Enhancing Social Media Security for Login and Image Sharing

[1] Sushmita A. Kale, [2] Prof. P. S. Malage

[1]Student, [2] Assistant Professor

[1] Department of Electronics Engineering,

[1]WIT, Solapur, India.

Abstract : Users may have various login ids it will be hard to remember their passwords and alphanumeric passwords are difficult to remember. So the graphical password is one of a secure solution. Some threats of Internet security are spyware and shoulder-surfing attacks. This paper presents a new scheme for a graphical password that uses images that are unexplainable and have larger password space. The proposed scheme is also resistant to spyware and shoulder-surfing attacks. Security always remains a constraint when we talk about the sharing of any information or document. For enhancing the security, here we have first encrypted the image then this encrypted image is used as password, so the password will be hard to guess and much secure from the attack to guess the password. One of the most challenging issues in data sharing systems is the enforcement of access policies and the support of policy updates. The solution to this issue is Ciphertext policy attribute-based encryption (CP-ABE). Ciphertext–Attribute-Based Encryption scheme enables an encryptor to define the attribute set over a universe of attributes that a decryptor needs to possess in order to decrypt the ciphertext, and enforce it on the contents. Thus, every user needs a different set of attributes to decrypt different pieces of data. It is proposed to use the CP-ABE scheme to improve security and efficiency in attribute-based multimedia data sharing. The proposed multimedia data sharing system includes Key Generation Center, Data Owner, Data User, Data Storing Center system entities that help to share image securely using CP-ABE scheme. Here, specifically focus is on sharing the image in '.jpg' format**.**

***IndexTerms* - Image security, Image sharing system, Attribute base encryption, Access Control, Network security, CP-ABE, Image Encryption.**

I. Introduction

The image encryption can be described as the process of securely transmitting the images over the computer network may be wireless or it may be a physically connected network. The image is required to be transmitted in such a way that, no unauthorized Users will able to decrypt the image transferred. The concept of Image encryption and image decryption can be used in various purposes which are related to the fields of internet communication, transmission, medical imaging, the medicine and military Communication, etc.

There are several special properties of image data like bulk capability, high redundancy, and high correlation among the pixels which can be used as the basis for the process of the image encryption and image decryption. In general, we can explain the concept of encryption and decryption. By encryption, we can convert the plain message into a form called a ciphertext which cannot be read by any a person as it is encrypted and its actual meaning has been changed, and the actual meaning or message from the ciphertext cannot be obtained until and unless we decrypt the encrypted text [1].

Decryption [1] is considered as the reverse process of encryption, in this case, we will convert the encrypted text into its original plain text so that it can be read and derive the actual meaning from that. By encrypting the data we can protect the various data resources mainly when it has been available over the internet, intranets, and extranets. Ciphertext-policy attribute-based encryption (CP-ABE) [2],[3] has turned out to be an important encryption technology to tackle the challenge of secure data sharing. In a CP-ABE, the user's secret key is described by an attribute set, and ciphertext is associated with an access structure. DO is allowed to define access structure over the universe of attributes. A user can decrypt a given ciphertext only if his/her attribute set matches the access structure over the cipher-text. Employing a CP-ABE system directly into a cloud application that may yield some open problems. Firstly, the key escrow problem is nothing but security risk which arrived because all users secret keys need to be issued by a fully trusted key authority (KA).

By knowing the secret key of a system user, the KA can decrypt the entire user's ciphertext, which stands in total against the will of the user. Secondly, the expressiveness of an attribute set is another concern.

II. LITERATURE REVIEW

Bonneau et al. [4] proposed the concept of privacy suites which recommend users a suite of privacy settings that "expert" users or other trusted friends have already set so that normal users can either directly choose a setting or only need to do the minor modification. Ravichandran et al. [5] studied how to predict a user's privacy preferences for location-based data (i.e., share her location or not) based on location and time of day. Fang et al. [6] proposed a privacy wizard help users grant privileges to their friends. The wizard asks users to first assign privacy labels to the selected friends and then uses this as the input to construct a classifier to classify friends based on their profiles and automatically assign privacy tag to the unlabeled friends. More recently, Klemperer et al. studied whether the keywords and captions (which are provided by the users when they tag their photos) can be used to help users create and maintain access-control policies more intuitively, where the social tags created for organizational purposes can be re-purposed to help create reasonable access-control rules. The aforementioned approaches focus on deriving policy settings for only traits, so they mainly consider social context such as one's friend list. While interesting, they may not be sufficient to address challenges brought by images for which privacy may vary substantially not just because of social contexts but also due to the actual image content as considered in our work. Tonge and Caragea [9] integrated the deep features for image privacy prediction and Spyromitros-Xioufis et al. [10] leveraged user-dependent images and privacy settings to support personalized privacy-aware image classification. Both teams have found that the deep features can yield remarkable improvements on the performance as compared with other handcrafted visual features such as SIFT, GIST and color histograms. Compared to them, our approach provides a finer level of image classification and is much more efficient.

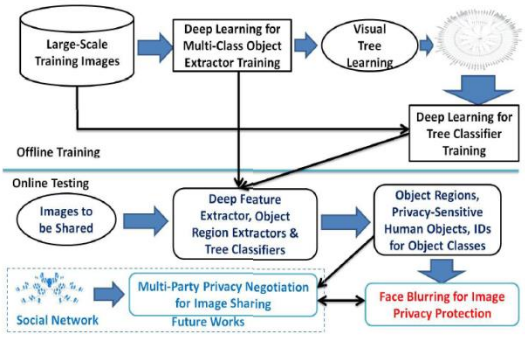

Large-Scale Training Images
Deep Learning for Multi-Class Object Extractor Training
Visual Tree Learning
Deep Learning for Tree Classifier Training
Offline Training
Online Testing
Images to be Shared
Deep Feature Extractor, Object Region Extractors & Tree Classifiers
Object Regions, Privacy-Sensitive Human Objects, IDs for Object Classes
Social Network
Multi-Party Privacy Negotiation for Image Sharing
Future Works
Face Blurring for Image Privacy Protection

Fig. 2.1 BLURRING THE IMAGE

Mitra A et al. [11] have proposed a random combinational image encryption approach with a bit, pixel and block permutations. Zhi-Hong Guan et al. [12] have produced a new image encryption scheme, in which shuffling the positions of pixel values and changing their grey values are combined to confuse the relationship between the cipher image and the plain image. Sinha A. and Singh K. [13] proposed an image encryption by using Fractional Fourier Transform (FRFT) and JigSaw Transform (JST) in image bit planes. Shujun Li et al. [14] have pointed out that all permutation-only image ciphers were insecure against known/chosen-plaintext attacks. In conclusion, to design highly secured images the secret permutations have to be combined with other encryption techniques.

1. Key generation center: It generates public and secret parameters for CP-ABE. It is responsible for issuing, revoking, and updating attribute keys for users. It gives differential access rights to individual users based on their attributes. That is, it will honestly execute the assigned tasks in the system; however, it would like to learn information about encrypted content as much as possible. Thus, it should be prevented from accessing the original text of the encrypted data even if it is honest.

2. Data-storing center: It provides a data-sharing service. It is in charge of controlling the accesses from outside users to the storing data and providing corresponding content services.

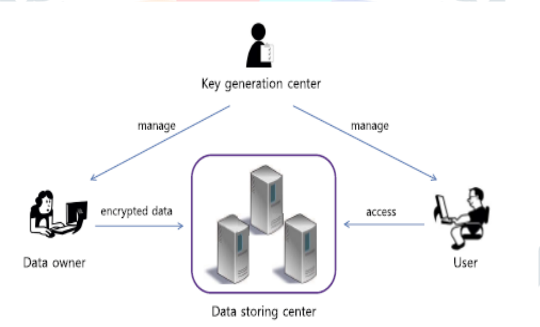
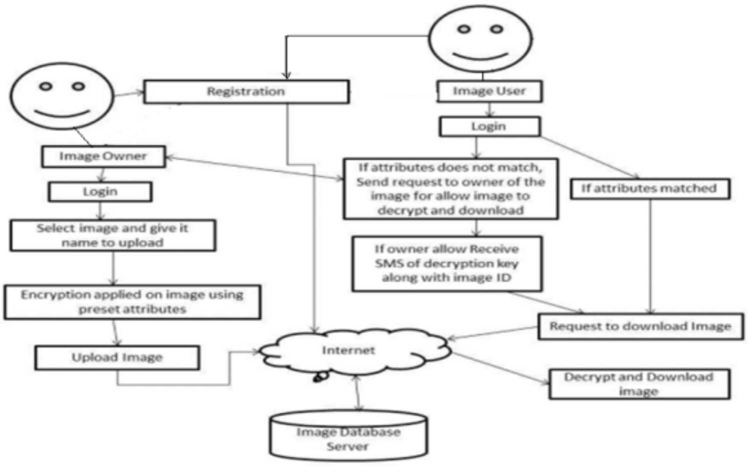


Fig. 2.2 ENCRYPTING THE IMAGE

3. Data owner: He is a client who wishes to upload his own data into the external data-storing center for ease of sharing or for cost-saving. A data owner is responsible for defining (attribute-based) access policy and enforcing it on its own data by encrypting the data under the policy before distributing it.

4. User: It is an entity that wants to access the data. If a user proposes a set of attributes satisfying the access policy of the encrypted data and is not revoked in any of the valid attribute groups, then he will be able to obtain the data by decrypting it. Since both of the key managers, the KGC and the data storing center, are semi-trusted, they should be deterred from accessing the plaintext of the data to be shared; they should able to issue secret keys to users. In order to realize this requirement, the two parties engage in the arithmetic 2PCprotocol with master secret keys of their own, and issue independent key components to users during the key issuing phase. As none of them can generate the whole set of secret keys of users individually because the 2PC protocol deters them from knowing each other's master secrets.

III. PROPOSED SYSTEM


Registration
Image User
Login
Image Owner
Login
If attributes does not match, Send request to owner of the image for allow image to decrypt and download
If attributes matched
Select image and give it name to upload
If owner allow Receive SMS of decryption key along with image ID
Encryption applied on image using preset attributes
Request to download Image
Internet
Upload Image
Decrypt and Download image
Image Database Server

3.1 PROPOSED SYSTEM

A novel concept is introduced as an image sharing system to secure image sharing by using CP-ABE scheme. Image is encrypted and key for decryption is stored in database. Image is decrypted using key when attribute matches otherwise user can send request of particular image to the owner of image then the key distribution is takes place with notification.

System uses methods such as generation of keys, encryption of image, and decryption. Stepwise descriptions of these methods are:

[1] Algorithm for Key generation:

a. Owner select image to upload
b. The system set attribute Pra and randomly get number as another attribute Ra.
Then these attributes generate key for encryption with time function T.
I.e. Pbk= E(Pra ,Ra ,T).
Where, Pbk is public key and E is encryption.
c. Ra and T together generate image ID.

[2] Algorithm for Encryption:

a. Image first converted to binary
b. Encryption is done using Pbk and base64 encryption algorithm.

Ci=Eb(Pi,Pbk)

Where, Ci is ciphertext of image, Eb is encryption, Pi is plaintext of image, Pbk is public key.

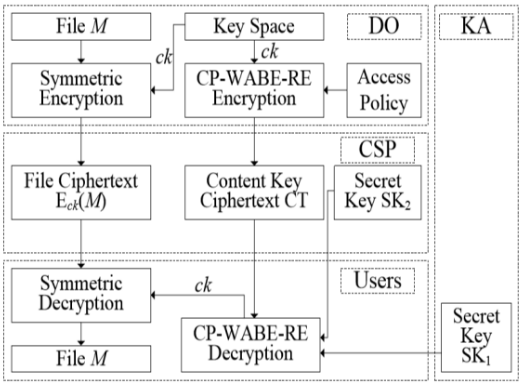
[3] Algorithm for Decryption:

a. User selects an image to download.
b. System check attributes of user with image attribute.
c. If attributes matches it generates key for decryption Prk and decrypt image

Pi=Db(Ci,Prk)

Where, Pi is plain text of image, Db is decryption, Ci is ciphertext of image, Prk is private key.
d. If attributes does not matches, send request to owner. If owner allow then key will be sent to user to download image.

IV. METHODOLOGY



4.1 SYSTEM BLOCK DIAGRAM

Key Generation:

The system model and framework of the CP-WABE-RE scheme in cloud computing are given, where the system consists of four types of entities: KA, CSP, DO and Users. In addition, we provide the detailed Definition of CP-WABE-RE scheme.

Key Authority (KA):

It is a semi-trusted entity in the cloud system. Namely, KA is honest-but-curious, which can honestly perform the assigned tasks and return correct results. Due to that, it will collect most of the sensitive contents. In the cloud system, the entity is responsible for the users' enrollment. Meanwhile, it not only generates most part of a system parameter but also creates the most part of the secret key for each user.

Cloud Service Provider (CSP):

It manages cloud servers and also a semi-trusted entity and also provide data storage, computation, and transmission. To solve the key escrow problem, it generates both parts of the system parameter and secret key for each user.

Data Owners (DO):

They are owners of file to be stored in the cloud system. They are in charge of defining 0. Access structure and executing data encryption operation. They also upload the generated ciphertext to CSP Users. They want to access ciphertext stored in a cloud system. They download the ciphertext and execute the corresponding decryption operation.

Definition 1. (CP-WABE-RE): The proposed scheme contains the following four phases:

Phase 1:

System Initialization. This phase includes both algorithms: KA. Setup and CSP.Setup.

(1) KA.Setup(1^{κ}) → (PP1,MSK1). It is executed by KA. The probabilistic operation inputs a security parameter κ. It returns a public parameter PP1 and a master secret key MSK1.

(2) CSP.Setup(1^{κ}) → (PP2,MSK2). This algorithm is run by CSP. It inputs a security parameter κ and generates PP2 and MSK2. The public parameter and master secret key of the system is denoted as PP = {PP1, PP2} and MSK = {MSK1, MSK2}, where MSK1 and MSK2 are stored by KA and CSP, respectively.

Phase 2:

Data Encryption: To improve the efficiency of encryption, DO first encrypts file M with content key CK by using a simple symmetric encryption algorithm, where file ciphertext is denoted as Eck(M). Then, the content key CK is encrypted by the following operation.

DO.Encrypt(PP, CK,A) → (CT): DO inputs PP, CK, and access policy A. It encrypts CK and outputs content key ciphertext CT which implicitly contains A. Then, DO delivers Eck(M) and CT to CSP.

Phase 3:

User Key Generation: This phase consists of KA. KeyGen and CSP. KeyGen.

(1) KA.KeyGen (MSK1, S) → (SK1): KA inputs MSK1 and a set of weighted attributes S. It creates a secret key SK1 described by S.

(2)In CSP.KeyGen: we propose an improved two-party key issuing protocol to remove escrow. KA and CSP perform the improved protocol with master secret keys of their own. Thus, none of them can create the whole set of secret keys of users individually. Meanwhile, we assume that KA does not collude with CSP since they are honest as in [16] (otherwise, they can obtain the secret keys of each user by sharing their master secret keys).

CSP.KeyGen (MSK2) → (SK2): CSP inputs MSK2 and the required information. It produces secret key SK2 by executing the following key issuing protocol.

• KeyComKA↔CSP (MSK1, IDT,r, MSK2) → (SK2): It is an interactive algorithm between KA and CSP. KA inputs MSK1, a user identity IDT and a personalized secret r. CSP inputs MSK2 and IDT. At last, only CSP generates a personalized key component SK2 for the corresponding user. Then, the user constructs the whole secret key SK with the key components separately receiving from KA and CSP, i.e. SK = {SK1, SK2}.

Phase 4 :

Data Decryption: This phase contains both algorithms: Users Decrypt and Data Decrypt. User first downloads file ciphertext Eck(M) and content key ciphertext CT from CSP. If he satisfies conditions, he can get content key CK by calling the Users Decrypt algorithm. Then, he uses CK to further decrypt file M by using Data Decrypt operation.

(1) Users Decrypt(PP,SK,CT) → (ck): User inputs PP, SK described by S, and CT which includes access policy A. Only when the weighted attribute set S matches the access policy A, the content key ck is obtained.

(2) Data Decrypt(Eck(M),ck) → (M): User inputs E ck(M) and ck. Based on symmetric decryption algorithm, it outputs file M.

V. Conclusion

Security is always an important concern in communication. So for the secure transmission of any data including the IMAGES, encryption techniques are always in demand and there always be a requirement for better techniques to be developed to provide more security. Similarly, Security also plays an important role in protecting resources against unauthorized access. So images as a password are the better alternative for securing the resources and there also better algorithms will always be required for making access more secure. Using CP-ABP we can provide security to social media.

References

[1] Rinki Pakshwaretal, A Survey On Different Image Encryption and Decryption Techniques, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 4 (1) , 2013, 113 – 116

[2] Balu and K. Kuppusamy. An expressive and provably secure ciphertext-policy attribute-based encryption. Information Sciences, 276(4):354–362, 2014.

[3] Z. Zhou, D. Huang, and Z. Wang. Efficient privacy-preserving ciphertext-policy attribute based encryption and broadcast encryption. IEEE Transactions on Computers, 64(1):126–138, 2015.

[4] J. Bonneau, J. Anderson, L. Church, "Privacy suites: shared privacy for social networks", in: SOUPS, 2009.

[5] R. Ravichandran, M. Benisch, P. Kelley, N. Sadeh, "Capturing social networking privacy preferences", in: SOUPS, 2009.

[6] L. Fang, K. LeFevre, “Privacy wizards for social networking sites’, ACM WWW, 2010.

[7] P. Klemperer, Y. Liang, M. Mazurek, M. Sleeper, B. Ur, L. Bauer, L. F. Cranor, N. Gupta, M. Reiter, “Tag, you can see it!: using tags for access control in photo sharing”, in: CHI, 2012, pp. 377–386

[8] Wang, S., Liang, K., Liu, J. K., Chen, J., Yu, J., & Xie, W. (2016). Attribute-Based Data Sharing Scheme Revisited in Cloud Computing. IEEE Transactions on Information Forensics and Security, 11(8), 1661–1673. doi:10.1109/tifs.2016.2549004

[9] Tonge, C. Caragea, “Privacy prediction of images shared on social media sites using deep features”, AAAI Symposium, 2015.

[10] E. Spyromitros-Xioufis, S. Papadopoulos, A. Popescu, Y. Kompatsiaris, “Personalized privacy-aware image classification”, ACM ICMR, 2016.

[11] Mitra, , Y V. Subba Rao, and S. R. M. Prasnna, "A new image encryption approach using combinational permutation techniques," Journal of computer Science, vol. 1(1), pp.127, 2006.

[12] G. Zhi-Hong, H. Fangjun, and G.Wenjie , "Chaos - based image encryption algorithm," Department of Electrical and computer Engineering, University of Waterloo, ON N2L 3G1, Canada.

[13] A.Sinha, K. Singh, "A technique for image encryption using digi tal signature," Source: Optics Communications, vol.218(4), pp.229-234, 2003.

[14] Li. Shujun, X. Zheng "Cryptanalysis of a chaotic imagevencryption method," Inst. of Image Process. Xi'anvJiaotong Univ., Shaanxi, This paper appears in: Circuits and Systems, ISCAS 2002.