ISSN [Online]: 2583-2654

Pairing-Free CP-ABE Based Cryptography Combined with Steganogrphy for Multimedia Applications

[1] Apoorva D, [2] Champa K P, [3] Meena S, [4] Lakshmi B R, [5] Yogendra N
Department of computer science, Dr T Thimmaiah Institute of Technology, Karnataka, India.

Abstract -- CP-ABE is used which is a cryptographic technique that controls access to the encrypted data. The pairing-based computation based on bilinearity is used in ABE due to which the requirements for resources like memory and power supply increases rapidly. Most of the devices that we use today have limited memory. Therefore, an efficient pairing free CP– ABE access control scheme using elliptic curve cryptography has been used.

Pairing based computation is replaced with scalar product on elliptic curves that reduces the necessary memory and resource requirements for the users. Even though pairing free CP-ABE is used, it is easier to retrieve the plaintext of a secret message if cryptanalysis is used.

Therefore, this paper proposes to combine cryptography with steganography in such a way by embedding crypto text into an image to provide increased level of data security and data ownership for sub-optimal multimedia applications. It makes it harder for a cryptanalyst to retrieve the plaintext of a secret message from a stego-object if steganalysis were not used. This scheme significantly improved the data security as well as data privacy.

Keywords -- Cipher Text-Policy Attribute Based Encryption (CP-ABE), pairing-based computation, pairing free, elliptic curve cryptography, steganography, stego-object, scalar product.

I. INTRODUCTION

Development of the internet in recent years has led to tremendous increase in demands for multimedia applications .Most of the devices like mobile phones, cars, electronic appliances depend on internet for sharing the multimedia data with other users. Due to this development, data management has become a tougher job. The major problem with data management is the requirement of memory for storing it. As these smart devices come with limited memory and storage capacity, one of the easiest ways to store and manage data is to make use of the cloud .

Cloud enables people to store, transmit and receive data anytime provided they are connected to the internet. As data are not directly managed by the owner, threat to data security and privacy increases . This can be avoided by limiting data access and by hiding the data from cloud services that cannot be trusted. Hiding data from the cloud services involves encrypting the data before storing it into the cloud. Data encryption not only helps to hide data but also to share data securely across an open source network or the environment.

Cryptography can be used to encrypt the files to be shared with the other users in multimedia applications. Technology development has led to rapid increase in demands for multimedia applications. Due to this demand, digital archives are increasingly used to store these multimedia contents. Cloud is the commonly used archive to store, transmit, receive and share multimedia contents. Cloud makes use of internet to perform these tasks due to which data becomes more prone to attacks. Data security and privacy are compromised.

This can be avoided by limiting data access to authenticated users and by hiding the data from cloud services that cannot be trusted. Hiding data from the cloud services involves encrypting the data before storing it into the cloud. Data to be shared with other users can be encrypted by utilizing Cipher Text-Policy Attribute Based Encryption (CP-ABE).

ISSN [Online]: 2583-2654

II. LITERATURE SURVEY

A literature survey or a literature review in a project report shows the various analyses and research made in the field of interest and the results already published, taking into account the various parameters of the project and the extent of the project. Literature survey is mainly carried out in order to analyze the background of the current project which helps to find out flaws in the existing system & guides on which unsolved problems we can work out which includes the current knowledge including substantive findings, as well as theoretical and methodological contributions to a particular topic.

Yinghui Zhang et al., [1] Security and privacy in smart health: Efficient policy-hiding attribute-based access control: With the rapid development of the Internet of Things (IoT) and cloud computing technologies, smart health (shealth) is expected to significantly improve the quality of health care. However, data security and user privacy concerns in shealth have not been adequately addressed. As a well-received solution to realize fine-grained access control, ciphertext-policy attribute-based encryption (CP-ABE) has the potential to ensure data security in s-health. Nevertheless, direct adoption of the traditional CP-ABE in s-health su_ers two flaws. For one thing, access policies are in cleartext form and reveal sensitive healthrelated information in the encrypted s-health records (SHRs). In this proposed PASH, a privacy aware smart-health access control system based on CP-ABE scheme that supports large universe and partially hidden access policies to efficiently address both data security and user privacy issues in smart-health.

Zhen Wang et al., [2] Enhanced Instant Message Security and Privacy Protection Scheme for Mobile Social Network Systems: Instant messaging (IM) systems can be considered the most frequently used applications in mobile social networks. Nowadays, people are becoming increasingly concerned about data security and privacy protection with IM applications. Therefore, a comprehensive enhanced secure IM scheme was proposed in this paper, which is based on the elliptic curve cryptosystem and the advanced encryption standard algorithm. An offline key agreement process between users was designed under the computational Dif_e_Hellman (CDH) assumption by updating the ephemeral key periodically. This proposed scheme supports denial of replaying attack and denial of forgery attack by utilizing timestamps and the elliptic curve digital signature algorithm.

Abid mehmood et al., [3] Anonymous Authentication Scheme for Smart Cloud Based Healthcare Applications: Many smart healthcare applications are adopting cloud to provide services to patients. However, the sensitive data can be disclosed to the authentication server/service provider. Therefore, security and privacy are crucial to its success and deployment at large scale. Patients don't want to disclose their identities to the cloud server. One way to protect their identities from cloud server is anonymous authentication. In this paper, they have proposed a system which provides complete privacy and anonymity to the users of health care applications from adversaries and the authentication server. In this proposed authentication scheme, they have utilized rotating group signature scheme based on Elliptic curve cryptography to provide anonymity to the patients. To add an extra layer of protection, we have used The Onion Router to provide privacy at the network layer.

Kan Yang et al., [4] Time-Domain Attribute-Based Access Control for Cloud-Based Video Content Sharing: A Cryptographic Approach With the ever-increasing demands on multimedia applications, cloud computing, due to its economical but powerful resources, is becoming a natural platform to process, store, and share multimedia contents. However, the employment of cloud computing also brings new security and privacy issues as few public cloud servers can be fully trusted by users. In this paper a cryptographic approach for cloud-based video content sharing that embeds both the cipher-texts and session keys in time division way such that only users who hold sufficient attributes in a specific time period can decrypt the data.

Jiguo Li et al., [5] Combining Data Owner-Side and Cloud-Side Access Control for Encrypted Cloud Storage: People endorse the great power of cloud computing, but cannot fully trust the cloud providers to host privacy-sensitive data, due to the absence of user-to-cloud controllability. To ensure confidentiality, data owners outsource encrypted data instead of plaintexts. To share the encrypted

ISSN [Online]: 2583-2654

files with other users, ciphertext-policy attribute-based encryption (CP-ABE) can be utilized to conduct fine-grained and owner-centric access control But this does not sufficiently become secure against other attacks. Many previous schemes did not grant the cloud provider the capability to verify whether a downloader can decrypt. Therefore, these files should be available to everyone accessible to the cloud storage. presented an efficient user collision avoidance attribute revocation by bounding together the user's private key and group secret key for the cloud storage system.

Samer Atawneh et al., [6] Steganography in Digital Images: Common Approaches and Tools: The art and science of using digital images for secret communication is known as image steganography. This paper presents a background on key concepts behind it. A representation of steganography area is graphically and mathematically shown. An introduction to steganalysis is provided. Distinctions between steganography, cryptography and watermarking in terms of technique and intent are briefly discussed. Details of the way images are represented are outlined. Common approaches used for embedding messages into images are discussed in some detail. Methods used for embedding messages into images are as well explored. Current steganography tools are highlighted. A demonstration of how secret information is embedded into an image through the use of available steganographic tools is shown. Comparisons between different image steganography algorithms are also provided.

Awdhed K Shukla 1,2 et al., [7] A Secure and High-capacity Data-hiding Method Using Compression, Encryption and Optimized Pixel Value Differencing: A high capacity data hiding method using lossless compression, Advanced Encryption Standard (AES), modified pixel value differencing (MPVD) and least significant bit (LSB) substitution is presented. Arithmetic coding was applied on secret message for lossless compression. The compressed secret message is subjected to AES encryption; this provides higher security in the cases of steganalysis attacks. After compression and encryption, LSB substitution and MPVD are applied. In MPVD, adaptive non-overlapping 3x3 pixel blocks or a combination of 3x3 and 2x2 blocks are used in raster fashion. In this proposed method is also proved to be secure against regular/singular (RS) steganalysis.

Tarun Kumar Misshral et al., [8] A Review of Multimedia Cryptography Techniques: Multimedia Cryptography is a complex process of hiding textual information into a multimedia file or it can be vice versa as well. A non-multimedia file can also accommodate a multimedia file given that its size or the pixel count is more than that of the container file. Cryptography is an essential part of data security services and data preserving and copyrighting preservence. Cryptography can also be termed as steganography, watermarking and etc.

III. PROPOSED MODEL

CP-ABE is used which is a cryptographic technique that controls access to the encrypted data. The pairing-based computation based on bilinearity is used in ABE due to which the requirements for resources like memory and power supply increases rapidly. Most of the devices that we use today have limited memory.

Therefore, an efficient pairing free CP–ABE access control scheme using elliptic curve cryptography has been used. Pairing based computation is replaced with scalar product on elliptic curves that reduces the necessary memory and resource requirements for the users.

In this scheme, the data owner can control the access to the data. Data can be accessed only by specific users that are authenticated by the data owner. The goal of cryptography is to convert the message into a form that cannot be understood by third party users who are not authenticated and tries to steal the message by eavesdropping. It does not try to hide the encoded message.

If cryptanalysis is used, then the secret message becomes accessible to unauthorized third parties. This can be avoided by using steganography.

Steganography is the technique of hiding secret data within a file. The file can be image, audio or video. The proposed scheme combines cryptography and steganography in such a way by embedding a crypto text generated using CP-ABE into the image.

ISSN [Online]: 2583-2654

In this way, the unauthorized users are unaware of the presence of the secret information and so it can be transmitted with utmost security. It makes it harder for a cryptanalyst to retrieve the plaintext of a secret message from a stego-object if steganalysis were not used.

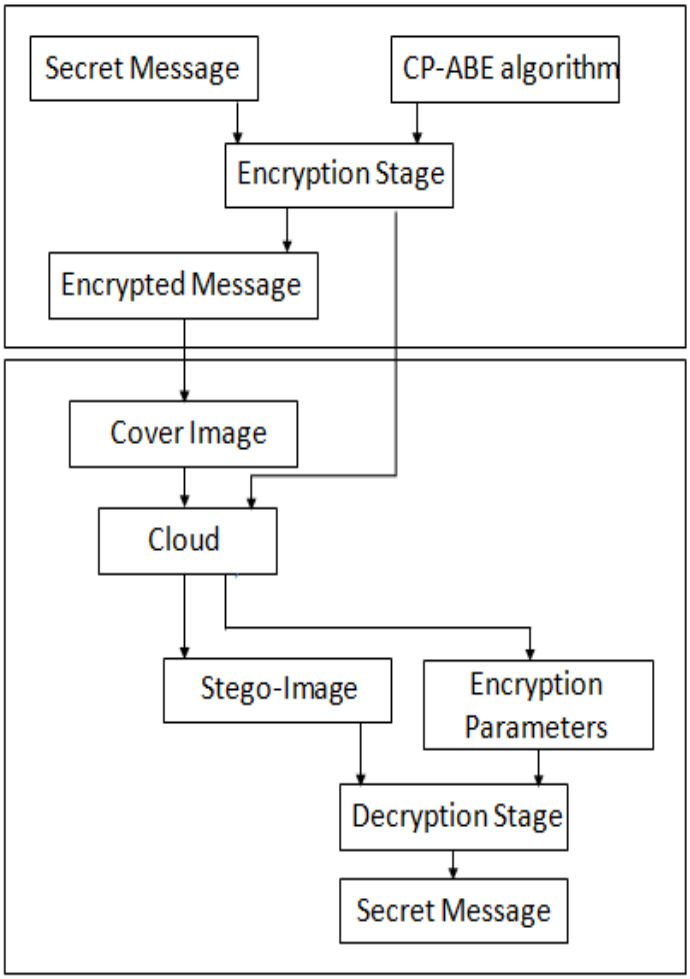

Fig 1: Architecture Diagram

Algorithm & System Flow

1. Encryption Process

Step 1: Reserving Room for Embedding Data - Consider the above matrix is a pixel representation of a image. This system reserves the pixels which are highlighted for embedding the data.

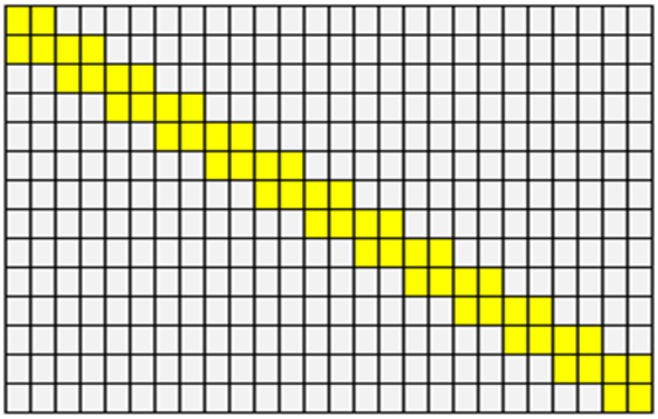

Fig 2: Pixel Representation of A Image

Step 2: Image Encryption - For Image Encryption this system uses two technique one is XOR Operation and another one is Bit Rotation Operation. For this operation system need two input Image, Image Encryption Key And the output will be Encrypted Image.

For Example Input Encryption Key is INDIA then from the input key, this system will generate a 8-bit key value (KV) by these methods Bit (ASCII(I)), XOR Bit (ASCII(N)), XOR Bit(ASCII(D)), XOR Bit(ASCII(I)) and XOR Bit (ASCII(A)). For each pixel following operations will take place a pixel consist of 3 color R,G,B. Each color represented by 8 bit.

1. Bit (R) Xor KV => ER [Encrypted Red]
2. Rotate ER 4 bit Right Side => RER [Rotated encrypted Red]

Note: In reserved area Value of R colour is not changed.

3. Bit (G) Xor KV => EG [Encrypted Green]
4. Rotate ER 3 bit Left Side => REG [Rotated encrypted Green]
5. Bit (B) Xor KV => EB [Encrypted Blue]
6. Rotate ER 3 bit Right Side => REB [Rotated encrypted Blue]

Replace the RER for Red byte, REG for Green byte and REB for Blue byte**.**

Step 3: Data Hiding on Encrypted Image - For this operation system need three input.

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

In this process we are using following two algorithms

ISSN [Online]: 2583-2654

1. Key Based Pixel Selection algorithm
2. LSB (Least Significant bit)replacement Algorithm

Consider our Data Hiding Key is ABCDEF, Separate each characters A,B,C,D,E,F
For A find ascii value that is 65 convert it into 8 bit binary "0101 1001"
For B find ascii value that is 66 convert it into 8 bit binary "0101 1011"…..

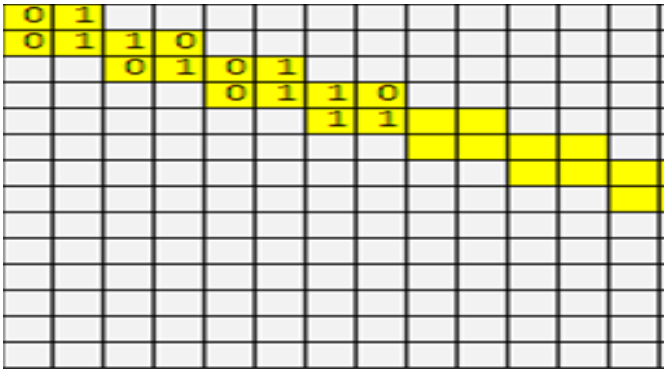

Fig 3: Converted Binary Values In The Reserved Pixel Space

Map the converted binary values in the reserved pixel space, which is shown in above image. This system going to hide the data in the pixels which are having value 1. In Selected pixel the colour channel R is going to hold the hidden data that also we are changing only last 4 LSB. Since we are changing the last 4 LSB for only one colour channel, there will not be any damage to the real image.

Example: if we are planning to hide a text X
X ASCII Value 88 then it Binary value is 0101 1000
Split Binary part into A and B like that A = 0101 and B = 1000
In Pixel selection matrix first two elements having 1 are 1,2 and 2,2
Let R value in 1,2 is 120 (R1) and R Value in 2,2 is 91(R2)
R1 = Binary(120) = 0111 1000
R2 = Binary(91) = 0101 1011
Replace last 4 bit in R1 by A and Replace last 4 bit in R2 by B
After Conversion R1 = 0111 0101 and R2 = 0101 1000 (R1 = 117 , R2= 88)

Embedding Method: Cryptography and steganography are the two main stages of embedding. Cryptography Part: User authentication is performed using CP-ABE, Secret message is encrypted using elliptic curve cryptography. Steganography Part: The simple Least Significant Bit (LSB) method can be used to embed the encrypted message into the given image and the Stego image is obtained and Least Significant Bit (LSB) technique insert data bits in the least significant bits of the image. The LSB method can be used in this way. Here the data is hidden by modifying the last bit of the pixel. It is mainly used because of its high perpetual transparency and low degradation in image quality.

Extracting Method: The stego image is sent to the cloud, If the receiver is authenticated, the data can be accessed from the cloud. Then with the help of ECC parameters, the secret message can be retrieved from the stego image.

Advantages of proposed scheme: Combining two techniques provides enhanced data security, ownership and privacy and Use of elliptic curve cryptography reduces usage of computational resources and power supply.

2. Decryption Process

In decryption process this system has following two options
A. Data Retrieval
Input : Encrypted Image with Data + Data Hiding Key
Output : Hidden Data
B. Image Recovery
Input : Encrypted Image with Data + Image Encryption Key
Output : Recovered Image without any damage

3. System Modules

A. Identity Based Encryption :

- Make the Identity Based verification for Data Accessing user.
- To make Identity Based token generation it will use the User ID + User details + Domain + Sub Domain and make a 128 bit hash code to identify.

B. Access policy Control for Cloud Storage :

- Once the Image File is Uploaded to cloud storage
- Data owner has to provide the access control to file over the Cloud Storage encrypted data. Uploaded

ISSN [Online]: 2583-2654

Image making policy using Domain and Sub Domain.
- While access particular file user has to be match with this token id to access the Cloud storage Files.

C. Image Scaling :
- Large pixel Image has to Select from local system
- Read the Image height and width.
- Divide the Height and width by number of size you need to scale.
- Read Input image pixel values byte store it in buffer.
- Create output image Buffered Image.
- Scales the input image to the output image.
- Writes to output file.

D. Encrypt Image
- Input Scaled Image has to select from Source
- Image Uploaded to Web Server using FTP
- Encryption using Key Input
- View Encrypted Image

E. Data Hiding
- Input -> Data Input + Data Hiding Key +Encrypted Image
- Pixel Selection Process based on Key
- Data Hiding process (Produce Encrypted Image where Data is hided)
- Downloading the Encrypted Image with Hidden data to the local system

F. Decrypt Image
- Selecting the Encrypted Image with Hidden Data from Local system
- Image Encryption Key Input (Optional)
- Data Hiding Key Input (Option)
- Based on the key provided do the following process
- If Image Encryption Key only given
- Do Image Decryption Process
- Show the Encrypted Image
- Download the Image to local system
- If Data Hiding Key only given
- Do Data Retrieval Process
- Display the Hidden Data

IV. DATA FLOW DIAGRAM

A data flow diagram (DFD) is a graphical representation of the "flow" of data through an information system, modeling its process aspects. A data flow diagram is often used as a preliminary step to create an overview of the system without going into great detail, which can later be elaborated. Data flow diagrams can also be used for the visualization of data processing.

In the given figure 5, admin handles the whole application, once the admin logins he can go to home page. There he can manage cloud details, data owners and can upload cloud details. m_cloud, m_owner, m_domain and m_subdomain are the databases for that particular field. Only the user which is registered with same domain and subdomain can access that file.

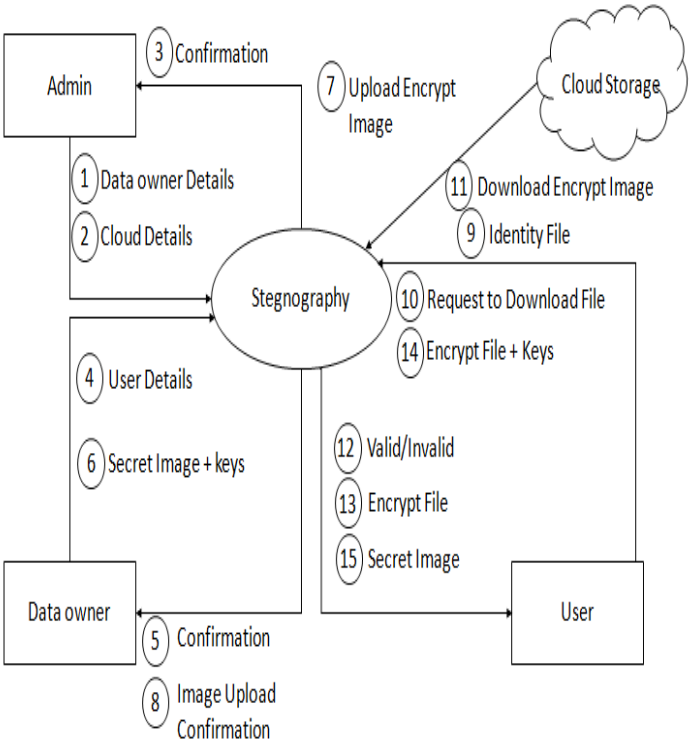

Fig 4: Context Analysis System

In the user session, the user as to provide username and password it checks whether the user is authenticated or not it is checked in the m_user database, if the username and password is correct, the user enters the homepage of the user session where the user can access profile and make change to the profile, can download file then decrypt the downloaded file which are stored in the database and user can view the secret image as it is shown the figure 6.

ISSN [Online]: 2583-2654

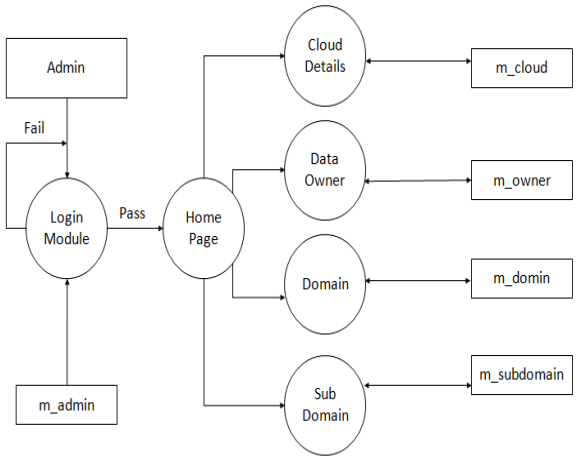

Fig 5: DFD_Admin_Session

In the data owner session, once the data owner logins it is verified in the m_owner database if it matches ,he gets access to the homepage, where the data owner can access the user details, files uploads, file access control and transactions which are stored in the particular database. where these process are shown in the figure 7.

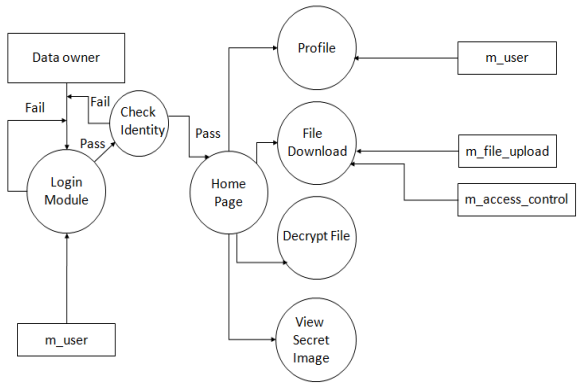

Fig 6: DFD_User_Session

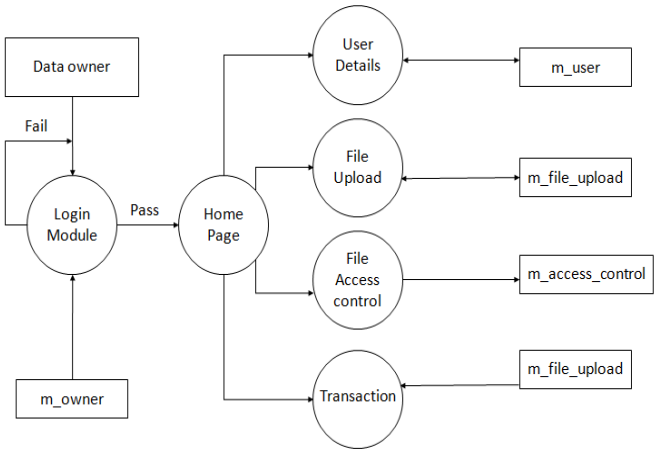

Fig 7: DFD_Data_Owner_Session

In the file uploading process shown in the figure 8, the data owner selects the image and scaling process is done. After this the scaled image enters encryption process 1 and again the encrypted image is encrypted in encrypted process 2 along with the key provided by data owner after double encrypted image is uploaded into the cloud.

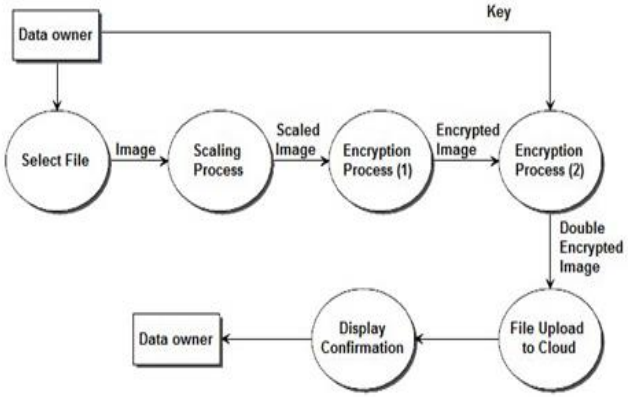

Fig 8: File Uploading Process

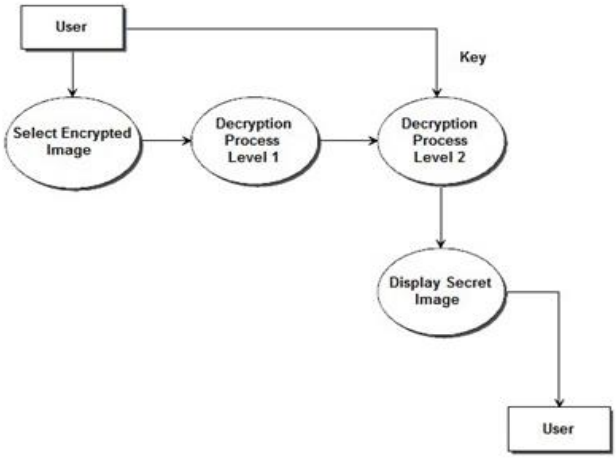

Fig 9: File Downloading Process

In the figure 5.9, it shows the file downloading process where the user selects a encrypted image and the image is decrypted twice in the level 1 decryption is done without key. In decryption level 2 the decryption is done with a key after the double decryption the secret image will be display.

V. USE CASE DIAGRAM

A use case is a set of scenarios that describing an interaction between a source and a destination. A use case diagram displays the relationship among actors and use cases. The two main components of a use case diagram are use cases and actors, shows the use

ISSN [Online]: 2583-2654

case diagram. A use case diagram can identify the different types of users of a system and the different use cases and will often be accompanied by other types of diagram as well.

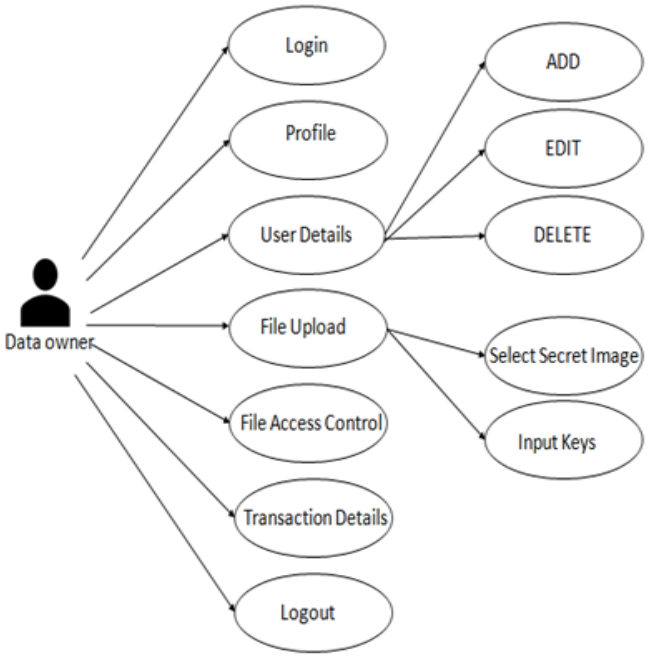

Fig 10: Usecase Diagram For Data Owner

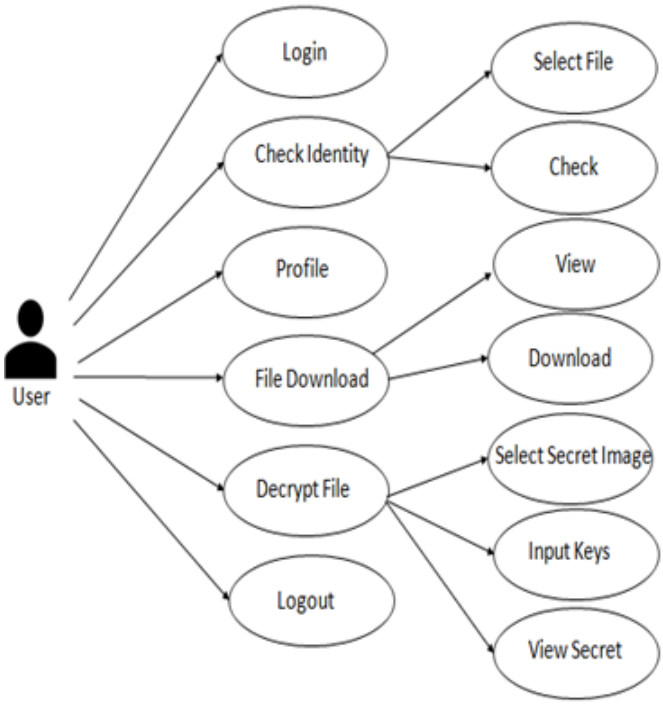

Fig 11: Usecase Diagram For User

VI. CONCLUSION

In this paper, efficient pairing free CP-ABE access control scheme using elliptic curve cryptography has been used for data sharing in sub optimal multimedia applications. Data can be accessed only by specific users that are authenticated by the data owner. Pairing based computation is replaced with scalar product on elliptic curves that reduces the resource and memory requirements for users. The features of both cryptography and steganography are combined by embedding crypto text into an image that enhanced data security, privacy and ownership

VII. FUTURE WORK

The user interface can be developed to provide more secure cloud-based processing for remote users along with user revocation features. Stand-alone application can be created that can be imported to any workstation.

REFERENCES

[1] Yinghui Zhang , Dong Zheng and Robert H. Deng, "Security and Privacy in Smart Health: Efficient Policy-Hiding Attribute-Based Access Control," IEEE Internet Of Things Journal, Vol. 5, No. 3, pp. 2130-2145, June 2018.

[2] Zhen Wang, Zhaofeng Ma,Shoushan Luo and Hongmin Gao," Enhanced Instant Message Security and Privacy Protection Scheme for Mobile Social Network Systems," IEEE Access,Special Section On Privacy Preservation For Large-Scale User Data In Social Networks,Vol. 6, No. 2, pp. 13706-13715, March 2018.

[3] Abid Mehmood, Iynkaran Natgunanathan,Yong Xiang, Howard Poston, And Yushu Zhang,"Anonymous Authentication Scheme for Smart Cloud Based Healthcare Applications" IEEE Access, Vol. 6, No. 4, pp. 33552-33567, July 2018.

[4] Kan Yang, Zhen Liu, Xiaohua Jia and Xuemin Sherman Shen,"Time-Domain Attribute-Based Access Control for Cloud-Based Video Content Sharing: A Cryptographic Approach," IEEE Trans. on Multimedia, Vol. 18, No. 5, pp. 940-950, May 2016.

[5] Jiguo Li , Wei Yao, Jinguang Han, Yichen Zhang and Jian Shen," User Collusion Avoidance CP-ABE With Efficient Attribute Revocation for Cloud Storage," IEEE Systems Journal, Vol. 12, No. 2, pp. 1-11, June 2018.

[6] Samer Atawneh, Ammar Almomani, and Putra Sumari,"Steganography in Digital Images: Common Approaches and Tools",IETE Technical review, Vol. 30, No. 6, pp. 344-358, 2013.

[7] Awdhesh K. Shukla1,2, Akanksha Singh3, Balvinder Singh1,4, Amod Kumar1,2, "A Secure and High-capacity Data-hiding Method Using Compression, Encryption and Optimized Pixel Value Differencing",IEEE Access", Vol. 6, No. 2, pp. 51130-51139, September 2018.

[8] Tarun Kumar Mishra1, Mamta Sakpal2," A Review of Multimedia Cryptography Techniques", International Journal of Research in Engineering, Science and Management Vol. 2, No. 7, pp. 764-766, July-2019.

[9] Kaiping Xue ,Weikeng Chen, Wei Li, Jianan Hong, and Peilin Hong, "Combining Data Owner-Side and Cloud-Side Access Control for Encrypted Cloud Storage," IEEE Transactions on Information Forensics and Security, Vol. 13, No. 8, pp. 2062-2074August 2018.

[10] Sorina Dumitrescu and Xiaolin Wu,"A New Framework of LSB Steganalysis of Digital Media," IEEE Transactions On Signal Processing, Vol. 53, No. 10, pp. 3936-3947, Oct 2015.

ISSN [Online]: 2583-2654

[11] Jianting Ning, Zhenfu Cao,Xiaolei Dong,Kaitai Liang, Hui Ma and Lifei Wei, "Auditable σ-Time Outsourced Attribute-Based Encryption for Access Control in Cloud Computing," IEEE Transactions On Information Forensics And Security, Vol. 13, No. 1, pp. 94-105, January 2018.

[12] Sheng ding, Chen li and Hui li,"A Novel Efficient Pairing-free CP-ABE Based On Elliptic Curve Cryptography,"IEEE Access Special Section on Security and Trusted Computing for Industrial Internet of Things, Vol. 6, No. 2, pp. 27336-27345, June 2018.

[13] Qiang Wang, Li Peng, Hu Xiong , Jianfei Sun, And Zhiguang Qin, "Ciphertext-Policy Attribute-Based Encryption with Delegated Equality Test in Cloud Computing,"IEEE Access, Vol. 6, No. 8, pp.762-771 ,February 2018.

[14] Jianghong Wei , Wenfen Liu, and Xuexian Hu," Secure and Efficient Attribute-Based Access Control for Multiauthority Cloud Storage," IEEE Systems Journal, Vol. 12, No. 2, pp.1731-1742 , June 2018.

[15] Shuming Qiu , Guoai Xu, Haseeb Ahmad and Licheng Wang," A Robust Mutual Authentication Scheme Based on Elliptic Curve Cryptography for Telecare Medical Information Systems," IEEE Access, Vol. 6, No. 3, pp. 7452-7463, March 2018.

[16] A. Xiong, Q. Gan, X. He and Q. Zhao, "A searchable encryption of CP-ABE scheme in cloud storage," 2013 10th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP), Chengdu, Vol. 11, No. 4, pp. 345-349, 2013.