© 2018 IJSRST | Volume 4 | Issue 5 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology

Shade Hope – A Protection Model

Abdul Laza[1], Madhavan B[2], Kapila Vani R K[3]

[1]Computer Science and Engineering, Prince Shri Venkateshwara Padmavathy engineering college, Chennai, Tamil Nadu, India

[2]Computer Science and Engineering, Prince Shri Venkateshwara Padmavathy engineering college, Chennai, Tamil Nadu, India

[3]Computer Science and Engineering, Prince Dr.K.Vasudevan college of engineering and technology, Chennai, Tamil Nadu, India

ABSTRACT

The cloud is considered to be one of the most emerging technologies all around the globe. Cloud differs massively from other methods rather than having a centralized server. Hence we present a protection model in order to present the cloud from the advanced persistent threats. The penetration the cloud leads the vulnerability to the data present in the cloud hence protection to the cloud is considered to be the one of the major action to be action to be taken. Hence we introduce the cloud watch technique by implementing the trust manager and monitor the cloud in order to prevent the cloud from penetration.

Keywords: Cloud computing, advanced persistent threats, centralized server, cloud watch, trust manager.

I. INTRODUCTION

The advantage of the cloud service provider enables certain advantages to the government agencies and the private sector. The current trend has established a massive hike towards cloud computing. They come up with economic benefits and transparency that suits many of the business organizations as well as users interest. It is the use of remote servers on the internet to store manage and process data rather than a local server. Initially, to host a website these are the following things you would need to do buy a stacked server, monitoring , and maintenance of your server. This leads to the setup expensive, troubleshooting problems can be tedious servers will be idle due to network traffic. After the cloud computing emergence no more buying expensive servers, scalability, cloud provider manage your servers. Various business organization are in detail concerned with the information security and reliability of information in the cloud.

There are several other issues which is related with end users ,communication channels. These simple security threats may in turn produce a very dangerous effects. Researchers have also identified various hacking techniques with respect to various applications .Hence the hackers probably invented various tools to penetrate into the cloud which are invented in other countries. These tools are invented to penetrate into the application and steal data. The main focus of anonymous users is to crack the data

A well-known cyber security company, Imperya Hacker Intelligence initiative report has found some of the breach holes in popular cloud service providers. They exposed that if a hacker get into client's computer where the services are installed, then they don't require any user login credentials for identity, to access the data. The experts found that, whenever services provide constant access towards the user, they share a security token that is stored over the Windows registry of the client's workstation. A switcher is

shared by the hacker through any mode of communication like e-mail or by cookies, which is automatically executed. This switcher replaces the original token with the hacker's token on the client's machine. Now the hacker is granted with access to the cloud account of the victim client.

Hence some mechanisms are implemented in this study to avoid the disaster by denial of service attack and recovery from such disasters. The main contributions of this paper are to develop a CCS reference architecture and a cloud security assessment model Cloud Trust that provides quantitative high level security assessments of IaaS CCSs and CSPs. Cloud Trust can assess the relative level of security offered by alternative CSPs or cloud architectures.

II. RELATED STUDY

The trusted zone is the one who monitors the cloud, monitors the clouds, secure your cloud the performance issues occur in IT infrastructure, APIS, Application. To manage and monitor performance takes place in application performance management and unified infrastructure management in order to ensure privacy and to protect data.

These methods are implemented data residency the data residency manages the information regarding access, who manage to access data, law regulation, how to detect a data breach, will data remain in the cloud even after termination. Hence for this data residency, the methods used are data encryption it is the technique of converting clear text into the cipher text which can't be read by anyone other the specified user.

It provides completes invisible to the data. The encryption also saves the cloud from the internal and external threats, provides secured cloud enablement and deployment, it also meets privacy and residency regulations globally. These are the advantages of using data encryption. Hence the trusted zone is implemented as the trusted third party who monitors the cloud in order to provide security to the cloud. There have been research and implementations which involved the monitoring of activities in the cloud environment.. Agents are involved to monitor malicious activity that holds the logs of the action, place, time and by whom.

Services such as Microsoft's Azure and Amazon's EC2, allow users to instantiate on demand and thus purchase recisely the capacity they require when they require it. Some of these risks are self-evident and relate to the new trust relationship between customer and cloud provider. For example, customers must trust their cloud providers to respect the privacy of their data and the integrity of their computations. However, cloud infrastructures can also introduce non-obvious threats from other customers due to the subtleties of how physical resources can be transparently shared between virtual machines (VMs).

III. SYSTEM ARCHITECTURE

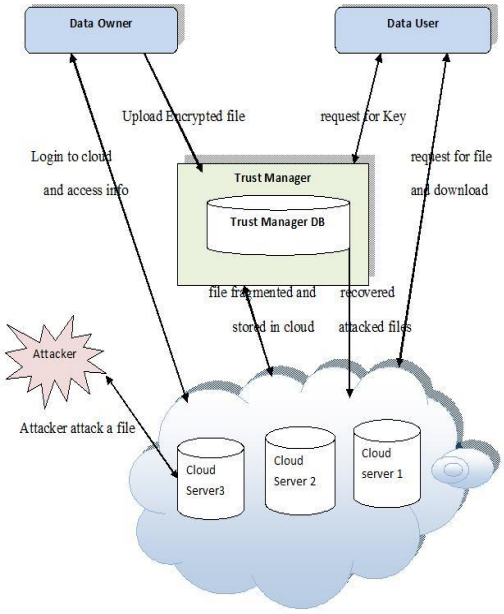

Figure 1

The main scope of the project is to protect files from internal and external attacks in the cloud server.

IV. EXISTING METHODOLOGIES

In this section, we discuss about some of the existing mechanisms that are used as proactive maintenance to avoid threats over the cloud.

1. Agents

Agents are autonomous entities in a particular environment, monitoring the actions and responses to the dynamic changes in the environment. Agents can communicate and can even form groups in order to solve complex issues. Agents must react instantaneously towards the change in infrastructure to detect the attacks or intrusion. Implementing such architecture is possible through connected sensors confined to certain action over the process or events. The detection by one agent may share related information to other agents so the task of repetition is reduced.

2. Audit trials

Audit trials are executed to monitor the events that come from different sources. They hold information related to the questions who, where, when and the operation. These are compared to the normal behaviour and if it seems to move in different path, then the action could be blocked or some alternate measures could be implemented.

3. Data Transfer Monitors

DTM are used to monitors API level communication that normally occurs between the cloud services. Some of the information may be private and they are not supposed to be share among the third-parties. Id of the tenants would be passed to the data controller so that they could take necessary actions upon the calls.

V. SECURITY THREATS

Some the security threats that could be identified over the cloud environment are provided below,

1. The attacker may be involved in the organization and he will have granted with access towards the login credentials of the internal users. This information may be utilized by himself or even be shared to others. Hence the certificate is more helpful to raise the standards of the cloud and to overcome these types of threats.

2. There are many threats that the users may not feel much vulnerable, but they do in some instance. Many attacks like shoulder behind attack or spoofing the communication without the use of keys to be shared, the hackers can easily trace out the passwords and access the cloud. Monitoring the passwords by screen capturing in hand held devices makes the hackers to easily trace the passwords and other credentials. Installation of some applications could disagree with the security and compliance and grants some of the access over the machines to the hackers.

3. There are many threats when any intruders get into the system of a client. Because tokens of various accounts could be replaced easily by the hacker's tokens The hackers can access accounts without the user login credentials and this is called "Man-in the cloud". The intruder can install tools that could do malicious activities like changing the SQL etc. Logging to the system of the client can let many paths to the hackers in accessing various accounts of the user.

VI. LIST OF ATTACKS

1. Disk injection

The attacker attempts to gain access to agency data by placing malicious code in the local attached storage of the targeted virtual machine and the attacker can conduct network surveillance inside the cloud. . This

attack becomes much more difficult if the local storage of the VM is encrypted. In such case, both the encryption must be compromised in order to complete the attack.

2. Side channel attack

First the Advanced Persistent Threats obtains access to the cloud and conducts surveillance. If the target is in a public cloud the only barrier to entry is a valid credit card to establish an account. The attacker instantiates Virtual Machines as needed to collect information on servers and Virtual Machines. To surveilance the cloud the attacker will run legitimate code or malware. This is known as side channelling.

3. CSP system admin

CSP sys-admins use VMM capabilities to migrate live VMs, to allow for hardware servicing without execution interruption, or to debug faults using core dumps and memory page snapshots. An attacker can repurpose utilities to compromise agency data. This is known as CSP system admin

4. Undetected configuration modification.

Restricting traffic to a single white listed IP address associate with an agency enclave is a common baseline security control- best practice for limiting access to resources provisioned in the cloud. It also provides the attacker with a mechanism to move resources across Trust Zones, for example by moving memory dumps, machine state, or entire VM instances from one physical machine to another. This is known as undetected configuration modification.

VII. PROPOSED METHODOLOGIES

The recovering of the attacked file is done with the help of the trust manager. The trust manager will have the backups for the list of the key generated hence in case of the attacker attacks a particular server, the attacker will get only one part of the whole encrypted content from only one cloud service provider. So there is no way that the data will not lose there might be chances such that if the attackers crash a particular file in case if the file is deleted or some unwanted character is added into the encrypted file content. The documented or the file can be recovered with the help of the trust manager.

The hacker will be identified with the help of the MAC address.

Based on the necessity of the cloud infrastructure different kinds algorithms could be implemented towards the encryption and for signatures or identity towards data integrity.

1. AES

Advanced Encryption Algorithm, high speed and low RAM requirements were criteria of the AES selection process. It requires 18 clock cycles per byte

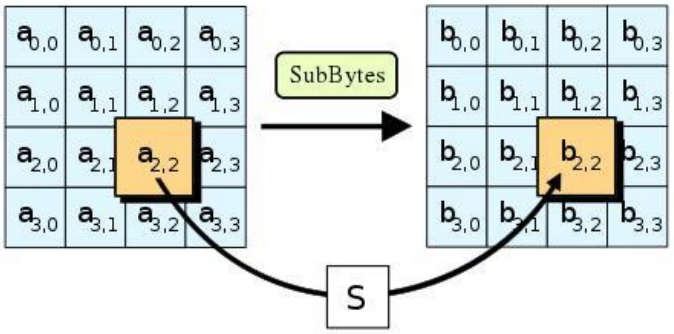

Figure 2. AES encryption

ALGORITHM

Add Round Key (state, w[0,N-1])
For round =1 step 1 to N-1
Sub Bytes (state)
Shift Rows (state)
Mix Columns (state)
Add Round Key (state, w[round*N,(round+1)*N-1)]
End for
Sub Bytes (state)
Shift Rows (state)
Add Round Key (state, w[N*N,(round+1)*N-1)]

2.Dynamic Block Partitioning

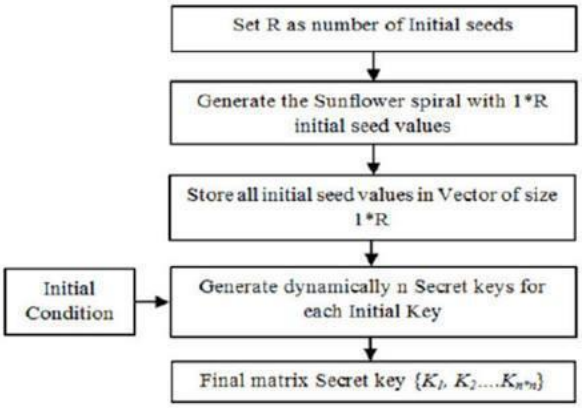

Figure 3. Dynamic block partitioning

ALGORITHM

Input: Blocks Bi, i<n, where n is the total number of blocks.

Output: Reallocated blocks Bi, i<n, where n is the total number of blocks.

Step 1: Blocks are stored in array like B[0], B[1],….,B[n]

Step 2: Choose any blocks in random manner where all blocks have status=”no”

Step 3: Set the status value to “yes” if it is allocated for the block for first time.

```
for(i=0;i<n;i++)
{
status=” yes”;
}
```

Step 4: Iterate all the blocks checking the status for “no” and assign the reallocated data to those blocks.

Step 5: After all the block’s register values are “yes”, then the blocks can be reallocated in any random manner but not repeating the same blocks in consecutive allocation.

VIII. USER CLASSES AND CHARACTERISTIC

1. Cloud Registration

Here the Cloud users have to register his account with appropriate rights whether it may be the data owner or data user. Based on the user type the options are given. The data owner can upload a file to cloud and the data user can download a file by giving a request to the Trust manager. The trust manager also has the login process and he can check the all information about the user, owner and cloud server. Each cloud server has the separate user id and password to check the information about the files and user.

2. Upload and fragment files

In this modal the data owner upload his files to cloud to save but first the file is encrypted and that encrypted content is fragmented into the files and store it into separate server location in a cloud. Also stored Uploaded information like MAC,IP address Time and date. Due to this action a file should be more secure in a cloud.The trust manager will split each encrypted file and stored it into database and also have one more copy to its database incase data is missed or corrupted he will replace the content of the file with exact location.

3. CCS Attacks

Incase if the attacker attacks a particular server, he/she will get the one part of the encrypted content of a file so data will not lose. If the attacker crash a file (Delete or add some unwanted character in a encrypted file content), we can also recover that file using the trust manager.

4. Recover attacked file

We recover a attacked files in a cloud with the help of the trust manager. Here the trust manager will check the file information if the attacker attacks a file, the trust manager will replace a original file to that particular server and protect a sever. This file is replaced by the trust manager only because he has the own copy and that is also the secure only because it is in encrypted format only then it will be replaced easily.

IX. FUTURE WORK

The aim of attacker to attack the information are classified into two types- general interest and Targeting particular individual. If the hacker does abuse of information because of general interest, then he tries attacking random user's information that have the breaches to easily loop into it. Hence the location of that user may not be tracked frequently. But in cases where the attacker tries to steal information or attacks of any specified user, then the probability of trying the same mechanism over the same user is high. This may be related to any business or finance information. Hence the location of the hacker is necessary to find. The hacker location can be identified by implanting the GPS tracker and finding the exact location from where the attack is done.

X. CONCLUSION

There have been research and implementations which involved the monitoring of activities in the cloud environment. This is helpful in creating certificates, which provides a proof for the society on the cloud. And the security is focused by different experts at different levels (based on architecture, entities etc.). Agents are involved to monitor malicious activity that holds the logs of the action, place, time and by whom. Hence the mechanism of implementing the trust manage is worthwhile in the cloud environment.

XI. REFERENCES

[1]. W. Jansen and T. Grance, "Guidelines on security and privacy in public cloud computing," NIST Spec. Publ. 800–144, National Institute of Standards and Technology, Gaithersburg, MD 20899, Dec. 2011.

[2]. P. Mell and T. Grance, "The NIST definition of cloud computing," NIST, Gaithersburg, MD, USA, Tech, Rep. SP 800-145, 2011.

[3]. P. Jamshidi, A. Ahmad, and C. Pahl, "Cloud migration research: A systematic review," IEEE Trans. Cloud Comput., vol. 1, no. 2, pp. 142–157, Jul.–Dec. 2013.

[4]. L. Vaquero, L. Rodero-Merino, and D. Moran, "Locking the sky: A survey on IaaS cloud security," Computing, vol. 91, no. 1, pp. 93–118, Jan. 2011.

[5]. T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, "Hey, you, get off of my cloud: Exploring information leakage in third-party compute clouds," in Proc. 16th ACM Conf. Comput. Commun. Security, 2009, pp. 199–212.

[6]. A. Sood and R. Enbody, "Targeted cyber-attacks-a superset of advanced persistent threats," IEEE Security Privacy, vol. 11, no. 1, pp. 54–61, Jan./Feb. 2013.

[7]. B. Krekel, "Capability of the people's republic of china to conduct cyber warfare and computer network exploitation," U.S.-China Economic and Security Review Commission, Northrop Grumman Corp., DTIC Document, 2009.

[8]. S. Zevin, Standards for Security Categorization of Federal Information and Information Systems, DIANE Publishing, 2009.

[9]. J. Somorovsky, M. Heiderich, M. Jensen, J. Schwenk, N. Gruschka, and L. Lo Iacono, "All your clouds are belong to us: security analysis of cloud management interfaces," in Proc. 3rd ACM Workshop Cloud.

[10]. Comput. Security Workshop, 2011, pp. 3–14. V. J. Winkler, Securing the Cloud: Cloud Computer Security Techniques and Tactics. Amsterdam, The Netherlands: Elsevier, 2011.