A SURVEY: DATA SECURITY IN CLOUD USING CRYPTOGRAPHY AND STEGANOGRAPHY

GADDE SWETHA [1, 2]
[1] *Research Scholar, Department of Computer Science and Engineering,*
Visveswaraya Technological University, Belagavi, Karnataka, India
[2] *Department of Information Technology, RVR & JC College of Engineering, Chowdavaram, Guntur,*
Andhra Pradesh, India.
Email: ursgadde@gmail.com
K. JANAKI [3]
[3] *Department of Computer Science and Engineering, Rajarajeswari College of Engineering, Bengaluru,*
Karnataka, India.
Email: karur.janaki@gmail.com

---***---

Abstract - *As of late, cloud computing is a quick developing innovation. Cloud computing gives administration to the client through a web association. Cloud is a gathering of data focus and servers that spot at an alternate area and this application is utilized by a client as compensation on administration with the assistance of web. A client will pay the sum as indicated by the measure of extra room utilized. The primary explanation behind utilizing the cloud is that the client can store and access the put away data in the cloud from anyplace whenever. The cloud client need not stress over the upkeep of programming, equipment and extra room. The primary bit of leeway of cloud computing is every one of these administrations are given requiring little to no effort to the client. Consequently, all clients moving his data on the cloud. The serious issues in cloud computing are security in light of the fact that the data put away in the cloud isn't straightforwardly kept up by the client. While sending the data through the web any unapproved client can alter the data or access it. To beat the security issues different cryptography and steganography calculation is proposed. In this paper, concentrated on the essential of cloud computing and examined different cryptography and steganography calculation present in the current work.*

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

1. INTRODUCTION

CLOUD COMPUTING:

Cloud computing is the drifting innovation that uses the system to give administration to the client. Cloud go about as a product virtualized. Huge scale and little scale business are spending the huge measure of cash to store and keep up their data. Cloud computing give the support of the specialists by putting away, calculation and keeping up the data requiring little to no effort. Cloud computing permits the business client or individual client to utilize the application through web without introducing in their framework. For instance: Gmail, face book, YouTube, drop box. The client will pay the sum according to the data use. The fundamental preferred position of cloud computing is ease, expanded capacity and adaptability. The significant hazard in cloud computing is security and protection (for example by putting the significant data on another person's server in an obscure area).

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)

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].
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 examples for PaaS is J2EE, Ruby, and LAMP.

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	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 confidential data.	This type of attack is avoided by using advanced authentication mechanism such as site key, virtual key and one time password.

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].

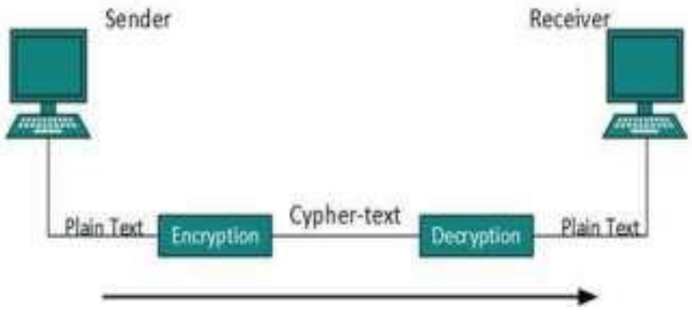


Figure 1: cryptography

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].

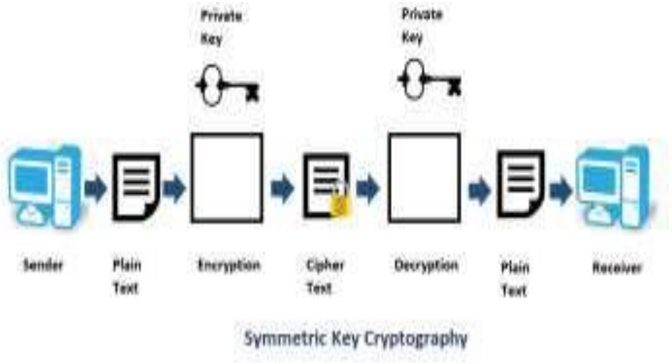


Figure 2: Symmetric key cryptography

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].

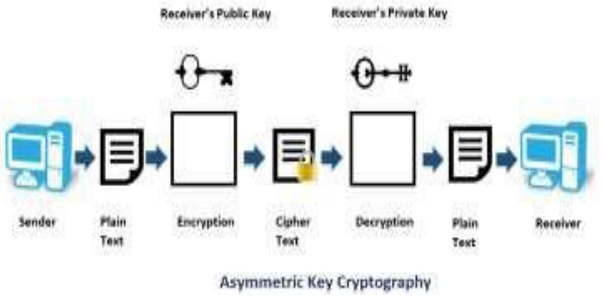
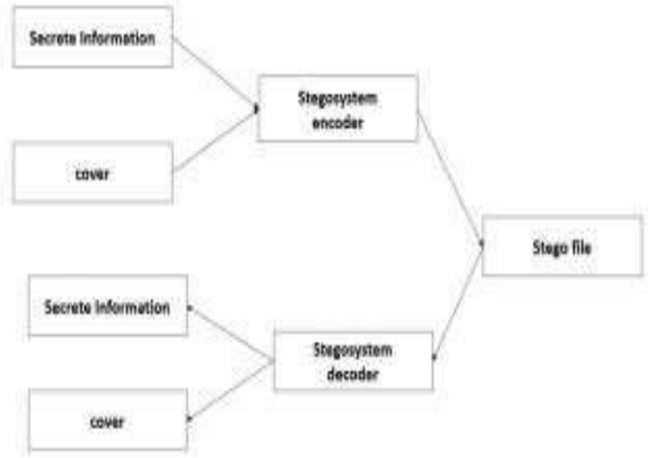


Figure 3: Asymmetric key cryptography

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.



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]

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
Structure of the	Altered	Not altered
Popularity	Highly popular	Less popular
Supported Security principles	Confidentiality, Data integrity, nonrepudiation, authentication	Authentication, Confidentiality.
Implemented on	Only on text files	Audio, video, image
Output file	Cipher file	Stego file
Attacks	Cryptanalysis	Steganalysis
Visibility	Visible	invisible

5. BENEFITS OF COMBINE CRYPTOGRAPHY AND STEGNOGRAPHY [7]

Both the 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 creator Garima Saini and Naveen Sharma give security of data in cloud computing utilizing a triple calculation like DSA, DES, and Steganography. DSA is utilized for confirmation and check of data in the cloud. DSA guarantee the genuineness, uprightness, and inventiveness of data. DES depends on a symmetric key calculation and is utilized for encryption of data. Stenography is accustomed to concealing the data inside the sound document to guarantee security in the cloud. The fundamental downside in this paper is time unpredictability is high a result of individually process, for verification initially apply DSA calculation and for encryption procedure apply AES calculation and after that stenography procedure. For unscrambling procedure turn around all the procedure at recipient side so time intricacy is high.

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

In this paper, the creator Mirnal Kanti Sarkar and Trijit Chatterjee utilized steganography procedure to unapproved data access from the cloud. This upgraded steganography strategy is utilized to store data at cloud data stockpiling and recovers data from the data focus when it is required. The downside in this paper, the proposed plan can understand a lone predetermined number of security dangers.

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

In this paper, the creator Karun Handa and uma Singh utilized the solid encryption calculation AES to scramble the client chose data and after that transferred to the server. Next, the concealing calculation is applied to the scrambled data and put away in the server and switched procedure is done to decode the data and recover the first data. The proposed plan is utilized to tackle the data security issue.

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

In this paper, the creator Aparjita Sidhu and Rajiv Mahajan proposed the mixture approach with brightened content utilizing AES and MD5 calculation. The plain content contains the content that should be encoded and convert the substance of the plain content to the brightened content. In this paper to give better security in the cloud condition, to the message, the encryption as the hash capacity is given. This plan is utilized to avoid insider assaults in the cloud administration condition.

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

In this paper, the creator Punam V.Maitri and Aruna Verma have proposed another security component to ensure data in the cloud utilizing the Symmetric key cryptography calculation and steganography. In this proposed plan utilized the mix of four calculations (AES, blowfish, RC6, and BRA) for abnormal state security to data in the cloud and utilized the LSB steganography method for key data security.

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

In this paper, the creators proposed a cryptography and steganography method to verify data in the cloud in time of data putting away and sharing.

The initial step of security is by utilizing cryptography method to verify the data. RSA calculation is utilized for encryption and decoding process and to create RSA key. The subsequent advance is utilized to conceal the encoded data utilizing the picture data concealing procedure of steganography. The calculation utilized in the paper for solid 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 creators proposed a method to upgrade data security in the cloud utilizing cryptography and steganography and hash work. For improving data security blowfish calculation is utilized for cryptography and another proficient inserted calculation utilizing Embedded Least Significant Bit (E-LSB) is utilized for steganography and SHA-256 Hashing calculation is utilized for respectability checking. Data decimation assault and data identification are applied to assess the security of steganography framework.

7. CONCLUSION

Cloud computing is a quickly developing innovation. The serious issue in cloud computing is security (for example unapproved client get to the data or adjust the data) in the cloud. Therefore, the data is first scrambled utilizing the cryptography procedure and concealing the data inside the content, picture, sound or video record utilizing steganography. Joining cryptography and steganography procedure to guarantee security in cloud computing. In this paper, talked about the fundamental idea in cloud computing, sorts of cloud computing and cloud computing model. In this paper principally center around the different security issues in the cloud and talk about security measure in the cloud utilizing cryptography and steganography. The paper surveys the current cryptography and steganography calculation in the cloud.

8. REFERENCE

[1] Patidar , S "Review on cloud computing" , in Advanced computing and correspondence innovations , IEEE , Jan-2012..

[2] V.K. Zadiraka and 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 and Dr. Shailendra Singh," A Survey of Cryptographic calculations 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., and Jaatun, Martin Gilje. (2013). Past lightning: A review on security challenges in cloud computing. PCs 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, "Data security dependent on steganography and cryptography strategies: An audit," International Journal, vol. 4, no. 10, 2014.

[7] P. R. Ekatpure and R. N. Benkar, "A relative investigation of steganography and cryptography," 2013

[8] SA Garima and 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 and TR Chatterjee. (2014). "Improving Data Storage Security in Cloud Computing Through Steganography". ACEEE Int. J. on Network Security, Vol. 5, No. 1.

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

[11] Enhancing security in cloud computing structure by half and half 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 and Aruna Verma.(2016).Secure FileStorage in Cloud Computing Using Hybrid Cryptography Algorithm, IEEE WiSPNET 2016 meeting

[13] Vinay Kumar gasp, Jyoti Prakash and Amit Asthana.(2015). "Three Step Data Security Model for Cloud Computing dependent on RSA and Steganography strategies", 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 utilizing Cryptography and Steganography with E-LSB Encoding System". IJCSNS International Journal of Computer Science furthermore, 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". Global Journal of UbiComp (IJU), Vol.7, No.1.