ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 6, June 2018

A Survey on Visual Threshold Cryptography for Data Security in Cloud Computing

Madhuri Kashte[1]

P.G. Student, Department of Computer Engineering, PICT College, Pune, India[1]

ABSTRACT:Cloud computing is most dominating and emerging technology in IT organizations and institutions. It provides computing resources to user at any time, from anywhere as they want, with very low cost. Computing resource like hardware, software, storage etc. Cloud computing is an effective solution for the easily storing of the data and fastest retrieve. However, confidentiality, integrity and access control are the main challenges in the cloud computing. Many more approaches are there to assure these security challenges but they are deficient in some ways such as violation of data confidentiality due to collusion attack and heavy computation (due to large no keys). To address these issues, we propose a scheme that uses visual threshold cryptography in which data owner divides users in groups and gives single key to each group for decryption of data and, each user in the group shares parts of the key and each part of key is hide in the image. When threshold number of images get collected then only user will get complete key. We are going to use capability list to control the access. This scheme not only provides the strong data confidentiality but also reduces the number of keys.

KEYWORDS:Access Control, Capability list, Malicious outsiders, Threshold Cryptography, Visual Cryptography.

I. INTRODUCTION

Now-a-days people are having tremendous data. Cloud is one the best third-party storage. It provides storage as well as computing services to the user. It provides services according to three fundamental service models infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS). As cloud provides lots of the services and the benefits still there are some challenges regarding to the data security. People are still fearing to store their data on the cloud. They fill that cloud is not safe place to store data, they believe that they lose their control on the data after placing it on cloud. So, integrity, access of data and confidentialitybecome more vulnerable. Cloud is third party storage, we are going to store the data on external server and operated by the external service providers so we can't fully trust them. Data owner cant trust on service provider since he is going to load data CSP can stole data or can change the data. Data which is store on cloud, number of people are going to use it there may be possibility of malicious user, he can steal or destroy the data. Data confidentiality may violet through collusion attack of malicious user and service provider. There are many more challenges for the data security, confidentiality and for access control.

II. REVIEW OF LITERATURE

The scheme proposed in [1] is the group key, in this scheme there is single key for each group. here no of keys are reduced but there is lots of chances of key may leak. If there is any one user malicious he can leak the whole data, so here is problem of collusion attack.

The scheme proposed in [2] symmetric key is used, which is known to only DO and respected user. DO encrypt data using symmetric key and store it on cloud. So CSP cant see the original data. When user request to CSP, session key is shared between user and CSP by modified diffie-hellman protocol which will protect outsider attack on data. This scheme definitely provides complete data security but still each user has its separate key, which increase number of keys. This is good for some applications where the no of user are less. But not good for the application where we have large number of user.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 6, June 2018

The scheme proposed in [3] uses the concept of threshold cryptography and symmetric key. There is a single key corresponding to each group of users for decryption process. But the key is distributed in all user in such a way that when minimum user come together i.e. threshold value, then only the key is decrypted. For sure this scheme is very secure. Since no anyone user know the full key. The scheme used in [3] is somewhat same with proposed scheme, but the proposed scheme is more secure since the number of keys are reduced and very useful for the people work as team or group.

III. SYSTEM ARCHITECTURE / SYSTEM OVERVIEW

Data confidentiality between DO and CSP:

To understand proposed scheme better we take an example of real life scenario, DO may be a software industry who stores its data on to the CSP and the users may be its employees who view their data from the CSP.

- DO first collect user with the same need in to one group, so first groups are made. And encrypt the data of the respected group using one single symmetric key.
- DO computes digest of data by using 128-bit MD5 hash algorithm and then encapsulates the digest and data using the symmetric key.
- And the some part of symmetric key is distributed in all user of the group in the form of image.
- Since we have calculated digest which provide integrity, symmetric key encryption provides data confidentiality.
- DO then fills the capability list, which contain details of the user like UserID, FileID, and Access Rights. Now the encapsulated thing and capability list is encrypted by the private key of the DO after that public key of the CSP and, now it sends to the CSP.
- After CSP get the message, CSP decrypts message first by using its own private key and then by using the public key of the DO. And store the capability list and the encrypted data in the storage.
- Since, data are encrypted using symmetric key which is known only to DO and respected user group, CSP cant see data even though users credential comes through it.

Secure data exchange between CSP and USER:

- To exchange the data between user and CSP, we are going to use modified Diffie-Hellman algorithm. Session key is shared between User and CSP.
- When user will request to CSP for any file, then the digest and the encrypted file is again, encrypted by session key and it to the user
- This over encryption ensures the confidentiality of the message between cloud service provider and the user.
- user then decrypts the message (according to visual Threshold Cryptography) and calculates the digest of File and then matches it with stored digest. If digest matches, File is original otherwise File is modified by outsiders and user then sends an error notification message to DO.

Visual Threshold Cryptography concept:

- After getting encrypted message, users main concern how to decrypt it because he alone cant decrypt.
- Since we are going to distribute the key by hiding it in the images, when threshold number of images comes together then and then only the whole key is visible to user.
- So, the first initiative user share his image and ask for the other user of the group to share their image.
- Whenthresholdusersharestheirimageinitiativeuser get the whole key.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

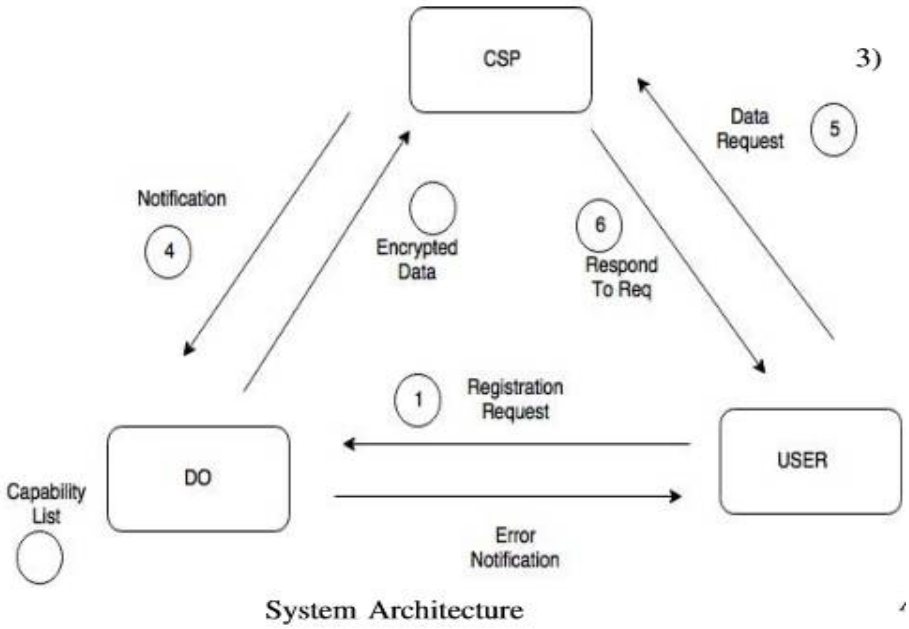
(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 6, June 2018

- Initiator user then decrypts the message and gets it/Most modern programming languages provides MD5 algorithm as built-in functions

IV. SYSTEM ARCHITECTURE



System Architecture

V. ALGORITHM

- **AES Algorithm For Encryption:**

AES(advanced encryption standard). It is symmetric algorithm. It is used to convert plain text into cipher text. The need for coming with this algorithm is weakness in DES. The 56 bit key of DES is no longer safe against attacks based on exhaustive key searches and 64-bit block also consider as weak. AES is to be used 128-bit block with128-bit keys.

Input: 128 bit /192 bit/256 bit input(0,1)
secret key:(128 bit)+plain text(128 bit)
Process: 10/12/14-rounds for-128 bit /192 bit/256 bit input Xor state block (i/p)
Final round:10,12,14
Each round consists: sub byte, shift byte, mix columns, add round key

Output: cipher text(128 bit)

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 6, June 2018

- **MD5 Message-Digest Algorithm:**

It is a widely used cryptographic hash function producing a 128-bit (16-byte) hash value, typicallyexpressed in text format as a 32 digit hexadecimal number. MD5 has been utilized in a wide variety of cryptographic applications, and is also commonly used to verify data integrity.

After getting encrypted message, users main concern how to decrypt it because he alone cant decrypt.

Since we are going to distribute the key by hiding it in the images, when threshold number of images comes together then and then only the whole key is visible to user.

• So, the first initiative user share his image and ask for the other user of the group to share their image.
• Whenthresholdusersharetheirimageinitiativeuser get the whole key.
• Initiator user then decrypts the message and gets it/Most modern programming languages provides MD5 algorithm as built-in functions

- **SHAMIR Algorithm:**

Key Share :
Input:
1.Encrypted Key(K)
2.Image(I)
3.User Group(G)
Step:
Step 1: Take Encrypted Key K Genarated By MD5. Take a Simple Image which chulk to be share into group.
Step 2: Divide Image Into n parts I=i1,i2,i3.in, Divide Key Into Chunks as per group K=k1,k2,k3kn; Image divide into range of User Group G=g1,g2,g3,,,,gn
Step 3: Now Add Key Chunk into image parts..every image part contain part of key New Image is i1k1,i2k2,i3k3,..user Group Limit
Step 4: Add Stamping to chunk of image ..add cover to image to improve security to avoid send original img.
Step 5: Share chunks of part to user with add threshold to decrypt data.

Key Combine :
Input:
1.Stamped Image
2.User Group
Step:
Step 1: Start
Step 2: if user request file to admin.
Step 3: Admin send and divide key into user(key share)
Step 4: user share the part of chunk of image to decrypt file Img=imgPart1,imgPart2; by GroupMem=m1,m2,m3.
Step 5: If img match threshold count Remove stamp from all chunk of image Else Msgreq more permission to decrypt file
Step 6: If img=valid Get key block of image K Else Invalid data share msg print
Step 7: If K=valid key Decrypt file user view file Else Invalid key share msg
Step 8: End.

VI. MATHEMATICAL MODEL

Set Theory:S={s, e, X, Y, W }
Where, s = Start of the program.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 6, June 2018

1. Log in with webpage.
2. Load Files on cloud.

e = End of the program. Retrieve the file from cloud storage system.

X = Input of the program. Input should be File

Y = Output of the program. File will be first encrypted then it is again encrypted using static key and stored on cloud. when user request it will get encrypted file, then visual threshold cryptography is applied and finally user will get the file.

$X, Y \in U$

LetUbetheSetofSystem. U = {Client,E,T,K,D}

Where, Client,E,S,T,K,Daretheelementsoftheset.

Client = DataOwner,CSP,User

E = Encryption

S = Setofencryptedfile

T = SetofThreshold

k = SetofKeys

D = Decryption

W = FailuresandSuccessconditions

VII. CONCLUSION

Since we are going to encrypt data between CSP and DO, and key is known to only DO and user group so here we ensured data confidentiality. we are going to use capability list to get secure and fine grained access control. The use of key cryptography and MD5 gives the entity authentication and data integrity respectively. Outsider attacks are secured by using Public key cryptography and D-H exchange. Since we are using visual cryptography number of keys are also reduced, there is single key corresponding to each group.

REFERENCES

[1] H. Zhong, and H. Zhen, An Efficient Authenticated Group Key Agreement Protocol," Security Technology, 2007 41st Annual IEEE International Carnahan Conference on, vol., no., pp.250-254, 8-11 Oct. 2007.

[2] S. Sanka, C. Hota, and M. Rajarajan, Secure data access in cloud computing," Internet Multimedia Services Architecture and application (IMSAA), 2010 IEEE 4th International Conference on, vol., no., pp.1-6, 15-17 Dec. 2010.

[3] Sushil Kr Saroj, A. Hassanien, "Threshold Cryptography Based Data Security in Cloud Computing", Springer-Verlag Berlin Heidelberg, 2016, pp. 219-229.

[4] Naveed Islam, William Puech, Khizar Hayat, Robert Brouzet, Application of homomorphism to secure image sharing, 2011, Optics Communication, June 2011, PP 4412-4429.

[5] R. S. Fabry, Capability-Based Addressing," in Communications of the ACM, 17(7), July 1974, pp. 403-412.

[6] A. Shamir, How to share a secret," Communications of the ACM, v.22 n.11, p.612-613, Nov. 1979. [Online]. Available: http://portal.acm.org/citation.cfm?id=359168.359176.

[7] M. Chase, Multi-Authority Attribute Based Encryption, Proc. Fourth Conf. Theory of Cryptography (TCC), pp. 515534, 2007

[8] Yu S, Wang C, Ren K, Lou W. Achieving secure, scalable, and finegrained data access control in cloud computing. In: 2010 Proceedings IEEE INFOCOM. IEEE; 2010. pp. 1e9. http:// dx.doi.org/10.1109/INFCOM.2010.5462174.

[9] Yu S, Wang C, Ren K, Lou W. Achieving secure, scalable, and finegrained data access control in cloud computing. In: 2010 Proceedings IEEE INFOCOM. IEEE; 2010. pp. 1e9. http:// dx.doi.org/10.1109/INFCOM.2010.5462174.

[10] H. Zhong, and H. Zhen, An Efficient Authenticated Group Key Agreement Protocol," Security Technology, 2007 41st Annual IEEE International Carnahan Conference on, vol., no., pp.250-254, 8-11 Oct. 2007.