HOW EFFECTIVE IS CLOUD CRYPTOGRAPHY?

Mayuri Manish Kedar

Student

ABSTRACT

Nowadays cloud is been widely used all over the world. Cloud computing creates a virtual space on Internet, on which the user can store the data. Through cloud you can store huge amount of data virtually, rather than storing it on any physical system which will acquire space. One question comes here , "How secure is the data on cloud?", "Will it be accessed by any third-party?". Cloud computing has given solution to all these question and problems by providing "Cloud Cryptography" mechanism. Cloud cryptography adds a high layer of security to data and prevents it from any type of hacking or any third-party by encrypting the data on cloud. Currently Cloud cryptography uses different methods to secure the data. This research will discuss different methods which are used by cloud cryptography. How effective are these methods in securing the data stored on cloud. What is the future of cloud cryptography?, Will any other technology overlaps cloud cryptography? these all questions will be discussed in this paper.

Keywords: ciphertext, cryptography, encryption, decryption

INTRODUCTION

Cloud computing refers to providing applications and services on the Internet. Almost all the services present on the Internet have some or the other security protocols. Cloud Computing also provides a security protocol known as Cloud Cryptography. Cryptography is a combination of techniques for providing security to the communication online. The term crypto is derived from the Greek word "kryptos" which means hidden. The name itself refers to hiding the data. There are several threats present when it comes to data storing on Internet. Although cloud computing provides this mechanism for security, Is it really effective?, if yes how and if no how should we overcome its flaws?. There are different algorithms provided by cloud cryptography mechanism, but again comes a question how effective are they?. We will discuss it in this research thoroughly.

WHAT IS CLOUD COMPUTING?

Suppose you want to start a business or a start-up. You can store the data of your employees on a computer system, but as your company grows new employees will add up in your company then you will store the data on external hardware's, SSD's, hard drives etc which will cost you very high. You need to keep a tech-team to handle the data. In this situation, half of the systems are not being used which will cost a heavy price to the company. Here, cloud computing comes into play. Cloud computing refers to a network on internet which stores, manages and access the data. Cloud computing is provided by cloud providers such as Amazon Web Services, Azure, Google cloud etc. There are several benefits of cloud computing such as Pay-as-per go model in which cloud computing offers user to pay the charges as per the usage of the service, cloud computing gives unlimited storage of data to the users, it allows users to backup and restore the data, it allows to share information in cloud through storage, it allows to access cloud data through mobile, it allows to access and store information anywhere and anytime using Internet connection, it also reduces maintenance cost, etc. Cloud computing serves two types of models:

1. Service Models:

   Service model consists of 3 models which are:

   IAAS(Infrastructure as a Service) which helps users with the resources as a service, gives users GUI and API access, gives users dynamic and flexible services.
   PAAS(Platform As a Service) which gives facility to user regarding develop, test, run and manage the application, it supports multiple languages and frameworks, it provides users with Auto-scale property.
   SAAS(Software As a Service) which provides applications to the users which they can access with the help of internet, the services provided by the SAAS can be purchased based on pay as per use policy, it is managed from a central location and hosted on remote server.
2. Deployment Models:
   Deployment Model consists of four types of clouds mainly:

   Public Cloud: This cloud is available to all to store and access data via the Internet connection.

   Private Cloud: This cloud is only used by a particular organization to manage their data. It is divided into two types On-premise and Outsourced.

   Hybrid Cloud: This cloud is a combo of public cloud and private cloud. It provides more security to data. It provides flexibility through public cloud and security through private cloud.

WHAT IS CLOUD CRYPTOGRAPHY?

Cryptography in general means security. This security is applied to cloud which means “Cloud Cryptography”. Cloud Cryptography adds a security layer to data stored on cloud. It prevents data from any intruder by encrypting the data. By this mechanism, cloud users can access shared cloud services more securely. It protects private data and allows sharing data without any difficulty. It protects sensitive information without slowing down the information delivery. Users need not have to pay for any extra security mechanism for their data, all thanks to Cloud Cryptography. Cloud Cryptography works on encryption of the data. It alters the data into computer readable format known as ciphertext until an authorized user logs in and views the original data in plain text. It is wise because it secures the data no matter where it travels within cloud computing services.

How does it works?

Cloud cryptography works on both types of data:

1. Data in transit:
   It is the data moving between different locations over Internet. Data while travelling over Internet has threat to attacks. For this issue, the method provides a solution through the combination of encryption, network protection and authentication. While using URLs on Internet you might be observing http and https protocols been applied to the URLs. This protocol are applied by data in transit cloud encryption method.

2. Data at rest:
   Data at rest means data which reached its end point and will not be used further. It generally refers to data that is stored. The data here cannot be changed. Data at rest also uses encryption to secure the data.

How is it implemented?

Cloud cryptography is implemented in three ways as follows:

1. Symmetric technique:
   This is an encryption technique which does not require manual encryption or decryption of data. It automatically applies encryption on the data. It works on the key mechanism, in which one key is used for both encryption and decryption of data. This technique applies encryption on data and this data is only decrypted unless the user knows the required key. Key management is a necessary thing in this technique. You might use encryption for all types of data, which in turn applies keys on it. But it must keep track of all the keys. Symmetric technique also helps in key management. Symmetric techniques applies different algorithm to help in encrypting data:

   i. Standard for Advanced Encryption(AES):
   AES is one of the majorly used symmetric algorithm. In this algorithm there is only one key for encryption and decryption as well. Key sizes used by AES are 128,192 or 256 bits. This algorithm is also known as 4x4 series because it 4x4 sequence pattern for each byte. It is an effective means of algorithm in securing the data because of its key sizes.

   ii. Data Encryption Standard(DES):
   DES is another majorly used symmetric algorithm. It is developed by IBM. This algorithm also provides encryption to data. In this algorithm there is a 64 bit key, from which 8 bits are for error detection and remaining 56 bits are generated randomly while encryption. It is generally used for encrypting the hard drive data.

   iii. Blowfish algorithm:
   It is an algorithm designed by Bruce Schneier as an alternative algorithm for providing better security to the data. It uses key pattern for data encryption. The key size is of 32 to 448 bits and the block size is of 64 bits.

2. Asymmetric technique:
   This technique is also known as public key cloud cryptography technique. It uses a pair of key one public key and one private key for data encryption and decryption. The user can encrypt the data with the public key and can the data can decrypted only by the intended receiver with their private key or secret key. It is applied to system where many users needs to encrypt and decrypt the data. Asymmetric technique also provides algorithms:

i. Rivest Shamir Adleman (RSA) algorithm:
It is an algorithm which is based on generation of public and private key of two prime numbers in which public key is given to everyone while private key is kept private. Here strength of the encryption totally relies on key size. Greater the number of keys more will be the security.

ii. Elliptic Curve Cryptography(ECC):
This algorithm is based on a mathematical theory known as elliptic curve theory. This algorithm is an alternative of RSA algorithm. ECC is mostly used in the field of cryptocurrencies foe digital signatures. The algorithm merges the two keys and then the output produced by merging is used for encryption and decryption of data.

3. Hashing:
It is a function which converts the file of text into unreadable format while transmitting the text over network. Passwords, digital signatures are the concepts provided by hashing technique. It uses different algorithms such as MD5(Message Digest hashing fifth iteration), SHA-1(first iteration of secure hash algorithm), SHA-2(second iteration of secure hash algorithm), CRC32(Cyclic Redundancy Check).

RESEARCH METHODOLOGY

This study is based on secondary data which is collected from various resources such as journals, research papers, news articles and other trusted platforms.

ANALYSIS OF THE STUDY

Symmetric Technique is very effective and secure. It do not have any certain time delay problems because of encryption and decryption of data. It also provides authentication to data stored on cloud because data it uses only on key for encryption and decryption. Symmetric techniques are faster. It prevents data loss or data hacking. It is highly secure because it is uses authentication to data.

Asymmetric Technique is also secure and effective means of cryptography algorithm. Through this algorithm users need not have to exchange their keys of encrypted data. Because of this the security is increased more, as the keys do not transmit over any network. It applies non-repudiation concept because of which the user can send messages anywhere anytime. It also enables the use of digital signatures from which a receiver can understand that the message is send by particular user.

Hashing Technique is a secure, efficient and faster working algorithm provided by cloud cryptography. This technique is used in database management systems for the data location without any need of index. It makes it easier to determine whether the two data’s on the same network are identical or different. The data transmission process is faster in hashing.

CONCLUSION

Cloud computing is an emerging technology in today’s world. Mostly all organizations as well as all users are opting for this technology for storing data, accessing services and for much more things. We have seen that cloud is providing a concept of cloud cryptography for data security. Cloud Cryptography uses different techniques and algorithm for securing the data. From this paper we came to a conclusion that almost all the techniques or algorithms that are provided by the cloud are safe and secure. In future we will have some more advancements in cloud cryptography, but as far as present situation is concerned cloud cryptography is the best medium for data security on cloud. Cloud cryptography has a vast scope in future. Research is on-going to develop more secure techniques in cloud cryptography for securing cloud computing environment. Some of the areas include Quantum Resistant Cryptography, Homomorphic encryption which will allows to use the encrypted data without decrypting it first, Secure multi-party computation which allows multiple users to use a single platform without exposing the information to each other. Cloud cryptography will also provide security to 5G networks, Internet Of Things(IOT) in future. Blockchain technology is expected to have more scope in future with respect to securing cloud services and records of data transactions and securing communication between the cloud services.

REFERENCES

1. https://en.wikipedia.org/wiki/Cloud_computing
2. https://en.wikipedia.org/wiki/Cryptography
3. M. A. Vouk, “Cloud computing - Issues, research and implementations,” Proc. Int. Conf. Inf. Technol. Interfaces, ITI, pp. 31–40, 2008.
4. P. S. Wooley, “Identifying Cloud Computing Security Risks,” Contin. Educ.,vol. 1277, no. February, 2011.
5. J.N., Aws and Z.F. Mohamad. Use of Cryptography in Cloud Computing. Conference Paper published in IEEE November 2013.
6. Narang, Ashima and Deepali Gupta. Different Encryption Algorithms in Cloud. April, 2018. ResearchGate.
7. Prasad,P, A. Parul. Cryptography Based Security for Cloud Computing System.
8. Velte, T. A, Velte, T. J., Elsenpeter, R. Cloud Computing: A Practical Approach.
9. Cloud Computing Use Case Discussion Group, “Cloud Computing Use Cases Version 3.0,” 2010.
10. Cloud Security Alliance (CSA). (2010). Available: http:// www.cloudsecurityalliance.org/