Secure Image Sharing Using Visual Cryptography, Watermarking Technique and AES Algorithm

Miss. Dumbre Sayali P.[1] Mr. Butte Dhananjay B.[2] Mr. Borude Prakash B. Prof. Khatal Sunil S.[4]
[1,2,3]BE Student [4]HOD
[1,2,3,4]Department of Computer Engineering
[1,2,3,4]Sharadchandra Pawar College of Engineering, Otur, Pune, India

Abstract— Secure communication is important in current world ,when we communicate and sharing information between two or more users then secure the communication is main challenge. Currently data security is very important over the network as well as electronic devices . currently we using many algorithms and cyber security techniques to improve the cyber and network security to protect high confidential information and data .In this paper mainly focusing on the image security over the network using visual cryptography and digital watermarking techniques. In this paper we selecting one image and apply encryption followed by digital watermarking. Here we first select highly confidential images like architectures , blueprint , design etc. ,after that we storing it on to cloud . after uploading of image is done on to cloud then we apply visual cryptography techniques for divide the images into multiple part known as shares. After that we encrypting each share individually using advanced encryption standard algorithm. When its done then apply digital watermarking for hiding the images using another image to each shares ,then the images are send to the second user . when encrypted image are send to second user at that time first check the user are right or wrong using watermarking technique and cryptography techniques ,if user are right user then first remove the watermarking ,then decrypting the each share and then original images are seen to the second user . If the user are not right person then the encrypted image are seen to that person.

Keywords: Visual Cryptography, AES Algorithm, Digital Watermarking, Data Security

I. Introduction

Data security is the process of protecting the data and accounts of a network by adopting a set of application controls and techniques that demonstrate the importance of a separate data standard for its legal compliance requirements and then uses the appropriate protection to protect those resources. similar to other methods such as security file security or user performance data protection is not all that eliminates everything about security security. it is one way to assess and reduce the risk that comes with storing any kind of data. the key elements of data security are privacy and accessibility. also known as the cia triad is a security model with guides for organizations to keep their sensitive information protected from unauthorized access to data. privacy ensures that data is only accessible by authorized people. integrity ensures that the information is reliable and accurate. availability ensures that data is available and available to satisfy business needs. cryptography includes a set of methods of encrypting or encrypting data so that it is available only to the person who can restore the data in its original form. in modern computer systems cryptography provides the economic basis for maintaining the confidentiality of data and ensuring the authenticity of data. visual imagery is a cryptographic technique that allows visual text input etc. it is written in such a way that the summarized information appears as a visual image. one of the best-known techniques shown is a very transparent consultation system where the image is divided into n shares so that only the person with all the shares can present the image while the other n-shares do the details with the original pictures. each assignment was printed on a different opening and the translation was done on top of the assignment. once all allocations are covered the first picture will appear. there are several duplicates of the basic program including the k-out-of-n-cryptography visualization. it is used to view the same transparent objects to be used to perform encrypted encryption where the obvious exception is an innocently shared clip and other obvious actions such as cipher text. there is usually an increase in local demand in virtual cryptography. but if one of the two stocks is restructured the efficiency of virtual cryptography may increase. some decisions are based on secure communication and communication. visual imaging can be used to protect biometric templates where translation does not require complex visualization.

II. Literature review

Cryptographic privacy regarding the security purpose of the data in the encrypted scheme. This method uses binary images created from embedded blocks of SH1 and SH2 and dark brown color [1] .These systems are used by Naor and Shamir. After that, [2] Wu and Chen checked in on us and told us that they nailed the two binary image assignments, let's say the awesome and the second. The first can be uncovered by the addition of both shares and the second share can be revealed by rotating one of them at an angle. Borchert is referred to as visual segmentation based on the part used for encrypting messages containing alphanumeric symbols [3]. Indrakanti S. P. and Avadhani P are used in the visible part of the Key Distribution cluster [4]. SS Hegde, Bhaskar Rao, introduced a secret-sharing system where shares are hidden in logical cover images [5] .The annotations of Sian Jheng Lin and Wei-Ho Chung provide a possible model for a virtual cryptography system with a power group that means split the image. be n shares. [6]. we know that vc status is a combination of watermarking and virtual cryptography. naor m. shamir envisioned a private cryptosystem a class of authors first engaged in cipher testing and then another role for a secret cipher [7]. to protect the data a number of keys were generated thus affecting the performance of the system .therefore it is desirable to lower many keys with the help of the aes algorithm that provides maximum security and performance. users deprecation of the agents client agent model is not advisable so we avoid its use in the proposed system. previous uses of the dh algorithm introduced by sushil kr saroj for encryption or print suggestion have used a great computational power. it is therefore eliminated and instead the use of aes is introduced in the proposed system. previously only vc and watermarking were used but in the proposed new system the use of the aes algorithm was introduced by an additional layer of security

III. PROPOSED SYSTEM

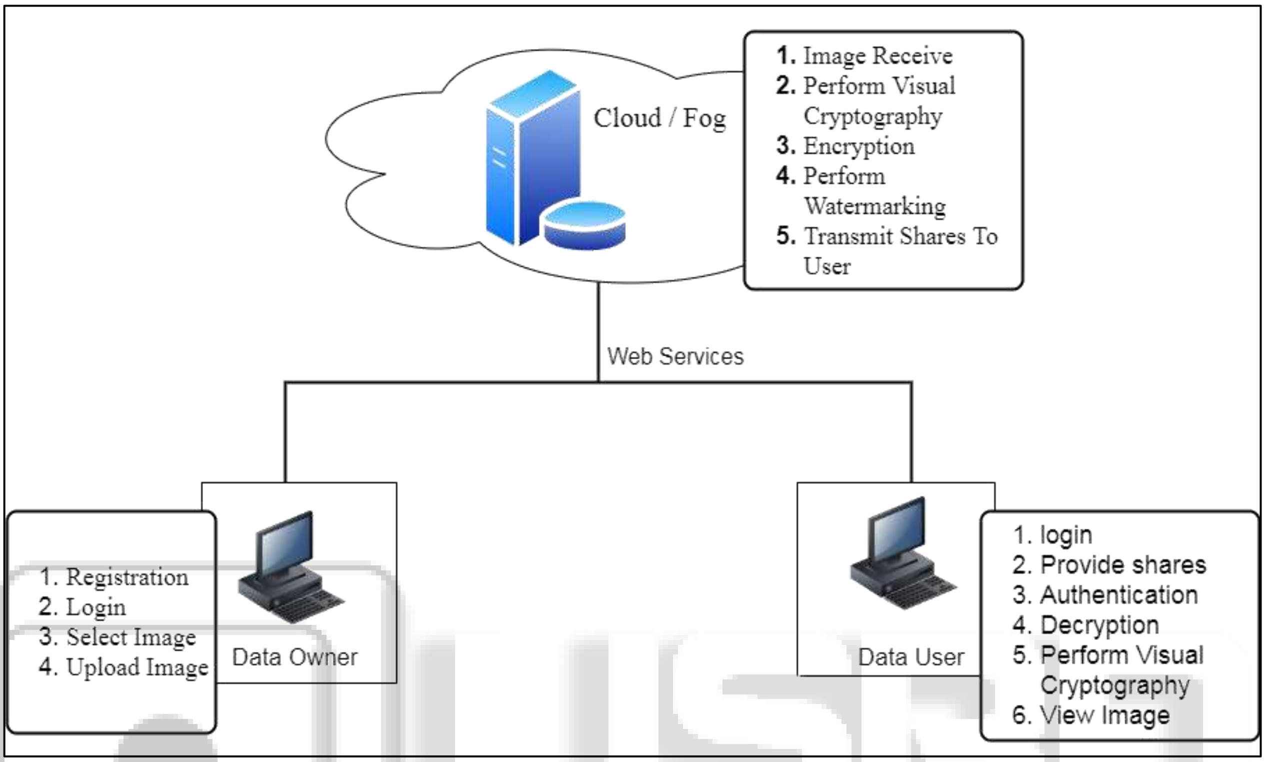

Fig. 1: Proposed System Architecture

Protecting multimedia data has become a major problem in the digital world. Where digital data such as image, video is instantly produced by the digital user and transmits over the cloud media. So to provide security for cloud media we use cloud computing cloud computing .An November 2015 by CISCO. In a cloudy environment, processing takes place in a data center on a smart device, or on a smart router or gateway, thus reducing the amount of data sent to the cloud. For safe transfer we use Cryptography visual and auditory methods. Digital watermarking used for accurate protection and authentication purposes. Virtual cryptography divides the image into parts of the image and steals users. In this uplifting system we are creating more data mining users. The benefits of the two strategies increase data integrity, availability and privacy. The cloud computing is exactly like the cloud and much like cloud computing it also provides its users with data, storage, computer resources and applications. The thing that distinguishes the fog in the cloud is its mobility support, its proximity to its end users and the distribution of its global image.

The fog computer helps to reduce app latency and improve QoS, which in turn leads to higher user experience. Data owners cannot trust external server users who are served by sales service providers. Dealing with the attacks of malicious users and cloud service providers and heavy computing is proposing a plan. Here we use Visual cryptography and digital watermarking, the two-way benefits of increasing data integrity, availability and privacy. Internet data transmission is done securely. The development of the nomination process involves three phases of phase registration, implementation phase, phase back. In the registration section, it provides personal details, id, password, should be provided by the user. All information is stored in a specific database. The data owner and data users must register on the server. In the processing phase, the image uploads the Data Owner to the system. Watermarking works on the image and the watermark image gives input to virtual cryptography and visual cryptography inserts the image received from the stock number and sends it to the loyal user. With back research it returns the original image so that. Indeed, only loyal users are rebuilding the original image by piecing together the shares. And the visualization process works to eliminate the image produced and produce the original image.

IV. CONCLUSIONS

In this paper we have suggested the security of a particular image for anyone with multiple users. the main purpose is to provide equal digital rights to image users. the transparent cryptography process is responsible for generating n shares based on the number of users and the page views confirm each users share. data protection is maintained using both visual text and visual recognition. the proposed procedures are therefore a requirement for security and digital rights management through the use of fog computing

V. FUTURE work

By using Visual cryptography and watermarking we would provide the security for the audio and video.

REFERENCES

[1] Manpreet Kaur, Sonika Jindal and Sunny Behal " A Study of Digital Image Watermarking" Volume 2, Issue 2(ISSN2249-3905) ,February 2012.

[2] Dr. Vipula Singh "Digital Watermarking: A Tutorial", (JSAT), January Edition, 2011.

[3] Darshana Mistry "Comparison of Digital Water Marking methods" (IJCSE)Vol. 02, No. 09, 2010.

[4] Saraju P. Mohanty "Digital Watermarking : A Tutorial Review" ,1999

[5] Prachi Khanzode, Siddharth Ladhake and Shreya Tank "Digital Watermarking for Protection of Intellectual Property" IJCEM, Vol. 12, April 2011.

[6] 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.

[7] A.J. Choudhury et al., "A Strong User Authentication Framework for Cloud Computing," Proc. IEEE Asia-Pacific Services Computing Conf., 2011, 12–15 Dec. 2011, pp. 110–15.

[8] B. Rong et al., "A Pyramidal Security Model for Large-Scale Group-Oriented Computing in Mobile Ad Hoc Networks: The Key Management Study," IEEE Transaction