Data security issues on cloud environment

Mr. Pravin R. Nerkar, Dr. Manoj K. Ramaiya
Sage University, Indore, India, pravinnerkar2007@gmail.com
Sage University, Indore, India, manojramaiya@gmail.com

Abstract

Today's people are dealing with data which is stored on server and it is increasing day by day. Before a decade it restricts to use different application over internet because of availability of internet. But now a day's every one talking about different types of data and wants to deal with it. As a use of internet generation of voluminous data and storing of data on server is very important with limitation on local site. But again the problem of sensitive data arises as a security, when it is stored on server. So it's necessary to protect sensitive data on cloud.

Keywords: **Cloud Computing, Security, Privacy.**
DOINumber:10.48047/nq.2022.20.22.NQ10271 **NeuroQuantology2022;20(22):2786-2788**

1. Introduction

Cloud computing has been evolved as a next step in the computation environment. Cloud environment is a combination of hardware and software that provide different services over the network as per the user requirement. In the cloud environment, application and computing resources are facilitated as a service over the internet when it required, so it refers to offering computing services from servers in a network. Typically cloud services are available on demand, can be accessed over a network, share resources between multiple applications and tenants, scale elastically based on dynamic computing needs, and provide measured service[1].

Organizations use various cloud computing facilities, with IaaS, PaaS, and SaaS, and diverse public, private, and hybrid cloud computing representations[7][8]. These architectures and facilities provide several cloud security tasks. Each facility prototypical has several difficulties linked with it. Security complications are seen from two perceptions: first, the facility provider assurances that their facilities are protected and control their documentation. The other perception is that of the user, who assurances that the facility is adequately protected.

Multi-tenancy

A cloud model is established to enable resource distribution, memory distribution, storage distribution, and collaborative computing [2]. Multi-tenancy permits more operative resource use, which decreases costs. It involves sharing computing capital, storage space for facilities, and requests with other occupants who share a similar physical/logical stage on the benefactor's facilities. Therefore, it compromises information confidentiality, resultant in information leakage and encoding and growing the likelihood of an outbreak.

Elasticity

Elasticity is defined as a system's capacity to adapt to changing workloads via autonomous resource allocation and depletion, ensuring that available resources match the current demand as accurately as possible at any moment in time. The concept of elasticity implies scalability. Consumers may adjust their scales as necessary, it says. This scalability enables occupants to use capitals that were earlier reserved for another occupant. This, however, may raise apprehensions about secrecy.

2. Literature Review

The fast growth of Cloud Computing has prompted many academics and businesses to concentrate their efforts and study all elements

of the Cloud in general, but a significant portion of their work has concentrated on data security and privacy. Numerous studies have been suggested increasing data security and providing Cloud users with an appropriate level of privacy via various approaches and strategies [3].

Diffie Hellman:

Diffie Hellman is a set of instructions for making a shared secret key to transfer data steadily. DH is one of the first practical applications of public-key conversation in cryptography, laying the groundwork for a slew of verified protocols. For instance, DH provides the highest forwarding secrecy in the ephemeral shipping layer security (EDH or DHE depending on the cipher suite). The method generates a key by using the exponentials module computation, which secures the key.

Asymmetric key:

General public-key cryptography is encoding that uses two distinct keys: one for encryption (public key) and another for decryption (private key). The final public key is visible to everyone, and the proprietor only recognizes the private key[4]. The most well-known feature of universal public key cryptography is its authentication mechanism, requiring just one character change to flop. While asymmetric encoding does not have a problem with key dispersal, it is sluggish than symmetric encoding since it consumes a large amount of energy throughout the encryption process.

Figure 1: Asymmetric key Processing

RSA Algorithm:

For any n, the RSA method is encryption in which the plaintext and ciphertext are numerals between 0 and n-1. It employs exponentials to encrypt plaintext in blocks through C = Me mod n, where C is the ciphertext and M is the plaintext. Correspondingly, the plaintext is found using the formula M = Cd mod n, where d is the private key. The primary characteristics of RSA are that it applies to encryption and decoding, digital signatures, and key conversation. It is by far the greatest used asymmetric encoding algorithm. When a private key is used to encrypt data, the cipher stylistic content may be decoded using just the public key. It is used for SSL/TLS (secure sockets layer/transport layer security), which is used to safeguard the information you send and receive over the internet, such as when you conduct online banking or log into a website. The primary disadvantage of the RSA method is that once d is known, the textual content of the encryption may be readily decrypted.

3. Security Issues In Cloud

Location detection: - Data storage is the prominent work of cloud which is in discussion, but finding it could be the challenge that location at which place it is actually. So without knowing the [5] location of data it could misinterpret and violated.

Data Security:- On the level of basic security[6] of data it is provided by provider at some extend in terms of encryption . Data encryption is a process that helps to fix various external and malicious threats. Unencrypted data can be easily accessed by unauthorized users and these data is very vulnerable for susceptible data, as it does not provide any security mechanism. Unencrypted data risks the user data which leads to cloud server to escape various data information to unauthorized users.

Trust Chain in Clouds: Trust plays an important role in attracting more consumers by assuring on cloud providers. Due to loss of control, cloud users rely on the cloud providers using trust mechanisms as an alternative to giving users precise control over their data and cloud resources[7][8]. Therefore, cloud providers build

confidence amongst their customers by assuring them that the provider's operations are certified in conformity with organizational safeguards and standards.

4. Conclusion

As a way of change in use of storage structure with different type of data so it is challenge to provide solution to such sensitive problem in data storage. There is no escape form cloud technology to not use for personal or business work. So this paper focuses on issues in data security on cloud.

5. REFERENCES

[1] Rohan Jathanna, Dhanamma Jagli "Cloud Computing and Security Issues" Int. Journal of Engineering Research and Application ISSN : 2248-9622, Vol. 7, Issue 6, (Part -5) June 2017, p.31-38

[2] U. Ahmed, I. Raza, and S. A. Hussain, "Trust evaluation in cross-cloud federation: Survey and requirement analysis," ACM Computing Surveys (CSUR), vol. 52, no. 1, pp. 1–37, 2019.

[3] D Chopra, D Khurana, K Govinda, "CLOUD COMPUTING SECURITY CHALLENGES AND SOLUTION," International Journal of Advances in Engineering Research, vol. 3, no. 2, 2012.

[4] K. Kumar, V. Rao, S. Rao, and G.S. Rao, "Cloud Computing : An Analysis of Its Challenges & Security Issues," IJCSN,vol. 1, no. 5, 2012.

[5] Monjur Ahmed and Mohammad Ashraf Hossain "CLOUD COMPUTING AND SECURITY ISSUES IN THE CLOUD" in International Journal of Network Security & Its Vol 11, Issue 6,June/ 2020 ISSN NO: 0377-9254 www.jespublication.com Page No:1147 Applications (IJNSA), Vol.6, No.1, January 2014.

[6] I. Ahmad, H. Bakht, and U. Mohan, "Cloud Computing – Threats and Challenges", Journal of Computer Management Studies, vol. 1, no. 1, 2017. Journal of Computer Management Studies, vol. 1, no. 1, 2017.

[7] G. R. Vijay, "An Efficient Security Model in Cloud Computing based on Soft computing Techniques," vol. 60, no. 14, pp. 18–23, 2012.

[8] H. Tsai, N. Chiao, R. Steinmetz, and T. U. Darmstadt, "Threat as a Service?: Virtualization's Impact on Cloud Security," no. February, pp. 32–37, 2012.