International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 04 | Apr 2021 www.irjet.net p-ISSN: 2395-0072

Study of Cloud Computing and its Data Storage Security Issues

Arin Shrivastava[1], Suniti Purbey[2]

[1]Student Amity Institute of Information Technology, Amity University Chhattisgarh, Raipur, India
[2]Assistant Professor Amity Institute of Information Technology, Amity University Chhattisgarh, Raipur, India

---

Abstract - *Cloud computing offers online on demand services to its clients. Data storage is among one of the primary services offered by cloud computing. Cloud service facilitator hosts the data of the client on their server and client can access their data from these servers. As data, owners and servers are different identities, the standard of data storage calls upon many security challenges. In this paper, we will study cloud computing and its storage security issues*

Key Words: (**Cloud, Hybrid, corporate, data**)

1. INTRODUCTION

The cloud computing model permits access to computer resources and information so that a network connection is available from anyplace. Cloud computing makes available a shared pool of resources, together with data storage space, networks, computer processing power, and user applications and specialized corporate company. Cloud computing is a model for enabling as more convenient, on-demand network services access to a shared pool of configurable computing resources (e.g., servers, storage, applications, networks, and services) that can be quickly provisioned and released with minimal management effort or interaction between service providers.

Various organizations are switching into cloud because it allows the users to store their data on cloud online and can access at anytime from anywhere. Data breaching is possible in cloud environment since data from various users and business organizations lie together in cloud. By sending the data to the cloud, the data owners transfer the control of their data to a third person that may raise security problems. Sometimes the Cloud Service Provider (CSP) itself will use/corrupt the data illegally.

Security and protection remain as significant obstacle on cloud computing for i.e., preserving confidentiality, integrity and availability of data. A straightforward arrangement is to encrypt the data before transferring it onto the cloud. This method guarantees that the data is not noticeable to outside clients and cloud administrator but rather has the limit that plain text-based searching algorithm are not applicable.

2. CLOUD STORAGE

Cloud storage is one of the primaries uses of cloud computing. We can define cloud storage as storage of the data online in the cloud. A cloud storage system is considered as a distributed data centers, which typically use cloud-computing technologies and offers interface for storing and accessing data.

2.1 Cloud deployment models

i. **Personal Cloud Storage:** It is also known as mobile cloud storage. In this type storage, individual's data is stored in the cloud, and he/she may access the data from anywhere.

ii. **Public Cloud Storage:** In Public cloud storage the enterprise and storage service provider are separate and there are not any cloud resources stored in the enterprise's data Centre. The cloud storage provider fully manages the enterprise's public cloud storage.

iii. **Private Cloud Storage:** In Private Cloud Storage the enterprise and cloud storage provider are integrated in the enterprise's data Centre. In private cloud storage, the storage provider has infrastructure in the enterprise's data Centre that is typically managed by the storage provider. Private cloud storage helps resolve the potential for security and performance concerns while still offering the advantages of cloud storage.

iv. **Hybrid cloud storage:** It is a combination of public and private cloud storage where some critical data resides in the enterprise's private cloud while other data is stored and accessible from a public cloud storage provider.

3. CHARACTERISTICS OF CLOUD COMPUTING

- **Ultra-large-scale**: In ultra-large-scale computing, the scale of cloud is large convergence. For example, IBM, Microsoft, Yahoo, Rediff, Amazon they have more than hundreds of thousands of servers.

- **Virtualization**: creation of virtual servers, infrastructures, devices, and computing resources.
- **High reliability**: By using cloud computing is highly reliable than local computer process interaction.
- **Versatility**: Cloud computing can produce several types of application supported by cloud service, and single cloud can maintain different applications running at the same time.
- **High extendibility**: the scale of the cloud can highly extend or dynamically prefer to meet the increasing requirements of cloud services.
- **Versatility**: Cloud computing can produce several types of applications supported by cloud service, and single cloud can maintain different applications running at the same time.
- **High extendibility**: The scale of cloud can highly extend or dynamically prefer to meet the increasing requirement of cloud services.
- **On demand service**: Cloud provides tremendous amount of resource pool, which you can pay for on the basis of your requirements and needs.

4. Security and privacy issues in data storage.

Cloud computing facilitates the users with data storage on the remote location which is maintained by a third-party provider. So once data is uploaded of the user, the user loses its control over its personal data as it can be accessed or tampered by attackers which can be an internal or external. Weak access control also commonly causes unauthorized access. The protection of information arises the following challenges: The security and privacy issues related to data storage are confidentiality, integrity, and availability.

a. Confidentiality

Confidentiality is keeping the client's data secret and accessible to only the client as a part of authentication process. But confidentiality is a major security issue nowadays as the data is stored on a remote server which is thereby can be controlled by the service provider.

So, to overcome this issue, algorithms like Cryptographic encryption and strong authentication mechanisms can be used. Encryption is the technique which converts the simple data into ciphered text which can only be understood by the authorized users, Blowfish is an example of a fat and simple encryption algorithm.

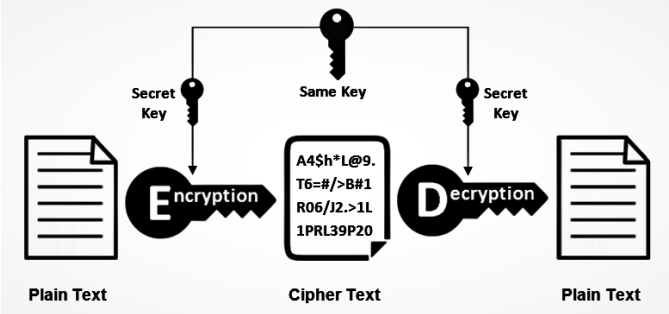

Fig 1. Symmetric encryption

But however, with these encryption techniques comes along the limitation in which searching the data from the file, entire file must be decrypted, which was time consuming. Thus, searchable encryption was introduced which facilitates build an index for the file containing the keywords so that while the data is searched only the keywords are decrypted instead of the entire file and the search is made on it.

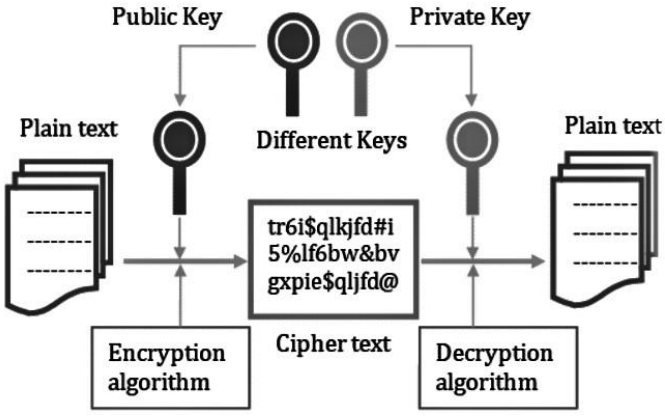

Fig 2. Asymmetric encryption

b. Integrity

Integrity is another serious issue faced by Cloud computing. Integrity makes sure that the user's data has not been changed by an unauthorized individual in an unauthorized way. It ensures that data is genuine, correct and protected from unauthorized users, after all cloud supports resource sharing, so there's possibility of data corrupting by attackers. So, to provide and preserve integrity Digital Signatures and Message Authentication Code (MAC) can be used.

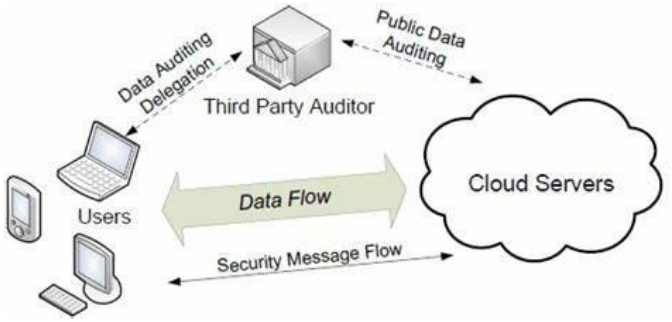

Fig 3. Remote auditing mechanism

c. Availability

Availability alludes to being accessible and available to approved clients on request. The point of accessibility in Cloud computing is to guarantee that its clients can utilize them at any spot, at any time.

5. CONCLUSION

Cloud computing facilitates the user with storing their data online. Yet, data security is the significant danger in distributed computing. Because of this numerous associations are not able to move into cloud services. To resolve this, Confidentiality, Integrity, Availability ought to be embodied in a CSP's Service-Level Agreement (SLA) to its clients. Otherwise make sure no delicate data is placed into a public cloud but if any make sure it must be encrypted.

REFERENCES

[1] V. Nirmala, R.K. Sivanandhan, Dr.R. Shanmuga Lakshmi, "Data Confidentiality and Integrity Verification using User Authenticator scheme in cloud", Proceedings of 2013 International Conference on Green High-Performance Computing (ICGHPC 2013). March 14-15, 2013, India.

[2] Arjun Kumar, Byung Gook Lee, HoonJae Lee, Anu Kumari, "Secure Storage and Access of Data in Cloud Computing", 2012 International Conference on ICT Convergence (ICTC), 15-17 Oct. 2012.

[3] M.R.Tribhuwan, V.A.Bhuyar, Shabana Pirzade, "Ensuring Data Storage Security in Cloud Computing through Two-way Handshake based on Token Management", 2010 International Conference on Advances in Recent Technologies in Communication and Computing.

[4] Mr. Prashant Rewagad, Ms. Yogita Pawar, "Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing", 2013 International Conference on Communication Systems and Network Technologies.

[5] Uma Somani, Kanika Lakhani, Manish Mundra, "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing", 1st International Conference on Parallel,

[6] M. AlZain, E. Pardede, B. Soh, and J. Thom, "Cloud computing security: From single to multi-clouds," in System Science (HICSS), 2012 45th Hawaii International Conference on, Jan 2012, pp. 5490–5499.

[7] M. Sookhak, H. Talebian, E. Ahmed, A. Gani, and M. K. Khan, "A review on remote data auditing in single cloud server: Taxonomy and open issues," Journal of Network and Computer Applications, vol. 43, pp. 121–141, 2014.

[8] E. Aguiar, Y. Zhang, and M. Blanton, "An overview of issues and recent developments in cloud computing and storage security," in High Performance Cloud Auditing and Applications. Springer, 2014, pp. 3–33.

[9] I. Gul, M. Islam et al., "Cloud computing security auditing," in Next Generation Information Technology (ICNIT), 2011 The 2nd International Conference on. IEEE, 2011, pp. 143–148.

[10] E. M. Mohamed, H. S. Abdelkader, and S. El-Etriby, "Enhanced data security model for cloud computing," in Informatics and Systems (INFOS), 2012 8th International Conference on. IEEE, 2012, pp. CC–12.

[11] S. Ramgovind, M. M. Eloff, and E. Smith, "The management of security in cloud computing," in Information Security for South Africa (ISSA), 2010. IEEE, 2010, pp. 1–7.

[12] F. Sabahi, "Cloud computing security threats and responses," in Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on. IEEE, 2011, pp. 245–249.

[13] X. Wang, B. Wang, and J. Huang, "Cloud computing and its key techniques," in Computer Science and Automation Engineering (CSAE), 2011 IEEE International Conference on, vol. 2. IEEE, 2011, pp. 404–410

[14] Sultan Aldossary, William Allen, "Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current

Solutions", in International Journal of Advanced Computer Science and Applications, Vol. 7, No. 4, 2016

[15] Latifur Khan and Bhavani Thuraisingham, "Security Issues for Cloud Computing", in Technical Report UTDCS-02-10, February 2010.

Distributed and Grid Computing (PDGC - 2010).

[16] https://www.researchgate.net/figure/Asymmetric-Key-Encryption_fig2_341891901

[17]https://content.sciendo.com/view/journals/amns/1/1/article-p145.xml

[18] http://trainnetsystems.blogspot.com/