International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 02 | Feb 2020 www.irjet.net p-ISSN: 2395-0072

STUDY PAPER ON VARIOUS SECURITY MECHANISM OF CLOUD COMPUTING.

Bachkar Tejashri [1], Bangar Gitanjali [2], Sonawane Monali[3], Shinde Bipin[4]

[1]Bachkar Tejashri, Student, Dept. of Computer Technology, Amrutvahini Polytechnic Sangamner, Maharashtra
[2]BangarGitanjali, Student, Dept. of Computer Technology, Amrutvahini Polytechnic Sangamner, Maharashtra
[3]Sonawane Monali, Student, Dept. of Computer Technology, Amrutvahini Polytechnic Sangamner, Maharashtra
[4] Prof. Shinde Bipin, Lecturer, Dept. of Computer Technology, Amrutvahini Polytechnic Sangamner, Maharashtra

---

Abstract - - In the today's era the field of information technology offered the people ease, comforts, and convenience, but still there are many security-related issues. Today cloud computing provide vast range of services and connected with each other in the form of cluster. Using cloud computing people can share computing recourses and store their personal as well as business information. Hence form information security point of view enhances cloud security measures need to be utilized. Traditionally many security mechanisms are used such as encryption, hashing, digital signature, Public Key Infrastructure (PKI), Identity and access management (IAM), Single Sign-On (SSO), Could base security groups, Hardened Security server images, user Behavior Technology and Decoy technology. Several of which can be used to counter the security threats[1]. This paper focuses on various security mechanisms and their effectiveness on cloud computing.

Keywords: Security, Cloud Technology, User Behavior Profiling, Decoy Technology.

1. INTRODUCTION

Cloud computing is the the use of various services, such as software development platforms, servers, storage and software, over the internet, often referred to as the cloud. Cloud computing consists of a shared pool resources shared among users per subscription basis. The way computer-stored information and personal data can cause new data security challenges. In today's world scenario every organization using cloud computing to protect their data and to use the services like IaaS, PaaS, SaaS. The technology of distributed data processing in which some scalable information resources and capacities are provided as a service to multiple external customers through internet technology.

2. SECURITY MECHANISMS

Encryption

Data, by default, is coded in a readable format known as plaintext. When transmitted over a network, plaintext is vulnerable to unauthorized and potentially malicious access. The encryption mechanism is a digital coding system dedicated to preserving the confidentiality and integrity of data. It is used for encoding plaintext data into a protected and unreadable format. Encryption technology commonly relies on a standardized algorithm called a cipher to transform original plaintext data into encrypted data, referred to as cipher text.

Hashing

The Hashing mechanism is used when a one-way, non-reversible form of data protection is required. Once hashing has been applied to a message it is locked and no key is provided for message to be unlocked. The common application of this mechanism is storage of passwords. hashing technology can be used to derive a hashing code or message digest from a message, which is often of a fixed length and smaller than the original message.

Digital Signature

The digital signature mechanism is a means of providing data authenticity and integrity through authentication and non-repudiation. A message is assigned a digital signature prior to transmission, which is then rendered invalid if the message experiences any subsequent, unauthorized modifications[3]. A digital signature provides evidence that the message received is the same as the one created by its rightful sender. Both hashing and asymmetrical encryption are involved in the creation of a digital signature, which essentially exists as a message digest that was encrypted by a private key and appended to the original message. The recipient verifies the signature validity and uses the corresponding public key to decrypt the digital signature, which produces the message digest.

Public key infrastructure

A Common approach for managing the issuance of asymmetric keys is based on the public key infrastructure (PKI) mechanism, which exists as a system of protocols, data formats, rules, and practices that enables large-scale systems to securely use public key cryptography. This system is used to associate public keys with their corresponding key owners (known as public key identification) while enabling the verification of key validity.

Identify and Access Management (IAM)

The identify and access management (IAM) mechanism encompasses the components and policies necessary to control and track user identifies and access privileges for IT resources, environment and systems.

Four main components:

1. Authentication:

Username and password combinations remain the most common forms of user authentication.

2. Authorization:

The authentication component defines the correct granularity for access controls and a oversees the relationship between identifies, access control right, and IT resource availability.

3. User management

Related to the administrative capabilities of the system. The user management program is responsible for creating new user identifies and access groups, resetting passwords, defining password policies, and managing privileges.

4. Credential management

The Credential management system establishes identifies and access control rules for define user accounts which mitigates the threat of insufficient authorization.

The IAM mechanism is primarily used to counter the insufficient authorization denial of service, and overlapping trust boundaries threats.

Single sign-on

Propagating the authentication and authorization information for a cloud service consumer across multiple cloud services can be a challenge, especially if numerous cloud services or cloud-based IT resources need to be invoked as part of the same overall runtime activity. single sign-on (SSO)mechanism enables one cloud service consumer to be authenticated by a security broker, which establishes a security context that is persisted while the cloud service consumer accesses other cloud services or cloud-based IT resources[5]. Otherwise, the cloud service consumer would need to re-authenticate itself with every subsequent request. The SSO mechanism essentially enables mutually independent cloud services and IT resources to generate and circulate runtime authentication and authorization credential

Cloud Based Security Groups

The resource segmentation is a process by which separate physical and virtual IT environments are created for different users and groups.

For ex, an organizations WAN can be partitioned according to individual network security requirements.

Once network can be established with a resilient firewall or external internet access, while a second is developed without a firewall because its users are internal and unable to access the internet.

Hardened Security server images

A virtual server is created from a template configuration called a virtual server image (or virtual machine image).Hardening is the process of stripping unnecessary software from a system to limit potential vulnerabilities that can be exploited by attackers. Removing redundant programs, closing unnecessary server ports, and disabling unused services, internal root accounts, and guest access are all examples of hardening[4]. A hardened virtual server image is a template for virtual service instance creation that has been subjected to a hardening process (Figure 10.13). This generally results in a virtual server template that is significantly more secure than the original standard image.

User Behavior Profiling:

User behavior profiling is a popular technology in Cloud Computing which is utilized to detect when and how frequently the user access his data in the cloud[8]. The way to access cloud user information is predictable. This type behavior of the user is continuously checked for abnormal activity. Each user has its unique profile consist of the number of times he has accessed his files on cloud. These profiles maintain the count of that file has accessed.

Decoy Technology

The file system is mounted with devices which are transferred on the system by the CSP. These devices incorporate archives, for example, credit card details, tax returns, bank statements. This technology is incorporated with user behavior profiling. At the point when an unlawful access is resolved and later checked by different strategies, for example security question, a disinformation assault might be begun. This will verify the genuine information for the client. But all were failed from time to time for various reasons like lack of security procedures, error codes, insider attacks, wrong implementations, failed to envision on creative and effective attacks and misconfigured services.

3. CONCLUSION

With the increase of data, the attack the security of user's private data over the cloud is becoming a serious issue for cloud service providers[1]. This Paper focus on different security mechanism on cloud computing. Most of mechanism provide enough level of security but each and every mechanism fails at certain cases. Out this mechanism user behavior profiling and decoy technology is play an important role. In cloud computing this technique helps in predicting and monitoring the behavior of user. Once user identification is done, whether it is authorize user or not then one can decide to send original data or duplicate file dynamically generate by decoy technology. This will provide security to

system data and for enhancement purpose encryption algorithm can also be used.

REFERENCES

[1] Security implementation in cloud computing using user behavior profiling and decoy technology KM Reena, SK Yadav, NK Bajaj… - … Conference on Inventive …, 2017 - ieeexplore.ieee.org

[2] Cloud Security Alliance, Top Threat to Cloud Computing V1.0, March 2010.Available: https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

[3] Prevention of Malicious Insider In The Cloud Using Decoy Documents by S. MuqtyarAhmed, P. Namratha, C. Nagesh

[4] Cloud Security: Attacks and Current Defenses Gehana Booth, Andrew Soknacki, and anil Somayaji.

[5] Overview of Attacks on Cloud Computing by Ajay Singh, Dr. ManeeshShrivastava

[6] D.Jamil and H. Zaki, Security Issues in Cloud Computing and Countermeasures, International Journal of Engineering Science andTechnologyVol. 3 No. 4, pp. 2672-2676, April 2011.

[7] Cloud Computing Concepts, Technology & Architecture by Thomas Eri with Zagham Mahmood and Ricardo Puttini.

[8] M. Ben-Salem and S. J. Stolfo, "Modeling usesearch-behavior for masquerade detection," inProceedings of the 14th International Symposiumon Recent Advances in Intrusion Detection. Heidelberg: Springer, September 2011, pp. 1–20

BIOGRAPHIES

Bachkar Tejashri, Student,
Dept. of Computer Technology,
Amrutvahini Polytechnic,
Sangamner, Maharashtra

Bangar Gitanjali, Student,
Dept. of Computer Technology,
Amrutvahini Polytechnic,
Sangamner, Maharashtra

Sonawane Monali, Student,
Dept. of Computer Technology,
Amrutvahini Polytechnic,
Sangamner, Maharashtra

Prof.Shinde Bipin, Lecturer,
Dept. of Computer Technology,
Amrutvahini Polytechnic,
Sangamner, Maharashtra