International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 4, Issue 1, pp 28-31, January-2020

A Study of Data Storage Security Issues in Cloud Computing

[1]Miss.Aditi Mangle, [2]Miss.Snehal Ajmire, [3]Mr.Anurag Dwivedi

[1,2,3]MCA-III, Department of Research and PG Studies in Science & Management, Vidyabharati Mahavidyalaya, Amravati, India

***Abstract* - Cloud Computing is the internet established enabler for sharing of technological infrastructural resources, software and digital content, allowing them (Infrastructure, Platforms, Software) to be presented on pay-for-use basis, like any utility service. The exponential growth of computing capacities, the extraordinary growth in the consumption of digital contents, then the explosive growth of applications have triggered the emergence of cloud computing. It is probable to herald a new wave of Computing and is probable to wield enormous influence on how IT services will be consumed in future. Cloud Computing conveys down dramatically the cost of IT use, in addition to providing flexibility in terms of large capacity-on-demand coupled with higher reliability. As it does not call for large capital expense and need for highly skilled IT professionals to build and manage the infrastructure, range and scale of Cloud applications are bound to grow enormously, even as resource focused applications can be within the reach of a number of Small and Medium Sized Businesses, Educational and Research organizations.**

Keywords: Cloud Computing, Data Storage, Cloud Storage Server.

I. Introduction

Cloud computing means that instead of all the hardware and software that you use on your desktop or anywhere in the corporate network, it is provided as a service by another company and is generally accessible from transparently on the Internet. And the software and how it all works don't matter to you. The user is simply somewhere in the nebulous "cloud" that represents the Internet.

Cloud computing is a slogan that has different meanings for different people. For some, this is just another way of explaining "outsourcing" of information technology. Others refer to any IT service provided over the Internet or a similar network; and some define it as any purchased IT service that you use outside of your firewall. Whatever the definition of cloud computing, there is no doubt that it makes more sense to stop talking about abstract definitions and look at some simple, real examples - so let's do it

Security and data protection is a major obstacle to cloud computing. H. Maintain confidentiality, integrity and availability of data. A simple solution is to encrypt the data before uploading it to the cloud. This approach confirms that the data is not visible to external users and cloud administrators, but has the limitation that search algorithms based on simple text are not applicable. This article describes data storage security vulnerabilities and the mechanisms to overcome them.

II. Cloud Storage

Cloud storage is one of the main applications of cloud computing. We can define cloud storage as online data storage in the cloud. A cloud storage system is thought of as a distributed data center that typically uses cloud computing technologies and provides some sort of interface for storage and access to data. When storing data in the cloud, it appears that the data is stored in a specific location with a specific name.

There are four main types of cloud storage:

2.1 Personal Cloud Storage

It is also known as mobile cloud storage. In this type of storage, a person's data is stored in the cloud and they can access the data from anywhere.

2.2 Public Cloud Storage

In public cloud storage, the enterprise and the storage service provider are separate, and no cloud resources are stored in the enterprise data center. The cloud storage provider fully manages public enterprise cloud storage.

2.3 Private Cloud Storage

In private cloud storage, the enterprise and the cloud storage provider are integrated into the enterprise data center. With private cloud storage, the storage provider has infrastructure in the enterprise data center that is typically

International Research Journal of Innovations in Engineering and Technology (IRJIET)
ISSN (online): 2581-3048
Volume 4, Issue 1, pp 28-31, January-2020

managed by the storage provider. Private cloud storage solves potential security and performance issues while providing the benefits of cloud storage.

2.4 Hybrid Cloud Storage

It is a combination of public and private cloud storage, with some important data in the corporate private cloud, while other data is stored and accessed by a public cloud storage provider.

III. Characteristic of Cloud Computing

There are five characteristics of cloud computing. The first is on-demand self-service, in which the required resources are made available to a customer without human intervention and without interaction with the cloud provider. The second feature is wide network access, which means that resources can be accessed from anywhere using a standard mechanism from thin or thick client platforms such as cell phones, computers laptops and desktop computers. Another feature is the pooling of resources. This means that the resources are combined so that multiple clients can share the resources. In the multi-tenant model, resources are dynamically allocated to one consumer and, once the consumer is finished, they can be allocated to another to meet a high resource requirement. Even if resources are allocated to customers as needed, they do not know the location of these allocated resources.

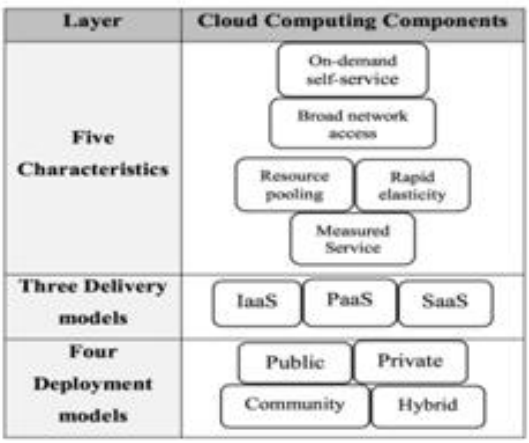

Figure 1: Cloud environment architecture

Sometimes they know the location of a high-level abstraction, for example B. Country, State, and data center. Storage, processing, memory and network are the allocated resources. Another feature is rapid elasticity, which means that resources are dynamically increased and reduced when needed. One of the properties that a consumer needs is to measure performance to know how much is consumed.

IV. Encrypted Data Storage for Cloud

Since the data is stored anywhere in the cloud, it is important that the data is encrypted. We use a secure coprocessor as part of the cloud infrastructure to enable efficient encrypted storage of sensitive data. By integrating a secure coprocessor (SCP) into the cloud infrastructure, the system can process encrypted data in a professional manner. Parts of the proposed instrument (see Figure 2). Basically, SCP is tamper-proof material that allows limited computation for general purposes. For example, IBM 4758 Cryptographic Coprocessor (IBM) is a single card computer with a processor, memory and special cryptographic hardware in a tamper-proof shell certified FIPS PUB 140-1 at level 4. Once installed on the server, it can perform local calculations that are completely hidden from the server. If a forgery is detected, the secure coprocessor erases the internal memory. Since the secure coprocessor is tamper-proof, you may be tempted to run the entire confidential data storage server on the secure coprocessor. It is not possible to transfer all data storage functionality to a secure coprocessor for many reasons. First, because of the tamper-proof shell, secure coprocessors generally have limited memory (only a few megabytes of RAM and a few kilobytes of non-volatile memory) and limited computing power (Smith, 1999). Performance will improve over time, but issues such as heat dissipation / power consumption (which must be controlled to avoid disclosure of the treatment) create a gap between general and secure data processing. Another problem is that the software running on the SCP must be absolutely reliable and verified. This security requirement requires that the software running on the SCP be as simple as possible. We can encrypt confidential records with random private keys, and to increase the risk of key disclosure, we can use tamper-evident hardware to store some of the encryption / decryption keys (i.e. a master key that encrypts all other keys).

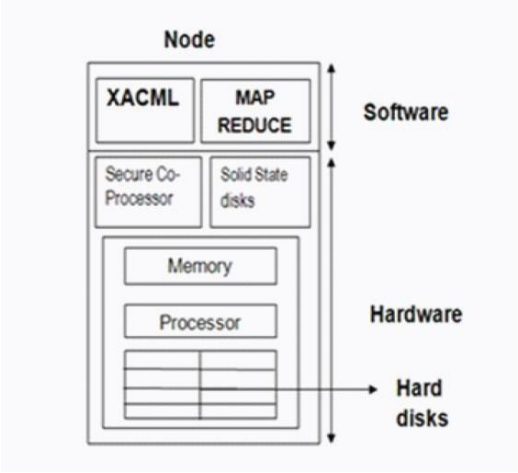

Figure 2: Parts of the proposed instrument

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 4, Issue 1, pp 28-31, January-2020

V. Security and Privacy Issues in Data Storage

Cloud computing allows users to store their data in a location kept by a third party. Once the data is uploaded to the cloud, the user loses control of the data and the data can be manipulated by attackers. The attacker can be internal (CSP) or external. Unauthorized access is also common practice due to poor access control. Protecting information poses the following challenges:

The security and confidentiality issues associated with data storage are confidentiality, integrity and availability.

5.1 Confidentiality

The main difference in cloud computing is privacy. Data confidentiality means that only authorized users can access the data. It is closely linked to authentication. In another way, privacy means keeping user data secret in cloud systems. Since we save the data on a remote server and transfer control of the data to the provider, the following questions arise:

Strong cryptographic encryption algorithms and authentication mechanisms can be used to ensure confidentiality. Once encrypted, the data is converted into a form called encrypted text, which can only be understood by authorized users. Encryption is an effective technique to protect data, but it prevents data from being lost as soon as the encryption key has stolen algorithms. Blowfish is a simple and daring encryption algorithm.

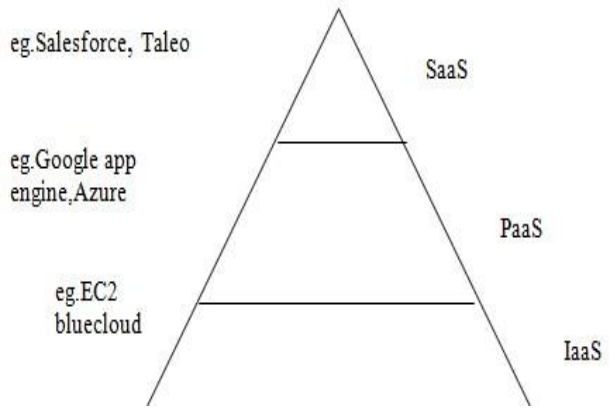

Figure 3: Symmetric encryption

The above encryption techniques have the limitation that the entire file must be decrypted to find the data in the file. It is a time consuming process and therefore searchable encryption has been introduced. Searchable encryption creates an index on the file that contains the keywords, and is encrypted and stored with the file so that when the data is searched, only the keywords are decrypted and not the entire file is searched.

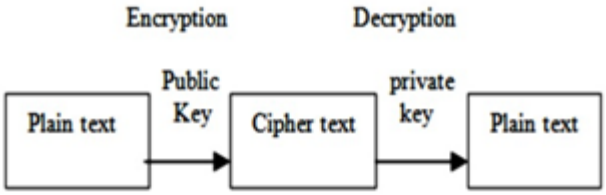

Figure 4: Asymmetric encryption

5.2 Integrity

Another serious problem facing cloud computing is integrity. Data integrity means that the data has not been modified by unauthorized persons or in an illegal manner. It is a method of ensuring that the data is authentic, accurate and protected from unauthorized users. Since cloud computing supports resource sharing, it is possible that data may be corrupted by unauthorized users. Digital signatures can be used to maintain data integrity. The simplest way to ensure integrity is to use the Message Authentication Code (MAC).

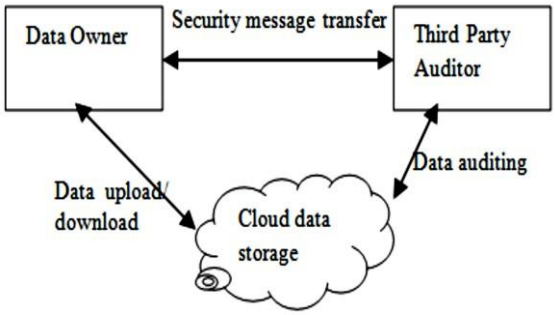

Figure 5: Remote auditing mechanism

5.3 Availability

Availability refers to the availability and availability of certified users upon request. The goal of availability in cloud computing systems is to confirm that users can use them anytime, anywhere

VI. Conclusion

Cloud computing allows users to store their data in a remote location. However, data security is the biggest threat in cloud computing. For this reason, many companies do not want to move to a cloud environment. To overcome this, confidentiality, integrity and availability must be included in a CSP's service level agreements (SLAs) for its customers. Otherwise, make sure confidential information is not placed in a public cloud and is stored encrypted if necessary. Effective testing mechanisms can also be used to ensure data integrity.

ISSN (online): 2581-3048
Volume 4, Issue 1, pp 28-31, January-2020

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.*

Citation of this Article:

Miss.Aditi Mangle, Miss.Snehal Ajmire, Mr.Anurag Dwivedi, "A Study of Data Storage Security Issues in Cloud Computing" Published in *International Research Journal of Innovations in Engineering and Technology (IRJIET)*, Volume 4, Issue 1, pp 28-31, January 2020.

****

