Review on an Approach Towards sharing of Secret Digital Image in Cloud Environment by Using Meaningful Secret Sharing Technique.

Ms. Avanti M. Ganorkar[1], Prof Vijay B. Gadicha[2]
[1, 2] Department of Computer Science & Engineering
[1, 2] P. R. Pote (Patil) Welfare & Education Trust's college of Engineering & Management, Amravati

Abstract- *Cloud computing offers enormous benefits of shared resources to its users, especially for image space to store up personal digital images / photos. Existing system uses the method to secure the image by overlapping the cover images and save at the cloud, which enhance image security and privacy over cloud computing environment.*

The proposed system uses the secret sharing method for image by adding the checksum value to the encrypted image by using mobile mac address and store at the cloud as well as on image. When user want that image and try to decrypt the image, firstly user need to calculate checksum value by the same mac address if the stored checksum value and calculated checksum value is same and valid then only the secret image decrypted at the receiver side. It enables to add security parameter and only valid user can decrypt the image. It will also enable the information to check for image manipulation after the encryption.

Keywords- cloud computing, image privacy, secret sharing, visual quality.

I. INTRODUCTION

Steganography is the method of concealing a file, message, image, or video within another file, message, image, or video. The container (cover file) may be a digital image, audio file, or video file. Generally, the hidden messages appear to be (or be part of) something else: images, articles, shopping lists, or some other cover text. Whereas cryptography is the practice of protecting the contents of a message alone, steganography is concerned with concealing the fact that a secret message is being sent as well as concealing the contents of the message [1].

Cloud computing offers enormous benefits of shared resources to its users, especially for image space to store up personal digital images [2]. But, it also faces with some problems about security and privacy concerns. In order to enhance image security and privacy over cloud computing environment. For this reason, secret sharing technique is used camouflage the existence of confidential images.

II. LITERATURE SURVEY

Cloud computing is one of the popular methods for the users to host and deliver services over the Internet by dynamically providing computing resources. Cloud computing eliminates the overhead of planning ahead for acquiring different resources. The National Institute of Standards and Technology (NIST)[1] defines cloud computing as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction". The key characteristics of cloud computing are [7]:

- **On-demand self-service:** The users have access and the power to change cloud services online. User can add, delete, or change storage networks and software as needed.
- **Broad network access:** User can access cloud services using their Smartphone, tablets, laptops, or desktop computers. These devices can be used, wherever they are connected with online access point.
- **Resource pooling:** The cloud computing enables users to enter and use data within the software, hosted in the cloud at any time, and from any location.
- **Elasticity:** The cloud computing is flexible and scalable according to the user's needs. User can easily add or remove other users, resources or software features.
- **Measured service:** Cloud provider can measure storage levels, processing, the number of user accounts and the user are billed accordingly
- **Pricing:** Cloud computing cost is based on amount of resources used by the user. Cloud computing is transparent to capture for accurate billing information.
- **Quality of service:** Cloud computing guarantees, best performance, adequate resources and on round-the clock availability service for the users [11].

Steganography refers to the method of writing hidden messages in a manner that no one other person but sender and receiver would be able to securely understand and communicate the information hidden in the means of communications (e.g., images)[10]. The steganography is a channel of communication through which secret data can be transmitted in total secrecy to avoid misuse of data steganography covers secret data into some kind of medium like images, audio or video and transmits them in total secrecy from sender to receiver to avoid suspicious attacks. To provide the mean of trust management between data parties over the cloud computing environment. The two methods achieve the required goal through providing three levels of authentication, from data owner to the destinations, from the data owner to the cloud service provider and finally from the destination to data owner. For the first approach, the idea of the spatial watermarking techniques is used. While in the second approach, a hybrid model based on the idea of the spatial and the transform techniques are used [9].

F. Eljamal and N. Hikal describes the watermarking technique in 2013 to provide the mean of trust management between data parties over the cloud computing environment [1].

Saravankumar and Arun introduced ASCII-BCD based steganography technique in 2014 which provides an interoperable security services over the cloud [6].

H. Reza, and M. Sonawane describe Steganography technique in 2016 which provides an additional layer of security, namely, confidentiality of data [2].

Al-Khanjari and Alani introduced Cryptography and steganography in 2017 cryptography algorithm LEOPARD required less execution time as compared to AES algorithm [10].

III. RELATED WORK

The concept of secret sharing from cryptography and employ it to protect a secret color image. A secret RGB color image is first transformed into YCbCr color space in which chrominance components are condensed for saving storage capacity. Then, several cover images are used to create n shares. Each share carries with a portion of the secret image. During the recovery, utilizes t shares in order to reconstruct that secret image. However, it will not reveal the secret color image when holding t－ 1 or less shares. In order to transfer a color and confidential image over the cloud securely, this system proposes an image protection scheme. It consists of two main phases: share construction and secret rebuild. The share construction phase is to generate n shares using a secret image and n cover images, while the secret rebuild phase is to recover the secret image from any t of n shares. In fact, a hacker will not perceive the existence of the confidential image even though he intrudes into the clouds illicitly. For the owner, the only thing to recover that secret image is to offload any t of n shares.

IV. PROPOSED WORK

From below figure 3.1 here the process of uploading the image on cloud takes place .First the secret image is selected and a secret RGB color image is first transformed into YCbCr color space in which chrominance components are condensed for saving storage capacity. Then, several cover images are used to create n shares. Encrypted image updated by the client added checksum value before uploading to the cloud.

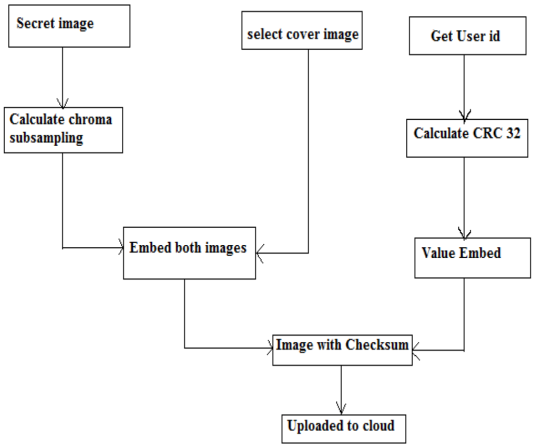

Figure 1. Process of Uploading the image on cloud.

From below figure 3.2 while accessing or fetching the image from the client side first checksum value calculated with the CRC 32. This checksum value generated by using the client user id if image modified by any other user the checksum value change and identified by the authorized user.

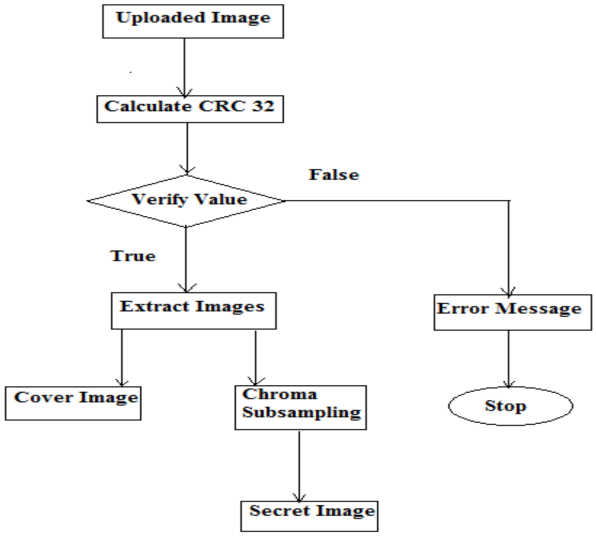

Figure 2. Process of downloading the image from the cloud.

V. CONCLUSION

This paper introduced the concept of cloud computing, challenging security issues, various existing security frameworks and finally some solutions that increase the security in the Cloud computing environment. Cloud computing is a transformative technology that can change the nature of computing so often, specifically for business purposes. It offers on-demand network access for configurable computing resources like servers, networks, storage, applications, and different cloud services that can be rapidly installed and uninstalled with minimal management effort.

VI. ACKNOWLEGEMENT

The author would especially grateful to guide Prof. Vijay B. Gadicha Head of Computer Science and Engineering Department who has provided guidance, expertise and encouragement to complete this assignment.

REFERENCES

[1] F. Elgamal, N. Hikal, and F. Abou-Chadi, “Secure medical images sharing over cloud computing environment,” International Journal of Advanced Computer Science and Applications, Vol. 4, No. 5, 2013, pp. 130-137.

[2] H. Reza, and M. Sonawane, “Enhancing mobile cloud computing security using steganography,” Journal of Information Security, Vol. 7, No. 4, 2016, pp. 245-259.

[3] Prof V. B. Gadicha “Authentication using Image Fusion & Cryptography”, International Journal of Modern Embedded Systems (IJMES), vol.02, issue 01, Feb2014, ISSN : 2320-9003.

[4] J. Stone, “Reddit Fappening ban triggers outraged response from nude photo distributor,” International Business Times, 2014.

[5] Prof V. B. Gadicha “Enhanced Authentication Scheme using Image fusion & Multishared Cryptography”, International Journal of Modern Computer Science (IJMCS), vol.02, issue 04,Aug 2014, ISSN : 2320-7868

[6] Saravankumar, C. and Arun, C. (2014) An Efficient ASCII-BCD Based Steganography for Cloud Security Using Common Development Model. Journal of Theoretical and Applied Information Technology, 65, 1992-8645.

[7] W.C. Wu, “Quantization-based image authentication scheme using QR error correction,” EURASIP Journal on Image and Video Processing, Vol. 2017, No. 1, 2017, pp. 1-12.

[8] Prof V. B. Gadicha “An Approach Towards Digital Rights management system using blind decryption algorithm”, International Journal of Advanced Research in Computer Engineering & Technology, (IJARCET), Vol.05, issue 05, May 2016 and ISSN: 2278-1323.

[9] M.G. Charate, and S.R. Bhosale, “Cloud computing security using Shamir’s secret sharing algorithm from single cloud to multi cloud,” International Journal of Advanced Technology in Engineering and Science, Vol. 3, 2015, pp. 349-357.

[10] Al-Khanjari, Z. and Alani, A. (2014) Developing Secured Interoperable Cloud Computing Services. The European Interdisciplinary Forum 2014 (EIF 2014), Vilnius, 18-19 June 2014, 341-350.

[11] A. Shamir, “How to share a secret,” Communications of the ACM, Vol. 22, No. 11, 1979, pp. 612-613.

[12] G.R. Blakley, “Safeguarding cryptographic keys,” Proc. of AFIPS National Computer Conference, Vol. 48, 1979, pp. 313-317.

[13] C.C. Chang, Y.H. Chen, and L.Y. Chuang, “Meaningful shadows for image secret sharing with steganography and authentication techniques,” Journal of Information Hiding and Multimedia Signal Processing, Vol. 5, No. 3, 2014, pp. 342-352.

[14] Prof V. B. Gadicha "A Novel Approach towards Authentication by Generating Strong Passwords", ACM Digital Library", International Conference on Information & Communication Technology for Competitive Strategies (ICTCS-2016), Udaipur, March 2016.