ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

# Hybrid Protocol Employing Steganography & Cryptography for Cloud Storage Security

**Anuradha Porwal**
PG Student, Dept. of Computer Science and Engineering, DPGITM Gurgaon, India

**Abstract**
*Cloud computing is a style of computing in which dynamically scalable and commonly virtualized resources are provided as a service over the Internet. In order for this to become reality, however, there are still some challenges to be solved. Most important among these are security and trust issues, since the user's data has to be released to the Cloud and thus leaves the protection sphere of the data owner.In this proposed system we have the process for embed the data in an cover medium and then encrypt it using Biometric Authentic key generation. This system combines the effect of these two methods to enhance the security of the data. This article presents the new techniques that provide triple level security to data by using stegnography to hide data, cryptography to encrypt data, and using biometric authentic key generation which provide security a step ahead.*

**Keywords**
*Cryptography, Stegnography, Biometric Authentic key generation*

## I. Introduction

Cloud Computing moves the application software and databases to the large data centers, where the management of the data and services may not be fully trustworthy. This unique attribute, however, poses many new security challenges. There are many benefits to using cloud storage, most notable is file accessibility. Files stored in the cloud can be accessed at any time from any place so long as you have Internet access. Another benefit is that cloud storage provides organizations with off-site (remote) backups of data which reduces costs associated with disaster recovery. . Data hiding techniques have been widely used to transmission of hiding secret message for long time.

## II. Related Work

Through the years, a large body of academic literature has been published related to the security of cloud computing. Hopes have been placed in the area of cryptography, in particular such that decryption keys with the csp is not necessary.

a. New Cryptographic Challenges in Cloud Computing Era by Aurentiu Burdusel. This article presents the new techniques that provide security to the private data, and also provide mechanisms for searching or processing encrypted data, like PE and FHE. The FHE represents a big step in modern cryptography and opens new challenges to cryptology researchers and also it helps the new IT technologies to be faster adopted

b. Data Security in Cloud Computing with Elliptic Curve Cryptography by Veerraju Gampala, Srilakshmi Inuganti, Satish Muppidi. This paper concern here data security with Elliptic curve cryptography to provide confidentiality and authentication of data between clouds.

c. Encryption Techniques for Cloud Data Confidentiality by Aized Amin Soofi1, M.Irfan Khan and Fazal-e-Amin. This paper present a review on question What encryption approaches have been used to ensure data confidentiality in cloud computing?

d. Data Security in Cloud Computing using Encryption and Steganography by Karun Handa, Uma Singh. This paper is based on the principle of securing data both during transmission and while data-at rest at servers.

e. Data Security in Cloud by Jijo.S. Nair, BholaNath Roy. This paper states using combination of Steganography and Storage System (Markov Chain Model) for security purpose.The idea of using Steganography is for the process of hiding messages inside a computerized image file so that if at all unauthorised recipient is able to get data any how then also he will not be able to access the secret data stored within the image.

## III. Proposed Work

The proposed system first perform stegnography in which secure image is hidden in cover image.. Cover image must have high resolution and secure image should have low resolution. Stegnography is performed using LSB algorithm. Then Cryptography is performed by using **variable length mix key generation algorithm** to create random key. .Minuitia is used in cryptography key generation. .Random function is used with size of image to encrypted and minuitia text file. This system improves the security of the data by embedding the data and then encrypting it.. The block diagram of the system is as shown in figures below.

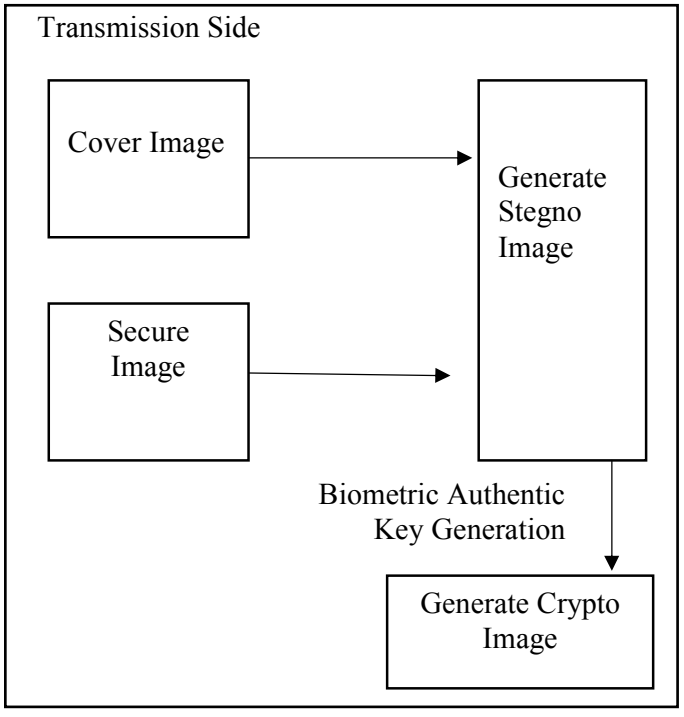


Fig.1: Transmission side of Proposed Sysyem

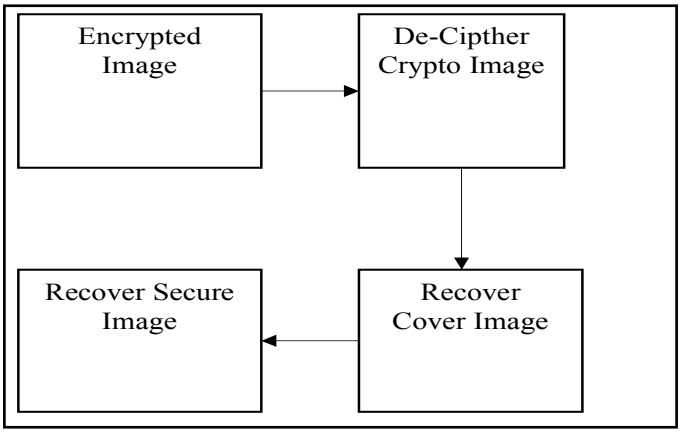


Fig. 2 : Receiving side of Proposed System

### Method Used for Stegnography

Least Significant Bit (LSB) substitution method

Least Significant Bit (LSB) substitution method is a very popular way of embedding secret messages with simplicity. The fundamental idea here is to insert the secret message in the least significant bits of the images. A basic algorithm for LSB substitution is to take the first N cover pixels where N is the total length of the secret message that is to be embedded in bits. After that every pixel's last bit will be replaced by one of the message bits.

### Minuitia Extraction

Many algorithms have been developed for minuitia extaraction based on orientation and gradients of orientation Fields of the ridges. The method used in this process is shown in Block diagram

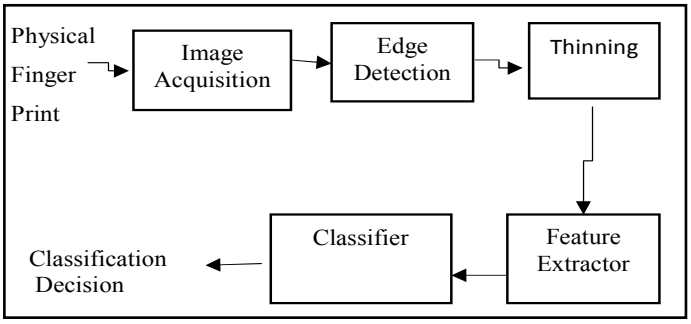


Fig. 3 : Minuitia Extraction

In a nutshell, the reason that we use this system is :
Cryptography + Steganography = Secure Steganography

- Use of cryptography with stegnography for enhanced security in cloud Computing.
- Implementation of Biometric authentic Key Generation.
- Use triple layer Security by using cryptography stegnography and minuitia used in cryptography key Generation.
- Enhance social networking by enabling selected content sharing according to user rights

### IV. Conclusion

We defined the high-level goal as enabling cloud consumers to securely deploy and run their virtual machines in the cloud, while protecting their high-value cryptographic credentials against external as well as internal attackers. With the more and more interest of the IT community in the Cloud, new security problems are found. The protection of the data stored in the Cloud face new vulnerabilities. Best solutions for remote data protection remain cryptography. This article presents the new techniques that provide triple level security to data by using stegnography to hide data, cryptography to encrypt data, and using biometric authentic key generation which provide security a step ahead.

### V. Acknowledgement

This Paper is the result of my post-graduation project at the Department of Computer Science Engineering, in College DPGITM, GURGAON. I wish to thank my supervisor Ms. Taruna, under whose supervision and guidance I was able to work on a highly interesting and intriguing topic, she always help me to understand topic in all technical aspect. Furthermore, I am deeply grateful to my Family, on whom I could always rely during my Project. It was a great pleasure for me to work with them.

### References

[1] *Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R.,Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I.,& Zaharia, M. (2010). A view of cloud computing. Communications of the ACM,53(4), 50-58.*

[2] *Veerraju Gampala, Srilakshmi Inuganti, Satish Muppidi ,2012, International Journal of Soft Computing and Engineering (IJSCE)*

[3] *Laurenţiu Burdsel,2013,Proceeding of the Romanian Academy.*

[4] *Hongwei Li1, Yuanshun Dai1, , Bo Yang, University of Electronic Science and Technology of China*

[5] *J. Abawajy,2009 "Determining Service Trustworthiness in InterCloud Computing Environments," 10th International Symposium on Pervasive Systems, Algorithms, and Networks (I-SPAN 2009*

[6] *Geethu Thomas Prem Jose V P.Afsar, Cloud computing security using encryption technique*

[7] *Seny Kamara,Kristin Lauter,Microsoft Research*

[8] *Jashanpreet Pal Kaur, Rajbhupinder Kaur,july 2014, International Journal of Advanced Research in Computer Science and Software Engineering*

[9] *William Stalling,2009, A Handbook on "Cryptography and network Security" by Pearson Education,*

[10] *K. Dubey, M. Namdev, S. Shrivastava, 2012,"Cloud-User Security Based on RSA and MD5 Algorithm for Resource Attestation and Sharing in Java Environment", IEEE sixth international conference*

[11] *Arnold et al. 2003; Johnson et al. 2001; Kahn 1996; Wayner 2002.*

[12] *American university of Beirut,EECE695C – Adaptive Filtering and Neural Networks*

### Author Profile

*Anuradha Porwal, M-Tech Computer Science Engineering, B-Tech Information Technology*