IJESRT
INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

SECURITY PROTECTION FOR MULTI OWNER FIRM

Chandrashekhar Pardeshi*, Chinmay Niphadkar, Indrajit Dhalpe, Saurabh Barge,
Prof. S. S.Biradar
DEPARTMENT OF COMPUTER ENGINEERING, RMD SINHGAD SCHOOL OF ENGINEERING,WARJE,
PUNE-58,INDIA

ABSTRACT

With the increasing use of digital communication the security of data or the information has been a concern. The proposed secure sharing scheme allows users to upload multiple data pieces to different clouds, making it impossible to derive the whole information from any one cloud. In addition, the proposed scalable watermarking algorithm can be used for authentications between personal users and the media cloud. Furthermore, we introduce a new solution to resist multimedia transmission errors through a joint design of watermarking and Reed-Solomon codes. Our studies show that the proposed approach not only achieves good security performance, but also can enhance media quality and reduce transmission overhead.

KEYWORDS: cloud, security, advanced encryption standard, watermarking, visual cryptography

INTRODUCTION

In the fast growing world and increasing use of digital media, images and videos, the issue of security and confidentiality is at risk. Digital multimedia content such as images and videos can easily be sent through the Internet to the cloud system. In particular, data access over wireless networks from the media cloud has recently found increased popularity due to the fast growth of wireless multimedia applications.

However, multimedia security has become an increasingly major concern for cloud media data access control. It is important to ensure secure and reliable multimedia data transmissions between users and the media cloud.

The "Security Protection for Multi Owner Firm" is a project which focuses on the security and confidentiality of user data. It is a security system which can be used by a company having multiple owners. It gives you the security that no data can be viewed without the data of each user. It also gives the confidentiality that if any of the owner changes the data, the data can be easily judged and the security remains intact.

The algorithm used are-

a. Visual Cryptography.
b. Image Encryption (AES).
c. Water Marking Algorithm.

RELATED WORK

In recent years, media cloud applications are growing with wide use of digital communication.The key issue for realizing the media cloud application is concerns about data security and privacy. In the literature, the security issues within the cloud have been well studied and many solutions have been provided. However, there are only a few studies on the methods of securing the services between the end user and the cloud.

Multimedia has its own properties, and the standard security methods for the cloud storage and have issues such as higher computational and communication complexity. Along with this issues the researchers are needed to be aware of the copyright protection, image authentication, proof of ownership, and other legal rights of the owner.

Some image hiding techniques to increase the security of the image have also been proposed. However, the common weakness of these previous techniques is that the image data are all in a single user account. The secret data cannot be acquired completely if the user account is hacked or interrupted. On the other side, if we use many copies to overcome the weakness, the danger of security exposure will increase. Secret sharing schemes are based on the principle of sharing secret information among a group of users.

Only when a group of expected users submit their shares together can secrets be recovered. In the proposed idea, the secret image data may be revealed only if a considerable number of image shares have been submitted.

PROPOSED SYSTEM

Disadvantages of Existing Systems:

- The android apps developed before has lack of security due to open source system.
- The encryption still had a problem of a user or a shareholder changing the contents.
- The size of the application and the relative mobile hardware system becomes a constraint.
- Due to limited processing power of the portable devices the complex encryption/decryption algorithms may face problem while executing.

Proposed System Introduction:

Modules:

- **Agent module**

The agent is an admin or the sender of the confidential data (image). The admin have to select the no. of the owners which he wants to share data with.

- **Owner module**

The owner module is the module where the owner receives his share which is in encrypted format. The owner receives his share (image) with the mail from the server.

- **Server module**

The server module is the part of automated systems where the entire encryption process along with the watermarking takes place. Once the agent(admin) uploads the image the server is responsible for entire encryption process.

- **Database module**

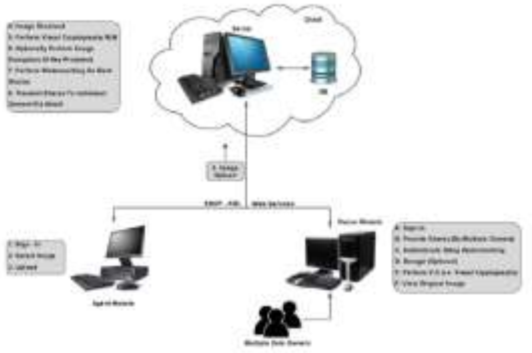
The database (cloud) is used to store the image in the shares format where no of shares is directly proportional to no. of owners.

System Architecture

Cloud is the large repository of resources. Cloud is responsible for storing all user's data and granting access to the file within a group to other group members based on publically available revocation list which is maintained by agent.

The agent uploads the image, with the no. of owners in form of shares. Once the image is uploaded on the server, the server uses visual cryptography algorithm to generate the shares. No. of shares depends on the no. of owners. The AES algorithm is applied on each share for encryption along with watermarking.

The owner will get his share on his mailing account and he has to decrypt it. If the decryption process runs successfully, the owner needs to upload it on a common window with a use of a key assigned by an agent. When all the shares are uploaded the common window de-watermarks the shares to check if each share is genuine. If the result is true the image is displayed on common window which is visible to all owners.



Algorithm

- **AES Algorithm-**

Key_Expansion -round keys are derived from the cipher key using Rijndael's key schedule. AES requires a separate 128-bit round key block for each round plus one more.

1. Initial_Round
    1. Add_Round_Key—each byte of the state is combined with a block of the round key using bitwise xor.
2. Rounds
    1. Sub_Bytes-a non-linear substitution step where each byte is replaced

with another according to a lookup table.

2. Shift_Rows—a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.
3. Mix_Columns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.
4. Add_Round_Key

3. Final Round (no Mix_Columns)

1. Sub_Bytes
2. Shift_Rows
3. Add_Round_Key.

- **Watermarking Algorithm-**

Step1: The watermarked image W values of two treatments, then the image was B Arnold

Transform scrambling; the watermarked image is obtained after pretreatment with

W', then zigzag Scan on the W', one dimensional watermark information sequence of W (1, K);

Step2: Two Dimensional DWT transform of the carrier image two levels, two level approximation sub image LL1;

Step3: Two level approximation sub image LL1 into K disjoint 8*8 block X;

Step4: Discrete cosine transform for each sub block X, the DCT coefficient matrix Y, zigzag

Scans were performed on Y, DCT coefficient sequence F

Step 5: Select the appropriate high frequency DCT coefficients of F (k, high), according to the formula of each DCT coefficient sequence in F (k, high) average of 6 adjacent coefficients of ave (k), and according to the formula F (k, high) and ave (k) absolute difference between A(K);

$$ave(k) = \frac{1}{6}(\sum_{i-3}^{-1} F(k, mid + i) + \sum_{j-1}^{3} F(k, mid + j))$$

$$\Delta(k) = |F(k, high) - ave(k)|$$

Step 6: watermark information sequence W (1, K) according to the following rule order approximation image sub block is embedded in high frequency DCT coefficients where c is the volume control.

Feasibility study:

P type problem -

If the running time is some polynomial function of the size of the input, for instance if the algorithm runs in the linear time or cubic time, then we say the algorithm runs in polynomial time and the problem it solves is in class P[3] The P(polynomial time) class problems can be solved using inputs that are traceable and are easy to solve.

NP-complete-

An NP problem X for which it is possible to reduce any other NP problem Y to X in polynomial time. Intuitively this means that we can solve Y quickly if we know how to solve X quickly. Precisely, Y is reducible to X if there is a polynomial time algorithm f to transform instances y of Y to instances x = f(y) of X in polynomial time with the property that the answer to y is yes if and only if the answer to f(y) is yes.

NP-Hard Problem-

An NP problem X for which it is possible to reduce any other NP problem Y to X in polynomial time. Intuitively this means that we can solve Y quickly if we know how to solve X quickly. Precisely, Y is reducible to X if there is a polynomial time algorithm f to transform instances y of Y to instances x = f(y) of X in polynomial time with the property that the answer to y is yes if and only if the answer to f(y) is yes.

Taking into consideration the above mentioned points and after analysis of our project algorithm it can be inferred that the problem is a NP-Complete type problem.

Mathematical Model:

1. Let 'S' be the set of element

$S= \{S, O, A, Db, K, U, P\}$

Where S be the,

S<= Set of Server.

$S= \{S_1\};$

//Finite set of element.

O<= Set of Owner.

$O= \{O_1, O_2, O_3 \ldots O_n\};$

//Infinite set of elements.

A<=Set of Agents.

$A= \{A_1\};$

//Finite set of element.

Db <= Set of Database.

$Db= \{Db_1\};$

//Finite set of element.

K <= Set of Keys.

$K= \{K_1, K_2, K_3 \ldots Kn\};$

//Infinite set of elements.

U <= Set of Users.

$U = \{U_1, U_2, U_3 \ldots\ U_n\}:$

//Infinite set of elements.

P <= Set of Passwords.

$P = \{P_1, P_2, P_3 \ldots P_n\};$

//Infinite set of elements

E <= Set of Emails.

$E = \{E_1, E_2, E_3 \ldots E_n\};$

//Infinite set of elements

2. Morphism:

- Owner's App

  Reg_With_Keys(user, key, email, password);

  returns Boolean.

  Login(user, password);

  returns Boolean.

  Dec_for_AES(key);

  returns Boolean.

  DeWatermarking(share);

  returns Boolean.

  Img_Retrival();

  returns Image.

  Logout();

  returns Boolean.

- Agents App.

  Authentication(username, password);

  returns Boolean.

  Upload_Image(key, email, image);

  returns Boolean.

  Wait_Status();

  returns Status.

- Server App.

  App_vc_Algo(Image);

  returns Shares.

  Img_Enc_AES(shares);

  returns Encrypted_Shares.

  Watermarking(Encrypted_Shares);

  returns Boolean.

  Send_email(username);

  returns Boolean.

Advantages of the proposed System:

- Security- Provides security as data is encrypted
- Integrity- It takes care that data is not lost during the process of communication.

- User Friendly- It provides attractive and easy-handling UI which makes it easy to use.
- Cost-effective- Cheap cost once the system is installed. Providing security in very low cost.

FEATURES

- Secured sharing of the confidential data (image). It also takes care that no data is lost during the entire communication process.
- Multiple users (owners) can access data at single time and removes the chances of doubt of data being manipulated.
- Easy to transfer the data as agent (admin) can send data to multiple owners at single time.
- The visual cryptography is used to divide the image in shares which makes it makes intruders life more difficult.
- The encryption enhances the security by making image unreadable.
- Watermarking assures the owners that no data is manipulated.

CONCLUSION

Taking the current world in to considerations, sending the data over the network is quite risky and may lead to leak of confidential data. This might lead to the heavy loss to the firm/organization. To provide a tension free and secured transfer of data (images), the proposed system is quite helpful for sending the privileged data. Moreover this system is helpful for sending the data over WAN (Wide Area Network).

4. Future Scope:

This project can be used for the transfer of secured images of military welfares. This is a secured way where the agent can send the data to multiple owners and no single owner can retrieve it without the access of others. Either one will get access or no one can.

The company or firm where multiple owners exist can also use this to increase the security and overcome the trust issues.

With growing size and hardware configuration of portable devices, the system can be developed for smartphones and tablets which give major advantage of location transparency.

REFERENCES

[1] Security Protection between Users and the Mobile Media Cloud
Honggang Wang, University of Massachusetts Shaoen Wu, Ball State University Min Chen, Huazhong University of Science and Technology Wei Wang, South Dakota State University

[2] S. Dey, “Cloud Mobile Media: Opportunities, Challenges and Directions,” Proc. Int’l. Conf. Computing, Networking and Commun., 2012, pp. 929–33.

[3] F. Sardis *et al.*, “On the Investigation of Cloud-Based Mobile Media Environments with Service-Populating and QoS-Aware Mechanisms,” *IEEE Trans. Multimedia*, vol. 15, no. 4, June 2013, pp. 769–77.

[4] Y. Xu and S. Mao, “A Survey of Mobile Cloud Computing for Rich Media Applications,” *IEEE Wireless Commun.*, vol. 20, no. 3, June 2013.

[5] S. Wang and S. Dey, “Adaptive Mobile Cloud Computing to Enable Rich Mobile Multimedia Applications,” *IEEE Trans. Multimedia*, vol. 15, no. 4, June 2013, pp. 870–83.

[6] R. G. van Schyndel, A. Z. Tirkel, and C. F. Osborne, “A Digital Watermark,” *Proc. IEEE Int’l. Conf. Image Processing*, vol. 2, 1994, pp. 86–90.

[7] Feasibility Study - P type problems: https://www.quora.com/What-are-P-NP-NP-complete-and-NP-hard

[8] Feasibility Study - NP type problems: http://mathworld.wolfram.com/NP-Problem.html

[9] Huang and C. Yang, “Image Digital Watermarking Algorithm Using Multi-Resolution Wavelet Ttansform,” *Proc. IEEE Int’l. Conf. Systems, Man and Cybernetics*,2004, pp. 2977–82.

AUTHOR BIBLIOGRAPHY

	Chandrashekhar Pardeshi is currently pursuing the degree of B.E in Computer Engineering from the RMD Sinhgad School of Engineering which is affiliated to the Savitribai Phule Pune University (formerly The University of Pune)
	Chinmay Niphadkar is currently pursuing the degree of B.E in Computer Engineering from the RMD Sinhgad School of Engineering which is affiliated to the Savitribai Phule Pune University (formerly The University of Pune)
	Indrajit Dhalpe is currently pursuing the degree of B.E in Computer Engineering from the RMD Sinhgad School of Engineering which is affiliated to the Savitribai Phule Pune University (formerly The University of Pune)
	Saurabh Barge is currently pursuing the degree of B.E in Computer Engineering from the RMD Sinhgad School of Engineering which is affiliated to the Savitribai Phule Pune University (formerly The University of Pune)
	Shripad S. Biradar received the B.E. and M.Tech. Degree in Computer engineering. He is now is working with RMDSSOE, Warje, Pune as Asst. Professor. He has experiences of 3 years and his Area of specialization – Computer Networks.