry point. Thus, the attacker does not have to flood all n servers that provide a certain service in target, but merely can flood a single, Cloud-based address in order to perform a full loss of availability on the intended service .

B. Cloud Malware Injection Attack:

A first considerable attack attempt aims at injecting a malicious service implementation or virtual machine into the Cloud system. Such kind of Cloud malware could serve any particular purpose the adversary is interested in, ranging from eavesdropping via subtle data modifications to full functionality changes or blockings. This attack requires the adversary to create its own malicious service implementation module (SaaS or PaaS) or virtual machine instance (IaaS), and add it to the Cloud system. Then, the adversary has to trick the Cloud system so that it treats the new service implementation instance as one of the valid instances for the particular service attacked by the adversary. If this succeeds, the Cloud system automatically redirects valid user requests to the malicious service implementation, and the adversary's code is executed. A promising countermeasure approach to this threat consists in the Cloud system performing a service instance integrity check prior to using a service instance for incoming requests. This can e.g. be done by storing a hash value on the original service instance's image file and comparing this value with the hash values of all new service instance images. Thus, an attacker would be required to trick that hash value comparison in order to inject his malicious instances into the Cloud system. The main idea of the Cloud Malware Injection attack is that an attacker uploads a manipulated copy of a victim's service instance so that some service requests to the victim service are processed within that malicious instance. In order to achieve this, the attacker has to gain control over the victim's data in the cloud system (e.g. using one of the attacks described above). In terms of classification, this attack is the major representative of exploiting the service-to-cloud attack surface [3]. The attacker controlling the cloud—exploits its privileged access capabilities to the service instances in order to attack that service instance's security domains.

C. Side Channel Attacks:

An attacker could attempt to compromise the cloud by placing a malicious virtual machine in close proximity to a target cloud server and then launching a side channel attack. Side-channel attacks have emerged as a kind of effective security threat targeting system implementation of cryptographic system's resilience to side-channel attacks is therefore important for secure system design [4].

D. Authentication Attacks:

Authentication is a weak point in hosted and virtual services and is frequently targeted.There are many different ways to authenticate users; for example, based on what a person knows, has, or is. The mechanisms used to secure the authentication process and the methods used are a frequent target of attackers. Currently, regarding the architecture of SaaS, IaaS, and Paas, there is only IaaS offering this kind of information protection and data encryption. If the transmitted data is categorized to high confidential for any enterprise, the cloud computing service based on IaaS architecture will be the most suitable solution for secure data communication. In addition, the authorization of data process or management for those data belonged to the enterprises but stored on the service provider's side must be authorized by the user side (enterprises) to instead of the service providers. Most user-facing services today still use simple username and password type of knowledge-based authentication, with the exception of some financial institutions which have deployed various forms of secondary authentication (such as site keys, virtual keyboards, shared secret questions, etc.) to make it a bit more difficult for popular phishing attacks.

E. Man-In-The-Middle Cryptographic Attacks:

This attack is carried out when an attacker places himself between two users. Anytime attackers can place themselves in the communication's path, there is the possibility that they can intercept and modify communications.

III. BACK GROUND

1. Cloud computing:

Cloud computing is an information technology (IT) paradigm that enables ubiquitous access to shared pools of configurable system resources and higher-level services that can be rapidly provisioned with minimal management effort,

often over the Internet. Cloud computing relies on sharing of resources to achieve coherence and economies of scale, similar to a public utility.Third-party clouds enable organizations to focus on their core businesses instead of expending resources on computer infrastructure and maintenance.[1] Advocates note that cloud computing allows companies to avoid or minimize up-front IT infrastructure costs. Proponents also claim that cloud computing allows enterprises to get their applications up and running faster, with improved manageability and less maintenance, and that it enables IT teams to more rapidly adjust resources to meet fluctuating and unpredictable demand.Cloud providers typically use a "pay-as-you-go" model, which can lead to unexpected operating expenses if administrators are not familiarized with cloud-pricing models. Since the launch of Amazon EC2 in 2006, the availability of high-capacity networks, low-cost computers and storage devices as well as the widespread adoption of hardware virtualization, service-oriented architecture, and autonomic and utility computing has led to growth in cloud computing.

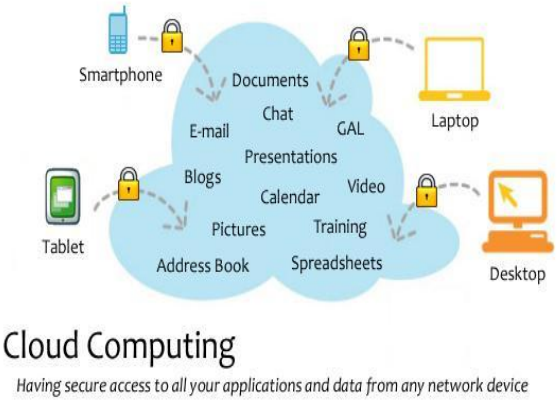

Figure 1. cloud computing

2. Related works

Evolution of cloud computing is start in early 1950 when large mainframe system were installed in schools and universities. These servers are connected to large number of dumb system (the system which doesn't have their processing power). Mainframe system are too costlier, because of that organization can't provide mainframe system to individual that's make the evolution of large server room's connected to dumb system i.e. known as time and resource sharing mainframe systems. Cloud computing has evolved through a number of phases which include grid and utility computing, application service provision (ASP), and Software as a Service (SaaS) But the overarching concept of delivering computing resources through a global network is rooted in the sixties. However, Malware detection in a Cloud Computing service was explicitly introduced in,what we now commonly refer to as cloud computing is the result of an evolution of the widespread adoption of Virtualization,

This paper proposes a malware detection system to be built on cloud environment to be safe by using the two techniques they are:

A. Behavioral Blocking :

US activity. Use this feature to ensure a higher level of protection against new, unknown, and emerging threats. After detecting malicious activity, Malware Behavior Blocking performs one of the following actions:

- **Block:** Prevents programs exhibiting malicious behavior from making changes to the computer.
- **Terminate:** Closes programs that exhibit malicious behavior.
- **Clean:** Closes programs that exhibit malicious behavior. If a program is verified to be athreat, deletes files and other objects associated with the malicious program.Malware Behavior Blocking analyzes program behavior to proactively protect against both known and unknown threats. Malware Behavior Blocking observes system events and blocks programs that exhibit malicious.

B. Heuristic Analysis or Pro-Active Defenses:

Heuristic analysis is a method employed by many computer antivirus programs designed to detect previously unknown computer viruses, as well as new variants of viruses already in the "wild".Heuristic analysis is an expert based analysis that determines the susceptibility of a system towards particular threat/risk using various decision rules or weighing methods. MultiCriteria analysis (MCA) is one of the means of weighing. This method differs from statistical analysis, which bases itself on the available data/statistics.

The threats on files kept in cloud by malware area unit increasing within the recent years. Resulting in increase in value in business through several access management policies area unit provided to guard the information kept in cloud, the malicious users attack the information exploitation malwares. In such a situation, it's necessary to guard the cloud knowledge exploitation in effective ways. Hence, a replacement intelligent agent to malware detection and hindrance model is projected during to boost the protection of cloud knowledge storage [2]. The main aim during this work is to find malware infected files whereas causation it from server to consumer and to produce a way or thanks to transfer the file firmly.

This work additionally focuses on up the energy potency in comparison with different existing system. By classifying the malwares supported their families; it's straight forward to spot them as every malware contains a signature. This can facilitate to find the malware infected file throughout transmission across systems and can be extremely economical in comparison with the prevailing systems. The main objective of the work is to find malware infected files

whereas transmission of the files from server to consumer and to produce a secure way to transfer files among users. So as to attain this, the malwares area unit is initially classified according to their families so they're compared with actual matching rule and most matching rule. By exploiting this, during this work the presence of malwares area unit detected [2]. During this work [2], a replacement rule for agent based mostly intelligent system for malware detection is projected. For this propose, a replacement feature choice rule known as fuzzy rule {based mostly primarily based mostly feature choice rule and a replacement classification rule known as an agent based rule matching call tree rule area unit projected. Additionally, an intelligent agent based mostly malware hindrance algorithms are additionally projected during this work for effective hindrance of malwares.

IV. PROPOSED SYSTEMS

This paper involves in the study of malware detection in cloud computing environment.First of all, SOA starts with a simple idea – the concept of *service*. This makes it possible to introduce other ideas, such as *service bus*, *service composition*, and *service virtualization*, each of which can be applied to the architecture of an enterprise to deliver benefits. As an architect, it is your job to evaluate the needs of your enterprise, and the costs of the different potential solutions, to determine which of these ideas should be applied, and how they should be applied, in your SOA.
An architect should always probe into the information given, about both requirements and solutions, to reach a level of understanding that goes deeper than the buzzwords. For example, it is often said that "SOA delivers enterprise agility". What does "agility" mean for your enterprise? Is it the ability to re-combine existing functions to meet changing customer requirements? Is it the ability to develop new functions rapidly? Is it the ability to scale operations to meet different levels of demand? Within the broad concept of SOA, there are three very different ideas that can help you meet these different agility requirements: service composition, model-driven development, and service virtualization. You can build all of these ideas into your SOA, but they each require different – and expensive – supporting infrastructure. You must choose your solution to fit the requirements.

This section will help you to match the features of SOA to the needs of your enterprise, so that you can determine the kind of SOA that is appropriate.

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. When finding cases of suspected, unknown virus Signature automatically added to our database system.

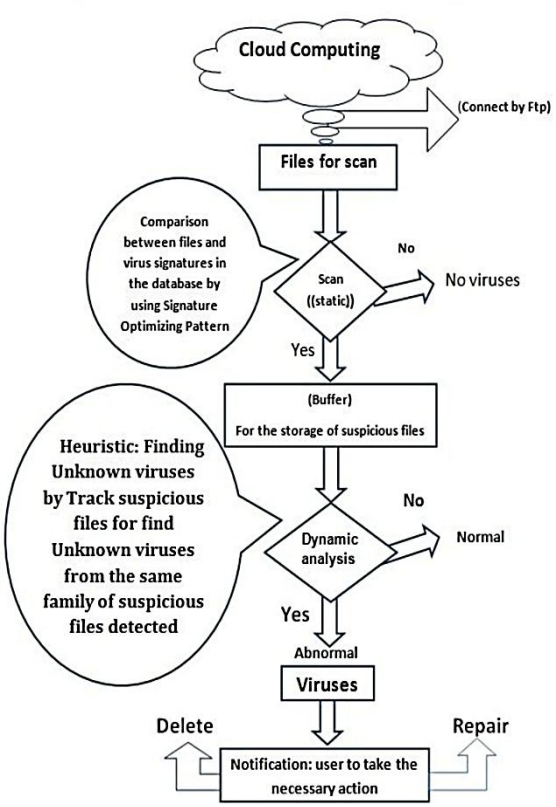

Figure 2, shows the simple outline of Mechanisms in the proposed system

Why cloud computing *a*pplied to C.M.D?
1) Reduction of costs – unlike on-site hosting the price of deploying applications in the cloud can be less due to lower hardware costs from a more effective use of physical resources.
2) Universal access - cloud computing can allow remotely located employees to access applications and work via the Internet.
3) Up-to-date software - a cloud provider will also be able to upgrade software keeping in mind feedback from previous software releases.
4) Choice of applications- This allows flexibility for cloud users to experiment and choose the best option for their needs.Cloud computing also allows a business to use, access and pay only for what they use, with a fast implementation time.
5) Potential to be greener and more economical – the average amount of energy needed for a computational action carried out in the cloud is far less than the median amount for an on-site deployment. This is because different organizations can share the same physical resources securely, leading to more efficient use of the shared resources.
6) Flexibility – cloud computing allows users to switch applications easily and rapidly, using the one that suits them

needs best. However, migrating data between applications can be an issue.

The proposed system 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. Consequently ,these processes saves latest malware protection in a local cache on your computer then send to cloud server, So that it protects your PC even when you aren't connected to the cloud.Elsewhere, our system also features a Lightweight, Dispute of the famous anti-virus Products. Figure 6, shows the effect of cloud on size comparison between Cloud malware detection (CMD) and famous antivirus.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 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 more-safe at malware Known and unknown to continuous update of the database of viruses and automatically.

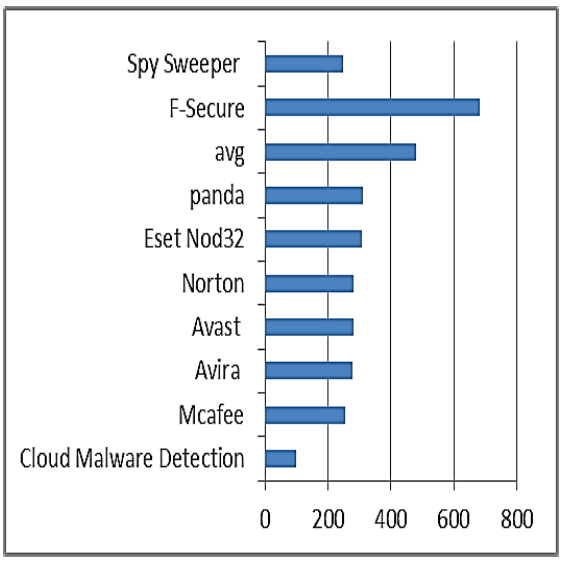

Fig. 3. Size (MB) of each installed anti-virus software has been download updates after installation to being include in the result

V. CONCLUSION AND FUTURE WORKS

The proposed system 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. Consequently ,these processes saves latest malware protection in a local cache on your computer then send to cloud server, So that it protects your PC even when you aren't connected to the cloud. Elsewhere, our system also features a Lightweight, Dispute of the famous anti-virus Products. Figure 6, shows the effect of cloud on size comparison between Cloud malware detection (CMD) and famous antivirus. 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 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 more-safe at malware Known and unknown to continuous update of the database of viruses and automatically.

REFERENCES

[1] Bo Li, Eul Gyu I'm " A signature matching optimization policy for antivirus programs" Electronics and Computer Engineering, Hanyang University, Seoul, Korea. © IEEE 2011

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

[3] Scott Treadwell, Mian Zhou "A Heuristic Approach for Detection of Obfuscated Malware", Bank of America, 1201 Main St, Dallas, TX 75202, © IEEE 2009.

[4]Lajos Nagy, Richard Ford, and William Allen, "N-version programming for the detection of zero-day exploits", In IEEE Topical Conference on Cybersecurity, Daytona Beach, Florida, USA, 2006.

[5] A. Ibrahim, J. Hamlyn-Harris, J. Grundy, and M. Almorsy, "Cloudsec: A security monitoring appliance for virtual machines in the iaas cloud model," in Network and System Security (NSS), 2011 5th International Conference on, Sept 2011, pp. 113–120.

[6] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," ACM Computing Surveys (CSUR), vol. 41, no. 3, p. 15, 2009.

[7] A. K. Marnerides, M. R. Watson, N. Shirazi, A. Mauthe, and D. Hutchison, "Malware analysis in cloud computing: Network and system characteristics," IEEE Globecom 2013, 2013.

[8] C. Wang, V. Talwar, K. Schwan, and P. Ranganathan, "Online detection of utility cloud anomalies using metric distributions," in Network Operations and Management Symposium (NOMS), 2010 IEEE. IEEE, 2010, pp. 96–103.

[9] S.K. Sharma, L. Gupta, "A Novel Approach for Cloud Computing Environment", International Journal of Computer Sciences and Engineering, Vol. 4, Issue.12, pp.1-5, 2014.

[10] S.L. Mewada, C. Srivastava, "A Novel Approach for Cloud Environment", International Journal of Computer Sciences and Engineering, Vol. 4, No.10, pp.1-15, 2010.

