AN APPROACH ENHANCING SECURITY FOR CLOUD COMPUTING USING HYBRID CRYPTOGRAPHY AND IMAGE STEGANOGRAPHY

Mr. D Surendra[1], CH. Pushpalatha[2]

[1]Assistant Professor, Dept of CSE, Audisankara College of Engineering and Technology (AUTONOMOUS), Gudur, AP, India.

[2]PG Scholar, Dept of MCA, Audisankara College of Engineering and Technology (AUTONOMOUS), Gudur, AP, India.

Abstract: Cloud computing has experienced rapid growth in recent years. Cloud computing offers users services via an internet connection. A user uses the cloud, a collection of data centres and servers located in many locations, as a pay-as-you-go service through the internet. The cost is determined by the quantity of storage space used by the user. The ability to store data in the cloud and access it from any location at any time is the primary benefit of using the cloud. The upkeep of software, hardware, and storage space is not necessary for cloud users. The primary benefit of cloud computing is the cheap cost at which all of these services are offered to users.

All users are now migrating their data to the cloud because of this. Because the data kept in the cloud is not directly maintained by the client, security is one of the fundamental concerns with cloud computing. Any unauthorised user has access to the data while it is being sent over the internet and has the ability to modify it. Numerous cryptography and steganography algorithms are offered to address security concerns. This study addressed numerous cryptography and steganography algorithms found in previous works while concentrating on the fundamentals of cloud computing.

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

1.INTRODUCTION

1.1CLOUD COMPUTING

The cutting-edge technology known as cloud computing makes advantage of the internet to offer services to users. In the cloud, software is virtualized. Both large and small businesses spend a lot of money maintaining and storing their data. Businesses can benefit from low-cost data storage, processing, and maintenance thanks to cloud computing. Using cloud computing, a business or individual user can access an application over the internet without installing anything on their computer. Gmail, Facebook, YouTube, and Drop Box are a few examples. The user will pay a fee based on how much data is used. The key benefit of Cloud computing offers improved flexibility, increased storage, and low cost. The main security and privacy concern associated with cloud computing is that it places your sensitive information on a server that is located somewhere you don't know.

1.2 TYPES OF CLOUD

There are various cloud options accessible depending on the user or business demand. There are four distinct cloud types: [4]

Private Cloud - Only one organisation or group can access a private cloud. A third party or organisation is in charge of managing it. Larger organisations and the government sector frequently employ private clouds because of their high levels of security and flexibility.

Public Cloud - Anyone with an internet connection and the will to pay for their usage can access a public cloud. A third party hosts the files. Amazon, the Windows Azure Service Platform, and sales force are some examples.

Community Cloud: Two or more organisations with comparable cloud requirements will be able to access a community cloud.

1.3 CLOUD COMPUTING MODEL

Cloud service providers will provide users more or less control over their cloud, depending on their needs for how to use the space and resources connected to the cloud. For instance, a cloud need will differ depending on whether it is for company or personal use at home. SaaS (software as a service), IaaS (infrastructure as a service), and PaaS (platform as a service) are the three types of cloud providers (PaaS).

1. SaaS, also referred to as cloud application services or software as a service. Third parties manage SaaS. SaaS is most frequently used in business since it doesn't need to be installed on the user's computer; instead, it may be executed immediately through a web browser [5]. GoToMeeting and Google Apps are a couple of typical SaaA instances.

2.Infrastructure as a service (IaaS) offers a variety of computer hardware, software, and storage devices on demand. IaaS users can use the internet to access the service [5]. Amazon, 3 Tera, and Go Grid are a few frequent IaaS case studies.

3.Platform as a Service - A PaaS system is an improvement over a setup using code as a Service. The components that subscribers require to create and run applications over the application are made available to them by a PaaS provider [5]. Several examples of PaaS include J2EE, Ruby, and lamp

1.4CYBER ATTACK ON CLOUD

The cyberattack seriously harms cloud users in a number of ways. Cyber attacks against cloud computing primarily try to obtain user data and cloud services. Sensitive data will be stored by the user on the cloud. The cloud service provider intends to take the appropriate action to safeguard cloud data. The most frequent types of attacks against cloud computing include

ATTACKS	DESCRIPTION	SOLUTION
Denial Service attacks	Denial of service attack will overload The server by Sending large number frequest 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	At the provider's side needs to Install the Hypervisor to

	creates A backdoor for Attacker in the cloud environment. The aim of	protect the cloud Environment from the malware
	malware injection attack is take control of user information from the cloud environment.	injection attack.
Side channel	Side channel attack	By executing the
Attacks	Is happen by	virtual firewall in
	placing a	The cloud
	malevolent virtual	Computing
	Machine and	environment can
	Extracts the	prevent from side
	Sensitive	Channel attack.
	information from	Another method
	The cloud	By using
	environment.	Encryption and
		Decryption
		Algorithm to
		secure the
		Confidential
		information from
		The cloud
		environment.
Man-in-middle	During this type of	Using proper
Attack	attack, the hacker	Authenticated
	Reconfigures and	Mechanism this
	Intercepts the	Attack can be
	communication	avoided. The
	between the two	Various
	nodes or system	Encryption and
	and modifies the	Decryption
	content of message	Algorithm like
	or sequence of the	AES,DES,MD5 are
	message between	used to protect
	two users.	the data between
		the two users
Authentication	Authentication	This type of
Attack	attack arises by	attack is avoided
	using the simple	By using
	password and user	Advanced
	name. The attacker	Authentication
	will captured the	mechanism such
	Mechanism used	as site key, virtual
	for authentication	key and one time
	and the attacker	password.
	Will access the	
	confidential data.	

2. LITERATURE SURVEY

In order to identify faults and increase performance, the creator of the project suggests a strategy that uses data hashed message authentication codes (HMAC) and index creation. On the basis of secrecy, integrity, and availability, encryption algorithm performance is also evaluated. In this work, many algorithms are discussed along with their benefits and drawbacks. The author also offers a method for creating a secure environment for cloud computing using the Rivest Shamir Adleman (RSA) algorithm and MD5. By combining the blowfish symmetric and RSA algorithms, the authors offer a cloud computing environment that is more reliable, valuable, and safe. The use of the aforementioned technique was able to lessen or resolve the cloud's key challenges, including data security. [1] Attribute-based encryption was

suggested by the author (ABE). Later works concentrated on the question of what expressions various authorities' policies may achieve. A general KEM/DEM structure that can encrypt messages of any length was also suggested by the author for use in hybrid encryption. Based on their brilliant work, the KEM/DEM concept for hybrid encryption was created by combining a one-time MAC with symmetric encryption. [2]

The suggested structure Our goal is to produce an intermediate image whose channel compressed version is exactly the same as the stego-image given an original image and the secret data to be hidden. To achieve this, we first create the stego-image by data-embedding any of the available JPEG steganographic techniques onto the original, channel-compressed image. Then, based on the stego-image and the original image, we suggest a coefficient adjustment technique to create the intermediate image. This method guarantees that the intermediate image's channel compressed version and stego-image are identical. [3]

When comparing private cloud and open cloud in 2011, Ling Zheng et al. [9] noted disparities in the centre of them and advanced a building design of private distributed computing to support savviness, describes the construction of each layer, and illustrates the concept of the working framework and system virtualization for private distributed computing. It provides a hypothetical example of how to set up a private distributed computing system, advancing the growth of the intelligent network. Ming Li et al. [10] presented a contextual study in 2011 They first illustrate the necessity for pursue ability approval that decreases the security presentation caused by the list items using online Personal Health Records (PHR), and then they put up a flexible structure for Authorized Private Keyword Search (APKS) over scrambled cloud data. Then, in light of a modern cryptographic primitive called Hierarchical Predicate Encryption, they suggest two fresh solutions for APKS (HPE). Their responses allow for the classification and renunciation of pursue abilities; they empower skilled multi-dimensional catchphrase seekers with reach inquiry. They improve the question protection, which hides client questions from the server.

Yanjiang Yang et al. [11] make the argument that Storage-as-a-Service is an essential component of the distributed computing system in 2011. Database outsourcing is a common application for distributed storage services, and information encryption is a good way to allow the information owner to maintain control over the outsourced data. A cryptographic primitive known as searchable encryption allows for secret watchword-based database searches. For all intents and purposes, every single existing plan takes the single-client setting into consideration. The setting of a large corporate outsourcing database to the cloud demands multi-client searchable encryption. They offer a practical multi-client searchable encryption scheme that has a number of advantages over the established approaches in order to bridge this gap.

The idea that distributed computing has been envisioned as the leading edge building design of IT Enterprise was put forth in 2011 by Wang et al. [12]. It transfers the databases and application programmes to concentrated large server farms, where the management of the information and administrations may not be entirely reliable.

A writer focuses on the concern of ensuring the integrity of data archiving in cloud computing. They specifically take into account the task of allowing a third-party

auditor (TPA) to assess the credibility of the dynamic information stored in the cloud for the benefit of the cloud customer. The evaluation of whether the customer's information stored in the cloud is indeed there, which can be done by TPA, terminates the relationship with the consumer rucial for achieving scale economies in cloud computing. A formal approach for evaluating the impact of adaptability and heterogeneity on the coordinated Cloud security administrations is presented by Syed Naqvi et al. in 2012 [13]. They plan to develop a method of evaluating the impact of unified Cloud arrangements on security capacities under various working settings and characteristics. Their findings from this analysis will help firms choose the appropriate security structural measures planning that will work with their cloud architectures and requirements for execution.

Huaglory Tianfield et al. [14] offer a thorough analysis of the challenges and concerns with distributed computing security in 2012. They first look into how the essential characteristics of distributed computing—more specifically, multi-tenancy, adaptability, and outsider control—affect the security requirements. Then, they analyse the requirements for cloud security in light of the key concerns, namely, privacy, respectability, accessibility, trust, and review and consistency. They discuss the classification of security issues in distributed computing according to scientific principles. By using a cloud security building design, they describe the security concerns in distributed computing.

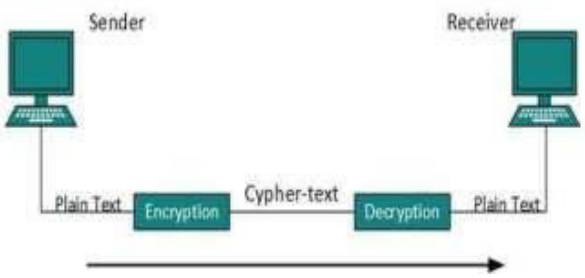
Abdullah Abuhussein et alrecommendations .'s from 2012 [15] Healthcare, education, business, and many other industries look to distributed computing to understand the ongoing lack of volume, foundation, availability, and observing power. On the other hand, moving data to the cloud implies ambiguously shifting control of the client's data to the cloud administration provider. As a result, the safety and protection of the client's data become crucial issues. In order to choose security options that are both suitable and robust at the same time, learner clients interested in moving their work to the cloud must survey and examine potential distributed computing administrations. They try to identify and categorise a list of traits that correspond to the various aspects of cloud security protection, too. These credits can be used to research and evaluate distributed computing services so that users can make well-informed choices. They can be used by cloud administration providers to create and/or provide better cloud arrangements.

In 2012, Wentao Liu et al. [16] made the argument that distributed computing's security problem is crucial and can halt the field's rapid advancement. As indicated by the distributed computing concepts and characters, it introduces some distributed computing frameworks and deconstructs distributed computing security issues and its approach. The most important security concern in distributed computing is the protection of information and management accessibility. A single security strategy is insufficient to address the distributed computing security challenge; instead, a variety of established and novel advancements and methodologies must be used to safeguard the whole distributed computing architecture.

The procedures for cloud appropriation and cloud security are presented by Nikhilesh Pant et al. in 2014 [17] evaluation to look into any security and consistency recommendations in a cloud context. They go into great detail on how a company may continue to evaluate security and consistency while using cloud computing. The associations involved in the cloud

reception process would benefit from their technique and specific concepts presented in this study.

Liu X [18] discusses distributed computing information security challenges in 2015, including issues with information transmission security, information hoarding security, and information security



administration security. Focus on comprehensive information management affect cloud security examination, highlighted as a significant step in the development of distributed computing, and made an effort to list the contrasting techniques and long-term improvement direction.

Gupta et al [19].'s innovative structural planning of the IT industries was envisioned in 2016. Due to the transparent architecture modelling of the cloud environment, security and protection are the main challenges. They look at the risks associated with cloud security and discuss the most recent security measures to deal with securing the cloud environment. Additionally, they put forth a cutting-edge Trisystem for cloud protection against information leaks, providing comprehensive security for cloud structural planning.

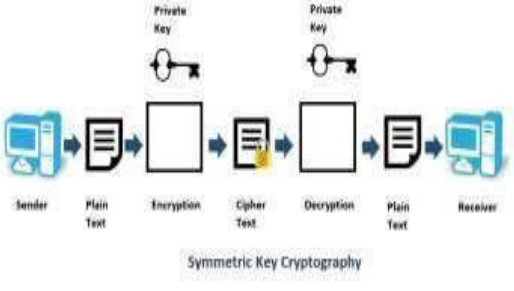
3. CRYPTOGRAPHY

Writing hidden information in a format that is secret yet unreadable by humans is the process of cryptography. Use a secret key that is unreadable by outsiders to encrypt the plaintext into the cypher text, then send the cypher text between the parties across an insecure channel. The cypher text is decoded using the current secret key after the data has been received at the receiver's end, restoring the original message. The attacker cannot have access to the secret message without knowing a secret key. For secure communication via an unsecure channel, such as for privacy, secrecy, non-repudiation, and authentication, cryptography is utilised. To safeguard the data, two different types of cryptographic techniques are offered. They are Equal in Size.

private key cryptography and Asymmetric / public key cryptography. Figure 1 shows the cryptography process [6].

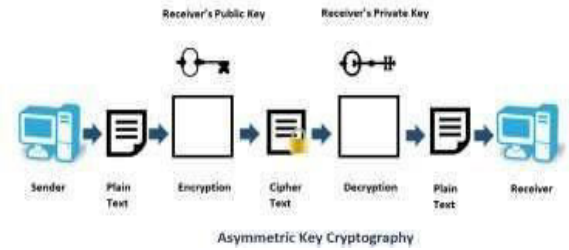
3.1Symmetric / private key cryptography

Symmetric key cryptography is sometimes referred to as single-key, shared key, private key cryptography, secret key cryptography, and eventually private key encryption. A single secret key is used on both sides in symmetric cryptography. The same key is used to encrypt the data on the sender's side and to decode the data on the receiver's side of the communication. Before any transmission can begin, the sender and recipient must concur on the private key. If the key is discovered or stolen, the attacker will have little trouble accessing all of the data. DES, 3DES,and AES are examples of symmetric-key. Figure 2 displays symmetric key encryption.



3.2Asymmetric / public key cryptography

Asymmetric key cryptography makes use of two distinct keys: a public key and a private key. The sender has access to the public key, which is used to encrypt messages, and the recipient has access to



Asymmetric Key Cryptography

the private key, which is used to decode messages. Any sender can encrypt a message using the public key, but only the recipient or someone who has been given permission can decode it. The primary characteristic of this encryption is that only authorised users may read messages. ElGamal, RSA, and ECC are examples of asymmetric key cryptography. Asymmetric key cryptography is seen in Figure 3 [6].

3. STEGANOGRAPHY

Steganography is the method of concealing a secret communication by enclosing text, audio, video, and picture messages within the other message. A certain method may be used to embed a hidden message in cover material like text, audio, or video whether it be plaintext, cypher text, images, or anything else. The attacker might recognise the secret information [6].

3.1Types of steganography

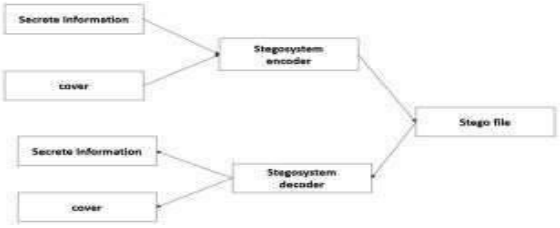
Text Steganography: using text entails hiding the message within the text file. Little memory is needed for the text steganography. There are several ways to conceal information in a text file. The techniques include linguistic, format-based, and random and statistical approaches.

Picture steganography: This technique involves hiding the message within a single image pixel. The original message cannot be located by the hacker. In picture steganography, the LSB algorithm is frequently employed.

Image steganography: The message is hidden inside the audio files using audio steganography. In AU,WAV, MP3, and sound files, information is concealed using

audio steganography: The techniques for audio steganography are numerous. The techniques include phase coding, low bit encoding, and spread spectrum.

Video steganography: is the practise of concealing sensitive data within a digital video file. Mp4, MPEG, and AVI are a few of the formats utilised for video steganography.



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
Suppord security principles	Confidential, data integrity, non-repudiation, authentication	Authenti n, confident iality.
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 ANDSTEGNOGRAPHY [7]

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

The authors of this project, Garima Saini and Naveen Sharma, offer security for data in cloud computing using triple algorithms, including DSA, DES, and Stegano DSA for data authentication and verification. Data uniqueness, authenticity, and integrity are guaranteed by DSA.

Data encryption is done using the symmetric key algorithm DES. To maintain data security in the cloud, stenography is employed to hide the data within the audio file. The primary flaw in this work is its high temporal complexity, which results from its one-by-one procedure of using the DSA algorithm first for authentication, the AES algorithm next for encryption, and finally the stenography process. Time complexity is high since the entire decryption procedure is reversed at the recipient side.

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

The authors of this research, Mirnal Kanti Sarkar and Trijit Chatterjee, employed steganography to prevent unwanted access to cloud-based data. When necessary, this improved steganography technique pulls data from the data centre and stores it in the cloud. The suggested system in this study has the limitation that it can only address a small number of security concerns.

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

The user-selected data in this project was encrypted by the author Karun Handa and Umasingh using the powerful encryption technique AES before being uploaded to the server. Following the application of the concealment algorithm to the encrypted data, which is then saved on the server, a reverse procedure is carried out to decode the data and retrieve the original data. The proposed plan is utilised to address the issue of data security.

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

The hybrid technique with the notion of whitened text utilising the AES and MD5 algorithm was proposed in this research by the authors A parjita Sidhu and Rajiv Mahajan. The text that has to be encrypted and converted from plain text to whitened text is contained in the plain text. This study offers message encryption in the form of a hash function in order to improve message security in a cloud setting. This system is employed in the setting of cloud services to combat insider assaults.

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

The authors of this research, Punam V. Maitri and Aruna Verma, have suggested a brand- new security method that combines steganography and the symmetric key cryptography algorithm to safeguard data on the cloud. For high-level security of the data in the cloud, this suggested approach combines the four algorithms (AES, blowfish, RC6, and BRA) and uses the LSB steganography technique.

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

The designers of this project suggested using steganography and cryptography to protect data being stored and shared in the

cloud. The first stage in security is to safeguard the data using encryption. The RSA algorithm is used to encrypt and decode data as well as to create an RSA key. The encrypted data is concealed in the second stage through steganography, a picture data concealing method. The method employed in the study for robust cloud and online security.

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

The developers of this research suggested a method for improving data security in the cloud utilising cryptography, steganography, and hash function. In order to increase data security, the blowfish method for cryptography is employed, along with a novel, effective embedded technique that uses the Embedded Least Significant Bit (E-LSB) for steganography and the SHA-256 Hashing algorithm for integrity checks. Data detection and data destruction attacks are used to assess the steganography system's security.

6.CONCLUSIONS

The technology of cloud computing is expanding quickly. The main problem with cloud computing is security (i.e., unauthorised users accessing or changing data). Because of this, the data is first encrypted using the encryption procedure, and then it is Stegano graphically hidden inside the text, picture, audio, or video file. steganography and cryptography are used to assure cloud computing security. The fundamentals of cloud computing, its many forms, and cloud computing models are covered in this essay. This article discusses numerous cloud security challenges and discusses cloud security measures utilising steganography and cryptography. The study examines the steganography and cryptography algorithms used nowadays in the cloud.

7.REFERENCE

[1] S. Patidar, "Survey on Cloud Computer," Advanced computing and communication technologies, IEEE, Jan-2012.

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

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

[4] C. Rong, Son T. Nguyen, & Martin Gilje Jaatun (2013). Beyond lightning: A study of cloud computing security issues. Electrical engineering and computers, 47–54.

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

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

[7] A comparison of steganography and cryptography by P. R. Ekatpure and R. N. Benkar, 2013

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

[9] TR Chatterjee and Mr. KA Sarkar. Steganography to Improve Data Storage Security in Cloud Computing (2014). International Journal of Network Security, Volume 5, Issue 1.

[10] Karun and Uma are SI (2015). "Data Security in Cloud Computing Using Steganography and Encryption." 786-791 in Volume 4 Issue 5 of the International Journal of Computer Science and Mobile Computing.

[11] Aparjita Sidhu and Rajiv Mahajan's article, "Hybrid encryption improves security in cloud computing framework," appeared in the January 2014 issue of the International Journal of Recent Scientific Research, Volume 5, Issue 1.

[12] Aruna Verma and Punam V. Maitri (2016). Hybrid Cryptography Algorithm for Secure File Storage in Cloud Computing, IEEE WiSPNET 2016 conference

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

[14] Mohammad Obaidur Rahman, Md. Shahnur Azad Chowdhury, Md. Golam Morsad, Md. Kamal Hossen, and Animesh Chandra Roy.

[15] (2018). Using cryptography, steganography, and the E-LSB encoding technique, a method for improving the security of cloud data is presented. International Journal of Computer Science and Network Security, September 2018, Vol. 18 No. 9

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

Author's Profile:

Mr. D. SURENDRA, He has guided P.G and U.G students. At present he is working as Assistant Professor in Audisankara College of engineering and technology, Gudur, Tirupati (Dt), Andhra Pradesh, India.

CH. PUSHPALATHA has Pursuing her MCA from Audisankara College of Engineering and Technology (AUTONOMOUS), Gudur. affiliated to JNTUA in 2022. Andhra Pradesh, India