Journal of Advances and Scholarly Researches in Allied Education
Vol. 17, Issue No. 2, October-2020, ISSN 2230-7540

Data Safety & Security in Cloud Computing

Lalit Kumar Mahore*

Madhyanchal Professional University, Bhopal

Abstract – Cloud computing is named as the conveyance of computing overhauls above the Web. Today many characters make utilization of cloud computing services for their very own needs. Cloud computing system is accessed using network which provides software, hardware, processing power etc. to the user when demand is generated. Cloud Computing is a virtual pool of computing resources which provides the pool to users through internet. Cloud Computing provides various services to user by creating group of clusters and grids of computers. The main goal behind this is to provide services in virtualized manner to reduce burden of user to maintain everything by itself. It also refers to the web-based computing which provides devices with shared pool of resources, information or software on demand and pay per-use basis. Instead of having local servers or own devices to manage applications, people use sharing computing resources model of Cloud. The Cloud computing provides a numerous advantages to its users but at the dark side it's also suffers from lots of issues like Integrity or Storage Correctness, Availability, Confidentiality and more.

Keyword: Cloud Computing, Software, Web-Based Computing

----------X----------

INTRODUCTION

Cloud is an Internet-based computing technology, where shared resources such as software, platform, storage and information are provided to customers on demand. Cloud Computing is a computing platform for sharing resources that include infrastructures, software, applications, and business processes. Cloud Computing is a virtual pool of computing resources. It provides computing resources in the pool for users through internet. Cloud computing as an emerging computing paradigm aims to share storage, computation and services transparently among massive users. Current Cloud computing systems poses serious limitation in protecting users' data confidentiality. Since users' sensitive data is presented in unencrypted forms to remote machines owned and operated by third party service providers, the risks of unauthorized disclosure of the users' sensitive data by service providers may be quite high. There are many techniques for protecting users' data from outside attackers. An approach is presented to protecting the confidentiality of users' data from service providers, and ensures service providers cannot collect users' confidential data while the data is processed and stored in Cloud computing systems.

Cloud computing systems provide various internet based data storage and services. Due to its many major benefits, including cost effectiveness and high scalability and flexibility, Cloud computing is gaining significant momentum recently as a new paradigm of distributed computing for various applications, especially for business applications along with the rapid growth of the Internet. With the rise of the era of "Cloud computing", concerns about "Internet Security" continue to increase. How will customers of the "Cloud" know that their information will be available to them, as well as secure and safe from others? The term "Cloud" in Cloud computing is the communication network or a network which is Combined with computing infrastructure.

OBJECTIVE OF THE STUDY

1. To analyze the security issues and safety measurements in high performance cloud computing systems.

2. To accomplish information classification through encoded re-appropriated contented previous to re-appropriating to cloud servers.

CLOUD MODELS

Cloud provides three types of models: Public Cloud which is open for all; Private Cloud where access is only permitted to the user who are the user of that private area; Hybrid cloud which is performing compromise task of both types of services provided by public and private Cloud. There are four deployment models which are defined as below: Private Cloud: This structure is for any single

organization whose employee internally uses it. Generally, this Cloud infrastructure is managed by organization itself or can take help from any third party

Public Cloud: The organization providing Cloud services by giving platform open for access to general public who can access it from anywhere and pay as per use.

Community Cloud: This is cloud system used by the several communities together where all the members are having equal access to this infrastructure.

Hybrid Cloud: Two or more of above cloud models jointly providing efficient services to client makes a hybrid infrastructure where some of the art may be restricted for general public and some parts are open to all for access.

Cloud Service Lifecycle:

The service life cycle for Cloud consists of the following steps showing in figure:

1. Request Formulation: The user defines at design time the functional and nonfunctional SLA requirements for the requested Cloud service.

2. Discovery and Monitoring: Discovers the candidate service offers and stores their Monitored SLA metrics and pricing information in different data repositories.

3. Matchmaking: Selects the suitable Clouds for provisioning the requested service by matching the SLA requirements to the candidate computing and storage resources.

4. Deployment: Deploys the service components on the selected providers.

5. Execution: The service is executed and its status is continually monitored at the runtime. 6. Termination: The service can be terminated upon user request. (e.g., in case of repeated SLA violations)

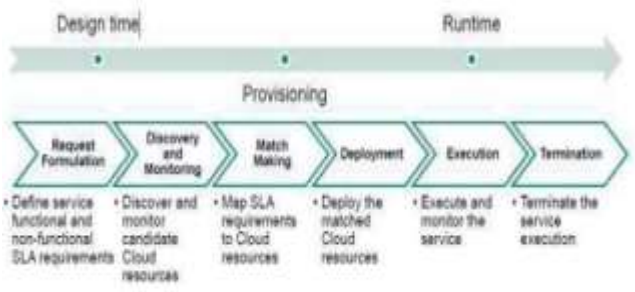

Figure 1.2: Cloud Service Lifecycle

DATA SECURITY IN CLOUD COMPUTING

Data security in cloud computing involves more than data encryption. Requirements for data security depend upon on the three service models SaaS, PaaS, and IaaS. Two states of data normally have threat to its security in clouds; Data at Rest which means the data stored in the cloud and Data in Transit which means data that is moving in and out of the cloud. Confidentiality and Integrity of data is based upon the nature of data protection mechanisms, procedures, and processes. The most significant matter is the exposure of data in above mentioned two states.

A. Data at Rest

Data at rest refers to data in cloud, or any data that can be accessed using Internet. This includes backup data as well as live data. As mentioned earlier, sometimes it is very difficult for organizations to protect data at rest if they are not maintaining a private cloud since they do not have physical control over the data. However, this issue can be resolved by maintaining a private cloud with carefully controlled access.

B. Data in Transit

Data in transit normally refers to data which is moving in and out of the cloud. This data can be in the form of a file or database stored on the cloud and can be requested for use at some other location. Whenever, data is uploaded to the cloud, the data at time of being uploaded is called data in transit. Data in transit can be very sensitive data like user names and passwords and can be encrypted at times. However, data in unencrypted form is also data in transit.

Safety Issues in Cloud Computing: Cloud computing and storage enables the clients to both ensure the data as well as to enhance the handling power. Diverse service models are sent by various organizations to appreciate the advantages of the cloud. Cloud computing categorizes the authentication feature as mentioned underneath: authentication issues experienced by cloud suppliers and authentication experienced by their clients. Authentication of the data at the customer side, so as that of the applications and the structural features ends up being the goal of the client in a cloud computing environment, so here comes the requirement for the client to plan strong usernames and passwords so as to guarantee data authentication. At whatever point the approach to a server that is responsible for posting contents is lost, at that point eventually the framework loses its ability to secure the data that is considered confidential from intra assaults. According to a continuing Cloud safety agreement statement, inside attacks are

considered as the 6th furthermost hazard in cloud computing.

Security Threats: Traditional corporate environments face a great deal of threats on the data put away, these threats for the most part target on data tapping. Cloud environments on other hand also experience the ill effects of the same issue, as the volume of data put away in this environment appears to be massive the cloud suppliers turned into the potential goal of a hacker. Authentication measures to be taken to guarantee legitimate data protection exceptionally depends on the affectability of the information that is to be protected here the attack and damage of the data concerned is again profoundly subject to the affectability level of the information. Data cracks talks about the damage caused on the data independent of the sort of information that it carries, here the potential outcomes of presenting information's related to finance, health mysteries and even about property rights is by all accounts amazingly high. In situations of data breaks the company is accounted for complete responsibility, as the breach may bring about the introduction of amazingly touchy data, thus the company may be asked to compensate for the misfortunes or complaints would be documented against that company and they may be compelled to face those charges legally. A data burst determination isn't that easy, it requires additional facilities so as to carry out that task productively; this procedure would bring about additional costs. Data protection is considered as the prime responsibility of an organization; here despite the fact that the cloud suppliers turn out with the ways and means of verifying the data, the organization alone is help responsible for any sort of breaches that happen. The CSA has structured couple of methods that would preferably verify data from such breaches, one of them is purported as the multifactor authorization system that licenses for more than one plan to guarantee data security, and it further prescribes its usage to defeat the issues of data breaches.

- Accorded Documentations and Ruptured Substantiation
- Hacked Interfaces and APIs
- Oppressed System Vulnerabilities
- Account Hijacking
- Malicious Insiders
- Cloud Service Abuses
- Dos Attacks

Cloud Security Controls

Appropriate implementation of various defensive mechanisms alone guarantees the stability of a standard Cloud security architecture. Proficient cloud security architecture must be in a position to distinguish the concerns that will occur with the security management strategies. This strategy in this way incorporated deal with these concerns with suitable security organizes. The vulnerabilities of a framework and its associated abuses can be reinforced only if the appropriate controls are located at the endorsed positions and activated as and when required. Cloud's structural safety is reliant on several issues, particularly its controls contribute more towards its protection and stability and coming up next is a couple of noticeable controls that guarantee the above mentioned features.

Cloud Security Encryption Algorithm

Some all-around created encryption algorithms which have been incorporated into the cloud computing method increases the protection of mystery. At the point when the requirement for data in the encryption procedure is invalidated then this method would essentially expel the keys and along these lines terminate the procedure.

SAFETY AND PROTECTING DATA USING ENCRYPTION

Encryption techniques for data at rest and data in transit can be different. For examples, encryption keys for data in transit can be short-lived, whereas for data at rest, keys can beretained for longer periods of time.

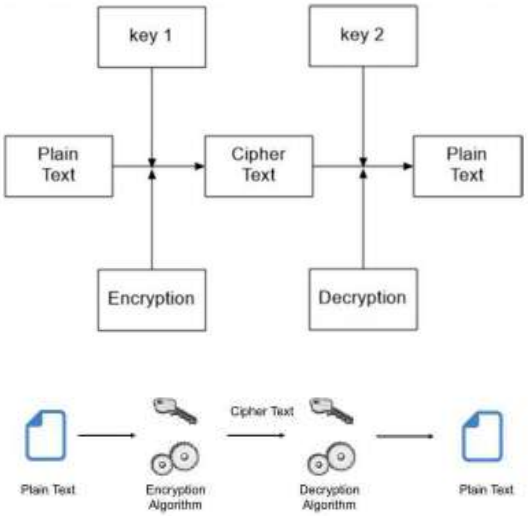

Fig 2: Basic Cryptography Process

Different cryptographic techniques are used for encrypting the data these days. Cryptography has increased the level of data protection for assuring

content integrity, authentication, and availability. In the basic form of cryptography, plaintext is encrypted into cipher text using an encryption key, and the resulting cipher text is then decrypted using a decryption key as illustrated in Fig 2.Normally there are four basic uses of cryptography:

A. Block Ciphers

A block cipher is an algorithm for encrypting data (to produce cipher text) in which a cryptographic key and algorithm are applied to a block of data instead of per bit at a time. In this technique, it is made sure that similar blocks of text do not get encrypted the same way in a message. Normally, the cipher text from the previous encrypted block is applied to the next block in a series. As illustrated in Fig 3, the plain text is divided in to blocks of data, often 64 bits. These blocks of data are then encrypted using an encryption key to produce a cipher text.

B. Stream Ciphers

This technique of encrypting data is also called state cipher since it depends upon the current state of cipher. In this technique, each bit is encrypted instead of blocks of data. An encryption key and an algorithm is applied to each and every bit, one at a time.

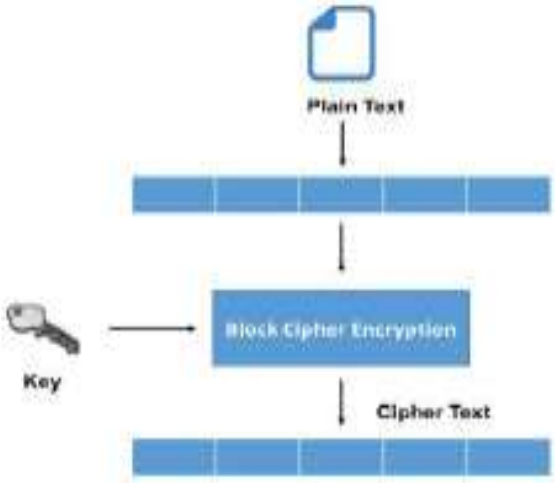

Fig 3: Block Cipher Mechanism

Performance of Stream ciphers is normally faster than block ciphers because of their low hardware complexity. However, this technique can be vulnerable to serious security problems if not used properly.

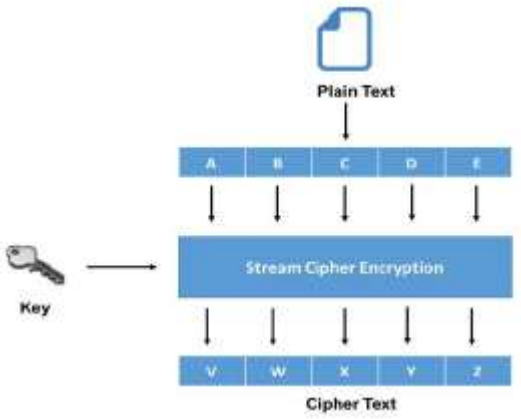

Fig 4: Stream Cipher Mechanism

As illustrated in Fig 4, stream cipher uses an encryption key to encrypt each bit instead of block of text. The resultant cipher text is a stream of encrypted bits that can be later decrypted using decryption key to produce to original plaintext.

C. Hash Functions

In this technique, a mathematical function called a hash function is used to convert an input text in to an alphanumeric string. Normally the produced alphanumeric string is fixed in size. This technique makes sure that no two strings can have same alphanumeric string as an output. Even if the input strings are slightly different from each other, there is a possibility of great difference between the outputs strings produced through them.

This hash function can be a very simple mathematical function like the one shown in equation (1) or very complex.

$$F(x) = x \bmod 10 \quad (1)$$

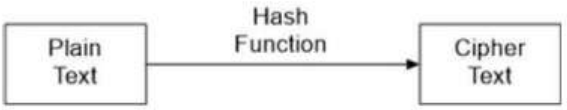

Fig 5, below shows the mechanism of hash function cryptography.

Fig 5: Cryptographic Hash Function Mechanism
All these above mentioned methods and techniques are widely used in encrypting the data in the cloud to ensure data security. Use of these techniques varies from one scenario to another. Whichever technique is used, it is highly recommended to ensure the security of data in both private and public clouds.

Advantages of Cloud Computing

Following are considered as the advantages of cloud computing:

1. Reduced IT infrastructure and computer expenses for users
2. Well improved performance
3. Reduced maintenance issues
4. Instant software upgrades
5. Improved and well established compatibility between Operating systems
6. Excellent backup and recovery
7. Improved performance 8. Excellent storage capacity
9. Well improved data security

Disadvantages of Cloud Computing

Instant convenience always arrives at a cost. Cloud computing enables us to buy services, cutting down the need for purchasing software or hardware models, this might sometimes seem expensive. An extremely reliable, high-speed, broadband Internet connection is always required for the entire duration when we make use of the software service model; hence here internet expenditures remain as a constraint. That's an aspect that we always take it for granted in countries like the United States, but it turns out to be an issue in developing countries or rural areas where the broadband services are unavailable. Dependency on our suppliers for all our needs is another drawback. Use of deaf terminals whose needs are totally limited by the provider is another limitation. Cloud computing resembles a flat that we owe for rent rather than possessing a home of our own. Clearly Cloud computing offers advantages in terms of convenience, yet there are limitations as far as the changes that we wish to incorporate.

- Easy to develop our applications.
- Scale either up or down at a very short notice.
- We need to pay for what we use alone.
- SLAS tend to administer all the happenings.
- Partition of complex systems is considered as another benefit of this technique.

CONCLUSION

Cloud computing is generally another innovation that gives tremendous advantages to the clients. Cloud computing has enormous dreams, yet the security perils put in cloud computing advance are straightforwardly identified with the advantages that it proposes. For mutually the organizations and the programmers or aggressors, cloud computing is an extraordinary possibility and gainful. Security is an unyielding necessity for cloud computing in high performance condition. In spite of the fact that cloud computing has numerous points of interest, there are as yet numerous real issues that should be explained. The primary issue is to keep up the privacy and the classification of the information. Information classification may be accomplished through encoded re-appropriated contented previous to re-appropriating to cloud servers and also for seclusion it is necessitated that lone the approved client may get to the information. Regardless of whether some gatecrasher gets access of the information unintentionally or purposefully, he won't almost certainly decode it.

REFERENCE

[1] Abbadi, I.M. and Martin, A. (2011). “Trust in the Cloud. Information Security”, Technical Report, 16, pp. 108-114.

[2] Bollavarapu, S. and Gupta, B. (2014). “Data security in cloud computing”, International Journal of Advanced Research in Computer Science and Software Engineering 4 (3), pp. 1208-1215.

[3] Chaudhary, N. (2017). “An overview of issues and data security expert reveal for cloud computing”, International Journal of Computer Science and Mobile Computing, 6 (3), pp. 154-159.

[4] Dou, W., Chen, Q. and Chen, J. (2013). “A confidence-based filtering method for DDoS attack defense in cloud environment”, Future Generation Computer Systems, 29 (7), pp. 1838-1850.

[5] Joint, A., Baker, E. and Eccles, E. (2009). “Hey, you, get off of that cloud?”, Computer law and security Review, 25, pp. 270- 274.

[6] K. Parsi & S. Sudha (2012). “Data Security in Cloud Computing using RSA Algorithm”, Int. Jou. of Research in Computer and Communication technology, Vol. 1, Issue 4.

[7] Kandukuri B. R., Paturi R. V., Rakshit A. (2009). “cloud security issues”, 2009 IEEE

Int. Conf. on Checks Computing, pp. 517-520.

[8] Khan, S. S. and Tuteja, R. R. (2015). “Security in cloud computing using cryptographic algorithms”, International Journal of Innovative Research in Computer and Communication Engineering, 3 (1), pp. 148-155.

[9] King, N. J. and Raja, V. T. (2012). “Protecting the privacy and security of sensitive customer data in the cloud”, Computer Law & Security Review, 28 (3) pp. 308-319.

[10] Mason, S. and George, E. (2011). “Digital evidence and ‘cloud’ computing”, Computer Law & Security Review, 27 (5) pp. 524-528.

[11] P. Tejas, Bhatt, A. Maheta (2012). “Security in Cloud Computing using File Encryption”, Int. Jou. ofEngg. Research and Tech., Vol. 1 Issue 9.

[12] R. Chandrahasan, S. Kalaichelvi, S. Priya, Arockiam L. (2012). "Research Challenges and Security Issues in Cloud Computing." Int. Jou. of Computational Intelligence and Information Security, Vol.3, Issue 3: pp. 42-48.

[13] Sanka S., Hota C., Rajarajan M. (2010). Secure data access in cloud computing. IEEE 4th international conference internet multimedia services architecture and application(IMSAA) 2010, pp. 1–6.

[14] Tu S., Niu S., Li H., Xiao-ming Y., Li M. (2012): Fine-grained access control and revocation for sharing data on clouds. IEEE 26th international parallel and distributed processing symposium workshops and PhD forum (IPDPSW) 2012, pp. 2146–2155

Corresponding Author

Lalit Kumar Mahore*

Madhyanchal Professional University, Bhopal

lalit.mahore13@gmail.com