International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.194 |

|| Volume 8, Issue 4, April 2020 ||

Design and Implementation of Security of Cloud Data using Cryptography and Steganography with E-LSB Encoding Technique

Veena Mindolli[1], Revati Obi[2], Spurthi Walishetti[3], Srijana Ankalagi[4], Vandana Kundargi[5]

Assistant Professor, Department of Computer Science and Engineering, S.G.Balekundri Institute of Technology Belagavi, Karnataka, India[1]

UG Students, Department of Computer Science and Engineering, S.G.Balekundri Institute of Technology Belagavi, Karnataka, India [2,3,4,5]

ABSTRACT: Cloud storage is a service model in which data is transmitted and stored on remote storage systems, where it is maintained, managed, backed up and made available to users over a network (typically the internet). The security of cloud storage services continues to be a concern among users. Service providers have tried to allay those fears by enhancing their security capabilities by incorporating data encryption, multi factor authentication and improved physical security into their services.But emerging data security and privacy issues have become a subject of primo to the users as well as the service providers. That's why we proposed a technique for enhancing the security of cloud data using cryptography, steganography. For cryptography, we use Henon mapping algorithm and for steganography, a new efficient embedded algorithm using Embedded Least Significant Bits (E-LSB). This system is implemented using Python. We first encrypt the data and then hide it in an image to fulfill our purpose. As Henon mapping is an existing encryption algorithm which is secure enough, so, we just check out the steganography method's security. After hiding the data in a cover image, data detection and data destruction attacks are applied to evaluate the security of this steganography system. So this steganography method is quite sensitive to destruction attack but it is secure in data detection attacks, which is the main purpose of steganography.

KEYWORDS: Cloud data storage, Steganography, Henon mapping, Embedded Least Significant Bits (E-LSB).

I. INTRODUCTION

Multimedia is defined as the field that deals with different forms of information such as text, images, audio and videos in an integrated fashion. Now-a-days digital images are used frequently for communication. Any information shared over Internet needs high level of protection from intruders Cryptography is the art of protecting information by transforming readable information (plain data) into unreadable format (cipher) with the help of well-structured encryption algorithms and secret keys.Steganography is the technique of manipulating information to cipher texts and hiding their actuality and existence itself. It refers to the process of hiding the presence of the secret message. It does not keep the message secret but it provides the secrecy of the message. As everything has its pros and cons, the risk of data corruption, forging,data extraction, etc. has been a boon to the hackers. Hence to protect from the above the technology called cryptography and steganography was introduced. Cloud computing is becoming more and more popular. With the help of cloud computing, users equipped with smart terminals (e.g. smart phones) can access their data stored in cloud storages, and obtain different services anywhere and anytime.It provides security of data through encryption and has applications to manage a private cloud in case a client has sensitive information that needs maximum protection.Cloud has numerous advantages: one can access applications as utilities,over the internet.Manipulate and configure apps online at any time. No software required to access or manipulate cloud application.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.194 |

|| Volume 8, Issue 4, April 2020 ||

II.LITERATURE SURVEY

Shivani Chauhan et al [1] proposes two main techniques that are used for information security are steganography and cryptography. Cryptography is basically secret writing; on the other hand Steganography is data hiding. In this paper, a hybrid technique is introduced by combining the cryptography and Steganography properties. Also for data encryption vary the block size in place of fixed block. The proposed image steganography algorithm works on spatial domain. LSB method is used for data hiding in different ways. The aim of this work is to design an algorithm for text security as well as improve MSE and PSNR value. The data hiding capacity is also considered. The technique has been designed and simulated in MATLAB 2013a using different format images. Also Qualitative and Quantitative analysis is done and compared with the existing results.

B.Karthikeyan et al [2] proposed an innovative idea to hide a message within an image of any dimension by encrypting the message through Data Encryption Standard algorithm and concealing the message by applying LSB encoding technique in a spiral manner thus enhancing the difficulty of the decoder. The main objective is that, securing of data becomes more potent and secretive than the previous ones.

Ammad Ul Islam et al [3] . In this a novel image steganography technique based on most significant bits (MSB) of image pixels is proposed. Bit No. 5 is used to store the secret bits based on the difference of bit No. 5 and 6 of cover image. If the difference of bit No. 5 and 6 is different from secret data bit then the value of bit No. 5 is changed.The results state that the proposed technique ensures significant improvements in signal to noise ratio. Usually, the hackers focus on LSB bits for secret data extraction but the proposed technique utilizes the MSB bits that make it more secure from unauthorized access. Furthermore, the presented technique is not only secure, but computationally efficient as well.

Qiangfu Zhao et al [4] Proposed a new type of steganography, in which secret is embedded as hidden information into a virtual but natural image synthesized through image morphing. The basic idea is to make the existence and the meaning of the information unaware, and to make it extremely difficult for unauthorized persons and groups to read or even to find the information. Initial analyses show that the proposed technology is secure, and can be a very promising technique for protecting secret information in cloud computing environments.

Ciarán Bryce [5] This work presents a cloud service that automates processes that make checks for such threats, implement mitigating procedures,and generally instructs client companies on the steps to take. For instance,a process that automates these arch for leaked credentials on the Dark Web will,in the event of a leak,trigger processes that instruct the client on how to change passwords and perhaps a micro-learning process on credential management.The security governance service runs on the cloud as it needs to be managed by a security expert and because it should run on an infrastructure separated from clients.It also runs as a cloud service for economy of scale:the processes it runs can service many clients simultaneously,since many threats are common to all.They also examine how the service may be used to prove to independent auditors (e.g.,cyber-insuranceagents)that accompany is taking the necessary steps to implement its security obligations.

III. EXISTING SYSTEM

The rapid development of data communication in modern era demands secure exchange of information. Steganography is an established method for hiding data from an unauthorised access.The two main techniques that are used for information security are steganography and cryptographyCryptography is basically secret writing; on the other hand Steganography is data hiding.

Disadvantages of existing system:

- They used either cryptography or steganography by this the application will become less secure.
- There is a limitation for key length.
- Storage problem.

IV. PROPOSED METHODOLOGY AND DISCUSSION

Information security is the major concern now a day since number of internet users is increasing and secret information is getting shared every second. This has also hiked the cyber crime and threat of malicious access.Earlier they used either cryptography or steganography but here we

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.194 |

|| Volume 8, Issue 4, April 2020 ||

used both cryptography and steganography for more security, but here cryptography means converting plain text into cipher text and vice-versa; steganography means data hiding within an image; and we used cloud for double security purpose. Cloud is the on-demand availability of computer system resources, or it is storing and accessing data and programs over the internet instead of our computer's hard drive.cloud has been credited with increasing competitiveness through cost reduction, greater flexibility, elasticity and optimal resource utilization. Here are a few situations where cloud is used to enhance the ability to achieve business goals : Infrastructure as a service and platform as a service,private cloud and hybrid cloud,Test and development,File storage,Big data analysis, Disaster recovery, Backup etc.

Advantages:

- More secure.
- Backup and recovery.
- There is no limitation for key length.
- There is no storage problem.
- More flexibility.
- More reliable.
- Less cost.
- Real time application.

System flow

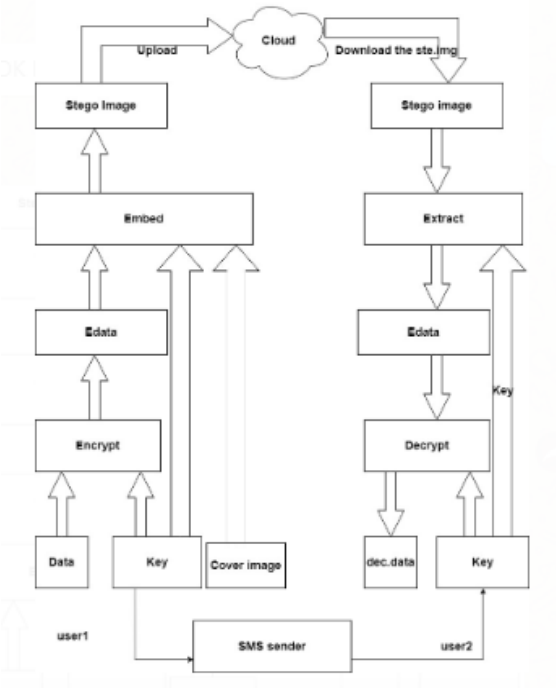

Fig 5.1: Embed and Extract process using cloud

Sender sends a secret data to the receiver with more security. The data it may be Text,Audio,Image,Video,File. Now sender will encrypt the data with help of Key, and the encrypted data is embedded into a cover image. The data is embedded in a particular image it is called as Stegoimage.

Now that image is uploaded to the cloud, the information is sent to the receiver but he needs key to extract the message from the cover image because of that sender will send a key to the receiver through mail or text.Using that key receiver will extract the data from the stegoimage, and he will decrypt it with help of key, later he will get the original data.It is Providing two dimensional security for the data. First we are encrypting the data and second part is we are uploading to the cloud with help of key. And also the data is embedded in cover image, this is also one way to provide security.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.194 |

|| Volume 8, Issue 4, April 2020 ||

ALGORITHM:
Henon Map:

- Henon map may be stated as a two-dimensional iterated discrete-time dynamical
- system with a chaotic attractor as proposed by Henon in 1976 [11]. It can be stated
- by following pair of equations
- Henon map may be stated as a two-dimensional iterated discrete-time dynamical
- system with a chaotic attractor as proposed by Henon in 1976 [11]. It can be stated
- by following pair of equations
- Henon map may be stated as a two-dimensional iterated discrete-time dynamical
- system with a chaotic attractor as proposed by Henon in 1976 [11]. It can be stated
- by following pair of equations
- Henon map may be stated as a two-dimensional iterated discrete-time dynamical
- system with a chaotic attractor as proposed by Henon in 1976 [11]. It can be stated
- by following pair of equations
- Henon map may be stated as a two-dimensional iterated discrete-time dynamical
- system with a chaotic attractor as proposed by Henon in 1976 [11]. It can be stated
- by following pair of equations
- Henon map may be stated as a two-dimensional iterated discrete-time dynamical
- system with a chaotic attractor as proposed by Henon in 1976 [11]. It can be stated
- by following pair of equations
- Henon map may be stated as a two-dimensional iterated discrete-time dynamical
- system with a chaotic attractor as proposed by Henon in 1976 [11]. It can be stated
- by following pair of equations
- Henon map may be stated as a two-dimensional iterated discrete-time dynamical
- system with a chaotic attractor as proposed by Henon in 1976 [11]. It can be stated
- by following pair of equations
- Henon map may be stated as a two-dimensional iterated discrete-time dynamical
- system with a chaotic attractor as proposed by Henon in 1976 [11]. It can be stated
- by following pair of equations
- Henon map may be stated as a two-dimensional iterated discrete-time dynamical
- system with a chaotic attractor as proposed by Henon in 1976 [11]. It can be stated
- by following pair of equations

Henon map may be stated as a two-dimensional iterated discrete-time dynamical system with a chaotic attractor as proposed by Henon in 1976. It can be stated by following pair of equations:

$X_{n+1} = 1 + y_n - \alpha x^2_n$……..Eq 5.1

$Y_{n+1} = \beta x_n$. …………….Eq 5.2

With x_0, y_0 as initial point, (x, y) denote the present state of the system. Henon showed that if S is the area bounded by four points (−1.33, 0.42), (1.32, 0.133), (1.245,−0.14) and (−1.06,−0.5), and if the initial point lies in the area S, then the subsequent points—(x_i, y_i) for $i \geq 1$, also lie in S.

The proposed work generates permutation matrix for shuffling of pixels of the image (confusion phase) and cipher image for encryption of the shuffled image (diffusionphase) using Henon chaotic map and the 128 bit externally supplied secret key. As it is a private key algorithm, the same key to be available at both sender and receiver ends.

V.RESULT AND ANALYSIS

Original image **Stego image**

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.194 |

|| Volume 8, Issue 4, April 2020 ||

Original Image is used for embedding purpose. Stego Image is consisting information within it.And data it may be anything text,audio,video,file,image.There is no difference between original image and stego image it's look like same. But practically the pixel values will be slighty changed it cannot be identified by human eyes.

VI.CONCLUSION

The proposed method uses combination of cryptography and steganography, and also uses cloud for increased security.This application will save the time and money. And also proposed method gives more security and accuracy. It is more reliable and flexible.

REFERENCES

[1] Shivani Chauhan, Jyotsna"Multiple layer Text security using Variable blocksize Cryptography and Image Steganography", 3rd IEEE International Conference on Computational Intelligence and Communication Technology (IEEE-CICT2017)
[2] B.Karthikeyan, A.Deepak "A Combined Approach of Steganography with LSB Encoding technique and DES Algorithm",3rd International Conference on Advances in Electrical, electronics, Information, Communication and Bio-Informatics (AEEICB 2017)
[3] Ammad Ul Islam, Faiza Khalid, Mohsin Shah2, Zakir Khan"An Improved Image Steganography Technique based on MSB using Bit Differencing",The Sixth International Conference on Innovative Computing Technology(INTECH 2016)
[4] Qiangfu Zhao,Tiyasu L Kunii "Steganography Based on Image Morphing"(2013)
[5] Ciarán Bryce "Security governance as a service on the cloud",Bryce Journal of Cloud Computing: Advances,Systems and Applications (2019)
[6].Saad MuhiFalih "A Simple Chaotic Image Cryptography Algorithm Based on New Quadratic Chaotic Map",Journal of Babylon University/Engineering Sciences/ No.(4)/ Vol.(25): 2017.
[7].X. J. Tong, M. Zhang & Z. Wang "A new image encryption algorithm based on the high-dimensional chaotic map", The Imaging Science Journal, Vol.65 no(5) :2015.
[8].AhmedMAEl-Sayed,ZakiFEEl-Raheem and SanaaMSalman" A new chaotic behaviour of a general model of the Henonmap, El-Sayedetal.Advances in Difference Equations", 2014:107