Scientific Journal of Impact Factor(SJIF): 4.14

e-ISSN(O): 2348-4470
p-ISSN(P): 2348-6406

International Journal of Advance Engineering and Research Development

Special Issue for ICPCDECT 2016,Volume 3 Issue 1

Secure Data Sharing Using Cryptography And Watermarking In Cloud Computing.

Secure Data Sharing On Cloud

*Neha Bonde[1], Diti Joshi[2], Aishwarya Kale[3], Sharmishtha Bankar[4]

[1]*Computer Science, AISSM's Institute of Information Technology, Pune,*
[2]*Computer Science, AISSM's Institute of Information Technology, Pune,*
[3]*Computer Science, AISSM's Institute of Information Technology, Pune,*
[4]*Computer Science, AISSM's Institute of Information Technology, Pune,*

***Abstract** -In today's world cloud computing is the most popular and widely used means for storage and computation. But data security, Integrity, confidentially is a serious impediment in cloud computing. Many data security techniques commonly used have issues like collision attack of malicious user, heavily computation and generation of large keys. In the previous system text based encryption is used therefore we implement image encryption and decryption along with watermarking making image sharingover cloud more secure. The proposed system uses Virtual Cryptography (VC) to decompose secret image into shares and distributed to multi users so they can reconstruction it to the original image.VC is used in combination with Watermarking for authentication. In VC, the shares created can be misused by third party. Therefore to insure Top-notch security we use higher level of Cryptography Algorithm; AES (Advanced Encryption Standards), is a symmetric Algorithm which is used to Encrypt and Decrypt the shares created by VC. With the help of this system data accessible only to the Authenticated client and we are able to ensure secure data sharing using cloud.*

***Keywords**- Visual Cryptography, Multi-owner, Encryption, Decryption, AES, Cloud Computing.*

I. INTRODUCTION

In the previous systems only a single owner/user could get access to the data,but in the proposed system multiple owners/users can get access to the data. The size of keys was much larger occupying a lot of space, whereas in this systemthe key is much smaller in size.With increase in technology there has been a lot of development in field of Arms and ammunition the need for securing confidentiality and authenticity of weapon design images over cloud. The previously designed systems had the drawback of providing secure images on cloud to multiple owners. With the help of the proposed system we can securely share images to multiple owner's on cloud. In cloud computing there are a lot of collision attacks taking place. Heavy computations by dividing users in groups and providing single key to each user group is major issue. Applying Visual Cryptography each user in group shares a part of key so that size of keys are reduced. Any tampering done to an single share will be detected by encryption and decryption and watermarking.Organization or individuals consuming cloud services must understand the delineation of responsibilities over computing environment and implication of security and privacy. Ensuring cloud computing solution satisfies organization's security and privacy requirements. It ensures client side computing environment meets security and privacy required for cloud computing.The final outcome of the proposed system is that the image is successfully transferred to the authenticated user in real time. If there is any tamperingdone to the image then the user will not be able to access the data. The image goes through to multiple encryption and decryption with the help of which tampering or hacking of data will be difficult.

II. PROPOSED SYTEM

In the previous systems only a single owner/user could get access to the data, but in the proposed system multiple owners/users can get access to the data. The size of keys was much larger occupying a lot of space, whereas in this system the key is much smaller in size.With increase in technology there has been a lot of development in field of Arms and ammunition the need for securing confidentiality and authenticity of weapon design images over cloud. The previously designed systems had the drawback of providing secure images on cloud to multiple owners. With the help of the proposed system we can securely share images to multiple owner's on cloud. In cloud computing there are a lot of collision attacks taking place. Heavy computations by dividing users in groups and providing single key to each user group is major issue. Applying Visual Cryptography each user in group shares a part of key so that size of keys are reduced. Any tampering done to an single share will be detected by encryption and decryption and watermarking.Organization or individuals consuming cloud services must understand the delineation of responsibilities over computing environment and implication of security and privacy. Ensuring cloud computing solution satisfies organization's security and privacy requirements. It ensures client side computing environment meets security and privacy required for cloud computing.The final outcome of the proposed system is that the image is successfully transferred to the authenticated user in real time. If there is any tampering done to the image then the user will not be able to access the data. The image goes through to multiple encryption and decryption with the help of which tampering or hacking of data will be difficult.

The image is carried as a single information carrier so to overcome this wedivide a single image into number of shares and carriers. Previously the emphasize was mainly on security of data, forgetting about theperformance of system. In order to secure data, number of keys were generated, thus affecting the performance of system .So it is desirable to reduce multiple keys, with the help of AES algorithm which provides high security and performance. User revocation for agent client-server model proposed by is notadvisable, so we avoid using it in the proposed system. Earlier usage of DH algorithm introduced by for encryption ordecryption purpose, used very large computational power so it is eliminatedand rather the use of AES is introduced in the proposed system.Previously, only VC and watermarking were used, but in new proposed systemthe use of AES algorithm has been introduced for additional layer of security.

In the proposed system there are three entities the client, the server and the agent. The client first registers, using a username and password. The users username and password are stored on the database. The database used in the system is MySQL. The user then logs-in and requests the agent to view an image. The agent receives the request. On receiving the request, the agent first verifies if the user is authentic or not. Post authentication the agent uploads the image on the server. Once the image is uploaded on the server it undergoes visual cryptography where the image is divided into multiple shares. Then image encryption (AES) is performed on each share based on the key given by the user. Thirdly watermarking is performed on each share. Watermarking is used to check for and tampering done to the image. After these three levels of security is performed on the image then it is sent to the client end.

Once the image is received on the client side it undergoes decryption (AES).As soon as AES is performed authentication of the image is done using de-watermarking. Lastly visual cryptography is applied. After all this the user is able to view the image. If any tampering is done to the image in the middle it will be detected through watermarking. If any individual tries to get access to the image during the process without authentication he will not be able to access it.

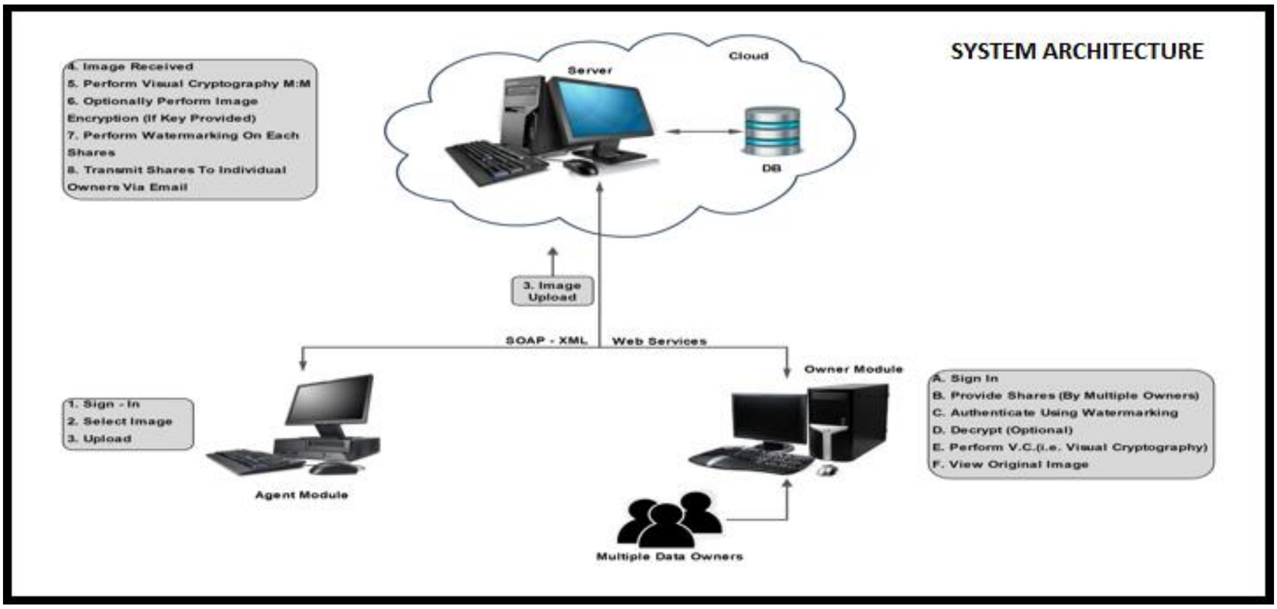
SYSTEM ARCHITECTURE
4. Image Received
5. Perform Visual Cryptography M:M
6. Optionally Perform Image Encryption (If Key Provided)
7. Perform Watermarking On Each Shares
8. Transmit Shares To Individual Owners Via Email
Server
Cloud
DB
3. Image Upload
SOAP - XML
Web Services
Owner Module
1. Sign - In
2. Select Image
3. Upload
Agent Module
A. Sign In
B. Provide Shares (By Multiple Owners)
C. Authenticate Using Watermarking
D. Decrypt (Optional)
E. Perform V.C.(i.e. Visual Cryptography)
F. View Original Image
Multiple Data Owners

Fig: System Architecture

2.1 Visual Cryptography

Visual cryptography is an algorithm used for hiding information in the form images which can be decrypted only if the correct key is used. In visual cryptography the image is divided into n number of shares. It basically divides the image into two part

a. Key – it is the transparent element.
b. Cipher-a printed page

When the shares are different then they make no sense,only on combining them can the image be visible.The image is portrayed in the form black and white pixels.

2.3 Advanced Encryption Standard (AES)

AES stands for Advanced Encryption Standard, it was originally known as Rijndal. AES supports a standard block length of 128 bits and supports 128, 192, 256 key lengths and it's sub- key lengths are of 11, 13 and 15, each of which are 128 bits. Every sub-key corresponds to a processing round in AES therefore each sub-key is also called as a round key. AES offers high security, flexibility, efficiency and performance making is much more tolerant against attacks as compared to others algorithms.

2.4 Watermarking

Digital watermarking involves digital signal processing, cryptography and image processing. It is embedded into any digital media such that it does not change the meaning or the value of the original file. The original copyright information of the owners is embedded into the media file. A watermark can be embedded into image, audio, video files or any media file. A watermark not only verify the owners information but it can also give all the relevant information about the carrier signals when needed. Watermarking consists of two phases, in the first phase the watermark is embedded and in the second phase the verification or extraction takes place.

III. SUMMARY AND CONCLUSION

The proposed system can be used by the Government for military purposes- the designs createdfor military weapons need to be shared with full security such that the designscannot be hacked by terrorists or by other countries' government**.**It can be used by Industries -To share images of products that are designedby them so that no other company can copy their products. Automobilesindustries, electrical appliances industries etc. It can also be used by artists-For sharing their work artists can make use of this system to avoid forgery of their work photographers, architects, painters andinterior designers, animators etc.

The studies shows that the proposed approach can manage the security challenges on
cloud. To realize full potential of cloud computing. This study provides three major contribution.

1) Security and privacy on cloud.
2) Authentication or copyright of image.
3) Confidentiality of multimedia data.

VC scheme is a special encryption technique to hide information in images in such a way that it can be decrypted by human vision if correct key image is used. There are two transparent images. One image contains random pixels and other image contains secret information. Watermarking is used to insert secret information into original image with different features, as a means to access the ownership of modified image. This provides solution for tampering, verification and resolution for disputes. AES is symmetric key algorithm to encrypt sensitive data.

Cloud computing is a new concept that provides user with many benefits, however it raises dreadful security problems which may downtrend its use. Understanding what vulnerabilities is in cloud, the proposed system introduces the technology to mitigate a variety of security issues like legal and contractual issues such as data loss, data breaches, service traffic hijacking.

IV. REFERENCES

[1] Honggang Wang, Shaoen Wu, Min Chen, Huazhong, Wei Wang, "*Security Protection between Users and the Mobile Media Cloud*" ,IEEE International Conference, 0163-6804/14, March 2014.

[2] Sushil Kr Saroj, Sanjeev Kr Chauhan, Aravendra Kr Sharma, Sundaram Vats, "Threshold Cryptography Based Data Security in Cloud Computing", IEEE International Conference, 12015.149.CICT/0.1109, 2015.

[3] Honggang Wang,Shaoen Wu, MinChen,Huazhong, "*Security Protection between Users & Mobile Media Cloud*" , IEEE Communications Magazine, 0163-6804/14/25.00, March 2014.

[4] Mr. Parjanya C.A Mr. Prasanna Kumar M,"*Advanced secure multi-owner data sharing for dynamic groups in cloud*", IJARCSSE, ISSN:2277 128X, 2014.

[5] Stelvio Cimato, James C.N. Yang, and Chih-Cheng Wu,"*Visual Cryptography Based Watermarking*", Springer, pp. 91–109, 2014.

[6] Ritesh Mukherjee and Nabin Ghosha, "*Steganography Based Visual Cryptography (SBVC)*", Springer, 10.1007/978-3-642-35314-7_63, 2013.

[7] S. Sridevi Sathya Priya, P. Karthigaikumar2, and N.M. SivaMangai, "*Generation of 128-Bit Blended Key for AES Algorithm*", Springer International Publishing Switzerland, 10.1007/s11277-014-1888-7, 2013.

[8] Salim MuhsinWadi , Nasharuddin Zain, "*High Definition Image Encryption Algorithm Based on AES Modification*" , Springer Science+Business Media, New York, 10.1007/s11277-014-1888-7, 2014.

[9] Guang Yu1 and Xue Jun Zhao, "*Study Based on Chaotic Encryption and Digital Watermarking Algorithm*", Springer-Verlag Berlin Heidelberg, pp. 619–625, 2012.

[10] Li-hua Wu, Wen-juan Jiang and Junkuo Cao, "*Research of Image Watermarking Algorithm and Application in Eco-Tourism Digital Museums Copyrights Protection*", Springer International Publishing Switzerland, 10.1007/978-3-319-03449-2_23, 2014.

[11] Kai-Hui Lee and Pei-Ling Chiu, "*Digital Image Sharing by Diverse Image Media*" , 2014.