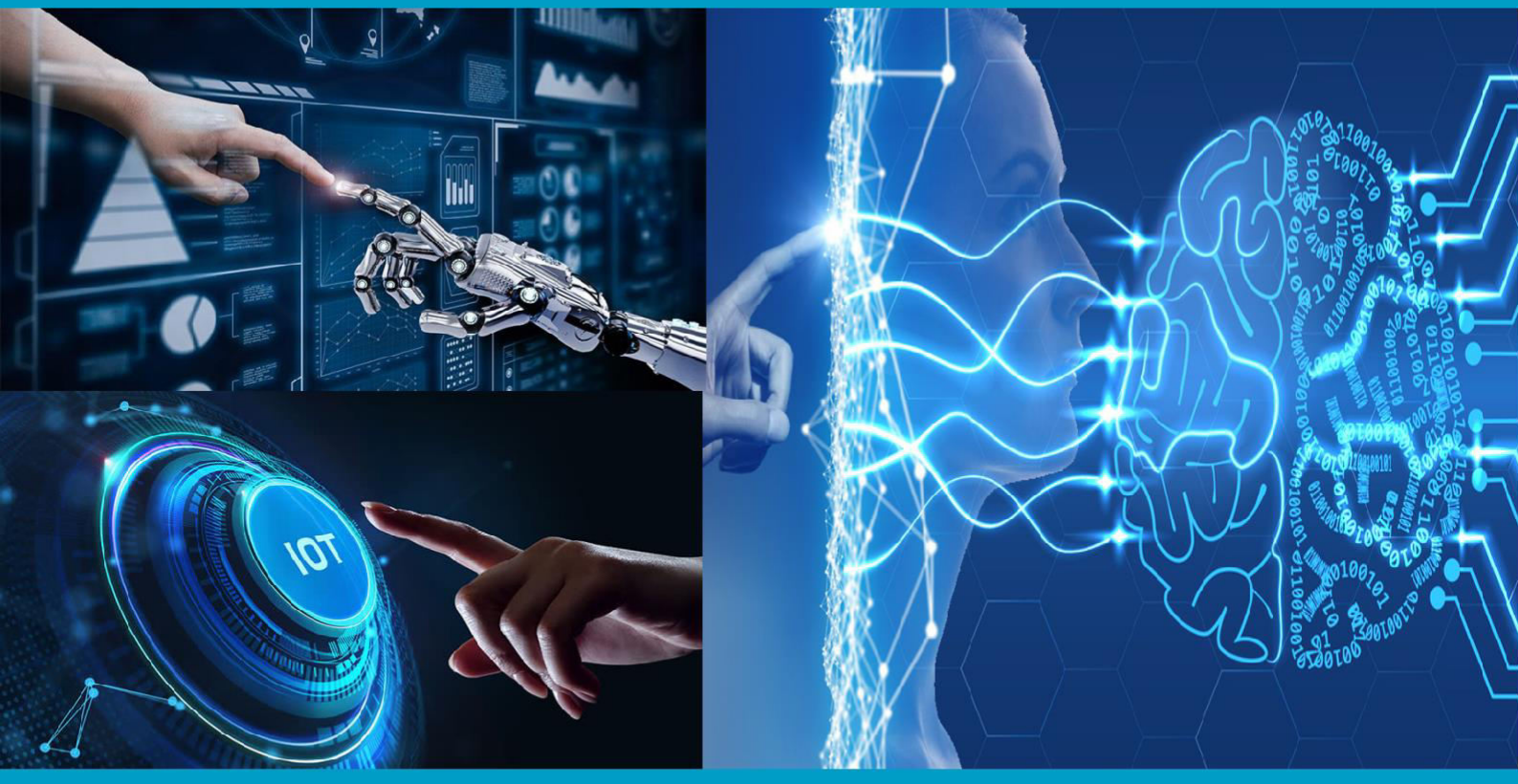
IJMRSETM

e-ISSN: 2395 - 7639



INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING, TECHNOLOGY AND MANAGEMENT

Volume 11, Issue 3, March 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.580

International Journal of Multidisciplinary Research in Science, Engineering, Technology & Management (IJMRSETM)

| ISSN: 2395-7639 | www.ijmrsetm.com | Impact Factor: 7.580| A Monthly Double-Blind Peer Reviewed Journal |

| Volume 11, Issue 3, March 2024 |

Image Security using Attribute Based Encryption

Mr. Pawar V.D, Mr. Chougule V.V, Patil A.L , Gaikwad P.P , Baje V.S , Ingale S.D , Arenavaru S.B

Vice Principal & HOD, S.V.S.M.D'S, Kai. Kalyanrao(Balasaheb) Ingale Polytechnic, Akkalkot, Maharashtra, India

Lecturer, Department of Computer Engineering, S.V.S.M.D'S, Kai.Kalyanrao(Balasaheb) Ingale Polytechnic, Akkalkot, Maharashtra, India

Department of Computer Engineering, S.V.S.M.D'S, Kai.Kalyanrao(Balasaheb) Ingale Polytechnic, Akkalkot, Maharashtra, India

ABSTRACT: Enforcing access policies and supporting policy modifications is one of the trickiest problems with data sharing platforms. The cryptographic answer to this problem is increasingly looking promising: ciphertext policy attribute-based encryption (CP-ABE). The attribute set that a decryptor must possess to decrypt the ciphertext can be defined by the encryptor and enforced on the contents of the ciphertext using the attribute-based encryption approach. As a result, according to the security policy, every user with a unique set of attributes is permitted to decrypt distinct pieces of data. The CP-ABE system is suggested as a way to enhance attribute-based multimedia data sharing's efficiency and security. The Key Generation Center, Data Owner, and Data are components of the suggested multimedia data sharing system.

KEYWORDS: ABE, cryptographic, encryptor, decryptor ,security

I. INTRODUCTION

Many people can share their data with others effortlessly thanks to network and computing technology when they use online external storage. To save money or make sharing their highly sensitive personal health records (PHRs) with their primary care physicians easier, users can upload their PHRs to online data servers such as Microsoft Health Vault or Google Health.. Alternatively, users can share their lives with friends by posting private photos or messages on online social networks. People's worries about access control and data security grow as they take advantage of these new services and technologies. Potential risks to their data include improper use of the data by the storage server or unauthorized access by other users. People want to limit who may access their private or sensitive data to those who are allowed and have the credentials they specified.

Key-policy ABE (KP-ABE) and ciphertext-policy ABE are the two varieties of attribute-based encryption (ABE). In CP-ABE, users' credentials are described by attributes, and an encryptor establishes a policy regarding who can decode the data. In KP-ABE, attributes are used to describe the encrypted data, and policies are integrated into users' keys. Because CP-ABE gives data owners the authority to decide on access policies, it is a better fit for the data sharing system than the other option [2], [3].

A single trustworthy authority, or KGC, has the ability to produce all of the users' private keys along with their master secret information in the majority of ABE schemes that are now in use [4, 5, 9, 10]. Because of this, the key escrow issue is intrinsic, meaning that any time a user generates their secret key, the KGC can decrypt any ciphertext that is directed to them in the system.

The distributed KP-ABE solution proposed by Chase and Chow [6] addresses the key escrow issue in a multiauthority system. In the identity-based literature, Chow [7] proposed an anonymous private key generation technique that would allow the KGC to issue a private key to an authenticated user without having access to the list of users' identities. The first key revocation techniques in CP-ABE and KP-ABE environments were proposed by Bethencourt et al. [4] and Boldyreva et al. [8], respectively.

By encrypting the message with the attribute set's validation time, these techniques allow the revocation of an attribute key.It would be intriguing to investigate attribute-based encryption schemes using cutting-edge cryptosystems for data exchange. Multimedia content, such photos, should be encrypted by the proposed system.

II. LITERATURE REVIEW

This scheme provide solutions to the issues such as robustness, security and tamper detection with precise localization. The features were extracted in Daubechies4 wavelet transform domain with help of PSO to generate the image hash.

In ref[10] paper they were used the algorithm of encoding technique to secure the medical documents such as patient details. But From a security point of view, even if it had worked in practice, this would have been a very weak encryption algorithm for two reasons. First, there is no secret key. Therefore, it is not a true encryption scheme, but an

| ISSN: 2395-7639 | www.ijmrsetm.com | Impact Factor: 7.580| A Monthly Double-Blind Peer Reviewed Journal |

| Volume 11, Issue 3, March 2024 |

encoding scheme. Anyone who knows its operation method can easily recover the original text. Second, even if the operation method is unknown to an attacker or even if a secret key is introduced, the algorithm is a simple substitution cipher, which means that the same plain character will always be encrypted into the same cipher character under the same key.It implies that, while using the same key, the same plain character will always be encrypted into the same cipher character.

In[11] Block-Based Algorithm there are various technique used as follows Blowfish algorithm has best performance for the smallest image block size so it is not applicable for large images. It resulted in higher correlation and lower entropy .So they proposed new algorithm In that original image was divided into blocks, which were rearranged into a transformed image using a transformation algorithm and then the transformed image was encrypted using the Blowfish algorithm but for rearranging the images it take lot of time than the actual encryption of images. which indicates that the algorithms were commercially available. They used the proposed algorithm in conjunction with the other algorithms to achieve better performance than just using the other algorithms alone on the ciphered image, which was the outcome of applying the proposed algorithm on various block sizes of the original image. Under the same key, the same plain character will always be encrypted into the same cipher character.

In ref[12] Steganography is the art of covering secret and confidential information within a carrier which could be an image file, video file or audio file. It was a technique which provides invisible communication since an image file which had the secret information embedded within it is delivered to the receiver instead of the secret information itself. It is a technique of protecting information by transforming into unreadable format called cipher text. The communication cannot be decrypted or decoded into plain text by anybody without the secret key.

In ref[13] they discussed the Particle swarm optimization (PSO) for image authentication and tamper proofing.

This system offers answers for security, resilience, and accurate localization in the event of tampering. To create the picture hash, the features were retrieved in the Daubechies4 wavelet transform domain with the assistance of PSO.

This system offers answers for security, resilience, and accurate localization in the event of tampering. To create the picture hash, the features were retrieved in the Daubechies4 wavelet transform domain with the assistance of PSO.

When it comes to picture authentication, hash-based techniques are distinct from watermark-based procedures. A compact representation of the image that can be used for authentication is created by extracting a collection of features from the image using an image hashing approach. The advantages of hash based techniques are no distortion is introduced in the image to be authenticated and content hash generated in frequency domain which has more robust to geometric distortions compared to their spatial domain counterparts

Cloud over data privacy is achieved by using encryption techniques. The security of network is consisting of different approaches and techniques to achieve the data cryptographic security. The most commonly used method in recent time is Attribute-based encryption (ABE). If a user sends through the access request to the cloud, the cloud will return to the same cipher text data user, a user to decrypt the data using your private key.

But this way would lead to various problems: (1) to be able to encrypt data, the data owner needs to obtain the data user's public key to finish this;(2) a lot of storage overhead would spend because of the same plaintext with different public keys In order to overcome these limitations, and so forth, an attribute-based encryption (ABE).

III.METHODOLOGY

Encrypting images according to the attributes of the users is possible with attribute-based encryption (ABE). This makes the photos accessible and decryptable to individuals who possess certain qualities only. Encryption-policy ABE (CP-ABE) and key-policy ABE (KP-ABE) are the two primary forms of ABE. The policy for access control is integrated into the ciphertext in CP-ABE and the user's key in KP-ABE. When there are several parties involved and stringent access control is needed, such as in IoT and smart home applications, ABE can be immensely helpful. Because so many parameters may be defined, the ABE technique offers highly customizable access control to the encrypted images at a fine level.

| ISSN: 2395-7639 | www.ijmrsetm.com | Impact Factor: 7.580| A Monthly Double-Blind Peer Reviewed Journal |

| Volume 11, Issue 3, March 2024 |

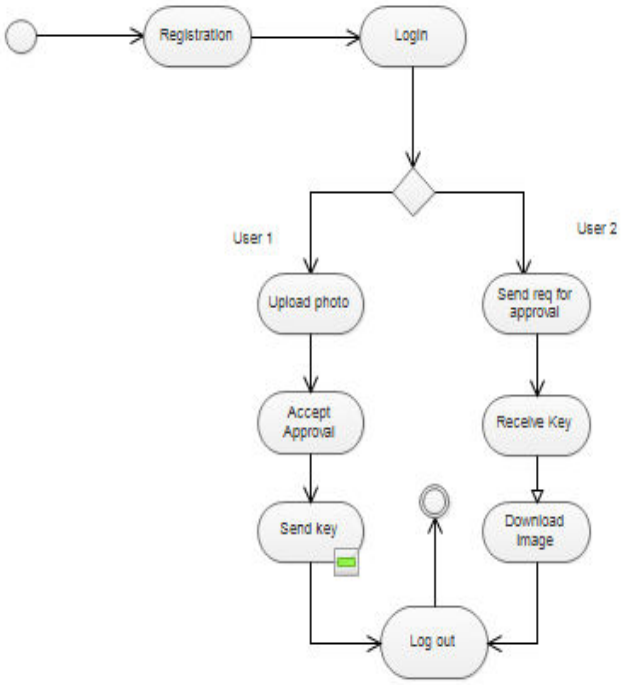


Fig. Activity Diagram

This activity diagram shows that a user must first register and log in. If the user is an administrator, they will then proceed to the User1 flow; otherwise, they will proceed to the User2 flow and log out.

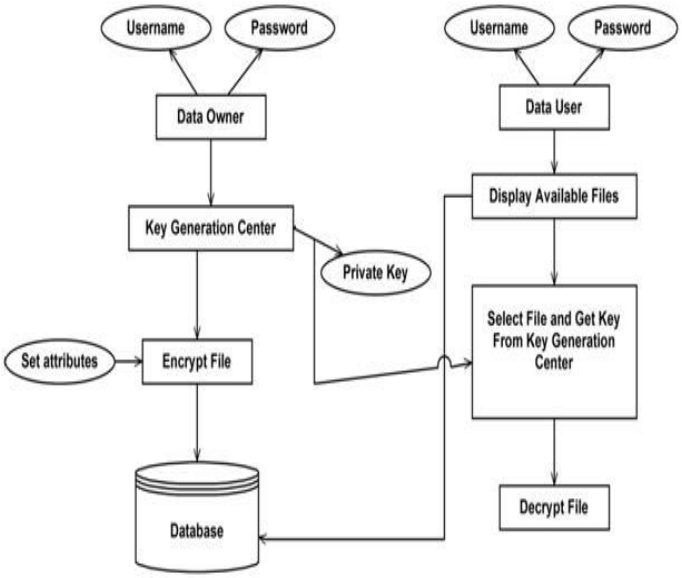


Fig. System Block Diagram

The above block diagram works in the following way

1. Data owner enter their username and password then select images to upload
2. This image will be encrypted and a unique key will be generated at Key generation center.
3. The images will be stored on database with the key.
4. User will select image and request for the key to owner. After that user will enter the key and the image will get decrypt to the original form.

Algorithms used:

| ISSN: 2395-7639 | www.ijmrsetm.com | Impact Factor: 7.580| A Monthly Double-Blind Peer Reviewed Journal |

| Volume 11, Issue 3, March 2024 |

1. Algorithm for Key Generation**:**

1. Owner select image to upload.

2. The system set attribute A and randomly generate number as another attribute B. Next, using time function T, these attributes form an encryption key.

i.e. pk= E(A ,B ,T).

where, pk is public key of the image owner and E is encryption tehnique [MD5].

3. B and T together generate image ID.

2. Algorithm for Encryption**:**

1.Image first converted to binary

2. Encryption is done using key and base64 encryption

algorithm.

Ci=Eb(Pi ,pk)

Where, Ci is ciphertext of image, Eb is base64 encryption PI plaintext of image, pk is public key of image owner

3. Algorithm for Decryption**:**

1. User select image to download.

2. System compares attributes of user with attribute of encrypted image.

3. If the user properties of the image match, create the decryption key and decode the image.

Pi=Db(Ci ,Prk)

Where, Pi is plain text of image,

Db is base64 decryption,

Ci is ciphertext of image,

Prk is private key of image user.

4. If image user attributes does not matches, send request to image owner.

5. If owner allow then key (Prk) will be sent to user to download image.

4. Algorithm for MD5**:**

• Step1 : Append padding bits

In order to make the input message's length (in bits) equal to 448 mod 512, it is "padded" or expanded. Even when a message is already 448 mod 512 in length, padding is always done. The process of padding involves appending a single "1" bit and subsequently many "0" bits to the message, resulting in a length in bits that is equivalent with 448 mod 512. Appended are at most 512 bits and at least one bit.

• Step2 : Append length

Attached to the outcome of step 1 is a 64-bit representation of the message's length. If the message length is longer than 2^64, just the lowest 64 bits will be utilized. After padding with bits and b, the resultant message has a length that is precisely multiple of 512 bits. The length of the input message will be an exact multiple of sixteen (32-bit) words.

• Step3 : Initialize MD buffer

A four-word buffer (A, B, C, D) is used to calculate the message digest. A, B, C, and D are all 32-bit registers. The following values, initialized in low-order hexadecimal bytes, are set for these registers:

| ISSN: 2395-7639 | www.ijmrsetm.com | Impact Factor: 7.580| A Monthly Double-Blind Peer Reviewed Journal |

| Volume 11, Issue 3, March 2024 |

word A: 01 23 45 67

word B: 89 ab cd ef

word C: fe dc ba 98

word D: 76 54 32 10

• Step4 : Process message in 16-word blocks

We'll define four functions, each of which accepts three 32-bit words as input and outputs another 32-bit word.

XY or not (X) = F (X, Y, Z) Z

G (X, Y, Z) = Y not (Z) or XZ

X xor Y xor H (X, Y, Z) = Z

I = Y xor (X or not (Z)) in (X, Y, Z)

5. Algorithm for base64

1. Divide the input bytes stream into blocks of 3 bytes.

2. Divide 24 bits of each 3-byte block into 4 groups of 6 bits.

3. Using the Base64 character set map, map each group of six bits to a single printed character based on the 6-bit value.

4. If the last 3-byte block has only 1 byte of input data, pad 2 bytes of zero (\x0000). Replace the final two letters with two equal signs (==) after encoding it as a regular block so that the decoding algorithm is aware that two bytes of zero were padded.

5. If the last 3-byte block has only 2 bytes of input data, pad 1 byte of zero (\x00). Replace the final character with one equal sign (=) after encoding it as a regular block so that the decoding algorithm is aware that one byte of zero was padded.

6. Carriage return (\r) and new line (\n) are inserted into the output character stream. The decoding process won't pay any attention to them.

IV. CONCLUSION

Using our Secure Image Sharing system, image owners can safely share their images with a large number of unknown users who meet the requirements for image access. Users who are not eligible for image access policies may submit a request to the owner of the image. The owner of the image grants the requests. The encrypted image will only be accessible to the approved requester. Addressed the gap highlighted for research and development.

REFERENCES

[1] J.-M. Zhu and J.-F. Ma, “Improving Security and Efficiency in Attribute Based Data Sharing,” IEEE Transactions on knowledge and data engineering , vol. 25, no. 10, october 2013.

[2] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, “Mediated Ciphertext-Policy Attribute-Based Encryption and Its Application,” Proc. Int’l Workshop Information Security Applications (WISA ’09), pp. 309-323, 2009.

[3] S. Yu, C. Wang, K. Ren, and W. Lou, “Attribute Based Data Sharing with Attribute Revocation,” Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS ’10), 2010.

[4] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-Policy Attribute-Based Encryption,” Proc. IEEE Symp. Security and Privacy, pp. 321-334, 2007.

[5] X. Liang, Z. Cao, H. Lin, and D. Xing, “Provably Secure and Efficient Bounded Ciphertext Policy Attribute Based Encryption,” Proc. Int’l Symp. Information, Computer, and Comm. Security (ASIACCS), pp. 343-352, 2009.

[6] M. Chase and S.S.M. Chow, “Improving Privacy and Security in Multi-Authority Attribute-Based Encryption,” Proc. ACM Conf. Computer and Comm. Security, pp. 121-130, 2009.

| ISSN: 2395-7639 | www.ijmrsetm.com | Impact Factor: 7.580| A Monthly Double-Blind Peer Reviewed Journal |

| Volume 11, Issue 3, March 2024 |

[7] S.S.M. Chow, "Removing Escrow from Identity-Based Encryption," Proc. Int'l Conf. Practice and Theory in Public Key Cryptography (PKC '09), pp. 256-276, 2009.

[8] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-Based Encryption with Efficient Revocation," Proc. ACM Conf. Computer and Comm. Security, pp. 417-426, 2008.

[9] V. Goyal, A. Jain, O. Pandey, and A. Sahai, "Bounded Ciphertext Policy Attribute-Based Encryption," Proc. Int'l Colloquium Automata, Languages and Programming (ICALP), pp. 579-591, 2008.

[10] Gonzalo Alvarez, Shujun Lib, Luis Hernandez "Analysis of security problems in a medical image encryption system"

[11] Mohammad Ali Bani Younes and Arnan Jantan "Image Encryption Using Block-Based Transformation Algorithm "

[12] Pritam Kumari, Chetna Kumar, Preeyanshi, Jaya Bhushan "Data Security Using Image Steganography And Weighing Its Techniques"

[13] K. Kuppusamy and K. Thamodaran "PSO based optimized security scheme for image authentication and tamper proofing "

Impact Factor: 7.580

INTERNATIONAL JOURNAL
OF MULTIDISCIPLINARY RESEARCH
IN SCIENCE, ENGINEERING, TECHNOLOGY AND MANAGEMENT

+91 99405 72462 +91 63819 07438 ijmrsetm@gmail.com