Secure Data Sharing Using Visual Cryptography in for Computing

Borude Prakash B.[1] Butte Dhananjay B[2] Dumbre Sayali P.[3] Prof.Khatal S.S.[4]
[1,2,3,]BE Student [4]Guide
[1,2,3,4]Department of Computer Engineering
[1,2,3,4]Sharadchandra Pawer College of Engineering, Dumbarwadi, Khamundi, Maharashtra, India

Abstract— In todays world the latest technology of fog computing is becoming the most popular and widely used means for storage and computation. Fog computing is nothing but extend of cloud computing. The data security, integrity, congeniality are security feature in fog computing. Many security techniques have issues like collision attack of malicious user, heavily computation and generation of large keys. In The existing system text based encryption is used, to implement image encryption and decryption along with watermarking image shearing over cloud to be a more secure. The proposed system uses Visual cryptography to provide equal digital right to all the owner and Watermarking is applied on each shear to authenticate each shear with its owner. To provide more security during transmission of the shears encryption can be applied on each shear. Visual Cryptography is used in combination with watermarking for authentication. In visual cryptography, the shears created can be misused by third party. Therefore to insure higher level of cryptography algorithm is a symmetric algorithm which is used to encrypt and decrypt the shears created by Visual cryptography. With the help of this system data accessible only to the authenticated client and we are able to ensure secure data shearing using fog computing.

Keywords: Visual Cryptography, Multi-owner, Watermarking AES, cloud server

I. INTRODUCTION

Data Security is a process of protecting files, databases, and accounts on a network by adopting a set of controls, applications, and techniques that identify the relative importance of different datasets, their sensitivity, regulatory compliance requirements and then applying appropriate protections to secure those resources.

Similar to other approaches like perimeter security, file security or user behavioral security, data security is not the be all, end all for a security practice. It's one method of evaluating and reducing the risk that comes with storing any kind of data.

The core elements of data security are confidentiality, integrity, and availability. Also known as the CIA triad, this is a security model and guide for organizations to keep their sensitive data protected from unauthorized access and data exfiltration.

- Confidentiality - ensures that data is accessed only by authorized individuals.
- Integrity - ensures that information is reliable as well as accurate.
- Availability - ensures that data is both available and accessible to satisfy business needs.

Cryptography includes a set of techniques for scrambling or disguising data so that it is available only to someone who can restore the data to its original form. In current computer systems, cryptography provides a strong, economical basis for keeping data secret and for verifying data integrity.

Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that the decrypted information appears as a visual image.

One of the best-known techniques has been demonstrated a visual secret sharing scheme, where an image was broken up into n shares so that only someone with all n shares could decrypt the image, while any n 1 shares revealed no information about the original image. Each share was printed on a separate transparency, and decryption was performed by overlaying the shares. When all n shares were overlaid, the original image would appear. There are several generalizations of the basic scheme including k-out-of-n visual cryptography.

Using a similar idea, transparencies can be used to implement a onetime pad encryption, where one transparency is a shared random pad, and another transparency acts as the cipher text. Normally, there is an expansion of space requirement in visual cryptography. But if one of the two shares is structured recursively, the efficiency of visual cryptography can be increased. Other antecedents are in the work on perception and secure communication.

Visual cryptography can be used to protect biometric templates in which decryption does not require any complex computations.

II. LITERATURE SURVEY

The image is carried into single information carrier so to overcome this we divide a single image into number of shares and carriers. Previously the emphasize was mainly on security of data forgetting about the performance of system.

Cryptographic confidential about security purpose of the data which is belongs from the encrypted scheme. This technique uses binary images which is consist from SH1 and SH2 encoded blocks and black white color[1].These systems is implemented by the Naor and Shamir. After that, [2] Wu and Chen experiments told to us encoded two binary images shares, suppose fiest and second. First can be revealed by stacking both shares and second share can be revealed by rotating one of them by some angle in both directions. Borchert mentioned about segment based visual cryptography used for the encryption of messages containing alphanumeric symbols [3]. Indrakanti S. P. and Avadhani P are worked on segment based visual cryptography for Key distribution [4]. S. S. Hegde, Bhaskar Rao, introduced secret sharing scheme in which secret shares are hidden in meaningful cover images[5].The expriments of Sian Jheng Lin and Wei-Ho Chung provides about a probabilistic model of visual cryptography scheme with dynamic group which means the divide the an image into n shares.[6]. We know VC scenario is the combination of watermarking and visual cryptography. Naor, M., Shamir thought that private key

cryptosystem, the phase of the encoded are first share the cipher test and another is role of secret key [7].

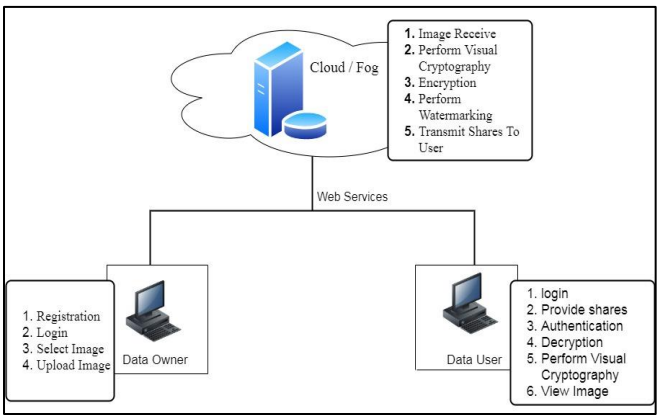
In order to secure data, number of keys were generated, thus affecting the performance of system .So it is desirable to reduce many key with the help of AES algorithm which provide high security and performance. User revocation for agent client-server model is not advisable, so we avoid usage of it in proposed system.

Earlier usage of DH algorithm introduced by Sushil Kr Saroj for encryption or decryption propose, used very large computational power. So it is eliminated and rather the use of AES is introduced in the proposed system. Previously, only VC and watermarking were used, but in new proposed system the use of AES algorithm has been introduced for additional layer of security.

III. PROPOSED APPROACH

Protecting the multimedia data has become a challenging issue in digital world. Where digital data such as image, video is rapidly generating by the digital user and transmit over the cloud media. So providing security for cloud media we are using fog computing which is extended version of cloud computing .It is introduced in Nov 2015 by CISCO. In a fog environment, the processing takes place in a data hub on a smart device, or in a smart router or gateway, thus reducing the amount of data sent to the cloud. More securely transmitting we are using visual Cryptography and watermarking techniques. Digital watermarking used for copy right protection and also for verification purpose. The visual cryptography divide image into n shares part of the image and shear to users. In this propose system we are creating multiple users for data shearing. The benefits of two technique is increasing the data integrity, availability and confidentially.

Fog computing is quite similar to cloud and just like cloud computing it also provides its users with data, storage, compute and application services. The thing that distinguishes fog from cloud is its support for mobility, its proximity to its end-users and its dense geographical distribution. Fog computing helps in reducing service latency and even improves QoS, which further result in a superior user experience. Data owners cannot trust the users external servers are operated by commercial service providers. To address the issues of collusion attack of malicious users and cloud service provider and heavy Computation we propose a scheme.



Here we are using Visual cryptography and digital watermarking, the benefits of two technique is increase the data integrity, availability and confidentially. Data transmission over the internet done securely. Propose system architecture consist three phases Registration Phase, Processing Phase, Reverse Processing Phase. In registration phase, provides the information of a person details, id, password, must be provided by User. All the information is stored in particular database. Data Owner and data users must register through the sever. In processing phase, Data Owner upload image in system. Watermarking apply to the image and watermark image give input to visual cryptography and visual cryptography splits the received Image into N number of shares and send to the trusted user. In reverse processing retrieve the original image so that. Indeed, only trusted users reconstruct the original image by simply stacking together the shares. And watermarking technique is apply to decode the generated image and generate the original image.

IV. CONCLUSION

In this paper, we proposed security for the particular image whoever having multiple users. The main objective is to provide equal digital rights to the users of the image. Visual cryptography technique refers for which generates N shares according to the number of users and the watermarking gives to authenticate each share with its user. The security of data is maintained using both visual cryptography and watermarking. Thus the proposed systems is the requirement of security and digital rights management by using the fog computing.

REFERENCES

[1] M. Naor and A. Shamir, "Visual cryptography," in Proc. Workshop Theory Appl. Cryptograph. Techno. (EUROCRYPT), Perugia, Italy, May 1994, pp. 1–12.
[2] E. Myodo, K. Takagi, S. Miyaji, and Y. Takishima, "Halftone visual cryptography embedding a natural grayscale image based on error diffusion technique," in Proc. IEEE Int. Conf. Multimedia Expo, Beijing, China, Jul. 2007, pp. 2114–2117.
[3] O. Kafri and E. Keren, "Encryption of pictures and shapes by random grids," Opt. Lett., vol. 12, no. 6, pp. 377–379, Jun. 1987.
[4] S. J. Shyu, "Image encryption by random grids," Pattern Recognit., vol. 40, no. 3, pp. 1014–1031, Mar. 2007.
[5] R. De Prisco and A. De Santis, "On the relation of random grid and deterministic visual cryptography," IEEE Trans. Inf. Forensics Security, vol. 9, no. 4, pp. 653–665, Apr. 2014.
[6] R. Ito, H. Kuwakado, and H. Tanaka, "Image size invariant visual cryptography," IEICE Trans. Fundam., vol. E82-A, no. 10, pp. 2172–2177, Oct. 1999.
[7] C.-N. Yang, "New visual secret sharing schemes using probabilistic method," Pattern Recognit. Lett, vol. 25, no. 4, pp. 481–494, 2004.
[8] F. Liu, T. Guo, C. Wu, and L. Qian, "Improving the visual quality of size invariant visual cryptography scheme," J. Vis. Commun. Image Represent. vol. 23, no. 2, pp. 331–342, Feb. 2012.

[9] Y.-F. Chen, Y.-K. Chan, C.-C. Huang, M.-H. Tsai, and Y.-P. Chu, "A multiple-level visual secret-sharing scheme without image size expansion," Inf. Sci., vol. 177, no. 21, pp. 4696–4710, Nov. 2007.
[10] Z. Wang, G. R. Arce, and G. D. Crescenzo, "Halftone visual cryptography via error diffusion," IEEE Trans. Inf. Forensics Security, vol. 4, no. 3, pp. 383–396, Sep. 2009.
[11] F. Liu and C. Wu, "Embedded extended visual cryptography schemes," IEEE Trans. Inf. Forensics Security, vol. 6, no. 2, pp. 307–322, Jun. 2011.
[12] X. Wu and W. Sun, "Generalized random grid and its applications in visual cryptography," IEEE Trans. Inf. Forensics Security, vol. 8, no. 9, pp. 1541–1553, Sep. 2013.
[13] X. Wu and W. Sun, "Extended capabilities for XOR-based visual cryptography," IEEE Trans. Inf. Forensics Security, vol. 9, no. 10, pp. 1592–1605, Oct. 2014.
[14] Y.-C. Hou and S.-F. Tu, "A visual cryptographic technique for chromatic images using multi-pixel encoding method," J. Res. Pract. Inf. Technol., vol. 37, no. 2, pp. 179–191, May 2005.
[15] S. F. Tu and Y. C. Hou, "Design of visual cryptographic methods with smoothlooking decoded images of invariant size for grey-level images," Imag. Sci. J., vol. 55, no. 2, pp. 90–101, Jun. 2007.
[16] Y.-W. Chow, W. Susilo, and D. S. Wong, "Enhancing the perceived visual quality of a size invariant visual cryptography scheme," in Proc. 14th Int. Conf. Inf. Common. Secur. (ICICS), Hong Kong, Oct. 2012, pp. 10–21

