IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 11, Issue 5, May 2022

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.118

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 5, May 2022||

| DOI:10.15680/IJIRSET.2022.1105239 |

Security Improvement of Cloud Data Using Cryptography and Steganography

Amisha Arjun Kedar [1], Riya Pardhi[2], Rahul Shende[3] , Vaishnavi Patke[4] , Gaurav Sawale[5]

Department of Computer Science, Sant Gadge Baba University, PRMITR, Badnera, Maharashtra, India [1-5]

ABSTRACT:Cloud computing has enabled people and enterprises to benefit from a low-cost utility. It gives enterprises more control by offering these services through the internet. The cloud may be used to transfer files. These files may contain important information that should be kept private from unidentified users. This is accomplished through the use of cryptographic techniques. Encrypting data with hybrid cryptography provides a high level of security. The Advanced Encryption Standard (AES) and the XOR-based encryption algorithm contribute to the provision of a hybrid cryptography model. The produced key's security can be further increased by employing the picture steganography method Least Significant Bit (LSB).

Cloud computing is a huge leap in information technology; however, the security of data storage is a major challenge in the cloud environment. As a result, this study proposes a method for increasing the security of cloud data through the use of encryption, information concealment, and hashing algorithms. In the data encryption step, we used hybrid encryption with the AES symmetric encryption method and the RSA asymmetric encryption algorithm. The encrypted data will then be concealed in an image using the LSB method. During the data validation step, we employ the SHA hashing method. In addition, in our approach, we compress the data using the LZW method before hiding it in the image. As a result, it enables the concealment of as much data as feasible. We can accomplish robust data security by utilising information concealment technologies and hybrid encryption. PSNR and SSIM values were computed in addition to the graph in this work to evaluate image masking performance before and after the compression procedure was applied. The results demonstrated that stego-image PSNR values are higher for compressed data than for uncompressed data.

KEYWORDS:Compressed data, strong data security, mixed encryption, LZW algorithm, SHA hashing algorithm, data validation phase, LSB algorithm, encrypted data, RSA asymmetric encryption, AES symmetric encryption, hybrid encryption, data encryption phase, hashing functions, data storage, security issue, Cloud computing, information technology, cloud data, security improvement

I. INTRODUCTION

The Cloud computing provides a novel way to handle data resources. Cloud servers can provide a variety of data services inside these computing environments, such as distant data storage and outsourced delegated compute, among others. Because cloud servers are not always trustworthy, file encrypted storage is an excellent way to prevent private data from being stolen or changed. In the interim, they may need to share data with the individual who meets certain criteria. Hybrid encryption is used to make such data exchange possible. The data to be delivered to the user/client is encrypted using multiple encryption techniques on the data owner's side, however instead of utilising a single encryption technique, we may utilise numerous encryption techniques by separating the data into distinct portions.

The goal of this project is to increase the security of cloud documents. In the current setup, cryptography is commonly employed to safeguard cloud documents using any well-known technique. However, if the key is compromised and the attacker is technically savvy, he can attempt to decode the document using a variety of well-known techniques. As a result, there is a risk of document leakage. However, if we employ steganography, the attacker will be able to examine the picture instead of the document, leading him to believe that the document is not encrypted. As a result, the likelihood of an assault decreases. As a result, in this research, we suggested a hybrid security model in which the text is secured using two separate encryption methods as well as steganography. During the data encryption stage, we used the AES symmetric encryption technique and the algorithm to construct hybrid encryption. The encrypted data is then concealed in an image using the LSB method.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 5, May 2022||

| DOI:10.15680/IJIRSET.2022.1105239 |

During the project's execution, we are learning how to use new technologies to achieve goals such as installing a web server and configuring servers for the given application in which handling of web-based communication is done in a safe setting.

II. LITERATURE SURVEY

- **Safe data storage in the cloud with a hybrid cryptography technique**

A security component that uses, Symmetrical key cryptography computation and steganography to ensure data in the cloud. This proposal used a combination of four computations (RC6, AES, blowfish) for abnormal state security of cloud information and the LSB steganography method for key information protection.

- **Steganography Advances Data Storage Security in Cloud Computing**

A steganography approach is used to prevent unauthorized data access from the cloud. This improved steganography approach is used to store data in the cloud and recover data from the data center when needed. The disadvantage in this research is that the proposed approach can only comprehend a single fixed number of security threats.

- **Encryption and Steganography for Data Security in Cloud Computing**

The client's data is scrambled using AES and then sent to the server. Following that, the scrambled data is scrambled and stored on the server, and a switching technique is used to decode the data and retrieve the first data. To address the data security issue, the recommended approach is used.

- **Hybrid encryption enhances security in cloud computing structures**

The AES and MD5 calculations were used in the mixed technique with brightened content. The plain content includes the content that should be encoded, while the brightened content contains the essence of the plain content. The encryption as the hash capacity is presented in this work to give greater security in the cloud situation to the communication. This strategy is used to protect cloud administrators from insider attacks.

- **Using Cryptography and Steganography with the E-LSB Encoding Technique to Improve Cloud Data Security**

In this study, steganography, cryptography and hash work were used to suggest a strategy for improving data security in the cloud. For data security, the blowfish computation is used for cryptography, another competent inserted calculation using Embedded Least Significant Bit (E-LSB) is used for steganography, and SHA-256 Hashing is used for respectability verification. The security of the steganography architecture is assessed via data decimation attack and data identification.

III. PROPOSED METHODOLOGY

Information security is the way of assuring that the private information is still secure not lost or stolen. Information isn't only theft but it can be damaged by system malfunction or any other way where data has a chance of being lost. Numerous government institutions, military departments, hospitals, educational institutes save utmost of their non-public data about their workers, guests, products on computers.

Steganography

The word ” Steganography ” comes from the Greek steganos(covered or secret) and graphy(jotting or delineation) and therefore means, literally, covered jotting. It's a data caching ways, which aims at transmitting a communication on a channel where some other kind of information is formerly being transmitted. The thing of steganography is to hide dispatches inside the images in such a way that doesn't allow any “adversary” to indeed descry that there's a secret communication present in the image. Steganography attempts to hide the actuality of communication. Steganography can be applied to numerous types of data, including audio, videotape, and images and can hide any

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 5, May 2022||

| DOI:10.15680/IJIRSET.2022.1105239 |

information.Steganography relies on hiding communication in unacquainted multimedia data and is generally used in secret communication between acknowledged parties.

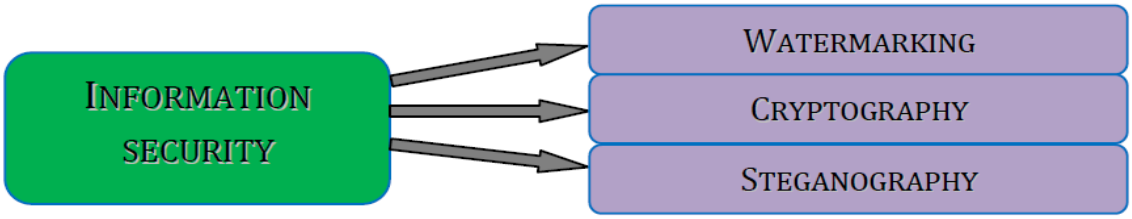

Fig 4.3.(i) Types of Information security

IV. EXPERIMENTAL RESULTS

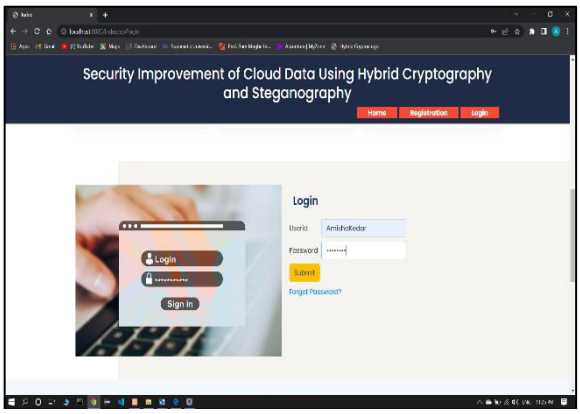

Fig.1. Login & Registration

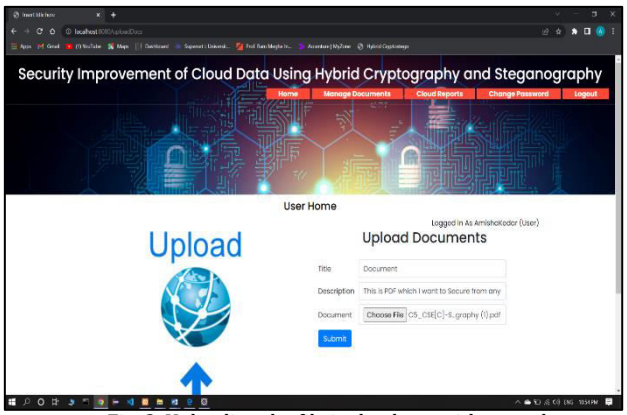

Fig. 2. Uploading the file in database with remarks

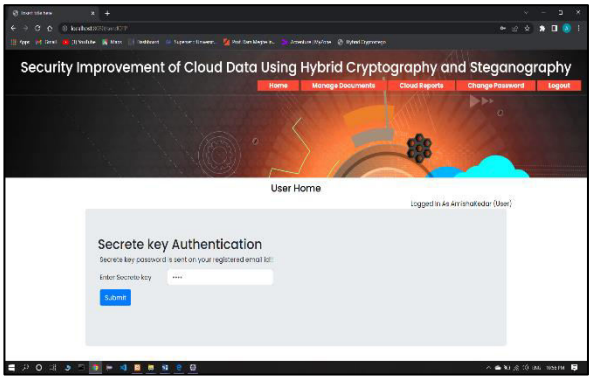

Fig. 3. Entering the password

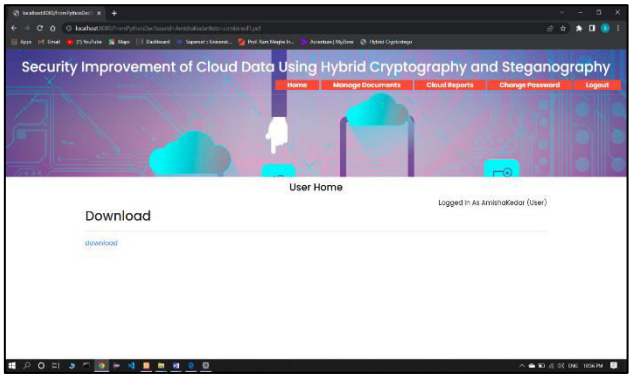

Fig 4. Download the file

V. CONCLUSION

Cloud computing is the on- demand vacuity of computer system operation, especially cloud storageand calculating power,without direct active operation bythe stoner. Large shadows frequently have functions distributed over multiple locales,each position being data center.The term is d educed from the Greek word kryptos, which means hidden. It's nearly associated to encryption, which is the act of scrabbling ordinary textbook into what is known as cipher-text and also back again upon appearance &

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 5, May 2022||

| DOI:10.15680/IJIRSET.2022.1105239 |

Steganography is the practice of hiding a secret communication inside of (or indeed on top of) commodity that isn't secret.

In this design, the cryptographic operation of the AES128 algorithm and LSB system steganography in cloud computing can be used to ameliorate data security in the form of JPG/ JPEG image format lines. The process of hiding a communication successfully done into a JPG/ JPEG image using the media oil as a communication insertion process with the LSB system steganography process into the image carried out on the cloud. The Advanced Encryption Standard (AES 128bit) algorithm can be used for communication randomization so that dispatches that will be fitted in the image are in the form of a ciphertext that will be delicate to read.

REFERENCES

[1] S. E. Elgazzar, A. A. Saleh, and H. M. El-Bakry, "Overview of using private cloud model with GIS," Int. J. Electron. Inf. Eng., vol. 7, no. 2, pp. 68–78, 2017.
[2] E. F. Coutinho, F. R. de Carvalho Sousa, P. A. L. Rego, D. G. Gomes, and J. N. de Souza, "Elasticity in cloud computing: a survey," Ann. Telecommand. des telecommunications, vol. 70, no. 7–8, pp. 289–309, 2015.
[3] S. C. Sukumaran and M. Misbahuddin, "DNA Cryptography for Secure Data Storage in Cloud.," IJ Netw. Secur., vol. 20, no. 3, pp. 447–454, 2018.
[4] S. William, Computer security: Principles and practice. Pearson Education India, 2008.
[5] L.-C. Huang, L.-Y. Tseng, and M.-S. Hwang, "A reversible data hiding method by histogram shifting in high quality medical images," J. Syst. Softw., vol. 86, no. 3, pp. 716–727, 2013.
[6] R. Shanthakumari and S. Malliga, "Dual-layer security of image steganography based on IDEA and LSBG algorithm in the cloud environment," Sādhanā, vol. 44, no. 5, p. 119, 2019.
[7] Y. Zhang, C. Xu, H. Li, and X. Liang, "Cryptographic public verification of data integrity for cloud storage systems," IEEE Cloud Comput., vol. 3, no. 5, pp. 44–52, 2016.
[8] A. A. Abdulla, "Exploiting similarities between secret and cover images for improved embedding efficiency and security in digital steganography." University of Buckingham, 2015

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 8.118

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details