A SURVEY ON DATA SECURITY IN DISTRIBUTED CLOUD COMPUTING

Vanaja Malgari, Dr. Raman Dugyala
Mtech, Professor
CSE,
Vardhaman College of Engineering, Kacharam (vill), Shamshabad, Telangana

Abstract: With the increase in cloud storage, there is an increase in data security too. In the cloud computing setting, it becomes significantly serious as a result of the info is found in numerous places even within the entire globe. Though there are many security levels available the data is not completely secured by the cloud. By using the single algorithm the data is not highly secured. Combination of algorithms is used to keep the data more secure in the cloud. This paper provides more information to the researches on the types of attacks and the use of hybrid algorithm.

***Index Terms*: Cloud computing, Security, Attacks, Hybrid algorithms**

I. INTRODUCTION

Cloud Computing is used to store and access the data over the internet instead of using our own computer hard drive. Cloud Computing is utilized in huge area like colleges, industries, military etc, to store large quantity of information [2]. Companies and colleges are increasing their use of services like Google drive, Drop box, Amazon Drive, Box and Microsoft one Drive. The data from the cloud can be accessed on the request of the user. Data security and privacy protection are the main factors of user's issues regarding the cloud technology. However several methods on the topic in Cloud Computing are examined in each research and industries, information security and privacy protection have become a lot of vital for the long run improvement of Cloud Computing technology in government, industry and business. Data security and privacy protection problem area unit related to each hardware and software with in the cloud design. Data stored on the cloud have to face many problems like data breaches, data theft and unavailability of cloud data. To provide solution to these problem there are many techniques available [2]. Cryptography and steganography techniques are more popularly used for data security.

This paper divided into four sections: Section II provides highlights with background study, Section III provides the existing work and Section IV contains the conclusion and future work

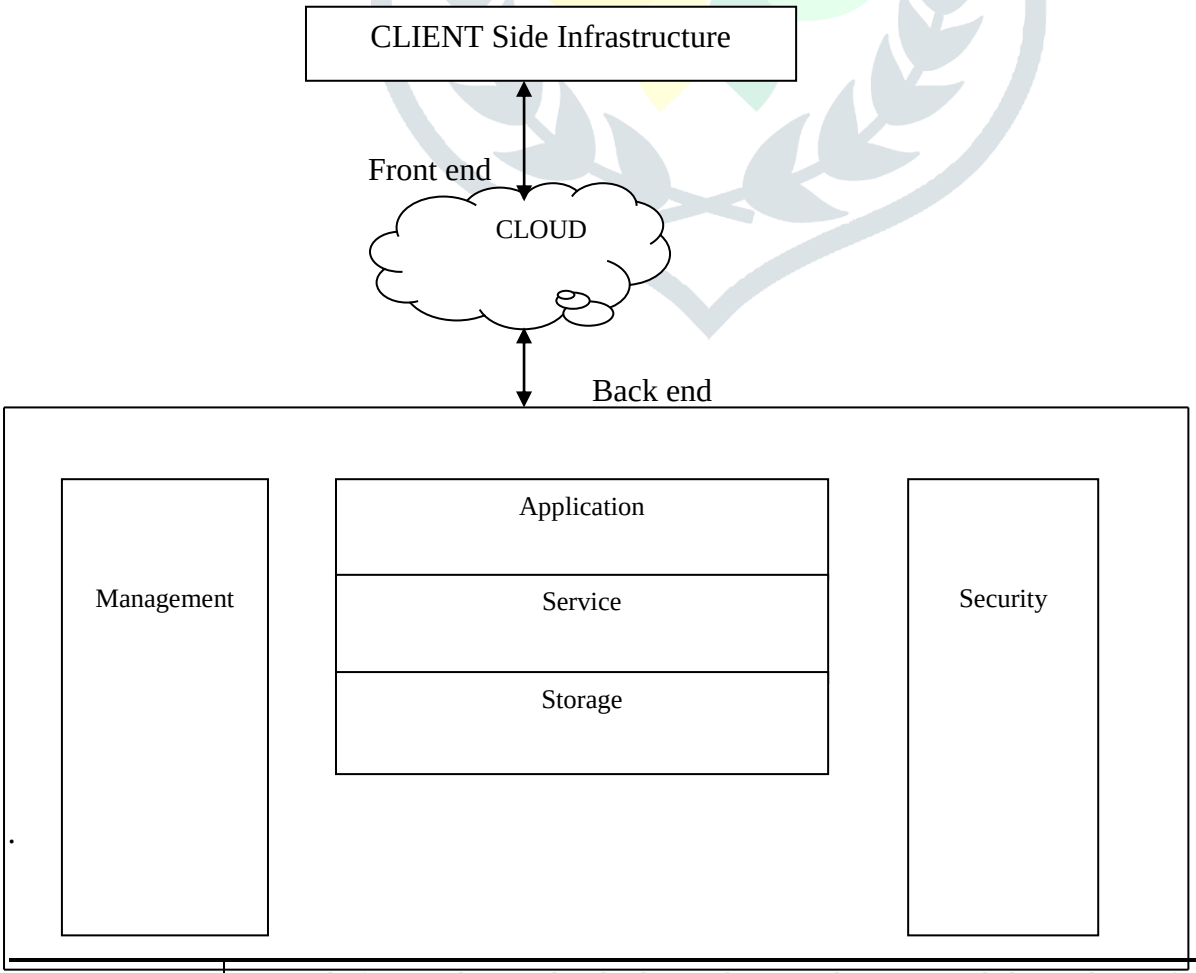


Fig.1. Cloud Computing Architecture

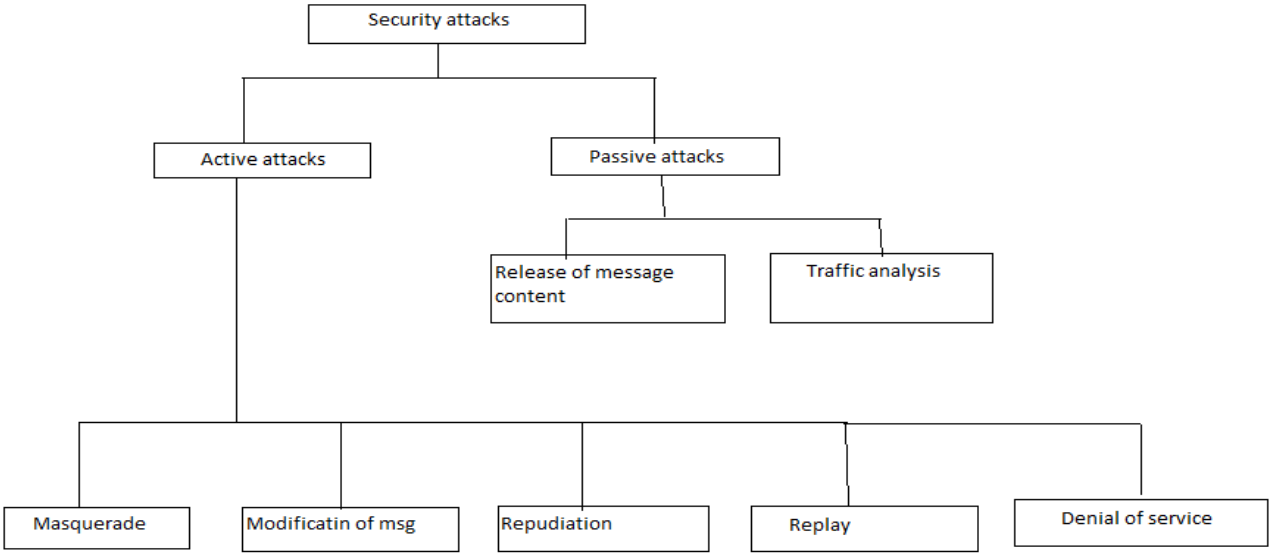
Background:
Security is the foremost necessity feature that is expected from the cloud service provider. Cryptography techniques translate original data into the unreadable form. There are firstly two types of encryption algorithms, symmetric and asymmetric. In cryptography, keys are used to turn data into an unreadable format. The single authorized person can retrieve data from the cloud server. Cipher text information is exposed for all people. The best thing about the symmetric algorithm is that they do not consume much of computation power and work with great speed for encryption. The main problem is to transfer the secret key to the receiver into a multi-user application. This algorithm needs a low delay for data encoding and decoding but provide less security. The key is well suited that is if one key encrypt the data, then other key decrypt the data and vice versa.

Security Services:
Confidentiality: No individual can read the message excluding the intended receiver. Normally, this function shows how maximum people recognize a secure system. That involves only the authenticated people are able to read the message content and no other.
Authentication: The method of providing identity of the user. It means that by using the system before sending and obtaining data, the sender and receiver specification should be confirmed.
Integrity: No modification should be done during the transmission.
Non-repudiation: It is the guarantee that no one can deny a transaction.
Types of security attacks:
Security attacks are of two types. They are Active and Passive attack.
Active attack: Active attack tries to modify system resources or change their operations. Active attacks include some change of the data stream or production of the invalid statement. Types of active attacks are as follows:

- Masquerade: Masquerade attack gets place when one entity assumes to be distinct entity.
- Modification of message: This determines that some part of a information is changed or that message is postpone or interchanged to provide an unauthorized effect.
- Repudiation: The attack is performed by either sender or receiver. The sender or receiver can deny that person has sent or received a message.
- Replay: This include that passive recovery of information and it is following the frequency to give an authorized effect.
- Denial of service: Traditional use of information facilities is restricted. This attack may have a specific target.

Passive attack: Passive attack tries to acquire or create use of data from the system without affect system resources. Passive attack exists in the creation of eavesdropping or monitoring of transference. The goal of the enemy is to get information is being transmitted. Types of passive attacks are as follows:

- The release of message content: Telephonic communication, electronic mail information or a transmitted file may include delicate or private data. We would prefer to stop an opponent from acquiring the content of certain transmissions.
- Traffic analysis: Assume that we held a method of masking of information so that the intruder even if obtained the information could not consider out any data from the information. The opponent could choose the place and identity of interacting host and could understand the frequency and length of information being exchanged. The data might be valuable in guessing the type of the communication that was taking place.



Fig[1]. Types of security attacks

In recent years there are many review articles are published on data security in cloud computing. Although these articles mainly focus on the hybrid algorithms to secure the data in the cloud. We focus on different algorithms to keep the data secure.

Utkarsh Gupta, Mrs. Shivani Saluja and Mrs. Twinkle Tiwari proposed "Enhancement of Cloud Security and Removal of Anti-patterns using Multilevel Encryption Algorithm" [1]. The main theme is to achieve security against unapproved information access. The authors used AES and Blowfish algorithm to provide structure encoding for prime degree of security

Punam V.Maitri, Aruna Verma proposed "Secure File Storage in Cloud Computing using Hybrid Cryptography Algorithm" [2]. The main theme is to reduce the time complexity by combination of the hybrid algorithms. The authors mainly focus on AES, Blowfish, RC6 and BRA algorithms and steganography, these algorithms are utilized to give block wise security to data [2]. In order to maintain the secret key, it is inserted into cover picture by utilizing the LSB method and the image is sent to valid receiver through email.

"Secure File Storage in Cloud Computing using Hybrid Encryption Algorithm" [3]. Authors of the paper are Mehul Batra, Prayas Dixit, Lalit Rawat and Rohini khalkar. The algorithms used in this paper are AES, DES, RC4 and steganography. The main theme is to reduce the time complexity from 17% to 20% less [3].

"A Brief Overview of Homomorphic Cryptosystem and Their Applications" [4]. Authors of this paper are Ayub Hussain Mondal, Manish Ranjan and Monjul Saikia. The authors mainly focus on the need of homomorphic cryptosystem and list out different types of homomorphic cryptosystem are present today.

"A Study on Data Encryption Using AES and RSA" [5]. Authors of the paper are Farheen Sultana, Bikiran Choudhury, Shobha M.S, Dr.Jitendranath Mungara. The main intention of the authors is to give better security and efficiency to the message by using the combination of two algorithms AES and RSA.

The overview of various algorithms used by the authors in the table given below:

Authors Names	Title	Combination of algorithms	Result
Punam V.Maitri, Aruna Verma	Secure File Storage in Cloud Computing using Hybrid Cryptography Algorithm [2], 2016.	AES, RC4, Blowfish and BRA [2]	Used minimum time for encryption and decryption.
Utkarsh Gupta, Mrs.Shivani Saluja and Mrs. Twinkle Tiwari	Enhancement of Cloud Security and Removal of Anti-Patterns using Multilevel Encryption Algorithm [1], 2018.	AES and Blowfish	Solve preceding security issues
Mehul Batra, Prayas Dixit, Lalit Rawat and Rohini Khalkar	Secure File Storage in Cloud Computing using Hybrid Encryption Algorithm [3], 2018	RC4, AES, DES and Steganography	Time taken for encryption is less than AES
Farheen Sultana, Bikiran Choudhury, Shodha M.S,	A Study on Data Encryption using AES and RSA [5], 2017.	AES and RSA	More reliable that increase speed and security

Dr.Jithendranath Mungara			
Fortine Mata, Minchael Kimwele, George Okeyo	Enhanced Secure Data Storage in Cloud Computing using Hybrid Cryptographic Techniques [6], 2017.	AES and Blowfish	Makes the formed hybrid algorithm

Table [1] Overview of the research papers

Conclusion:

This paper discussed about the latest review papers on hybrid encryption in the cloud computing. In my literature review I found that the data will be secured by combining different types of algorithms like DES, AES, TDES, Blowfish, IDEA, RSA, Homomorphic encryption etc. The combination of different algorithms is used to give a strong security to the data in the cloud. There are still many different types of algorithms, by using the algorithms we can improve the speed and security. The future enhancement to this study is to bring efficiency and effective result by the combination of different types of algorithms.

Reference:

[1]. Utkarsh gupta, Mrs. Shivani Saluja, Mrs. Twinkle Tiwari, "Enhancement of cloud security and removal of anti-patterns using multilevel encryption algorithms". International Journal of Recent Research Aspects ISSN, March 2018.
[2]. Punam V.Maitri, Aruna Verma, "Secure file storage in cloud computing using hybrid cryptography algorithm" IEEE 2016 conference.
[3]. Batra, Prayas Dixit, Lalit Rawat and Rohini Khalkar, "Secure file storage in cloud computing using hybrid encryption algorithm" IJCEA, June 2018.
[4]. Ayub Hussain Mondal, Manish ranjan, Monjul saikia,"A brief overview of homomorphic cryptosystem and their applications", NCIT 2015.
[5]. Farheen Sulthan, Bikiran Choudhur, Shobha M.S, Dr. Jitendranath Mungara, "A Study on Data Encryption Using AES and RSA.
[6]. Fortine Mata, Minchael Kimwele, George okeyo, "Enhanced secured data storage in cloud computing using hybrid cryptographic techniques".