A SURVEY: DATA SECURITY IN CLOUD USING CRYPTOGRAPHY AND STEGANOGRAPHY

GUNAVATHY.S[1], Dr.MEENA.C[2]

[1] Research Scholar, Avinashilingam Institute for Home Science & Higher Education for Women
[2] Head, Computer Center, Avinashilingam Institute for Home Science & Higher Education for Women

---***---

Abstract - *In recent years, cloud computing is a fast-growing technology. Cloud computing provides service to the user through an internet connection. Cloud is a group of data center and servers that place at a different location and this application is used by a user as pay on service with the help of internet. A user will pay the amount according to the amount of storage space used. The main reason for using the cloud is that the user can store and access the stored data in the cloud from anywhere anytime. The cloud user need not worry about the maintenance of software, hardware and storage space. The main advantage of cloud computing is all these services are provided at low cost for the user. For that reason, all users transferring his data on the cloud. The major issues in cloud computing are security because the information stored in the cloud is not directly maintained by the customer. While sending the data through the internet any unauthorized user can modify the data or access it. To overcome the security issues various cryptography and steganography algorithm is proposed. In this paper, focused on the basic of cloud computing and discussed various cryptography and steganography algorithm present in the existing work.*

Key Words: **cloud computing, steganography, cryptography, data security.**

1. INTRODUCTION

1.1. CLOUD COMPUTING:

Cloud computing is the trending technology that uses the network to provide service to the user. Cloud act as a software virtualized. Large scale and small scale business are spending the large amount of money to store and maintain their data. Cloud computing provide the service to the business people by storing, computation and maintaining the data at low cost. Cloud computing allows the business user or individual user to use the application through internet without installing in their system. For example: Gmail, face book, YouTube, drop box. The user will pay the amount as per the data usage. The main advantage of cloud computing is low cost, increased storage and flexibility. The major risk in cloud computing is security and privacy (i.e. by putting the valuable data on someone else's server in an unknown location).

1.2. TYPES OF CLOUD

Depending on the user or business need the different types of cloud is available. There are four types of clouds available, [4]

Private Cloud – A private cloud can be accessed by single group or single organization. It is managed by the third party or organization. Private cloud is highly secure and flexibility so private cloud is often used by larger organization or government sector.

Public Cloud – A public cloud can be accessed by any user with the internet connection and want to pay as per their usage. The files are hosted by third party. Example: Amazon, window Azure Service Platform and sales force.

Community Cloud – A community cloud will be accessed by two or more organization that has similar cloud requirements

Hybrid Cloud – A hybrid is the combination of two or more cloud (public, private, and community)

1.3. CLOUD COMPUTING MODEL

Depending on the need of user that on how to use the space and resources associated with the cloud, cloud service provider will give user a more or less control over their cloud. For example: if it will be for business use or personal home use, the cloud need will be of different types. There are three type of cloud provide: software as a Service (SaaS), Infrastructure as a service (IaaS), platform as a service (PaaS).

1. Software as a service – SaaS, also known as cloud application services. SaaS are managed by third-party. SaaS

is used most commonly used in business because do not require to install of application directly in the user system, application are directly run through the web browser [5]. Some common examples for SaaA are GoToMeeting, Google Apps

2. Infrastructure as a service – IaaS provide many computer resources, hardware, software and storage device on user demand. IaaS user can access the service using the internet [5]. Some common examples for IaaS are Amazon, 3 Tera, GoGrid.

3. Platform as a service – A PaaS system goes grade higher than the code as a Service setup. A PaaS supplier offers subscriber's access to the parts that they need to develop and operate applications over the application [5]. a number of example for PaaS is J2EE, Ruby, and LAMP

1.4. CYBER ATTACK ON CLOUD

The cyber attack causes various serious harm to cloud user. The main aim of cyber attacks on cloud computing to gain access to user data and to cloud service. The user will store sensitive information in cloud. The cloud service provider wants to take necessary step to protect data in cloud. Some of most common types of attacks on cloud computing are

Table 1: common types of attacks on cloud computing [15]

ATTACKS	DESCRIPTION	SOLUTION
Denial of Service attacks	Denial of service attack will overload the server by sending large number of request to the targeted server. The server cannot process the requests further.	Using signature based approach, firewall and filter based approach the Denial of Service attack is reduced.
Malware Injection attack	This attack injects the malicious code or any other service and creates a backdoor for attacker in the cloud environment. The aim of malware injection attack is take control of user information from the cloud environment.	At the provider's side needs to install the Hypervisor to protect the cloud environment from the malware injection attack.
Side channel attacks	Side channel attack is happen by placing a malevolent virtual machine and extracts the sensitive information from the cloud environment.	By executing the virtual firewall in the cloud computing environment can prevent from side channel attack. Another method by using encryption and decryption algorithm to secure the confidential information from the cloud environment.
Man-in-middle attack	During this type of attack, the hacker reconfigures and intercepts the communication between the two nodes or system and modifies the content of message or sequence of the message between two users.	Using proper authenticated mechanism this attack can be avoided. The various encryption and decryption algorithm like AES,DES,MD5 are used to protect the data between the two users
Authentication attack	Authentication attack arises by using the simple password and user name. The attacker will captured the mechanism used for authentication and the attacker will access the	This type of attack is avoided by using advanced authentication mechanism such as site key, virtual key and one time password.

	confidential data.	

2. CRYPTOGRAPHY

Cryptography is the process of writing the secret information in human unreadable secret format. Encrypt the plaintext into the cipher text by using the secret key which cannot be readable by an unauthorized person and transfer the cipher text between the parties on an insecure channel. After the data is received at the receiver side the cipher text is decrypted using the valid secret key and retrieves the original message. Without the knowledge of a secret key, the attacker cannot retrieve the secret message. Cryptography is used for secure communication across the insecure channel like privacy, confidentiality, non-repudiation, and authentication. There are two types of cryptography technique is available to secure the data. They are Symmetric / private key cryptography and Asymmetric / public key cryptography. Figure 1 shows the cryptography process [6].

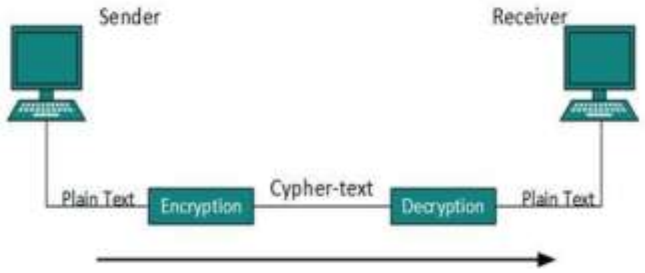
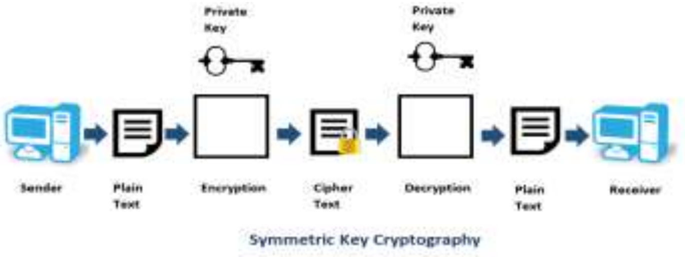


Figure 1: cryptography

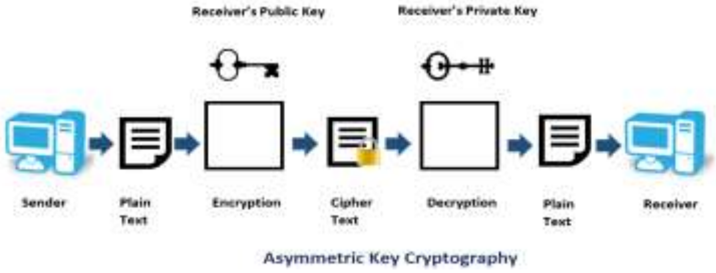
2.1. Symmetric / private key cryptography

Symmetric key cryptography also is known as private key cryptography, secret key cryptography, single-key, shared key cryptography and eventually private-key encryption. In symmetric cryptography uses a single secret key at both the side. The same key is used to encrypt the data at the sender side and the same key is used to decrypt the data at the receiver side. Both the sender and receiver must agree with the private key before any transmission starts. If anyone explores or stolen the key then the attacker can easily get the whole data without any difficulty. Example for Symmetric-key is DES, 3DES, AES. Figure 2 shows the Symmetric Key Cryptography [6].



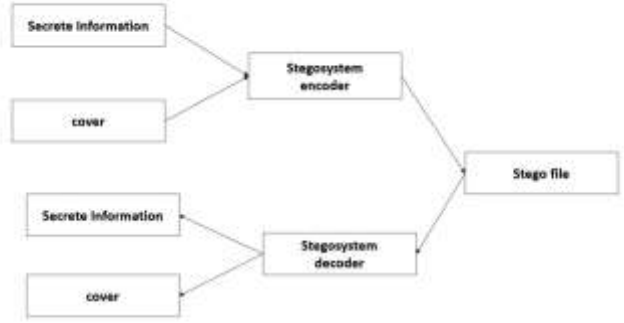
2.2. Asymmetric / public key cryptography

In Asymmetric key cryptography, two different key (I.e. public key, private key) is used. The public key is one which is available to the sender to encrypt the message and the private key is one which is available to the receiver for decrypt the message. Any sender can use the public key to encrypt the message but only receiver or authorized can use the public key to decrypt the message. The main feature of this cryptography is only authorized user can only read the message and no else. Example for Asymmetric key cryptography is RSA, ECC, ElGamal. Figure 3 shows Asymmetric key cryptography [6]



3. STEGANOGRAPHY

Steganography is the process of hiding a secret message by embedding messages within the other message like text, audio, video, and images. A secret message can be plaintext, cipher text, imaged or anything can be embedded into the cover media like text, audio, video with the help of a certain algorithm. The attacker an identify the secret information [6].



3.1. Types of steganography:

Text steganography: It consists of embedding the message inside the text file. The text steganography requires low memory. Various methods are available for hiding information in a text file. The methods are the random and statistical method, format based method and linguistic method.

Image steganography: It consists of embedding the message inside the pixel of the image. The hacker cannot identify the original message. LSB is a commonly used algorithm in image steganography.

Audio steganography: It consists of embedding the message inside the audio files. Audio steganography hides the information in AU, WAV and MP3, and sound files. There are various methods available in audio steganography. The methods are spread spectrum, low bit encoding, and phase coding.

Video steganography: it is the process of hiding the secret information inside the digital video format. Some format is used for video steganography are Mp4, MPEG, AVI.

4. CRYPTOGRAPHY VS STEGANOGRAPHY

Table 2 shows difference between cryptography and steganography [7]

Table 2: cryptography vs. steganography

DESCRIPTION	CRYPTOGRAPHY	STEGANOGRAPHY
Basic	Is to convert the message into a numerical or mathematical format which cannot identify by the hacker.	Is hiding secrete information inside the another information
Aim	Data protection	Secret communication
Structure of the message	Altered	Not altered
Popularity	Highly popular	Less popular
Supported security principles	Confidentiality, data integrity, non-repudiation, authentication	Authentication, confidentiality.
Implemented on	Only on text files	Audio, video, image and text
Output file	Cipher file	Stego file
Attacks	Cryptanalysis	Steganalysis
Visibility	Visible	invisible

5. BENEFIT OF COMBINE CRYPTOGRAPHY AND STEGNOGRAPHY [7]

Both cryptography and steganography is used for security propose. By combining these two methods can increase the security level in the cloud. In the sender side, the data is encrypted and hidden in the text file and send it to the receiver. The receiver will do the decrypt process and retrieve the original message. So a hacker cannot identify the original message.

6. LITERATURE SURVEY

A. Triple security of Data in Cloud Computing [8]:

In this paper, the author Garima Saini and Naveen Sharma provide security of data in cloud computing using a triple algorithm like DSA, DES, and Steganography. DSA is used for authentication and verification of data in the cloud. DSA assure the authenticity, integrity, and originality of data. DES is based on a symmetric key algorithm and is used for encryption of data. Stenography is used to hiding the data within the audio file to ensure security in the cloud. The main drawback in this paper is time complexity is high because of one by one process, for authentication first apply DSA algorithm and for encryption process apply AES algorithm and then stenography process. For decryption process reverse all the process at receiver side so time complexity is high.

B. Enhancing Data storage Security in Cloud Computing through Steganography [9]:

In this paper, the author Mirnal Kanti Sarkar and Trijit Chatterjee used steganography technique to unauthorized data access from the cloud. This enhanced steganography method is used to store data at cloud data storage and retrieves data from the data center when it is needed. The drawback in this paper, the proposed scheme is able to solve an only limited number of security threats.

C. Data Security in Cloud Computing using Encryption and Steganography [10]:

In this paper, the author Karun Handa and uma Singh used the strong encryption algorithm AES to encrypt the user selected data and then uploaded to the server. Next, the hiding algorithm is applied to the encrypted data and stored in the server and reversed process is done to decrypt the data and retrieve the original data. The proposed scheme is used to solve the data security problem.

D. Enhancing security in cloud computing structure by hybrid encryption [11]:

In this paper, the author Aparjita Sidhu and Rajiv Mahajan proposed the hybrid approach with the idea of whitened text using AES and MD5 algorithm. The plain text contains the text that needs to be encrypted and convert the content of the plain text to the whitened text. In this paper to provide better security in the cloud environment, to the message, the encryption in the form of the hash function is provided. This scheme is used to prevent insider attacks in the cloud service environment.

E. Secure file storage in cloud computing using hybrid cryptography algorithm [12]:

In this paper, the author Punam V.Maitri and Aruna Verma have proposed a new security mechanism to protect data in the cloud using the Symmetric key cryptography algorithm and steganography. In this proposed scheme used the combination of four algorithms (AES, blowfish, RC6, and BRA) for high-level security to data in the cloud and used the LSB steganography technique for key information security.

F. Three Step Data Security Model for Cloud Computing based on RSA and Steganography techniques. [13]:

In this paper, the authors proposed a cryptography and steganography technique to secure information in the cloud in time of data storing and sharing. The first step of security is by using cryptography technique to secure the data. RSA algorithm is used for encryption and decryption process and to generate RSA key. The second step is used to hide the encrypted data using the image data hiding technique of steganography. The algorithm used in the paper for strong security in cloud and web.

G. An Approach for Enhancing Security of Cloud Data using Cryptography and Steganography with E-LSB Encoding Technique. [14]:

In this paper, the authors proposed a technique to enhance data security in the cloud using cryptography and steganography and hash function. For enhancing data security blowfish algorithm is used for cryptography and a new efficient embedded algorithm using Embedded Least Significant Bit (E-LSB) is used for steganography and SHA-256 Hashing algorithm is used for integrity checking. Data destruction attack and data detection are applied to evaluate the security of steganography system.

7. CONCLUSIONS

Cloud computing is a rapidly growing technology. The major issue in cloud computing is security (i.e. unauthorized user access the data or modify the data) in the cloud. For that reason, the data is first encrypted using the cryptography process and hiding the data inside the text, image, audio or video file using steganography. Combining cryptography and steganography process to ensure security in cloud computing. In this paper, discussed the basic concept in cloud computing, types of cloud computing and cloud computing model. In this paper mainly focus on the various security issues in the cloud and discuss security measure in the cloud using cryptography and steganography. The paper reviews the existing cryptography and steganography algorithm in the cloud.

REFERENCE

[1] Patidar , S “Survey on cloud computing” , in Advanced computing and communication technologies , IEEE , Jan-2012..

[2] V.K. Zadiraka & A. M. Kudin, “ Cloud Computing In Cryptography And Steganography”, in Cybermetics and Systems Analysis, Vol. 49, No. 4, July-2013, UDC 681,3;519,72;003,.26

[3] Rashmi Nigoti, Manoj Jhuria & Dr. Shailendra Singh," A Survey of Cryptographic algorithms for Cloud Computing. In International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS), ISSN (print) 2279-0047, ISSN (online):2279-0055.

[4] Rong, C., Nguyen, Son T., & Jaatun, Martin Gilje. (2013). Beyond lightning: A survey on security challenges in cloud computing. *Computers and Electrical Engineering*, 47-54.

5] Yang, H., Tate, M.: A Descriptive Literature Review and Classification of Cloud Computing Research. Commun. Assoc. Inf. Syst. 31 (2012).

[6] P. Kumar and V. K. Sharma, "Information security based on steganography & cryptography techniques: A review," International Journal, vol. 4, no. 10, 2014.

[7] P. R. Ekatpure and R. N. Benkar, "A comparative study of steganography & cryptography," 2013

[8] SA Garima & SH Naveen. (2014). "Triple Security of Data in Cloud Computing. (IJCSIT) International Journal of Computer Science and Information Technologies", Vol. 5 (4), 5825-5827

[9] MR KA Sarkar & TR Chatterjee. (2014). "Enhancing Data Storage Security in Cloud Computing Through Steganography". ACEEE Int. J. on Network Security, Vol. 5, No. 1.

[10] HA Karun & SI Uma. (2015). "Data Security in Cloud Computing using Encryption and Steganography". International Journal of Computer Science and Mobile Computing, Vol.4 Issue.5, 786-791.

[11] Enhancing security in cloud computing structure by hybrid encryption by Aparjita Sidhu and Rajiv Mahajan in International Journal of Recent Scientific Research Vol. 5, Issue, 1, pp.128-132, January, 2014.

[12]Punam V.Maitri & Aruna Verma.(2016).Secure FileStorage in Cloud Computing Using Hybrid Cryptography Algorithm, IEEE WiSPNET 2016 conference

[13] Vinay Kumar pant, Jyoti Prakash & Amit Asthana.(2015). "Three Step Data Security Model for Cloud Computing based on RSA and Steganography techniques", IEEE.

[14] Mohammad Obaidur Rahman, Muhammad Kamal Hossen, Md. Golam Morsad†, Animesh Chandra Roy, and Md. Shahnur Azad Chowdhury.(2018). "An Approach for Enhancing Security of Cloud Data using Cryptography and Steganography with E-LSB Encoding Technique". IJCSNS International Journal of Computer Science and Network Security, VOL.18 No.9, September 2018

[15] Subramaniam.T.K, Deepa.B. January (2016) "Security Attack Issues And Mitigation Techniques In Cloud Computing Environments". International Journal of UbiComp (IJU), Vol.7, No.1.