Pairing-Free CP-ABE based Combination of Cryptography and Steganography for Secure Storage

[1]Pamulapati Supriya, [2]Jayarekha P

[1]Student, [2]Professor
[1]Department of Information Science and Engineering,
[1]BMS College of Engineering, Bangalore, India

***Abstract*: Ssocial media and applications have gained lots of demand due to increased usage and development of technology. This also increased the demand for storage. Cloud is the storage platform with less hardware, low maintenance and one can easily access. It uses the internet for all these actions which makes data directly exposed to the internet and have high chances of attack. The data security and privacy had become a major concern. This can be handled by providing limited accesses to the authenticated users. The data which need to be stored will be converted into cypher text by encrypting it and upload the encrypted data to the cloud. The data that must be sent or received to the other parties will be encrypted using Cipher Text Policy Attribute Based Encryption (CP-ABE). And to reduce the memory usage, here elliptic curves swapped the Pairing based computation. CP-ABE is technique that will provide a controlled access to encrypted data. The paper proposes a hybrid model of combining cryptography with steganography, operates on integrating crypto text into a cover image. This scheme noticeably enhances the security and privacy of data.**

Index terms: Cipher Text Policy Attribute Based Encryption, steganography, cryptography

---

I. INTRODUCTION

Increase in usage of Internet has developed gradually in the past years. This increase in the usage of the internet also developed the diamond for multimedia applications. where Internet is the main source for the devices like mobile phones, laptops and other gadgets to share the data. Data is growing day by day according to a survey Every day, we create roughly 2.5 to 3 quintillion bytes of data which might increase in the upcoming days. The data management and data storing has become a difficult task due to the huge data generation. The smart gadgets that are in use have the minimal storage capacity due to its reduced size. The best solution for all these problems is Cloud computing.

Cloud computing has become the most trending technology due to tremendous increase in the usage of internet and data generation. Cloud service allows people to preserve and exchange the data without any location dependency. The only dependency for cloud computation is internet connectivity. The Issue arising in cloud computing, data is directly exposed to the internet, due to which threat to data security and privacy came into the picture. Like access of data by the unauthorised users, access of network and application by the intruders or hacker who has the hawk eye to gain the access. These threats are caused due to compromise in security and protection for a storing environment like cloud, which affects the security and the privacy aspects of the sensitive data. This problem can be handled through restricting the access of data to the limited numbered clients, whereas intruders will have no access on the stored data. This access control can be done by encrypting the data using cryptographic techniques before storing it into the cloud. To enhance the level of security for highly confidential messages, this paper introduced to integrate the text message which is already encrypted into a cover carrier encrypted image using stenography techniques. This makes the cloud a secured platform to store, transmit and receive the data.

II. LITERATURE SURVEY

One can extract the secret message from the encrypted data by crypt analysis. Therefore, In this proposed work we went through a possibility of storing encrypted data into an image i.e., the hybrid model of cryptography with steganography. This model will increase the level of security and data privacy. To solve the issues of cloud for data privacy and security, few solutions, alternatives, precautions and some protocols have been put forward by researchers in associated field of areas, which is explained below. Yinghui Zhang, et al., [1] proposed PASH, a privacy aware smart-health access control system based on CP-ABE scheme Which prevents both data privacy and security issues in healthcare and also provides access policies to the clients and the respective authorities of a particular. Awadhesh Shukla, et al.,[3] presented a high proportioned data storing policy. Which combines compression without any loss, advanced encryption techniques, altered pixels anticipation and LSB interchange for improved level of security at odds with regular/ singular (RS) steganalysis.

Zhen Wang, et al.,[2] proposed an "Enhanced Instant Message Security and Privacy Protection Scheme for Mobile Social Network Systems". A Secure Instant Message system based on the Elliptic-Curve-Cryptography was proposed in this paper. Which increases the rate of security.Aya Y. AlKhamese, Ibrahim M. Hanafy and Wafaa R. Shabana., [7] discussed types of steganography with a major focus on image steganography. The main techniques explained in this paper are Least Significant Bit (LSB) and the Discrete Cosine Transform (DCT). LSB is a majorly used technique to hide data in different ways and also it is easy to encrypt and detect

the attacks with high payload. DTC technique is a bit complex and has a lower payload when compared to LSB, but it ensures a stronger level of security.

Eshraq Hureib., Adnan Gutub.,[12]. "Enhancing Medical Data Security via Combining Elliptic Curve Cryptography and Image Steganography". In this paper, a combined model of two techniques of elliptical curve cryptography and steganography was proposed. With these two techniques, the private data will be encoded and hidden in a safer way. Yuting Hu., Yihua Huang., Zhongliang Yang., Yongfeng Huang.,[17] proposed "Detection of Heterogeneous Parallel Steganography for Low Bit-Rate VoIP Speech Streams". This paper deals with detection of heterogeneous parallel steganography (HPS) on streaming multimedia data. The major job is to find out the secret messages hidden in the frames of streaming data with multiple kinds of orthogonal steganographic methods.

III. PROPOSED SYSTEM

The existing system makes use of Cipher-Text-Policy Attribute-Based-Encryption which provides limited on access of the cipher data. The pairing-based calculation on the bases bi-linearity used in attribute-based system requires an increased number of resources. So, we are replacing Pairing based computation with an effective pairing-less CP–ABE scheme with access control and making usage elliptic curve cryptography. Which have the reduced usage of resources when compared with Pairing based computation.

In this method, the data owner has the authority to control the access to data where only authorized users can access the data unauthorized users cannot access. Authorized users are those who gets authenticated under data owner. Considering an example of user needed to share his medical reports to any domain of an organization like HR department then he can give access in the following manner: (XYZ Organization ^ ABC Branch ^ HR department). The main purses of the cryptography to be used is to encrypt a message into an unreadable format, the third person cannot be able to read it without the proper decryption keys. Even though a third party or the unauthorized user tries to access the data by reaching into the network they will be unable to get the valid information from the data. But if they use crypto analysis then the third party can also access the encrypted data. This can be handled by steganography which can hide the secret data in a file. That may be in the form of image, audio or video.

The proposed method makes use of cryptography and the steganography by integrating the cypher text inside an image file with the help of CP-ABE. By this way the unauthorized users will not be aware of secret message text inside an image so we can share the data with the maximum level of security. In this method the image is used as a wrapper carrier which will hide the encrypted secret message. The text which needs to be embedded into the image will be encrypted using CPABE based on Elliptic curve cryptography. The ECC will come under the category of asymmetric cryptographic type which means we have 2 keys in it, public key and a private key. The public key can be distributed in the network or with the trusted ones, but the private key should be kept secure(secreta). If an individual has to share the data, then they will encrypt the message with the respective public key of the receiver. The receiver will decrypt the message using his own private key. The other way is if a sender wants to share an encrypted message, then he will encrypt it using his own private key and then the receiver can access it using the sender's public key. The pairing-based computation is swapped with a elliptic curves and their scalar product which has shorter and faster key generation, highly resistant to various attacks and require minimal computing power.

IV. IMPLEMENTATION:

Step 1: Reserving pixels to store the Embedding Data

In step:1 we receive the image from the data owner, and we extract the pixel information from it. And the system reserves or blocks the particular pixels in the image to store the embedded data as shown in the figure above.

Step 2: Image Encryption.

For the Image Encryption part techniques,
1.XOR Operation
2.Bit Rotation.
For this operation the user needs to insert two inputs one is Image, and the other is the key to encrypt the image. The output from this system is an encrypted stegno image.
Suppose if the user input Key to encrypt the text is CYPHER, then the system will produce 1-byte(8-bit) key value by the billow method and consider Bit as B and Asci as A in the below.
B(A(C)) XOR B(A(Y)) XOR B(A(P)) XOR B(A(E)) XOR B(A(E)) XOR B(A(R))
The following operations will take place in each pixel of an image

Each color in an image is represented by 1-byte (8 bits). Each pixel in an image contains three colors they are, Red(R), Green(G), Blue(B).

1. ER [Encrypted Red] = Bit (Red) Xor Key Value
2. RER [Rotated encrypted Red] = Rotate Encrypted Red 4-bit Right Side using Bit Rotation operation (In the blocked area at step 1 Value of Red color is not changed).EG [Encrypted Green] = Bit (Green) Xor Key Value

3. REG [Rotated encrypted Green] = Rotate Encrypted Red 3 bit Left Side
4. EB [Encrypted Blue] = Bit (Blue) Xor Key Value
5. REB [Rotated encrypted Blue] = Rotate Encrypted Red 3 bit Right Side

Replace all the rotated and encrypted values with its respective values like the Rotated encrypted Red for Red byte, Rotated encrypted Green for Green byte and Rotated encrypted Blue for Blue byte**.**

Step 3: Data Storing in an Encrypted Image

For this data hiding process we need two inputs from the user

1. Data to Hide
2. Data storing Key
3. Encrypted Image

This system makes use of two algorithms: Pixel selection based on Key, Least Significant bit replacement Algorithm.

Suppose the data hiding key is CRYPTO. The system separates the characters in the key such a way C,R,Y,P,T,O. Find the ascii values of each character, like C is 67 convert it into 8 bit binary "**1000011**" repeat this process for all other remaining characters.As we already reserved the pixels in the first step, map the obtained binary bits from ascii values in the blocked pixels spaces. The system will store the data into pixels that contains value 1. In the Selected pixel the color pixel with Red will hold the data in that we are just changing only the last 4 LSB. Since we are operating on the last four LSB for one color channel, there is no changes to the original image.

Step 4: Decryption Process

In the decryption time this system can undergo two operations

1. Data Recovery
   Provide Input as Encrypted Image with Data and Data Hiding Key
   The Output will be Hidden Data

2. Image Retrieval
   Provide Input as Encrypted Image with Data and Image Encryption Key
   The Output will be Recovered Image without any damage

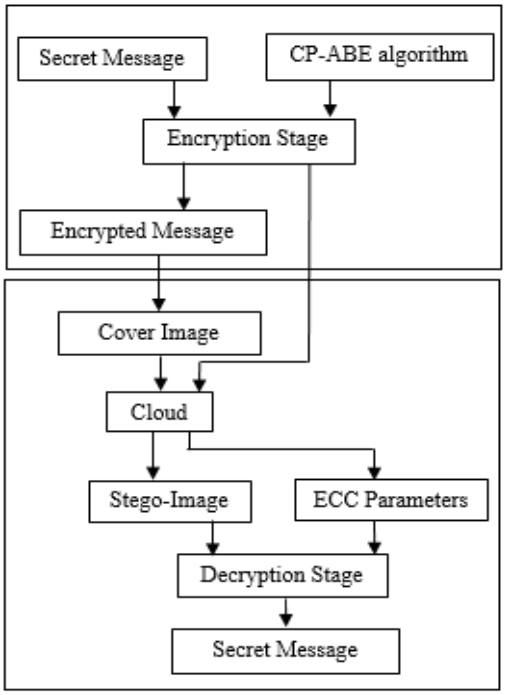


Fig. 1. Flow Diagram

The Data owner will upload the cover carrier image and the secret text with the appropriate encryption keys. The cover image will be scaled down by, Reading the Image height and width divide the Height and width by number of sizes you need to scale. Encryption process 1: After scaling down the cover image. The image will be encrypted will be encrypted with the image encryption

key k1 specified by the data owner. Encryption process 2: Once the image is encrypted, the secret message will be encrypted with the message encryption key k2 through cryptographic techniques. And then embedded into the cover image using steganographic techniques. Now the encrypted image embedded with secret message will be uploaded to the cloud and the acknowledgement will be sent to the data owner.

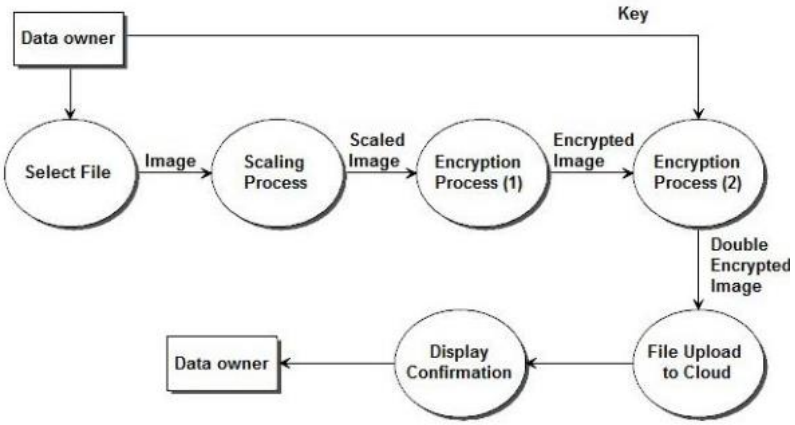


Fig. 2. File uploading process

An Admin is a superior user who adds the Data Owners, users to the network and keep track of cloud server's array. In this system only the admin has authority to alter or bring in the new data-owners to the network. Here The Data Owner is the one who has access to upload the secure encrypted data into the cloud. He can also give access to the Data Consumers to access the data. The best example that suits data owner is a Liberian who has all the rights to upload and provide access to the readers. And consumers are like readers who needs access to the stored data. Data Users need get registered and they will receive the identity token their respective mails email. Each time user wants to access the data he needs to provide the identity token.

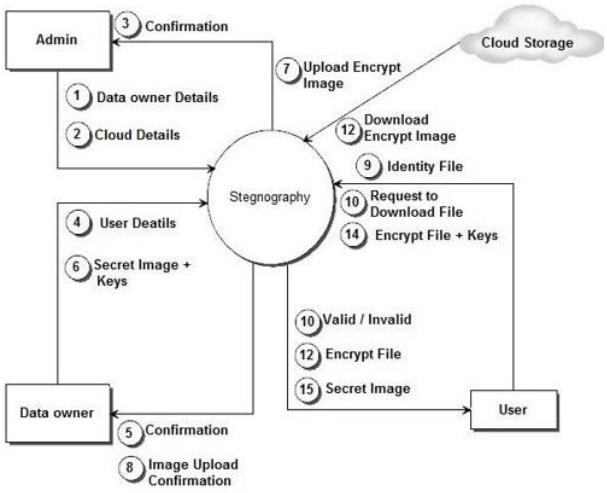


Fig. 3. Schematic Diagram

V. RESULTS

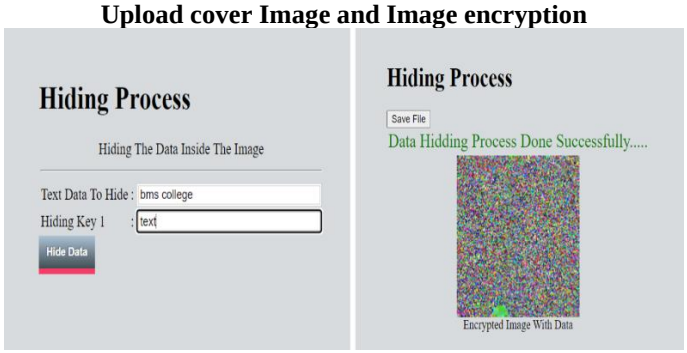
The primary step is to check the authentications. The home page of our ui contains authentication verification. We have three categories in this as shown in the below fig 11: the admin, the data owner and the user. Let us discuss one by one.

Admin: Admin is a superior user who can add the Data Owners, user to the network and also monitors the cloud servers connections. In this system only the admin has authority to alter or bring in the new data-owners to the network. Once the Admin logged in, the functions available are, View Profile where he can see admin profile, Proxy Server which displays server details and admin will have access to add a new server, edit and delete the existing one

Data Owner: After logging into the system, the Data Owner has the functions available explained below. View Profile, data owner can see the profile. User Details, the data owner will be able to view, add, delete the user's details. Once the user details are added into the network along with the mail-id, the user will be receiving an MD file to his mail-id which is used as a twostep verification. File Upload, where the data owner can select a cover image and provide an encryption key. Then the cover image will be encrypted and uploaded into the cloud. Once the encrypted image is uploaded, the data that can be stored into the cover image which is

encrypted by specifying the message to be hidden and the data hiding key. Thus, the data will be encrypted and stored inside an encrypted cover image.

Upload cover Image and Image encryption



Embedded Encrypted text inside the Cover Image

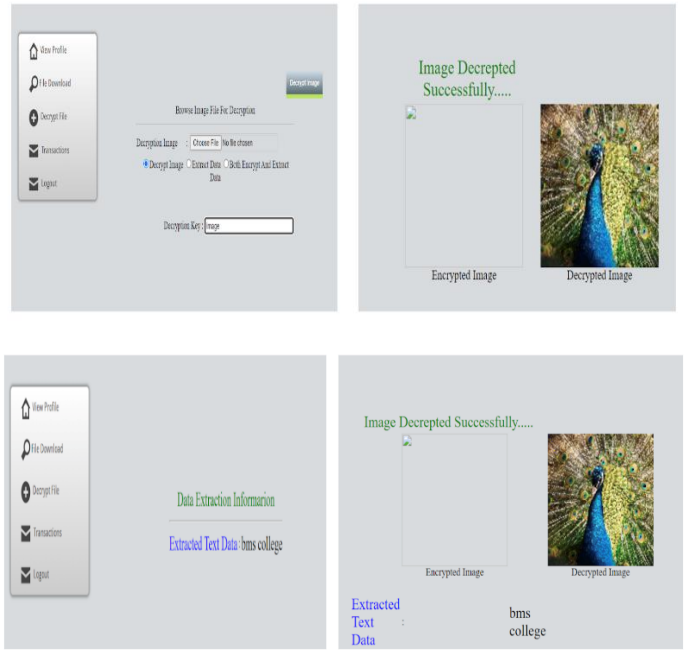
After uploading the encrypted file, the data owner can specify the access control to a particular file using Domain Attribute and Sub-Domain Attribute. Transactions, data owner can view the file transactions that are occurring in the network as shown in fig. 10. Finally, the logout option

File Access Control

Data User: Once the Data Consumer logged in and completed the Identity check by uploading the Identity Token which he has received through mail. The following options, View profile (view only). File Download where the user can download the file from cloud by providing domain attributes, if the user fails to give the correct domain and subdomain attributes, then the access will be denied downloading that particular file.

Identity Token Verification

After downloading the file, the user has the options to decrypt only the cover image, extract data from the image or both decrypt the image and extract the data at a time by providing the appropriate image decryption and text extraction keys.



Decryption process

VI. CONCLUSION.

Cloud dependent image processing and storing has data secrecy issues, which may further case confidentiality and privacy risks. This paper deals with the pairing free CP-ABE access control policy based on elliptic curve cryptography which is used to share the data securely in secure applications such as military, research centres, etc. Where data can be accessed by the authorized persons, The individuals they are authenticated by the approval of data owner. Which keeps the data safe from the unauthorised users. This model is a hybrid of cryptography as well as steganography which results in a highly enhanced security enhanced data security, by embedding crypto text into an image. Here both the message to be stored and the cover image which stores the text will be encrypted which doubles the level of security and confidentiality. The proposed system also considers the availability of resources. And to reduce the usage of resources like memory we replaced Pairing based computation with elliptic curves and their scalar products. Which reduces the usage of memory when compared with the other previously used techniques.

Future Scope: In the future work we can replace the key sharing process with key generation by making use of key transfer algorithms such as deffie helman. And have a conditional check in secret key selection process. Which makes the key stronger and if any intruder hacks the network he will not be able to receive the complete key.

References

1. Wicaksana, A., Tang, C.M.: Virtual prototyping platform for multiprocessor system-on-chip hardware/software co-design and co-verification (2018). https://doi.org/10.1007/978-3-319-60170-0_7.
2. Al-Juaid, N., A Gutub, A. and A Khan, E., 2018. Enhancing PC data security via combining RSA cryptography and video-based steganography.
3. AlKhamese., Ibrahim M. Hanafy and Wafaa R. Shabana.,"Data Security in Cloud Computing Using Steganography: A Review" International Conference on Innovative Trends in Computer Engineering (ICE 2019) 2-4 February 2019.
4. Christofer Derian Budianto., Arya Wicaksana., Seng Hansun., "Elliptic Curve Cryptography and LSB Steganography for Securing Identity Data". AICT- International Conference on Applied Computing and Information Technology, 27 August 2019.
5. Zihan Wang, Neng Gao, Xin Wang, Ji Xiang, and Guanqun Liu. Stnet:A style transformation network for deep image steganography. In In-ternational Conference on Neural Information Processing, pages 3–14. Springer, 2019.
6. Eshraq Hureib., Adnan Gutub.,"Enhancing Medical Data Security via Combining Elliptic Curve Cryptography and Image Steganography". IJCSNS International Journal of Computer Science and Network Security, August 2020.
7. Peter Eze., Udaya Parampalli., Robin Evans. and Dongxi Liu. "Evaluation of the Effect of Steganography on Medical Image Classification Accuracy". August 2020.
8. Shereen MA, Khan S, Kazmi A, Bashir N, Siddique R. "COVID-19 infection: Origin, transmission, and characteristics of human coronaviruses". Journal of Advanced Research 24 :91–98, 2020
9. Citation: Eze P, Parampalli U, Evans R, Dongxi L. "Evaluation of the Effect of Steganography on Medical Image Classification Accuracy". J Appl Bioinform Comput Biol 9:4, 2020
10. Eze PU, Parampalli U, Evans RJ, Liu. D. A New Evaluation Method for Medical Image Information Hiding Techniques. In the Proceedings of 42nd IEEE Engineering in Medicine and Biology 6119 – 6122, 2020.
11. Omar Elharrouss., Somaya Al-Maadeed., Ahmed Bouridane., "Image Steganography: A Review of the Recent Advances". IEEE, Volume: 9, 25 January 2021.