International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Cryptostega Mesh: A Triadic Approach for Secure Information Transfer using Cloud Environments

Leelendra Reddy Gogula*[1], Harshith Kurapati[2], Bhuvana Reddy Bhimireddy[3], Alekhya Nimmagadda[4], Radhika Rani Chintala[5], Vijaya Chandra Jadala[6]

Submitted: 10/12/2023 **Revised**: 21/01/2024 **Accepted**: 31/01/2024

Abstract: As technology evolves every day, the risks related to the internet are increasing rapidly. Some of the most common threats over the Internet include insecure data transmission and MITM attacks. Data integrity, privacy, and confidentiality are the main pillars to avoid these types of attacks. With the intention of tackling the risks mentioned, this paper presents an innovative approach where the information can be shared from one user to another in a secure way where the transfer was user specific i.e., no person other than the sender and the intended receiver can even know that the data was getting shared. The methods used in this paper include Cryptography, Steganography and Cloud Computing. This research implements a methodology combining cryptography and steganography along with cloud computing to provide more security that helps us avoid data security issues. The implementation includes RSA and DES encryption from Cryptography, data hiding in images using LSB Steganography, configuring cloud sources for storage, data transmission using cloud user management, and instant data deletion in the cloud with the help of various services offered by the cloud environment. The analysis of this approach is done by comparing the image obtained after completion of steganography which hides the data attained after encrypting it using hybrid cryptography with the image that is used for steganography to examine whether the changes made in the image can be identified easily or not. It is done using various types of graphs such as histograms, bar graphs, and difference images which are further explained in the results and analysis section.

Keywords: *Cryptography, Steganography, Cloud Computing, Storage, Hashing*

1. Introduction

Information Security is a challenging task to accomplish these days as many attacks are happening now and then. The graphs in Fig. 1 show the data leaks that happened over the past decade in the world of computers, data, and security. Sometimes vulnerabilities we don't concentrate on our part captivate attackers to exploit the data that we are holding whether it is at rest or in the transmit state. Securing information from our end whether it is stored or whether it is in transit should be our utmost priority while using the internet.

Information security was built on pillars of confidentiality, integrity, authentication, and authorization[1].

- Confidentiality refers to the way the information is kept secret and private from internet sources.
- Authentication is a way to find out whether we are communicating the data in transit to the right user using various means like password validation, biometric validation, user validation apps, and one-time validation either using links or numerals that are delivered to mobile or email.
- Authorization is a way to ensure that the person is permitted to access the information or not based on the role of the person.
- Integrity implies whether the data is transmitted correctly i.e., is the data that is transferred or stored was safe, not tampered with, and not modified.

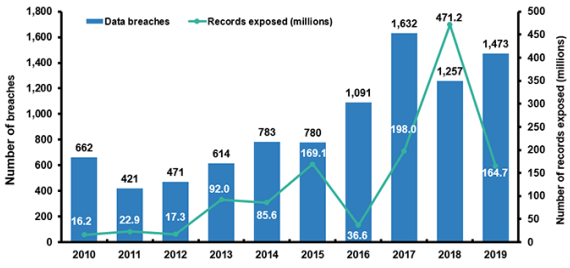

Fig. 1. Comparison of last decades data breaches, records exposed every year.

[1] *Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Guntur, Andhra Pradesh, India, 522302*
ORCID ID : 0009-0003-8883-5757
[2] *Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Guntur, Andhra Pradesh, India, 522302*
ORCID ID : 0009-0009-5867-1943
[3] *Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Guntur, Andhra Pradesh, India, 522302*
ORCID ID : 0009-0002-1636-1823
[4] *Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Guntur, Andhra Pradesh, India, 522302*
ORCID ID : 0009-0004-3340-6725
[5] *Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Guntur, Andhra Pradesh, India, 522302*
ORCID ID : 0000-0001-9078-7692
[6] *Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Guntur, Andhra Pradesh, India, 522302*
ORCID ID : 0000-0002-5149-5176
**Corresponding author email: leelendrareddygogula08@gmail.com*

As technology is getting more efficient, the attacks regarding security are becoming more intense[2]. The solutions that already existed in the past and worked without a hassle were flawlessly taken down by the new technology which makes securing the data difficult. To overcome this challenge, hybrid techniques that combine two or more fields are required. Concerning the challenge of information security, in this paper, we have used steganography, cryptography, and cloud computing together which makes a great trio to deal with issues of information security.

There are major ways to implement information security like cryptography, steganography, and cloud computing.

1.1. Cryptography

Cryptography is a way to encrypt data using various methods such as public key cryptography, private key cryptography, and block ciphers. Cryptography contains two processes, encryption, and decryption. Encryption is a way to change data from readable format to unreadable format. In other words, changing plain text to cipher text. Decryption is the method of changing cipher text to plain text[3]. Private key encryption uses only one key to encrypt and decrypt the data. In public key encryption, data is encrypted using a public key and decrypted using a private key. In more detail, in public key cryptography, there will be two keys for every user known as public key and private key. The private key is kept with the user themselves and the public key can be shared and accessed by any valid user. When sending data, the sender encrypts the text using the public key of the receiver, and the person receiving it decrypts the data using his private key. Block ciphers encrypt the data by dividing the whole message into small blocks. Hybrid cryptography refers to using one or more encryption algorithms for securing data. Among all the three types, public key encryption is said to be more secure.

1.2. Steganography

Steganography is a way to hide data from other sources such as text, images, audio, and videos which cannot be differentiated by humans. Text Steganography is a way to hide the data between the text using spacing, some text marks, and special symbols as shown in Fig. 2. Image Steganography is a way to hide data in images using a modification of pixels and RGB colors in the images as shown in Fig. 3. Fig. 4 portrays the Audio Steganography process of hiding data by modifying the amplitude in the audio files. Video steganography is the process of modifying the video stream to hide data that can't be noticeable[4].

Hidden _messages could also _appear in the form of miniscule typeface, size, or spacing _differences. _Extra spaces before certain words could _indicate that _those words _or the first letters of those words should be taken apart from the entire message to reveal a secret embedded _utterance. _This is especially handy in html files _since _extra spaces show up only in the source file and _not on the webpage _display. Letters that are slightly larger _might similarly be taken to reveal a hidden message. It could even be that, through use _of invisible ink between lines of text or tiny print within underlining or punctuation, the true message is _not visible at all. Some of these methods may be _easier to detect than others, but they have had their own practical uses in history, as we will saw in the previous section. Can _you find the message hidden in this paragraph?

answer: MADE IT OUT SEND MONEY

Fig. 2. Example of Image Steganography

In general image steganography is used to transfer data from one user to another. Steganography is majorly used by organizations that need to transfer highly secure information from one source to another source. Some of the most common uses of steganography are hiding sensitive data, secret communication, and data transfer over insecure channels.

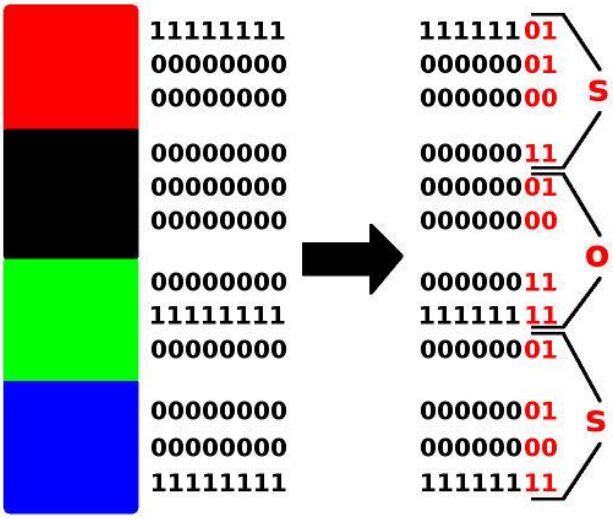

Fig. 3. Example of Image Steganography

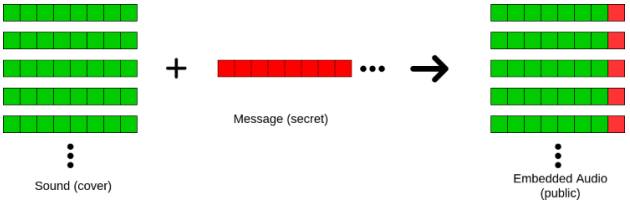

Fig. 4. Example of Audio Steganography

1.3. Cloud Computing

Cloud is the resource that provides computing services over the internet. Cloud also includes many services such as storage, virtual machines, operating systems, software, and many more. Cloud is considered as the safe way to store and access data for further purposes. The cloud uses a shared responsibility model which makes the cloud very secure to

use. The shared responsibility model defines what was taken care of by the cloud providers and which parts should be taken care of by the user. So, using cloud computing to store data and transfer data to other people is way more secure than using other sources of communication[5].

This paper uses cryptography and steganography with the aim of achieving information confidentiality, hashing for ensuring integrity of the image obtained after steganography and cloud computing for user authentication & secure transfer of data from one user to another. Providing confidentiality, integrity and authentication helps in ensuring the data is secure during the transfer or at rest.

2. Literature Review

Giridhar Maji and Sharmistha Mandal developed a Scheme that entails embedding a secret message into a cover picture and a stego key as an embed key. The reference image is broken into blocks, each of which has its binary code. The encrypted message is translated to binary and compared to block LSB pairings. If a matching block code is identified, it is added to the encoded message. If no match is found, the block with the fewest modifications is picked and its LSB is updated. For safe embedding and extraction, the shared secret key is encrypted using public-private key cryptography. A dictionary-based pre-encoding module, which is optional, decreases payload by indexing words in the secret message[6].

Arnold Gabriel Benedict proposed utilizing the ZIP technique to compress file formats such as music, video, pictures, and text. With a header, image-based files are randomly organized for encoding and decoding. Bit distribution methods such as sequential hashing and improved hashing enable safe and random payload distribution across pictures, making decryption exceedingly difficult. Image hashing is combined with a password for further protection, making decryption hard for hackers[7].

Ridhima Ahluwalia explained that several encryption methods are used to safeguard concealed communications, making it extremely difficult for hackers to break the security levels. The main task is to use DCT to transform a cover picture into a certain frequency domain, followed by RSA to convert a converted message. The frequency of JPEG compression is altered using the DCT-based approach. The Arnold transform encrypts the message further and provides a one-to-one point position shift. The suggested approach contains capabilities such as image complexity for efficient embedding, and the algorithm assures three-level security during the embedding process. The end user guarantees that data such as encrypted photographs are stored in the cloud, and consumers get access with confirmation IDs and tokens, assuring security[8].

Masoud Alajmi and Ibrahim Elashry created the system, which embeds an encrypted payload into QR codes by selecting the appropriate dimension N, creating a QR code with a message, encrypting the payload, and utilizing the XOR technique with the QR code. The procedure is reversed when extracting the data, using the original QR code, and conducting decryption to recover the payload. This technology focuses on the indistinguishable and secure embedding into QR codes, giving consumers false or harmless messages while assuring that it can survive steganalysis. The parameters for QR code production and decryption are critical for proper extraction and display as regular QR codes[9].

T. Kalaichelvi and P. Apuroop created the captcha system to address security issues such as confidentiality and authenticity. The captcha system that has been implemented is as follows. They constructed a random string with a policy like today's password policy that ends with a dot. They also created a system for obtaining a series of numbers to be encoded with the original text via steganography for each letter in the resulting string. The process is as follows: we first obtain the ASCII equivalent and then convert it to binary form. If the number of ones exceeds the number of zeros, append a zero to an empty string, followed by the length of the bitstream[10].

Mustafa S. Abbas and Suadad S. Mahdi proposed an approach in which the text to be encrypted was transformed into binary form. It was then saved in an array. The array is now separated into two pieces, with one portion encrypted using RSA encryption and the other using the AES technique. Both obtained strings were concatenated after encryption. The cipher text is now compressed to lower the transparency of a picture. To conceal the data, the text was later steganographed in a picture. This file's hash value is computed, and the image is subsequently saved in the cloud environment. To acquire the plain text, the receiver does the same process in reverse order[11].

Table 1. Analysis of each conventional method and drawbacks

Paper	Confidentiality		Integrity	User Authentication	Constraints Unrestricted
	Text Encryption	Securing data in Image			
[6]	✓	✓	✗	✗	✗
[7]	✓	✓	✓	✗	✗
[8]	✓	✓	✗	✓	✗
[9]	✗	✓	✗	✗	✗
[10]	✓	✓	✗	✗	✗
[11]	✓	✓	✓	✗	✗
[12]	✓	✓	✓	✗	✗
[13]	✗	✓	✗	✓	✓
[14]	✓	✓	✗	✗	✓
[15]	✗	✓	✗	✗	✗

Sabyasachi Pramanik and Samir Kumar Bandyopadhyay employed digital signatures in conjunction with steganography to ensure security standards. According to them, we generate a public and private key pair using the RSA algorithm. The sender's private key is now utilized to encrypt the signature image. The encrypted signature header information is included in LSB in blue and pixel information in red in the cover picture. The receiver now decrypts the data in a stego picture using the sender's public key[12].

According to Jacob Adeboye Ajala and Sanika Singh, Cloud Server Systems generate main and secondary keys at random. This data is saved by the user as a record pertaining to specific information. Second, the data owner immediately encodes the record hiding data into a picture, which is then separated and stored in the cloud. To prevent unauthorised users from accessing data, the cloud server generates a shared key for the sender and recipient. The server is essential during the data-sharing procedure. Steganography is used, and the key and data are encoded in an image. Later, encrypted data are recombined so that the recipient may access the original file. Finally, the recombined file is decrypted to obtain the original file[13].

Lipi Kothari and Rikin Thakkar applied the "change order of elements" data concealing approach. Steganography technology may be used to hide data on the internet in a variety of ways. All these strategies are well-detailed in the study. The strategy taken in this work is to encrypt a message or data before converting it to ASCII and subsequently to binary. Now, apply it to a webpage by using the random function to choose four techniques, conceal data with these methods, and lastly publish it on the internet. Decryption requires an open website and open-source code. The website's unenclosed data is binary. Recognize four ways for converting binary to ASCII and ASCII to text. Finally, the text must be decrypted[14].

Wen-Chuan Wu and Shang-Chian Yang proposed a method for securing private images in the cloud. They employed two methods: private image embedding and private picture extraction. Before we begin, we need two colour photos, known as the cover image and the secret image. The three least important bits of each colour pixel must be removed first in picture embedding. They employed a technique known as YCbCr colour conversion. The next step is private image extraction, which aims to remove the cover image's embedded hidden image. First, determine which picture is a cover image and remove it from the cloud system. Following that, the three least important components of each colour pixel are taken to create the previously reserved values[15].

N. Manohar and Peetla Vijay Kumar demonstrate how steganography may be used to hide secret messages in videos. First, they conceal the hidden messages inside the video. To do this, they employ three distinct approaches, like tools in a toolbox: SLSB, neural networks, and fuzzy logic. These strategies aid in the concealment and detection of hidden messages in videos. Following that, they will examine the video quality after concealing the secret message, as well as whether the communications are secure. They employ PSNR and MSE to assess the video quality after the messages have been buried[16].

Dev Kumar Chaudhary and Sandeep Srivastava demonstrated a Java program that employs sophisticated window tools and algorithms. They are Huffman coding and the Rjindeal algorithm for text compression and encryption, respectively. The program is intended for hiding data, which can be text or pictures, within an image. They encrypt the text before putting it into the picture to increase security[17].

Yani Parti Astuti and De Rosal Ignatius Moses Setiadi describe a method for hiding secret information in images (embedding) and subsequently detecting those concealed secrets (extraction). Scheme for Embedding is defined as combining a hidden message with an image. You have a standard image and a hidden message (in a particular code) of the same size. First, you read the picture as well as the hidden message. Then you utilize computer techniques (such as XOR) to combine them. The result is a new image with a concealed message inside. The scheme of Extraction is considered as revealing the secret message in the new image. You simply need the new image with the hidden message (known as a stego image). By using more computer operations (XOR), you reveal the hidden message. What you get is a black-and-white picture with the original secret message[18].

Information in the table (Table 1) shows which constraints were satisfied in the implementations that exists. It also shows that each methodology available has a restriction in one or more constraints. To satisfy all the constraints, this paper proposes a methodology with secure and safe standards for information transfer between two users.

3. Methodology

This methodology includes cryptography, steganography, and cloud computing along with a security topic known as hashing, which is used to check the integrity of any data for example text, images, documents, etc., This implementation focuses on encryption of data before steganography, then using the cloud as a service to transfer data using the cloud user management and access control. The total implementation is divided into 4 parts,

- Cryptography
- Steganography
- Cloud Computing
- Integrity Checking

The implementation works on the sender side and receiver side as shown in Fig. 5 and Fig. 6 respectively.

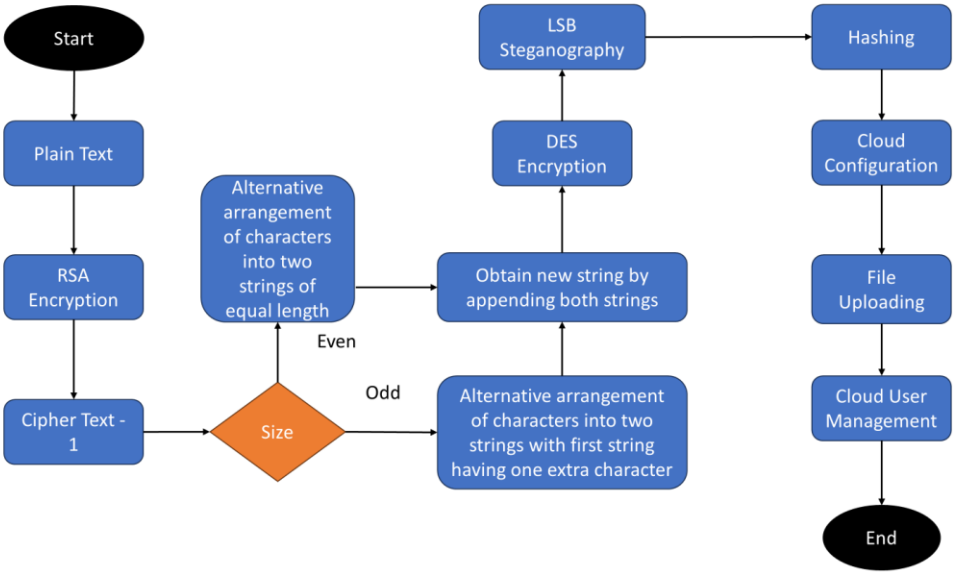

Fig. 5. Flow of steps on sender's side

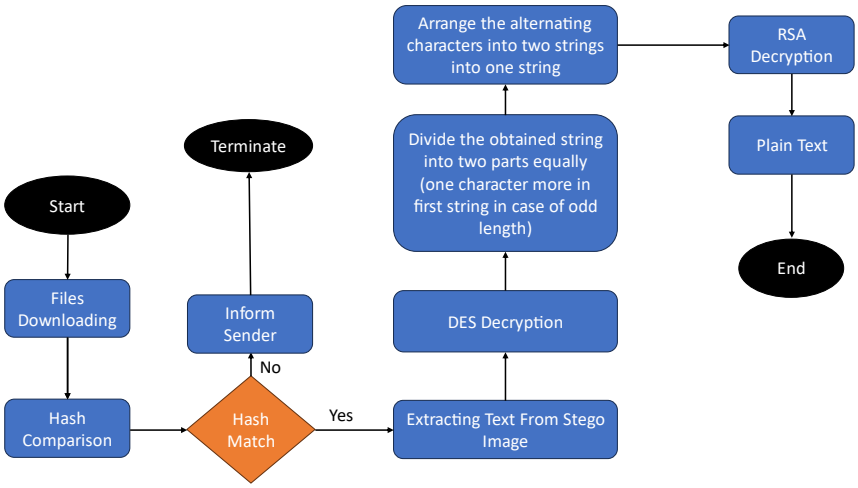

Fig. 6. Flow of steps on receiver's side

3.1. Cryptography

3.1.1. Sender Side

Firstly, the plain text is converted into cipher text using the RSA algorithm in public key encryption. Now, the obtained string is divided into two strings such that characters at odd positions are taken into one string and the characters at even positions are taken into another string. Next, append both the strings as one string placing the oddly positioned sub-string first and then the obtained string was encrypted using private key encryption by the DES algorithm.

3.1.2. Receiver Side

The Text extracted from the image will be decrypted once by using the DES algorithm with the key that was shared securely by the sender. Now, the text obtained will be divided into two parts with the same length. In case the length of the string is odd, then the first part contains one extra character. Now, a string is formed by appending one character at a time from each of these strings until all of them are done. The obtained string will be decrypted using the RSA algorithm using the private key of the receiver. Now the text obtained will be the plain text that was meant to be secured and it has received the person that was intended to reach.

3.2. Steganography

3.2.1. Sender Side

The encrypted text is hidden in an image using the least significant bit(LSB) steganography technique. The LSB technique modifies the last bit of every pixel in the image which makes it difficult for the human eye to see but data

can be stored in the images without getting noticed. The text that is to be stored in the image was converted into ASCII values for every corresponding character. Then every character is converted into 8-bit binary format[19]. Now every least significant bit in the pixel values of images was replaced by one bit of the binary string we generated.

3.2.2. Receiver Side

From the image that was obtained from the sender, the least significant bit of every pixel was extracted, and every 8 bits were grouped. After grouping every 8 bits, the corresponding decimal number was obtained, and then the ASCII character correlated with the number was appended to the string.

3.3. Integrity Checking

3.3.1. Sender Side

A hash value will be generated using a hashing algorithm which helps us in checking the integrity of the file. Even if there is a slighter modification in the stego image(the file obtained after steganography), the hash value will be changed drastically. So, the sender computes the hash value of the stego image and sends the hash values along with the key used for private key encryption in the DES algorithm in a text file along with the stego images in a cloud service to the user.

3.3.2. Receiver Side

The receiver generates the hash values of the files downloaded from cloud storage. The receiver compares the hash value computed to the hash value sent by the sender. If the hash values match, then the receiver starts extracting text else he reports to the sender that the data was compromised.

3.4. Cloud Computing

There are various cloud providers in the market. In this implementation, Amazon Web Services(AWS) is used. AWS provides a service named simple storage service(S3) to store data. The storage in S3 is known as a bucket and every file in the S3 bucket is called an object[20]. The files followed by steganography and hashing were uploaded into the S3 bucket. Now, using the cloud user management tools, create a user with access to only storage service. In the case of AWS, identity and access management(IAM) was the service that AWS provides for user management. Then, we build an IAM role that sends the email to the appropriate user. IAM is used because it supports temporary access and time-bound permissions, reducing the risk associated with long-standing access rights. Users can be granted access for a specific task and time, after which the permissions expire. After the sender has uploaded the files, we build a lambda function that deletes the files immediately after a specific time limit. Lambda serves as an essential tool for automating the timely and efficient removal of these access permissions, enhancing security and compliance. A Lambda function in AWS is a serverless service, which allows users to manage various services[21].

3.4.1. Cloud Procedure

- We first create a IAM role for a lambda service providing S3 full access and Lambda functions full access.
- Then, we now create a Lambda function using the role created in previous step.
- After that, we create an S3 bucket, and in lambda function we add this bucket to trigger for all write options i.e., addition of file.
- The lambda function contains the following code,

  - Import boto3 library.
  - Inside the default function provided, make the program sleep for a particular time in order to stop instant deletion and define the following steps inside the default function.
  - Specify the S3 bucket name that will be the focus of deletion actions.
  - Get a list of each object that is presently stored in the designated S3 bucket.
  - For each object identified in the list:
    - Using the object's unique key and the bucket name as references, issue a command to remove the object from the S3 bucket.

- Now, upload all the desired items that need to be communicated to the other party.
- The final steps involve creating an IAM user having only S3 access, and the AWS cloud shares the user credentials directly through the mail making us less worried about security.
- The sleep defined in the Lambda function ensures that the contents are deleted after mentioned time.

4. Algorithms and Implementation

To test the methodology that was discussed, let's start by encrypting sample data. Consider this as the plain text(PT). Now, PT is encrypted using the public key of the receiver using the RSA encryption algorithm. After the encryption, we get an encrypted string. Note this as cipher text 1(CT1). Now, the CT1 is divided into two parts such that the characters at even positions are considered as one string, and the characters at the odd positions are considered as another string. Assume these strings as divided cipher text odd(DCO) and divided cipher text even(DCE). Now, Append DCO and DCE as a single string called as divided cipher text(DC). Then, apply DES encryption on the DC.

The obtained text was the final encrypted text(ET). The ET obtained was hidden in the image using the LSB steganography. LSB Steganography is easier to implement and harder to detect by the human eye. The image obtained after the implementation of steganography is called a stego image(SI). Now, the hash value of the SI is computed and stored in a text file named hash of stego image(HSI). The SI and HSI are uploaded into a cloud storage. We store the SI and HSI files by creating a S3 bucket and uploading them as objects in this bucket. Now, create an IAM user for the receiver along with his mail and access only to the S3 service. AWS sends a mail to the receiver that he has a new account on AWS and gets to know that some data was uploaded for him to check out. As soon as the time limit has been reached, we delete the objects available in the AWS bucket using Lambda functions. The receiver applies the same implementation in reverse order to obtain the PT. The outputs and results of the implementation were discussed in the results and analysis section.

5. Results and Analysis

Each step shown in flow chart(fig. 5) are implemented and the results are as follows:

- Let PT be "Hey! This is a working example of steganography and Cryptography alongside cloud computing".
- Now, after encrypting once with the RSA algorithm with the public key of the receiver, we get CT1 as "m7SBbGFpoQF7C35T3SS1B1CQ991GE0Zrh04RAmFdscyVEYpG7QIy7EAxomOVCazM/MERTBOzfcAqpXSAYmWgPAJUY3dgpgpfXv14i6qGDe4qgUsC8ul4MpSGJL4wYnud+gIDjXM33Fo3SbCEMCwX7icilCh8JjJF/VGStrLXakwOyUqNO5XOxBf2wK8xpY9SP9IA/Jm3HhSl5lI6rkCS3bThvlrq2KPvvGV0IZTasNDlc+8AAbdrF4qcj9+r7iulzYBHOfOGkgDR+B5rnizJ+QD9i6cuPyqyitV/42J1Xf8avbPPD2naUtxXHRRUdBlIFj0yU+IlKflKlb+nl0Aw4A==".
- Next, divide CT1 into two strings DCO and DCE as mentioned in methodology and implementation. In this case, DCO is "mSbFoFC53SBC91EZh4AFsyEp7I7AoOCz/ETOfApSYWPJYdppX1iqD4gs8lMSJ4Yu+IjM3oSCMw7clhJJ/GtLawyqOXxfw8p9PI/mHS5IrC3Tvr2PvVITsDc8AdFqj+7uzBOOkD+5nz+DicPqiV4JX8vPDnUxHRdlF0UIKll+lA4=" and DCE is "7BGpQ73TS11Q9G0r0RmdcVYGQyExmVaMMRBzcqXAmgAU3ggfv46GeqUCu4pGLwndgDX3F3bECXiiC8jFVSrXkOUN5OB2KxYS9AJ3hll6kSbhlqKvG0ZaNl+Abr4c9rilYHfGgRBriJQ96uyyt/21fabP2atXRUBIjy+lfKbn0wA=".
- The next step is to combine DCO and DCE to obtain DC. Here, DC is "mSbFoFC53SBC91EZh4AFsyEp7I7AoOCz/ETOfApSYWPJYdppX1iqD4gs8lMSJ4Yu+IjM3oSCMw7clhJJ/GtLawyqOXxfw8p9PI/mHS5IrC3Tvr2PvVITsDc8AdFqj+7uzBOOkD+5nz+DicPqiV4JX8vPDnUxHRdlF0UIKll+lA4=7BGpQ73TS11Q9G0r0RmdcVYGQyExmVaMMRBzcqXAmgAU3ggfv46GeqUCu4pGLwndgDX3F3bECXiiC8jFVSrXkOUN5OB2KxYS9AJ3hll6kSbhlqKvG0ZaNl+Abr4c9rilYHfGgRBriJQ96uyyt/21fabP2atXRUBIjy+lfKbn0wA=".
- Applying the DES algorithm on DC, we get encrypted text(ET). In this instance, ET is "357rB22IFXEjAIYASAmwTst0EUo907P/rucGB0X9JkcERCdpJUni8hijuojAUaJ31V0UM1nUCLWfGfzB0sWrgpT59twd7y/j/B+OzQU42BJwzCyKaAQvRa5mgSdIwQxNXA0MUYHT2LKKamU6lhozkKRtqkxUsZZzG0I5EPJNksK8NnegAZFYI0CDCwfiMc1ERNHJ9T6NcGFrhScdIEExdVnMSjmBbvaNFK1WV+UO0F6AZeB5/EA/w+RpsAG9aE4LfbzCTZPIgCReJ7smNvXpT5xXOrqUUzeps9TMLgc2DWoZfeIdXOykglu7U05PBY74tMMXTInHCDPrlo0kpLsAeEyby4su4QkFdLt04d8qlFoiuC36kLAZBdXgvZvUg2I3Tl/i3FXiMFDMBEUCLgji/13HqC/RCYz36gLrU5CmADHDzrYNxdXW5PLZUciTXxkttx1SZ3hw4IMmyCG4HztUNw==".
- The obtained ET is now hidden in an image file by using steganography as discussed in the previous section. The images before and after steganography are shown in Fig. 7 and Fig. 8 respectively.
- Fig. 7 and Fig. 8 does not contain any difference that can be seen to the human eye. It is almost impossible to say that the images are modified by just looking at both of them.

Fig. 7. Image before implementation of steganography

Fig. 8. Image after implementation of steganography

- In order to perform more detailed analysis, histograms, bar graphs, and difference images were discussed for comparison of both the images.
- Fig. 9 shows the histograms of both the images before and after steganography. Fig. 10 displays the histogram of both the images combined. We can see that the lines almost overlapped on each other which shows that there is no drastic change in the image pixelation and modification in bytes.

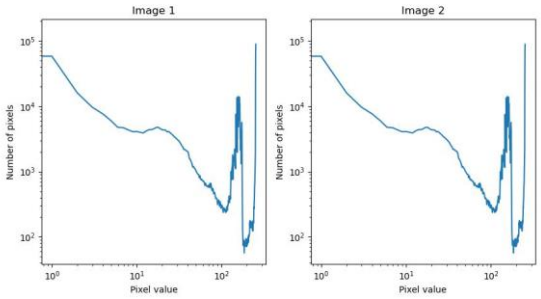

Fig. 9. Histograms of images before and after steganography

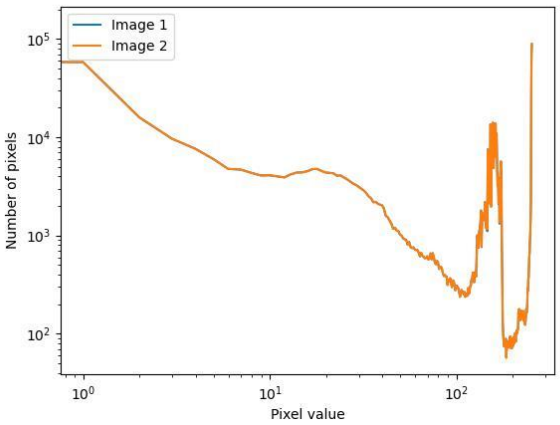

Fig. 10. Combined Histograms of images before and after steganography

- The graph in Fig. 11 shows the pixel values of each image compared against frequency. The graph portrays the frequency of every pixel in the image. Both the images show almost similar results apart from minor changes that are at some particular pixel values as shown in the below image. In this case, the frequency differs at higher pixel value, but it needs high analysis to find out whether it was caused by modification of image on purpose or losing data in transmission.

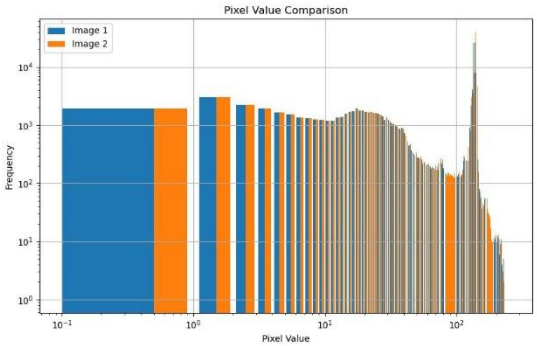

Fig. 11. Bar Graph of both images measuring pixel value against frequency.

- In order to compare pixel to pixel difference in both the images, a difference image is obtained. In the difference image shown in Fig. 12, there was no pixel modification that was more than 1 pixel since there is no colour that represents it as shown in the scale on the right side of the image. This is because in every byte, we only modified the least significant bits which are almost negligible in order to calculate the change.

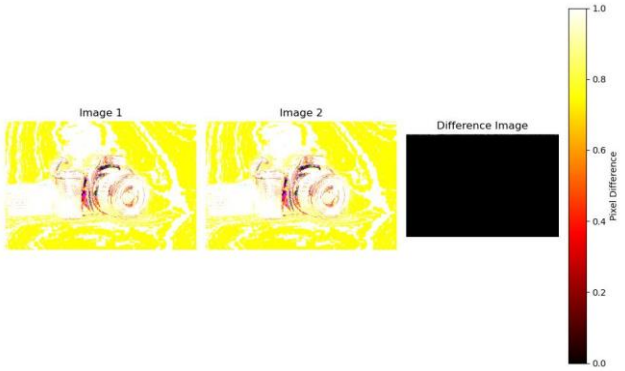

Fig. 12. Difference Image of both images

- The hash value(SHA-256) computed for the stego image is "fcb1c49abbc078bdeaaf2d40c23958495c13c017415a3c0a29b688ea5bc83944".
- The files stego image and hash value(stored in a text file) are uploaded into cloud storage using a service and the configuration is done in a way that a lambda function gets triggered after successful upload of files and this function deletes the files after certain time mentioned in the lambda function. The implementation regarding this is shown in Fig. 13, Fig. 14, Fig. 15, Fig. 16.
- Fig. 13 shows the creation of role that permits lambda function to access contents of only S3 bucket.

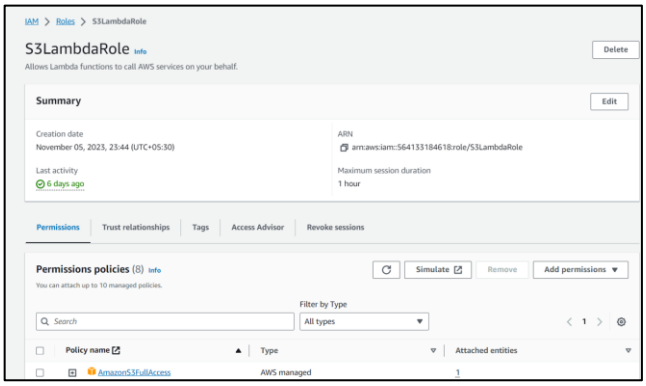

Fig. 13. Creation of IAM Role

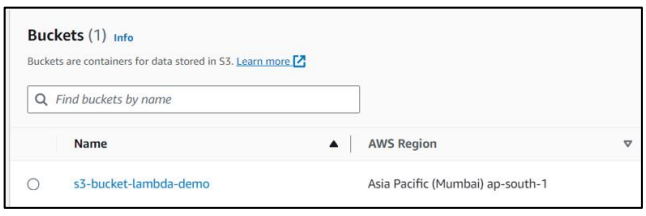

Fig. 14. Creation of S3 bucket

- The image(Fig. 14) represents the creation of a storage type service offered by AWS known as S3.
- The picture(Fig. 15) displays the successful build of a serverless service offered by AWS called as the Lambda.
- The representation in Fig. 16 shows that the lambda function is successfully mapped to the S3 bucket, i.e., after the uploading of files completes, the particular lambda function gets triggered, and execution starts.

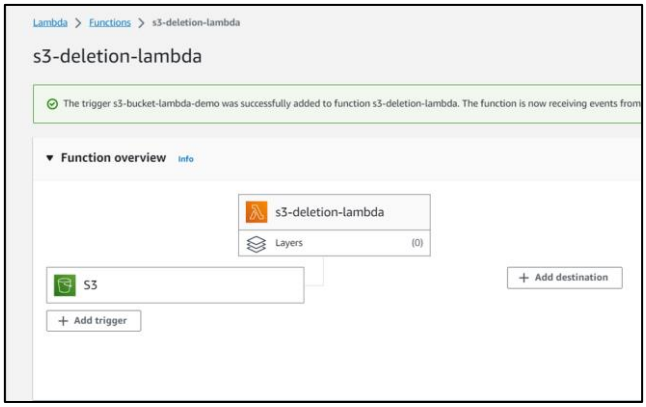

Fig. 15. Creation of Lambda Function

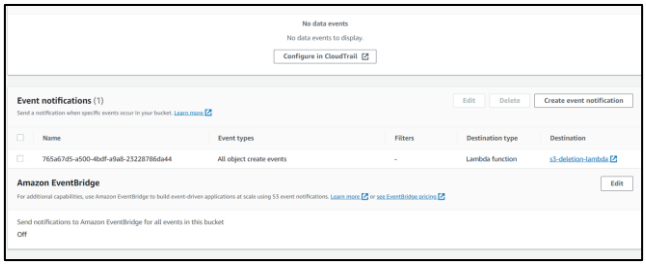

Fig. 16. S3 and Lambda integration result

- The images, Fig. 17 and Fig. 18 show the successful uploading of files and execution of lambda function by deleting the files after a particular time.

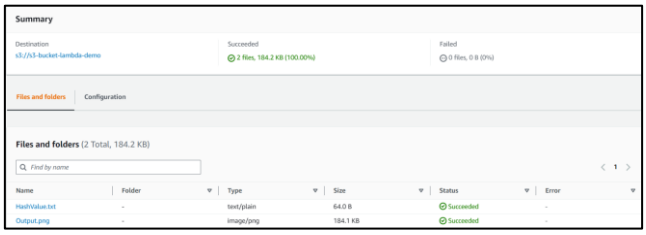

Fig. 17. Successful upload of Stego image and Hash value into S3 bucket

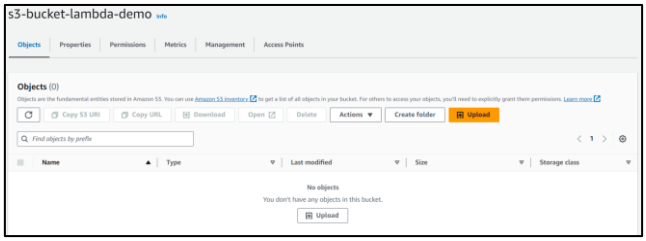

Fig. 18. Successful execution of Lambda function

The table below(Table 2) shows the constraints that were satisfied by the implementation and how the implementation is better.

Table 2. Units for magnetic properties

Criteria	*Metric*	*Explanation*
Picture Distinguishing	Satisfied	If both images are seen using the naked eye, the difference can't be found.
User Authentication	Satisfied	Any user other than the sender and receiver will not know that data is getting transferred between two people because of cloud user management.
Secure Transmission of Information	Satisfied	The receiver gets his account details with a randomly generated password via email which will not be known to any other party other than themself.
Integrity	Satisfied	The hashing helps to check the integrity of files transferred by the sender. If there is a mismatch of hash received and hash calculated, the receiver knows data was missed or modified during transit.
Confidentiality	Satisfied	The data that needs to be sent is encrypted twice using different algorithms at each stage and later it is hidden in an image using steganography.

This paper discussed about using user management(IAM) and AWS Lambda function in cloud environment to transfer data from one user to another user and maintain security by deleting all the contents automatically after a particular time instead of manually deleting which may cause information breaches. It also discussed hashing, hybrid cryptography with change in order and steganography to ensure integrity, and confidentiality of the data. The methodology discussed in the paper satisfies all the constraints that are mentioned in the literature review section.

6. Conclusion and Future Scope

As the classic data confidentiality techniques like using cryptography, steganography or cloud computing alone are failing these days due to rapid development of technology and high availability of crack-able tools over the internet, the discussed implementation helps to solve the rising issues regarding information confidentiality in current days as more than one procedure is used to tackle the issues regarding information confidentiality. These types of methodologies are known as hybrid procedures which generally include one or more strategies from different domains. This implementation uses RSA, DES algorithms for cryptography and LSB steganography for hiding the data in images. Cloud Computing helps to store and transfer data between both users and maintains the authenticity of the files. Some future works can be creating more advanced embedding methods that can accomplish greater embedding capacities without sacrificing the quality of the image and also steganography without getting captured when steganalysis is applied.

7. References and Footnotes

Author contributions

The authors confirm contribution to the paper as follows: **"Leelendra Reddy Gogula:** conceptualization, methodology, formal analysis, writing—original draft preparation, visualization **Harshith Kurapati:** software, validation, investigation **Bhuvana Reddy Bhimireddy:** methodology, resources, visualization **Alekhya Nimmagadda:** validation, resources, visualization **Radhika Rani Chintala:** investigation, writing—review and editing, supervision **Vijaya Chandra Jadala:** software, validation, project administration." All authors reviewed the results and approved the final version of the manuscript.

Conflicts of interest

The authors declare no conflicts of interest.

References

[1] S. A. Grishaeva and V. I. Borzov, "Information Security Risk Management," 2020 International Conference Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS), Yaroslavl, Russia, 2020, pp. 96-98, doi: 10.1109/ITQMIS51053.2020.9322901.

[2] B. Reddy Bhimireddy, A. Nimmagadda, H. Kurapati, L. Reddy Gogula, R. Rani Chintala and V. Chandra Jadala, "Web Security and Web Application Security: Attacks and Prevention," 2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2023, pp. 2095-2096, doi: 10.1109/ICACCS57279.2023.10112741.

[3] P. L. Sri, C. Nanda Krishna, A. D. Sai and S. Roshini, "Concealing the Data using Cryptography," 2023 Third International Conference on Artificial Intelligence and Smart Energy (ICAIS), Coimbatore, India, 2023, pp. 368-372, doi: 10.1109/ICAIS56108.2023.10073878.

[4] V. Sathya, K. Balasubramaniyam, N. Murali, M. Rajakumaran and Vigneswari, "Data hiding in audio signal, video signal text and JPEG images," IEEE-International Conference On Advances In

Engineering, Science And Management (ICAESM - 2012), Nagapattinam, India, 2012, pp. 741-746.

[5] S. Mishra, M. Kumar, N. Singh and S. Dwivedi, "A Survey on AWS Cloud Computing Security Challenges & Solutions," 2022 6th International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 2022, pp. 614-617, doi: 10.1109/ICICCS53718.2022.9788254.

[6] G. Maji, S. Mandal, S. Sen and N. C. Debnath, "Dual image based LSB steganography," 2018 2nd International Conference on Recent Advances in Signal Processing, Telecommunications & Computing (SigTelCom), Ho Chi Minh City, Vietnam, 2018, pp. 61-66, doi: 10.1109/SIGTELCOM.2018.8325806.

[7] A. G. Benedict, "Improved File Security System Using Multiple Image Steganography," 2019 International Conference on Data Science and Communication (IconDSC), Bangalore, India, 2019, pp. 1-5, doi: 10.1109/IconDSC.2019.8816946.

[8] R. Ahluwalia, A. Gupta and P. Chaudhary, "Steganography: Double Encrypted Image Deployed In Cloud," 2020 International Conference on Intelligent Engineering and Management (ICIEM), London, UK, 2020, pp. 519-525, doi: 10.1109/ICIEM48762.2020.9160279.

[9] M. Alajmi, I. Elashry, H. S. El-Sayed and O. S. Farag Allah, "Steganography of Encrypted Messages Inside Valid QR Codes," in IEEE Access, vol. 8, pp. 27861-27873, 2020, doi: 10.1109/ACCESS.2020.2971984.

[10] T. Kalaichelvi and P. Apuroop, "Image Steganography Method to Achieve Confidentiality Using CAPTCHA for Authentication," 2020 5th International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 2020, pp. 495-499, doi: 10.1109/ICCES48766.2020.9138073.

[11] M. S. Abbas, S. S. Mahdi and S. A. Hussien, "Security Improvement of Cloud Data Using Hybrid Cryptography and Steganography," 2020 International Conference on Computer Science and Software Engineering (CSASE), Duhok, Iraq, 2020, pp. 123-127, doi: 10.1109/CSASE48920.2020.9142072.

[12] S. Pramanik, S. K. Bandyopadhyay and R. Ghosh, "Signature Image Hiding in Color Image using Steganography and Cryptography based on Digital Signature Concepts," 2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), Bangalore, India, 2020, pp. 665-669, doi: 10.1109/ICIMIA48430.2020.9074957.

[13] J. A. Ajala, S. Singh, S. Mukherjee and S. Chakraborty, "Application of Steganography Technique in Cloud Computing," 2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE), Dubai, United Arab Emirates, 2019, pp. 532-537, doi: 10.1109/ICCIKE47802.2019.9004347.

[14] L. Kothari, R. Thakkar and S. Khara, "Data hiding on web using combination of Steganography and Cryptography," 2017 International Conference on Computer, Communications and Electronics (Comptelix), Jaipur, India, 2017, pp. 448-452, doi: 10.1109/COMPTELIX.2017.8004011.

[15] W. -C. Wu and S. -C. Yang, "Enhancing image security and privacy in cloud system using steganography," 2017 IEEE International Conference on Consumer Electronics - Taiwan (ICCE-TW), Taipei, Taiwan, 2017, pp. 321-322, doi: 10.1109/ICCE-China.2017.7991125.

[16] N. Manohar and P. V. Kumar, "Data Encryption & Decryption Using Steganography," 2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 2020, pp. 697-702, doi: 10.1109/ICICCS48265.2020.9120935.

[17] D. K. Chaudhary, S. Srivastava and T. Choudhury, "Steganography for Confidential Communication and Secret Data storage," 2018 Second International Conference on Green Computing and Internet of Things (ICGCIoT), Bangalore, India, 2018, pp. 461-465, doi: 10.1109/ICGCIoT.2018.8753034.

[18] Y. P. Astuti, D. R. I. M. Setiadi, E. H. Rachmawanto and C. A. Sari, "Simple and secure image steganography using LSB and triple XOR operation on MSB," 2018 International Conference on Information and Communications Technology (ICOIACT), Yogyakarta, Indonesia, 2018, pp. 191-195, doi: 10.1109/ICOIACT.2018.8350661.

[19] R. Dumre and A. Dave, "Exploring LSB Steganography Possibilities in RGB Images," 2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kharagpur, India, 2021, pp. 1-7, doi: 10.1109/ICCCNT51525.2021.9579588.

[20] David Clinton; Ben Piper, "AWS Storage," in AWS Certified Solutions Architect Study Guide: Associate SAA-C02 Exam , Wiley, 2021, pp.59-81.

[21] R. A. P. Rajan, "Serverless Architecture - A Revolution in Cloud Computing," 2018 Tenth International Conference on Advanced Computing (ICoAC), Chennai, India, 2018, pp. 88-93, doi: 10.1109/ICoAC44903.2018.8939081.