International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 1 | ISSN : 2456-3307

A Study of Data Storage Security Issues in Cloud Computing

A Venkatesh*[1], Marrynal S Eastaff[2]

*[1]PG Scholar, PG Department of IT, Hindusthan College of Arts and Science (Autonomous), Coimbatore, India

[2]Asst Professor, PG Department of IT, Hindusthan College of Arts and Science (Autonomous), Coimbatore, India

ABSTRACT

Cloud computing provides on demand services to its clients. Data storage is among one of the primary services provided by cloud computing. Cloud service provider hosts the data of data owner on their server and user can access their data from these servers. As data, owners and servers are different identities, the paradigm of data storage brings up many security challenges. An independent mechanism is required to make sure that data is correctly hosted in to the cloud storage server. In this paper, we will discuss the different techniques that are used for secure data storage on cloud.

Keywords : Cloud computing, Data storage, Cloud storage server.

I. INTRODUCTION

Cloud computing is the combination of many pre-existing technologies that have matured at different rates and in different contexts. The goal of cloud computing is to allow users to take benefit from all these technologies. Many organizations are moving into cloud because it allows the users to store their data on clouds 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 privacy stands as major obstacle on cloud computing i.e. preserving confidentiality, integrity and availability of data. A simple solution is to encrypt the data before uploading it onto the cloud. This approach ensures that the data are not visible to external users and cloud administrators but has the limitation that plain text based searching algorithm are not applicable. In this paper, we discuss the security flaws in data storage and the mechanisms to overcome it.

II. CLOUD STORAGE

Cloud storage is one of the primary use 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 centres, which typically use cloud-computing technologies and offers some kind of interface for storing and accessing data. When storing data on cloud, it appears as if the data is stored in a particular place with specific name.

There are four main types of cloud storage:

Personal Cloud Storage:

CSEIT1831389 | Received : 16 Feb 2018 | Accepted : 27 Feb 2018 | January-February-2018 [(3) 1 : 1741-1745]

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.

Public Cloud Storage:

In Public cloud storage the enterprise and storage service provider are separate and there aren't any cloud resources stored in the enterprise's data centre. The cloud storage provider fully manages the enterprise's public cloud storage.

Private Cloud Storage:

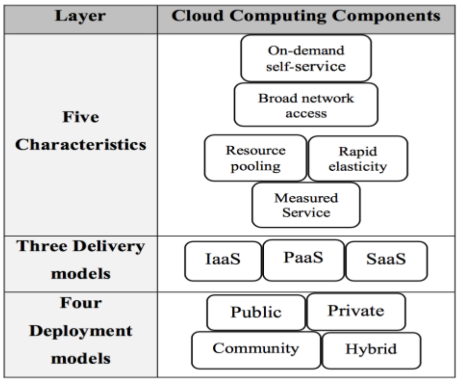
In Private Cloud Storage the enterprise and cloud storage provider are integrated in the enterprise's data centre. In private cloud storage, the storage provider has infrastructure in the enterprise's data centre that is typically managed by the storage provider. Private cloud storage helps resolve the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

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.

III. CHARACTERISTIC OF CLOUD COMPUTING

There are five characteristics of cloud computing. The first one is on-demand self-service, where a consumer of services is provided the needed resources without human intervention and interaction with cloud provider. The second characteristic is broad network access, which means resources can be accessed from anywhere through a standard mechanism by thin or thick client platforms such mobile phone, laptop, and desktop computer. Resource pooling is another characteristic, which means the resources are pooled in order for multi-tenants to share the resources. In the multi-tenant model, resources are assigned dynamically to a consumer and after the consumer finishes it, it can be assigned to another one to respond to high resource demand. Even if the resources are assigned to customers on demand, they do not know the location of these assigned resources.



Layer	Cloud Computing Components
Five Characteristics	On-demand self-service Broad network access Resource pooling Rapid elasticity Measured Service
Three Delivery models	IaaS PaaS SaaS
Four Deployment models	Public Private Community Hybrid

Figure. 1: Cloud environment architecture

Sometimes they know the location at a high-level abstraction, such as country, state, and data centre. Storage, processing, memory, and network are the kind of resources that are assigned. Rapid elasticity is another characteristic, which means that resources are dynamically increased when needed and decreased when there is no need. Also, one of characteristics that a consumer needs is measured service in order to know how much is consumed.

IV. Encrypted Data Storage for Cloud

Since data in the cloud is placed anywhere, it is important that the data be encrypted. We are using secure co-processor as part of the cloud infrastructure to enable efficient encrypted storage of sensitive data. By embedding a secure co-processor (SCP) into the cloud infrastructure, the system can handle encrypted data efficiently. Parts of the proposed instrument (see Figure 2). Basically, SCP is a tamper-resistant hardware capable of limited general-purpose computation. For example, IBM 4758 Cryptographic Coprocessor (IBM) is a single-board computer consisting of a CPU, memory and special-purpose cryptographic hardware contained in a tamper-resistant shell, certified to level 4 under FIPS PUB 140-1. When installed on the server, it is capable of performing local computations that are completely hidden from the server. If tampering is detected, then the secure co-processor clears the internal memory. Since the secure coprocessor is tamper-resistant, one could be tempted to run the entire sensitive data storage server on the secure coprocessor. Pushing the entire data storage functionality into a secure co-processor is not feasible due to many reasons. First of all, due to the tamper-resistant shell, secure co-processors have usually limited memory (only a few megabytes of RAM and

a few kilobytes of non-volatile memory) and computational power (Smith, 1999). Performance will improve over time, but problems such as heat dissipation/power use (which must be controlled to avoid disclosing processing) will force a gap between general purposes and secure computing. Another issue is that the software running on the SCP must be totally trusted and verified. This security requirement implies that the software running on the SCP should be kept as simple as possible. We can encrypt the sensitive data sets using random private keys and to alleviate the risk of key disclosure, we can use tamper-resistant hardware to store some of the encryption/decryption keys (i.e., a master key that encrypts all other keys).

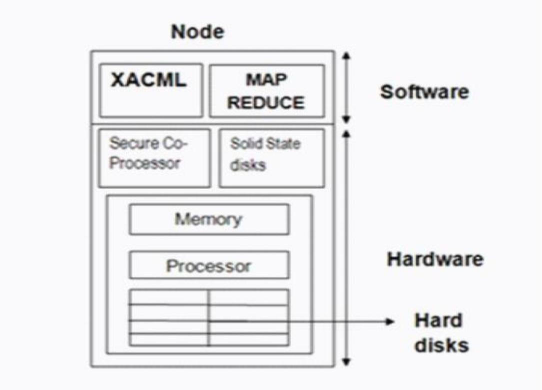


Figure 2. Parts of the proposed instrument

V. Security and Privacy Issues in Data Storage

Cloud Computing allows the users to store their data on the storage location maintained by a third party. Once the data is uploaded into the cloud the user loses its control over the data and the data can be tampered by the attackers. The attacker may be an internal(CSP) or external. Unauthorized access is also a common practice due to weak access control. The protection of information arises the following challenges:

The security and privacy issues related to data storage are confidentiality, integrity and availability.

A. Confidentiality

The major dispute in cloud computing is confidentiality. Data confidentiality means accessing the data only by authorized users and is strongly related to authentication.In another way confidentiality means keeping users data secret in the cloud systems. As we are storing the data on a remote server and transferring the control over the data to the provider here arises the questions such as:

For ensuring confidentiality, cryptographic encryption algorithms and strong authentication mechanisms can be used. Encryption is the process of converting the data into a form called cipher text that can be understood only by the authorized users. Encryption is an efficient technique for protecting the data but have the obstacle that data will be lost once the encryption key is stealed. algorithms. Blowfish is a fat and simple encryption algorithm.

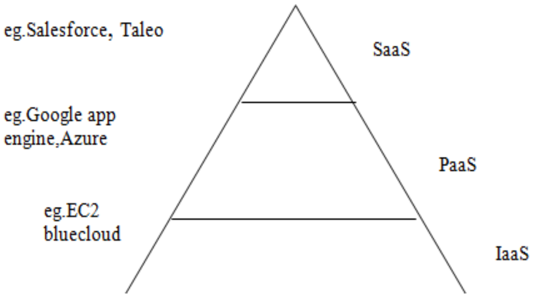


Figure 3. Symmetric encryption

The above encryption techniques have the limitation that for searching the data from the file, the entire file has to be decrypted. It is a time consuming process and thus searchable encryption was introduced. Searchable encryption allows build an index for the file containing the keywords and is encrypted and stored along with the file, so that while searching the data only the keywords are decrypted rather than the entire file and search is made on it.

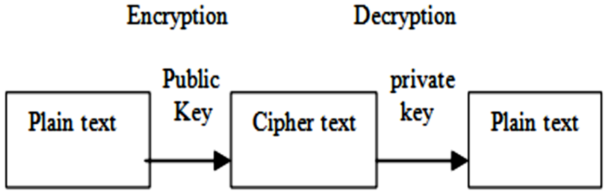


Figure 4. Asymmetric encryption

B. Integrity

Another serious problem faced by cloud computing is integrity. Integrity of data means to make sure that the data has not been changed by an unauthorized person or in an unauthorized way. It is a method for ensuring that the data is real, accurate and safeguarded from unauthorized users. As cloud computing supports resource sharing, there is a possibility of data being corrupted by unauthorized users. Digital Signatures can be used for preserving the integrity of data. The simple way for providing integrity is using Message Authentication Code(MAC).

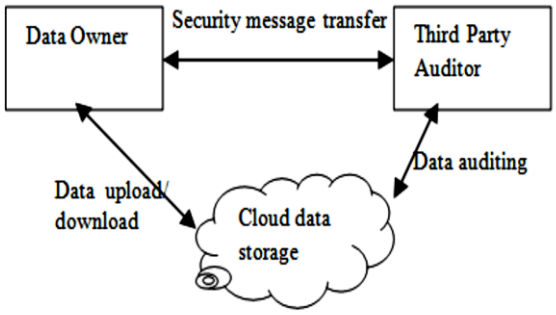


Figure 5. Remote auditing mechanism

C. Availability

Availability refers to being available and accessible to authorized users on demand. The aim of availability in cloud computing systems is to ensure that its users can use them at any place and at any time

VI. Conclusion

Cloud computing enables users to store their data in remote storage location. But data security is the major threat in cloud computing. Due to this many organizations are not willing to move into cloud environment. To overcome this, confidentiality, integrity, availability should be encapsulated in a CSP's Service- Level Agreement (SLA) to its customers. Otherwise ensure that any sensitive information is not put into a public cloud and if any it is to be stored in encrypted form. Effective auditing mechanisms also can be used for providing data integrity.

VII. REFERENCES

[1] V.Nirmala, R.K.Sivanandhan, Dr.R.Shanmuga Lakshmi, “Data Confidentiality and Integrity Verification usingUser 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,

Distributed and Grid Computing (PDGC - 2010).

[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.