IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

SECURING CLOUD WITH CRYPTOGRAPHY

Mr. Anubhab Bera
Student, Amity School of Engineering Technology
Amity University Chhattisgarh
Raipur, Chhattisgarh

Mr. Adwin Manhar
Asst. Professor, Amity School of Engineering Technology
Amity University Chhattisgarh
Raipur, Chhattisgarh

***Abstract*— Storage of data in cloud, is in hype these days. Everyone is moving towards cloud, as this is cheaper compared to buying hard disks every time to store data. And cloud is portable or, can say easy to use. However, as the number of individuals & organizations utilizing cloud is expanding and so is the information store in it, the the security of the information stored in cloud, has been a big concern for everyone. In this paper we will try to understand cloud a bit, and also have a look over the basics of cryptography. We will also discuss about the best suited method of securing data in cloud by use of cryptography. Further on, we will also give a glance upon the various suggestions provided by others.**

Keywords—Storage, Cloud, Data, Cryptography, Hash Function, Asymmetric Key

I. INTRODUCTION

One of the trends in today's digitalization era, is the storing of data in cloud. Many industries, as well as individuals, are preferring/shifting to use cloud to archive their data. It's much easier, space efficient and cheaper to store data in cloud, than to keep adding hard disks or creating an environment to store data. The most beneficial advantage of saving data in cloud is, even if the data gets deleted from local system due to any fault, we can always reclaim it from the cloud.

But with the rapidly increasing popularity of cloud, there is also the growing concerns related to the security of stored data in cloud ,among the users. Everyone becomes sensitive on the matter of privacy. And provided with the technology of today's generation, leaking of information has become a piece of cake. There have been numerous suggestions beforehand, related to the security of data, such as adding password, identification scanner etc. But the concern of security still remains.

In this particular paper ,we will be aiming to solve the concern of security of data in cloud through cryptography. We will be discussing about how using cryptography ,is more reliable in terms of security than others.

II. RELATED WORKS

The security of stored data in cloud has been a major topic of work among the researchers. Few among them are:

Rauber [1] proposed homomorphic and functional encryption with their strategies for securing cloud.

Kerchbaun [2] listed several security related issues of cloud, such as non-frequent queries, query optimization, permission & access control, and developed a prototype with high- performance.

Atyero and Feyistan [3] proposed the homomorphic encryption to secure cloud, while accessing data from it.

Jaatun et al. [4] developed an algorithm for securing data in cloud. His finding was named as, the redundant array of independent net-storage (RAIN). RAIN divides data into multiple segments, with each segment having very less information to share about the data stored in it.

Bleikertz et al. [5] gave the methodology of using the secret key principle, similar to what is used for accessing or setting up communication, between a client and a server system or between two server system, in a virtual machine but this emphasized on the security of hardware system and didn't provide any edge to the software of the system.

Sanyal and Iyer [6] designed an algorithm, on the backbone of the public key concept. A 128/192/256-bit cipher key was used for encrypting and deciphering of data, but the cons of this method is it can be used only in virtual machines, public or private cloud.
Mao [7] proposed network visualization with cryptography, including several applications.
Zheng [8] proposed encryption of information using the public key method of cryptography so that a sender can access data stored in cloud by a cipher text, without relying on the receiver of the cipher text. He developed a security enhanced mobile cloud. But using mobile cloud while surfing social networks, remained a constant issue of security.
Li et al. [9] suggested to use disorganized or fuzzy keywords to search for highly confidential data. He suggested to assign a specific key made up of fuzzy words or characters, to the files stored and giving that keyword as input, while searching and accessing the data.
Mufind mukaz ebedon [10] proposed to use of symmetric as well as asymmetric cryptography, to enhance the security of cloud.

There have been many other suggestions to enhance the security of cloud by using cryptography [11] some say to use only asymmetric cryptography, [12] some suggest to use both, asymmetric and symmetric cryptography to enhance security.
Dodis et al. [13] used the insulated asymmetric-key cryptography. Studies have found that cryptography can be useful for security, privacy and data integration. For providing a highly secured cloud storage through cryptography, the cryptographic solution used, must be of a high monitoring and performance level. And it should satisfy and ease the user, who is using cloud as a storage for their data.

III. WHAT IS CLOUD STORAGE?

Before going to the main topic of discussion, we should have some understanding about cloud and cryptography. In this section, we will be grasping some basics about cloud storage. Cloud can be described as a storage for data, applications, etc., and hence, increasing the processing power. Cloud computing provides the user, the accessibility of stored data through any remote server with a decent internet connection. It's a pay-as-you-use basis. Rather than owning infrastructures and data centers, Industries are renting access to cloud storage, for storing their data or to use any applications. This saves them from the cost of maintaining their own infrastructures, and from the labor charge it requires to maintain the data center. They can charge only for the application they use or for the storage capacity they are using. An example of such an organization is Netflix. And some other examples of cloud storage are: Gmail, and the cloud back-up of photos on smartphones.

There are total of 3 layers in cloud, that helps in cloud computing. These are: -

1.Infrastructure as a Service (IAAS)
it is the primary layer providing hardware of data center to users for low monthly price. IAAS empowers users to lease high performance servers packed with RAM, bandwidth etc.

2.Platform as a Service (PAAS)
It is the middle layer providing developers with all the needed tools for their development of applications/software.

3.Software as a Service (SAAS)
It is the uppermost layer of cloud with which the users interact.it is the finished applications/software.it helps to maintain a constant monthly revenue from the users of cloud data center.

IV. CRYPTOGRAPHY

Before discussing about the solution of security issues of cloud through cryptography, better to have some understanding about cryptography. In layman's terms cryptography can be determines as encryption of data. Cryptography is the method of converting the normal text data, into scrambled and unintelligible text. Cryptography is a way to secure data through algorithms based on mathematical concepts and calculations, with a set of rules applied to it. Cryptography revolves around 4 objectives:

1. It is totally confidential, no one can understand the data to whom it is not intended to, only user to whom the message is directed can decipher it.

2. It values integrity, i.e., the information cannot be altered while it is in storage or while it is being transited between the reciever and sender.

3. It is totally authenticated; the Transmitting and Receiving end have to confirm their identities to decipher the message.

4. The Transmitting body cannot deny the intentions behind creating the message, at a later stage.

Cryptography uses an algorithm set to encrypt and decipher data. There are mainly 3 type of cryptography:

1. Single -key or symmetric-key encryption:
   As the name suggest there is only a single key (or secret key) that the sender/creator use to encrypt data and the receiver use it to decipher the data. Using this single key, algorithms create fixed bit-length known as block cipher, of the data to be transmitted.

2. Public-key or asymmetric-key:
   In this there is a set of keys, public-key and a private-key. The public-key is related with the sender of the message to encrypt it. And the private key, that is known only by the original creator (originator), is used to decipher the data in receiver's end.

3. Hash functions:
   This is mainly used to maintain data integrity concern of cryptography. Hash functions returns a deterministic output for a input value. The output value is used to map data to a fixed data size.

So, the solution that I have come with to secure cloud storage, is by using asymmetric-key and hash function simultaneously. It will enhance the security of our data archived in cloud.

V. DISCUSSION

Asymmetric-key or (public-key) encryption, as discussed earlier, is a set of keys, that are associated with the sender and originator. The algorithm assigns the public -key to the sender of the information to encrypt the data. Without the public-key, a sender can't encrypt the data. And likewise, the private key which is associated with the originator, enables the receiver to decipher the data. Or if we see it in other way, anyone without the private-key wouldn't be able to access and decrypt the data send from the sender/creator. This encryption algorithm can be the most prefered encryption for securing our data in cloud.

This encryption method will provide the utmost level of security to the data in cloud. The sender of the data can encrypt the data with the use of public-key. This will secure the data in cloud and while on the receiver's end, only the intended receiver knowing the private key, can decipher the data and access it and no one else will be able to read or access the data, as they won't be knowing the private-key, because originator is the only one to know about the private-key and he shares the key only with the intended server.

Hash function can be used to enhance the security of our data while it is stored in cloud or being transmitted. Hash function helps to provide data integrity. With this the data can't altered while in storage or in the process of transmission.

After securing the authentication and confidentiality of the data through asymmetric-key, the only possible way of altering the data is in storage or while transmissions can solve this by using hash function. A hash function takes a bunch of characters (Key) and maps it to value of a definite length (Hash). The output values of hash function are used to index a file size. This makes the probability of collision among stored files will be less.

Hence, by using hash function & asymmetric-key in conjunction, we can level-up or enhance the security of cloud.

VI. CONCLUSION

In this paper we discussed about cloud, it's types, some basics about cryptography, many varieties of work in this field and various suggestions of various researchers worldwide. And at the last we discussed about our own idea of securing cloud through cryptography. Although there are so many ways of using cryptography to secure cloud, there is no perfectly secured method. With increase in technology, nothing is secured perfectly. Even with my own idea I believe, it can surely enhance the security of cloud, but it's not totally immune or safe. But I am sure, that this research would help people to secure their data in cloud and feel relieved of the security issues to a great level.

VII. REFERENCES

[1] Kelsey Rauber "Cloud cryptography",International journal of pure and applied mathematics, volume:85,no:1,pp:1-11,2013.

[2] Florian Kerschbaun "searching over encrypted data in cloud systems",in proceedings of 18th ACM symposium on Access control model and technologies,Amsterdam,The Netherlands.

[3] A. A. Atayero and 0. Feyistan "security issues in cloud computing: the potentials of homomorphic encryption",Journals of emerging Trends in computing and information sciences,volume:2,no:10,pp:546-552,2011.

[4] M. G. Jaatun " A farewell to trust: An approach to confidentiality control in the cloud.",pp: 1-5.

[5] S. Bleikertz "Client-controlled cryptography-as-a-service in the cloud".

[6] S.sanyal and P. P. Iyer " Cloud computing-An approach with modern cryptography", arXiv preprint arXiv:1303.1048,2013.

[7] W. Mao "The role and effectiveness of cryptography in network virtualization:a position paper." ,pp:179-182.

[8] Y. Zheng "Public key cryptography for mobile cloud",Information security and privacy, pp:435-435,Springer Berlin Heidelberg,2013.

[9] J. Li "Fuzzy keyword search over encrypted data in cloud computing",pp: 1-5.

[10] Mufind Mukaz Ebedon "Ensure data security in cloud computing by using cryptography".

[11] AWS Naser Jaber and Mohamad Fadli Bin Zolkipli "Use of cryptography in cloud computing", IEEE International Conference on Control System , Computing and Engineering.

[12] Y. Dodis "Key-insulated symmetric-key cryptography and mitigating attacks against crptographic cloud software",pp: 181-186.

[13] P. Mell, and T. Grance, "The NIST definition of cloud computing(draft), "NIST special publication, vol:800,no:145,pp.7,2011.

[14] V. Ustimenko, and A. Wroblewska, "On some algebraic aspects of data security in cloud computing,", proceedings of Applications of computer Algebra ACA 2013.Ma`laga.pp.155,2013.

[15] F. Rocha, and M. Correia, "Lucy in the sky without diamonds:Stealing confidential data in the cloud."pp.129-134.

[16] G. Ercolani, "Cloud computing services potential analysis.An integral model for evaluating software as a service," cloud computing, pp.77-80,2013.

[17] G. Zhao,C. Rong,J. Li,F. Zhang, "Trusted data sharing over untrusted cloud storage providers," pp.97-103.

[18] M. Van Dijk, and A. Juels, "On the impossibility of cryptography alone for privacy-preserving cloud computing,"IACR Cryptology eprint Archive ,vol:2010,pp.305,2010.

[19] V. Gampala,S. Inuganti, and S. Muppidi, "Data security in cloud computing with Elliptical curve cryptography,"International Journal of soft computing and Engineering (IJSCE)ISSN,pp.2231-2307,2012.

[20] D. Eyers, and G. Russello, "Toward unified and flexible security policies Enforceable within the cloud,"pp.181-186.