SECURITY IN CLOUD COMPUTING

SUBHASHISH BISWAS AND DEB BISWAS
Affiliation(Department of Mathematics Kalinga University Naya Raipur C.G)
(Department of Computer Science and Engineering, Siksha 'O' Anusandhan Deemed to be University, Bhubaneswar, Odisha, India)

Abstract:

As the major technological organizations are shifting to store data on cloud the demand for cloud storage is rapidly increasing. Though there are major barrier in using cloud as the primary storage the topmost is privacy and security. In today's world data leak of users of some major application has become a hot topic for discussion .This paper will cover various aspects of security breach in cloud computing and how they can be avoided .Cloud Security is been starting to become a major topic in today's world as most of our internet consumption data are cloud based and most of us has been storing our personal data and information in cloud because the data breaching is one of the most concerned topic in cloud storage.In the paper I am going to present important research directions in cloud security in areas such as Trusted Computing, Information Centric Security and Privacy Preserving Models.

KEYWORDs:
Cloud Computing, Data Risks, Encryption,Cryptography, Data in Rest, Data in Transit, Data Security

1. INTRODUCTION:

As the Information and Technology Based Corporates are shifting to the cloud based storage for been more efficient at a reduced cost than others. The COVID -19 pandemic had made the enterprises continue to embrace multi-cloud and hybrid cloud strategies as the demand of cloud increase , the concern of security also increases. The Cloud computing security detects and looks after every physical and logical security issues that comes with various service models.

One of the biggest advantages of cloud computing is data can be shared among various groups which also invites the risk of leakage of data. To avoid the risk of data breach, securing the repositories is must . Sometimes data is too private for an to be stored on the cloud in the fear of data breach because of data leakage then is recommended to store data using internal organizational cloud ,this helps the security by on-premises data policy ,though it still not fully provide data security and privacy .

This paper studies the various data security methods and technology that be used to protect the data and enhance privacy at the cloud. The remainder of the paper consist of various Cloud Encryption ,discussion and challenges.

2. NECESSITY OF DATA SECURITY IN CLOUD COMPUTING AND STATES OF DATA

The data security depend upon the three services models SaaS ,PaaS and IaasS,

Generally the data at rest and data at transit are the two states which are prone to data insecurity: Data in rest generally means the data which is stored in the cloud and Data in transit means in and out of data from the cloud.

- Data at Rest

It generally refers to the data that is stored in cloud. It is very difficult for the corporates to ensure data protection for this state if the corporate does not have its own private cloud as then they would not be having physical control over the data. But the problem can be resolved using private cloud having proper access guidelines.

- Data at Transit

It refers to the movement of data from and into the cloud .Whenever the data is been uploaded and been downloaded during the process of uploading and downloading is known as data at transit. As data at transit contains various private credentials such passwords and user-details the encryption and protection is must in it.

Since data in transit is always in movement it is more prone to risk of data leakage and changes in data by certain software have the ability to eavesdropping the data and sometimes have the ability to change the data.

3. PROTECTING DATA USING ENCRYPTION

Ways of encryption of data in rest and data in transit are different as the keys of encryption of data at rest last longer whereas key of encryption for data in transit are short lived. Various cryptographic methods are applied for encrypting the data nowadays. Cryptography had increased the level of data security and protection recently.

In the most basic cryptography technique the basic text is encrypted tocipher text using the encryption key and then decrypted when needed .Basic encryption methods are as below.

- BLOCK CIPHER

It is a method of encrypting where cryptographic key and the algorithm are used to a block of data at once on a group rather than to one bit at an instance.

- STEAM CIPHER

It is a symmetric cipher where the texts are manipulated with false random cipher digit stream. It is also called state cipher as the encryption of each digit is dependent on current state of the cipher

- HASH FUNCTION

In this mathematical hash function is considered for encryption of the data. In this technique the text is converted to an alphanumeric string. This techniques makes sure that no two string has same alphanumeric string as output .A hash function can be as simple as x=x mod 30 or may be also be very complex. All the above methods are widely used in encryption techniques. It is also necessary to make sure it must be applied properly.

3. CHALLENGES IN SECURITY

There are various challenges and barrier in obtaining a perfect cloud computing environment someone of the challenges are listed below.

o ensure providing safe and secure data record and transmission through the cloud .This challenges can be very dangerous from security point of view some of them are as follows

1. *Storage of data in public cloud* :Its another security concern in cloud computing. As in general the clouds are implemented in centralized way it is at high risk exposure to the hackers if a security breach occurs. In order to avoid this it is always recommended to have a private cloud for sensitive data.

2. *Data interception*: The data in cloud computing is segmented and poses threat and vulnerability of sniffing and spoofing and third party attacks
3. *Attacks from internal management* :Sometimes the managers and employee of the service providers acts as the agent of malicious attacks from internal they may put the data of the customers at risk at certain rare cases but this must taken in consideration by proper governance internally.
4. *Insecure Data Deletion*: Insecure data deletion can have traces of data left over possessing the threat of data recovery by a hacker,
5. *Lock In*: The incompatible standards of data format shortage of encryption tools among operators as the result customers have to depend completely on the vendor.
6. *Compromise of management interface*: As the cloud computing services are delivered over the internet the third party malicious attacks are quite possible. As a result the vulnerability of security and data is amplified.

CONCLUSION

As the use of cloud storage is increasing the need of ensuring the security of cloud needs to be improved. Data and credentials are at high potential risk if not protected in a good manner. In this paper it had been tried to cover the basic of different states of data and how it may protected from data breach. Different techniques of encryption like block cipher , steam cipher and hash function are discussed for securing the data .Some of the most frequent security challenges are also been discussed here like lock in , internal security threat . Since the various industries are shifting to cloud based storage they must ensure proper data protection policy and infrastructure to ensure there consumers a better security experience in the cloud .

REFERENCES

- Scott R. Ellis, in Computer and Information Security Handbook https://www.sciencedirect.com/topics/computer-science/block-ciphers [Accessed 12th April 2021]
- https://www.geeksforgeeks.org/cloud-computing/ [Accessed 12th April 2021]