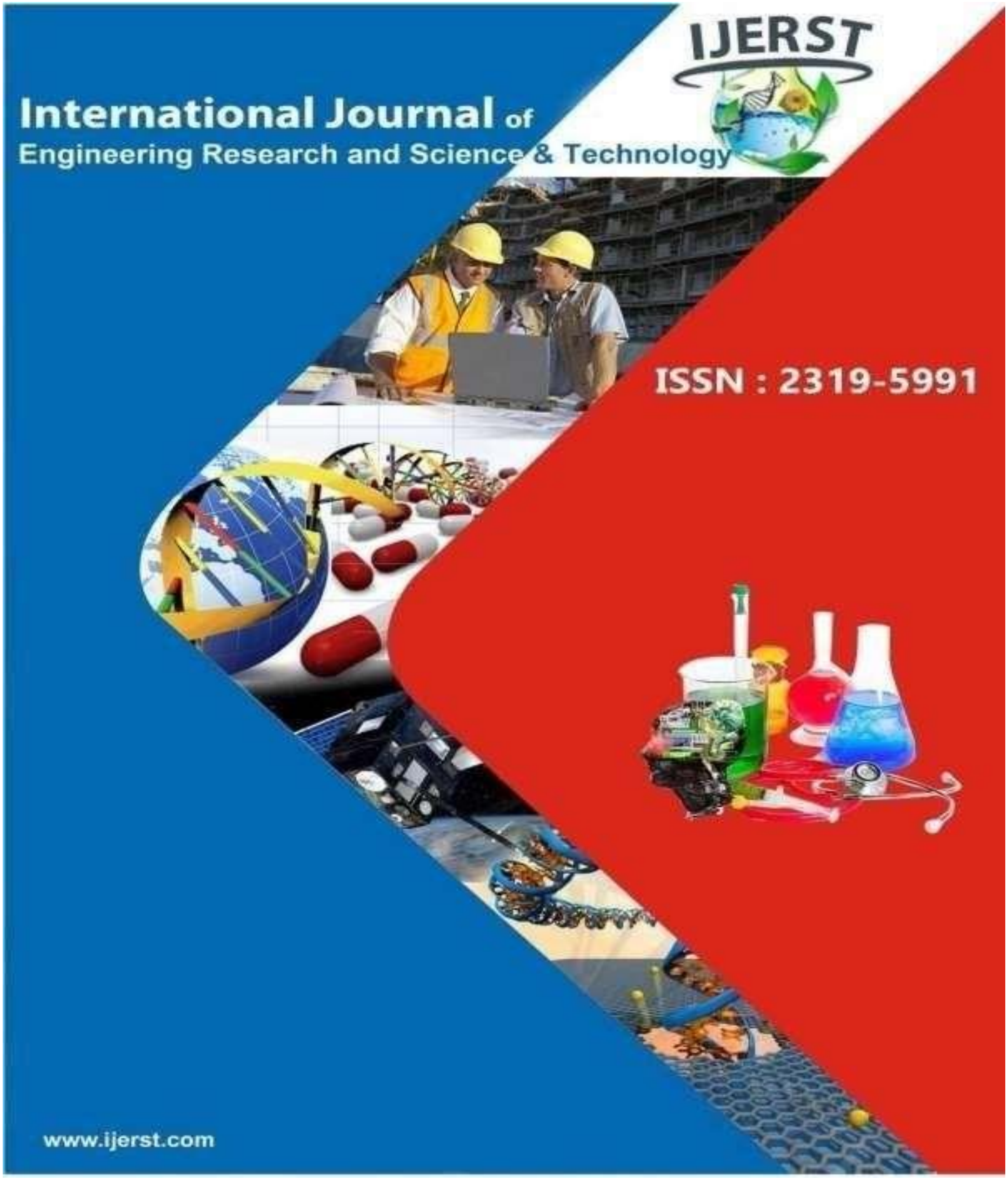

IJERST

International Journal of Engineering Research and Science & Technology

ISSN : 2319-5991

www.ijerst.com

Email: editor@ijerst.com or editor.ijerst@gmail.com

ISSN 2319-5991 www.ijerst.com

https://doi.org/10.62643/ijerst.2021.v17.i3.pp29-41

Vol. 17, Issue 3, 2021

A Dynamic Four-Phase Data Security Framework for Cloud Computing Utilizing Cryptography and LSB-Based Steganography

[1]Rajya Lakshmi Gudivaka,
Jawaharlal Nehru Technological University, Kakinada, Andhra Pradesh, India
[1]Email id: rlakshmigudivaka@gmail.com
[2]Raj Kumar Gudivaka
Sr Software Developer, Birlasoft Limited, Hyderabad, Telangana, India.
[2] Email id: rajkumargudivaka35@gmail.com

ABSTRACT

Maintaining strong data security has become essential as cloud computing continues to advance quickly in order to reduce threats like theft, data loss, and manipulation. Using cryptography and least significant bit (LSB) steganography, this research suggests a dynamic, four-phase data security system for cloud computing. LSB steganography encrypts data before embedding it into images, increasing security by hiding information within the least significant bits of image pixels. This method adds an additional degree of protection by encrypting the AES key and concealing it behind a cover object, combining RSA and AES encryption. In addition to protecting against potential attacks in cloud environments, the framework seeks to provide data redundancy, secrecy, and integrity. The selection of the cover item, the embedding rate, the vulnerability to steganography, and the computational complexity are factors that impact the effectiveness of LSB steganography. By emphasizing LSB steganography's effectiveness in cloud security on its own, as opposed to just combining it with cryptographic techniques, the study fills a major vacuum in the literature. Upcoming projects will focus on refining steganalysis methodologies, streamlining LSB embedding processes, and investigating integration with machine learning approaches. This framework provides a dependable and adaptable method for protecting sensitive data in cloud environments by tackling major security issues in cloud computing.

Keywords: Cloud computing security, LSB steganography, data confidentiality, steganalysis resistance, image quality, structural similarity index (SSIM), peak signal-to-noise ratio (PSNR), design science research methodology, RSA encryption, AES encryption, cover image selection.

ISSN 2319-5991 www.ijerst.com

https://doi.org/10.62643/ijerst.2021.v14.i3.pp29-41

Vol. 14, Issue 3, 2021

1. INTRODUCTION

This study investigates the usage of least significant bit (LSB) steganography as an independent security method in cloud computing. With the fast growth of cloud services, good data security is essential for preventing threats such as data loss and manipulation. By focusing primarily on LSB steganography, this study hopes to fill a research gap by examining its usefulness in improving data security and integrity. After conducting a thorough examination of previous research, the study aims to propose novel techniques to use LSB steganography to improve data security in cloud contexts.

With the rise of cloud computing, strong data security has become crucial in mitigating worries about data loss, manipulation, and theft. This study proposes a dynamic four-phase data security system for cloud computing that employs cryptography and LSB-based steganography. LSB, or Least Significant Bit, steganography hides information within an image's least significant bit by making imperceptible alterations to avoid detection. This method enhances security by encrypting raw data before embedding it in images, hence decreasing steganalysis vulnerabilities. The approach combines RSA encryption with AES, employing LSB to disguise the encrypted AES key beneath a cover object, providing an extra layer of security. This approach ensures data confidentiality, privacy, and integrity while also defending cloud data against potential attackers. This approach improves data protection and security in cloud situations by leveraging cryptographic and LSB steganography synergies.

Several factors influence the efficacy of using the Least Significant Bit (LSB) approach in steganography. First and foremost, the choice of cover item has a considerable impact on concealing capability and detection resistance. Image complexity, texture, and color distribution all have an impact on the ability to hide data while creating no visible changes. Furthermore, the embedding rate, which defines how much data may be buried per unit area, is crucial for striking a balance between data payload and visual distortion. The LSB method's susceptibility to steganalysis techniques is also significant, necessitating the use of encryption to prevent vulnerabilities. Furthermore, the efficiency and computational complexity of the LSB embedding and extraction procedures influence the method's suitability for real-world applications. Finally, the choice of LSB modification technique, such as random or sequential embedding, influences security and detection resistance. Consideration of these variables guarantees that LSB steganography is used effectively to improve data security in cloud computing environments.

The goal of this research study is to close the research gap on the use of Least Significant Bit (LSB) steganography as an independent security solution in cloud computing environments. Whilethe work acknowledges the integration of LSB steganography with cryptographic methods such asRSA and AES to improve data security, its primary focus is on determining the individual efficacyof LSB steganography. The research proposes to create a fast and resilient data security system

ISSN 2319-5991 www.ijerst.com
https://doi.org/10.62643/ijerst.2021.v14.i3.pp29-41
Vol. 14, Issue 3, 2021

customized specifically for cloud computing by relying solely on the LSB approach. This framework aims to address common security and privacy concerns, such as data loss, modification, and theft, by using the hiding capabilities of LSB steganography. The study aims to identify key difficulties and suggest new solutions by doing a thorough analysis of current literature and using a design science research methodology. Finally, the study aims to improve LSB-based steganography algorithms, resolve weaknesses, and investigate novel strategies for increasing their effectiveness in ensuring data confidentiality and integrity in cloud computing environments.

The goal of this research article is to create a comprehensive data security architecture for cloud computing that only uses Least Significant Bit (LSB) steganography. The primary goal is to address common security and privacy concerns in cloud environments, including data loss, manipulation, and theft. The research aims to identify key concerns and suggest an innovative solution by doing a thorough assessment of existing literature on cloud computing security models. The project will use a design science research process to identify problems, elicit requirements, design and construct artifacts, demonstrate, and assess. This research will result in a dynamic four-phase data security architecture that combines LSB steganography with encryption methods, notably RSA and AES, to improve data confidentiality, privacy, and integrity. The model's objectives include guaranteeing cloud data redundancy, adaptability, efficiency, and security, with the ultimate goal of protecting sensitive information from prospective attackers in cloud computing settings.

One significant research gap in the existing literature on data security in cloud computing is the investigation of efficient and robust ways for using LSB-based steganography as a standalone security mechanism. While the study covers integrating LSB steganography with cryptographic methods such as RSA and AES to improve data security, the emphasis is on the integrated approach rather than the solo efficacy of LSB steganography. Furthermore, the research emphasizes the vulnerability of LSB embedding to steganalysis, recommending encryption to avoid this risk. However, there has been little investigation into strategies especially designed to solve this problem and improve the durability of LSB steganography against discovery. As a result,there is a clear need for further research into optimizing LSB-based steganography techniques, addressing their vulnerabilities, and investigating novel methods to improve their effectiveness as standalone security measures for data confidentiality and integrity in cloud computing environments.

The rapid growth of cloud computing has raised worries about data security, with threats such as data loss, manipulation, and theft becoming more common. Despite the use of cryptographic algorithms such as RSA and AES, there is a significant research vacuum concerning the standalone efficacy of Least Significant Bit (LSB) steganography as a strong security solution. The goal of this research is to analyze and optimize LSB-based steganography for cloud environments,

ISSN 2319-5991 www.ijerst.com

https://doi.org/10.62643/ijerst.2021.v14.i3.pp29-41

Vol. 14, Issue 3, 2021

eliminating steganalysis vulnerabilities and increasing its effectiveness in maintaining data confidentiality, integrity, and privacy without relying entirely on traditional cryptographic approaches.

2. LITERATURE SURVEY

Patel et al. (2021) offer a cloud-based steganography approach for embedding pathological reports within medical photographs, which uses less storage space than keeping them individually. The model includes a new approach for generating secret keys, which are used to segment the medical image into five parts and embed the report. MSE and PSNR readings are used to validate the quality of medical images.

Hashim et al. (2020) present a new safe system for steganography-based authentication of medical data in IoT healthcare applications. To avoid cybercrimes, this framework uses a layered security approach and a chosen mechanism with a Henon function, demonstrating increased imperceptibility and security over previous methods. The study focuses on the application of steganography in medical photographs to conceal data, solves the constraints of existing schemes in balancing image quality and security, and includes a third random iteration with the Henon function to improve cyber threat protection.

Sukumar et al. (2020) present a safe steganography approach for cloud-based storage that uses a hybrid transform and support vector machine (SVM) to handle privacy concerns while improving speed. This multimedia steganography technique employs a hybrid transform that combines the Discrete Rajan Transform (DRT) and Integer Wavelet with the Diamond Encoding technique, as well as SVM for robust hidden content extraction. The suggested technique outperforms existing methods in terms of peak signal to noise ratio (PSNR), resilience, and security.

Bagaeen et al. (2019) assess the security challenges and solutions for storage as a service (STaaS) in cloud computing, focusing on data security, privacy, and availability. The article emphasizes the importance and popularity of STaaS, emphasizing data security as a critical concern for users and enterprises who use cloud storage. It also analyzes how cloud computing's fundamental features, such as multi-tenancy and virtualization, contribute to storage security challenges, as well as current methods presented in the literature to solve these issues.

Das et al. (2019) present an efficient and safe lip biometric system that improves recognition rate and template security. The system comprises a pre-processing step to improve the local properties of lip photos and a spatial steganographic method to reduce distortion and conceal the identity in the images. This method assures that the templates saved in the biometric system are secure, lowering the possibility of misuse. The results show that the suggested framework performs similarly to cutting-edge approaches while also offering the added benefit of identity concealment.

ISSN 2319-5991 www.ijerst.com

https://doi.org/10.62643/ijerst.2021.v14.i3.pp29-41

Vol. 14, Issue 3, 2021

Astuti et al. (2020) investigate the application of cryptography and steganography to enhance data security for JPG files within cloud computing platforms. Given the vulnerability of image files, particularly JPG files, to manipulation in cloud environments, the study explores the effectiveness of combining AES cryptography and LSB steganography for bolstering data security. The findings reveal that employing this combination leads to increased file sizes for JPG files, which correlates with the volume of inserted text, thus providing heightened security for stored data on cloud platforms.

Gambhir and Mandal (2021) provide a research study that introduces an OpenMP implementation of a chaos-based LSB steganography technique, with the goal of improving the efficiency of data security algorithms used for internet information sharing. The proposed implementation is intended to improve the efficiency of data security protocols in the online environment. The work methodically reports both standard statistical validation test results and the results of statistical testing on the created chaotic bit sequences. Notably, the multi-core implementation of the technique exhibits exceptional speedup and linear scalability as the number of cores rises, indicating its potential for improving performance in real-world applications.

In their study work, Rahman et al. (2019) investigate the area of steganography, focusing on the use of the Least Significant Bit (LSB) approach for secure communication and data hiding. They highlight steganography as a method for maintaining the confidentiality, integrity, and validity of secret material. Specifically, the paper dives into image steganography techniques, particularly the LSB method, and provides a thorough examination and comparison of the various steganography methods accessible. Through their analysis, they provide insights into cutting-edge steganography techniques and conclude with recommendations for practical steganography implementation.

Huang et al. (2016) present the proceedings of the International Conference on Cloud Computing and Security (ICCCS 2015), which took place in Nanjing, China, in August 2015. The conference, which aimed to facilitate debates on information security and cloud computing, brought together researchers, professionals, and government representatives. The study article is titled "Cloud Computing and Security," and it will be presented at the First International Conference on Cloud Computing and Security (ICCCS 2015) in Nanjing, China, from August 13 to 15, 2015. The conference proceedings were eventually published in book form.

Wan et al. (2016) analyze the proceedings of two conferences, CloudComp 2016 and the First EAI International Conference (SPNCE 2016), which were held in Guangzhou, China, in November and December 2016. The combined proceedings include 22 full papers, 10 from CloudComp 2016 and 12 from SPNCE 2016, which were carefully selected from several submissions. These conferences focus on new developments and experiences in cloud computing, as well as talks about security, privacy, and emerging computing environments.

ISSN 2319-5991 www.ijerst.com

https://doi.org/10.62643/ijerst.2021.v14.i3.pp29-41

Vol. 14, Issue 3, 2021

Dang et al. (2017) present the proceedings of the 4th International Conference on Future Data and Security Engineering, which took place in Ho Chi Minh City, Vietnam, on November 29–December 1, 2017. The conference, currently in its fourth year, received 128 entries and accepted 28 full papers and 7 short papers after a rigorous screening process. The accepted papers span a wide range of issues, including query processing, big data analytics, blockchains, data engineering tools, data protection, the Internet of Things, security and privacy engineering, and social network data analytics.

Reza and Sonawane (2016) provide a research study advocating the use of steganography to improve the security and privacy of data saved in the cloud by mobile applications. Their methodology offers embedding a key within photos to add another layer of security and confidentiality. They also present a case study to demonstrate the usefulness of this strategy. Mobile cloud computing is a common approach for accessing shared resources over a network, but it poses concerns about security and privacy. Unauthorized access by insiders or cloud administrators poses a serious hazard to cloud users. Using steganography emerges as a promising technique for addressing these concerns and strengthening the security and privacy of cloud-stored data accessed via mobile applications.

3. METHODOLOGY

3.1. Introduction to the Methodology

The process of implementing Least Significant Bit (LSB) Steganography as an independent data security technique in cloud computing settings is divided into many parts. Each procedure assures complete data security, from encryption and embedding to transmission and retrieval. This section describes the design science research approach, the process of merging LSB steganography with cryptographic algorithms, and the metrics used to assess the system's efficacy.

3.2. Design Science Research Methodology

Design science research methodology (DSRM) is a methodical way to creating and analyzing objects intended to solve specific challenges. The steps in the DSRM process are as follows:

Problem Identification and Motivation: Outlining the gaps in the current body of knowledge surrounding the application of LSB steganography and emphasizing the necessity of strong data security in cloud computing.
Goals for a Solution: laying out the specifications and objectives for the LSB steganography architecture and making sure that data loss, theft, and manipulation are adequately addressed.
Design and development include building the LSB steganography framework, incorporating cryptographic methods, and creating data extraction and embedding algorithms.
The framework will be put into practice in a cloud environment, and useful applications will be used to showcase its capabilities.

ISSN 2319-5991 www.ijerst.com

https://doi.org/10.62643/ijerst.2021.v14.i3.pp29-41

Vol. 14, Issue 3, 2021

Evaluation: Measuring the framework's efficacy with a range of measures, including security, robustness, and efficiency.
Communication: Writing up and presenting the study results to add to the corpus of information already available on cloud computing security.

3.3. Problem Identification and Motivation

Services provided by cloud computing have many advantages, such as cost-effectiveness, scalability, and flexibility. These benefits do, however, present serious security risks. Common threats include data breaches, unauthorized access, and data tampering. Even if they work well, traditional cryptographic techniques are not infallible. An inventive answer is provided by LSB steganography, which embeds data within images to reduce detection.

3.4. Objectives of the Solution

The following are the main goals of the suggested LSB steganography framework:

Data Confidentiality: Making sure that information stays confidential and is only available to those who are permitted.
Data integrity refers to safeguarding information against unwanted changes.
Data redundancy: guaranteeing the recoverability and availability of data.
Efficiency: Optimizing performance while minimizing computational overhead.
Adaptability: The framework's ability to change and adapt to different cloud settings.

3.5. Design and Development

3.5.1. *Cryptographic Techniques*

The framework includes cryptographic approaches to improve the security of LSB steganography:
RSA Encryption: The AES key is encrypted with RSA. With the use of two keys—public and private—RSA, an asymmetric encryption method, offers a high degree of security.
AES Encryption: The data itself is encrypted using AES. The symmetric encryption algorithm AES is renowned for its quickness and safety. LSB steganography is then used to embed the encrypted data.

3.5.2. *LSB Steganography Technique*

Data is embedded into the least significant bits of an image's pixel values via LSB steganography. The actions consist of:
Image Selection: Selecting a suitable cover image that has enough depth and color variety to guarantee that the embedded data is never seen.
Data Preparation: AES encryption of the data. Next, RSA is used to encrypt the AES key.
The encrypted data and AES key are embedded into the LSBs of the image pixels during the *embedding process*. To improve security, this procedure might be either sequential or random.

Image Transmission: Using the cloud network to send the stego-image.
Data Extraction: Using the reverse LSB method, extract the embedded data from the stego-image. RSA is used to decode the AES key, which is subsequently used to decrypt the actual data.

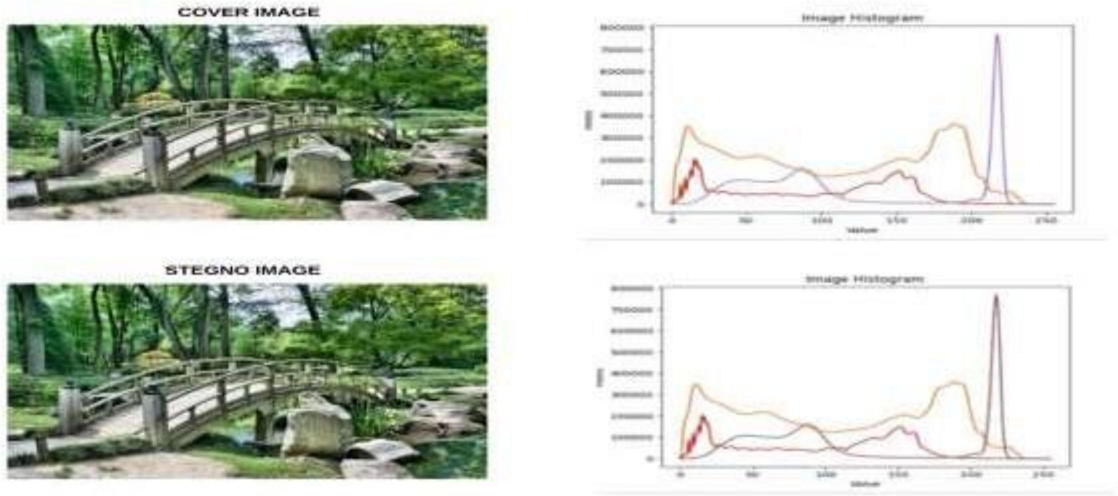

Figure 1: Shows the cover images, stego images, and the histograms.

3.5.3. Algorithm Development

The first step of the embedding algorithm is to convert the data into binary form. To maintain security, this data is encrypted using the Advanced Encryption Standard (AES). Next, an asymmetric encryption technique called Rivest-Shamir-Adleman (RSA) is used to encrypt the AES key itself. The least important bits of each pixel in an image contain both the encrypted data and the encrypted AES key.

The binary data is extracted by the extraction method from the least important portions of the image. The encrypted data and the encrypted AES key are separated by it. The RSA private key is used to decrypt the AES key, which is subsequently used to decode the data.

By combining the benefits of cryptography and steganography, this approach provides strong data security in cloud computing environments by ensuring that the data is secure even in the event that the steganographic embedding is discovered.

ISSN 2319-5991 www.ijerst.com

https://doi.org/10.62643/ijerst.2021.v14.i3.pp29-41

Vol. 14, Issue 3, 2021

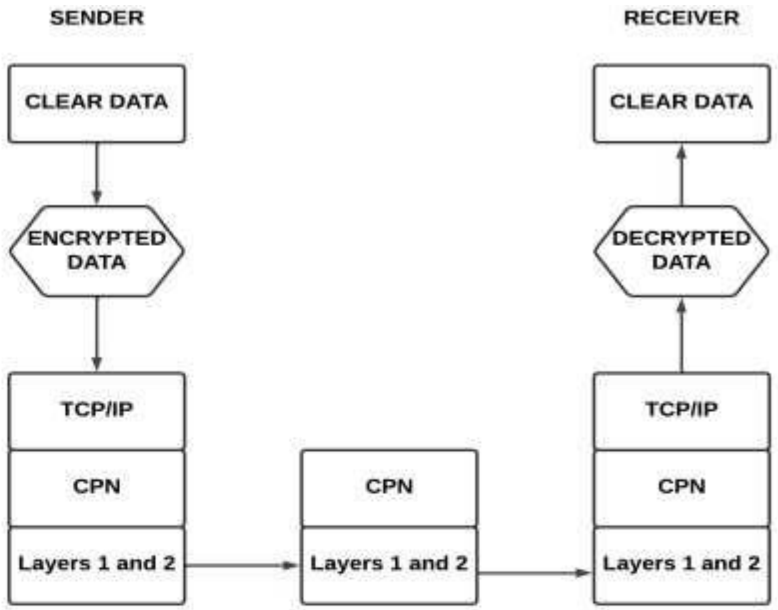

Figure 1: End-to-end encryption and external decryption of user data.

Embedding Algorithm

```
def embed_data(image, data, rsa_public_key):
    # Convert data to binary
    data_binary = ''.join(format(ord(char), '08b') for char in data)

    # Encrypt data using AES
    aes_key = generate_aes_key()
    encrypted_data = aes_encrypt(data_binary, aes_key)

    # Encrypt AES key using RSA
    encrypted_aes_key = rsa_encrypt(aes_key, rsa_public_key)

    # Combine encrypted data and AES key
    combined_data = encrypted_aes_key + encrypted_data

    # Embed combined data into the image
    data_index = 0
    for pixel in image.getdata():
        if data_index < len(combined_data):
            pixel_bin = format(pixel, '08b')
            new_pixel_bin = pixel_bin[:-1] + combined_data[data_index]
            image.putpixel((x, y), int(new_pixel_bin, 2))
            data_index += 1
    return image
```

Extraction Algorithm

```
def extract_data(stego_image, rsa_private_key):
    # Extract binary data from the stego-image
    extracted_data = "
    for pixel in stego_image.getdata():
        pixel_bin = format(pixel, '08b')
        extracted_data += pixel_bin[-1]

    # Separate encrypted AES key and data
    encrypted_aes_key = extracted_data[:len(rsa_private_key)]
    encrypted_data = extracted_data[len(rsa_private_key):]

    # Decrypt AES key using RSA
    aes_key = rsa_decrypt(encrypted_aes_key, rsa_private_key)

    # Decrypt data using AES
    data_binary = aes_decrypt(encrypted_data, aes_key)

    # Convert binary data to text
    data = ".join(chr(int(data_binary[i:i+8], 2)) for i in range(0, len(data_binary), 8))


    return data
```

3.6. Demonstration

Using the Python programming language, the suggested framework is presented in a controlled cloud environment. Important phases consist of:

Setup includes choosing cover photos, configuring the cloud environment, and getting the data ready for embedding.

Embedding Procedure: Using the embedding algorithm, encrypted data is concealed inside the selected images.

Transmission: Transferring the stego-images to specified storage locations or receivers via the cloud network.

Extraction Process: The embedded data is retrieved and decrypted using the extraction algorithm.

ISSN 2319-5991 www.ijerst.com

https://doi.org/10.62643/ijerst.2021.v14.i3.pp29-41

Vol. 14, Issue 3, 2021

3.7. Evaluation

A number of factors are used to assess the proposed framework's effectiveness:

3.7.1. Security Analysis

Steganalysis Resistance: Assessing how resilient the framework is against steganalysis attacks. To try to find the embedded data, a variety of instruments and methods are employed.
Encryption Strength: Evaluating how well the AES and RSA encryption methods safeguard data.
Confidentiality and Integrity: guaranteeing the privacy and integrity of data while it is being sent and stored.

Table 1: Important Features of the Framework Concerning Integrity, Steganalysis Resistance, and Encryption Power.

Characteristic	Description
Steganalysis Inhibition	An assessment of the framework's resilience against steganalysis attacks, which use a variety of instruments and methods to find hidden data.
Strength of Encryption	Evaluating how well the encryption techniques AES and RSA preserve the secrecy and integrity of data.
Confidentiality	Ensuring data privacy during transport and storage, and preventing illegal access or disclosure.
Integrity	Ensure that the data remains consistent and trustworthy throughout its lifecycle, preventing unauthorized changes or manipulation.

3.7.2. Performance Metrics

Embedding Rate: Quantifying the amount of information that may be incorporated into a cover image per unit area without significantly distorting it.
Computational Efficiency: Examining the amount of time and money needed for the extraction and embedding procedures.
Image Quality: The visual quality of the stego-images is evaluated by comparing them to the original images using the Structural Similarity Index (SSIM) and Peak Signal-to-Noise Ratio (PSNR).

5. CONCLUSION

Finally, by utilizing cryptographic methods and LSB steganography, this study suggests an all-encompassing data security architecture for cloud computing. It fills in research gaps and provides a strong answer to data security issues by concentrating on the independent efficacy of LSB steganography. Ensuring data confidentiality, integrity, and availability, the framework prioritizes efficiency and adaptability across a range of cloud environments. Improving steganalysis techniques, streamlining embedding algorithms, incorporating machine learning, and conducting

ISSN 2319-5991 www.ijerst.com

https://doi.org/10.62643/ijerst.2021.v14.i3.pp29-41

Vol. 14, Issue 3, 2021

real-world testing in various cloud environments are some of the future research directions. This framework offers a comprehensive technique that ensures a dependable, efficient, and adaptable approach to handling data security issues in cloud computing scenarios.

6. REFERENCE

1. Patel, S. K., Saravanan, C., & Patel, V. K. (2021). Cloud-based Reversible Dynamic Secure Steganography Model for embedding pathological report in medical images. International Journal of Computers and Applications, 43(10), 1002-1010.
2. Hashim, M. M., Rhaif, S. H., Abdulrazzaq, A. A., Ali, A. H., & Taha, M. S. (2020, July). Based on IoT healthcare application for medical data authentication: Towards a new secure framework using steganography. In IOP Conference Series: Materials Science and Engineering (Vol. 881, No. 1, p. 012120). IOP Publishing.
3. Sukumar, A., Subramaniyaswamy, V., Vijayakumar, V., & Ravi, L. (2020). A secure multimedia steganography scheme using hybrid transform and support vector machine for cloud-based storage. Multimedia Tools and Applications, 79(15), 10825-10849.
4. Bagaeen, A., Al-Zoubi, S., Al-Sayyed, R., & Rodan, A. (2019, November). Storage as a service (staas) security challenges and solutions in cloud computing environment: An evaluation review. In 2019 Sixth HCT Information Technology Trends (ITT) (pp. 208-213). IEEE.
5. Das, S., Muhammad, K., Bakshi, S., Mukherjee, I., Sa, P. K., Sangaiah, A. K., & Bruno, A. (2019). Lip biometric template security framework using spatial steganography. Pattern Recognition Letters, 126, 102-110.
6. Astuti, N. R. D. P., Aribowo, E., & Saputra, E. (2020, April). Data security improvements on cloud computing using cryptography and steganography. In IOP conference series: materials science and engineering (Vol. 821, No. 1, p. 012041). IOP Publishing.
7. Gambhir, G., & Mandal, J. K. (2021). Multicore implementation and performance analysis of a chaos based LSB steganography technique. Microsystem Technologies, 27, 4015-4025.
8. Rahman, S., Masood, F., Khan, W. U., Salam, A., & Ullah, S. I. (2019). The Investigation of LSB based Image Steganographic Techniques in Spatial Domain for Secure Communication: Image Steganography in spatial domain. Sukkur IBA Journal of Emerging Technologies, 2(1), 1-12.
9. Huang, Z., Sun, X., Luo, J., & Wang, J. (Eds.). (2016). Cloud Computing and Security: First International Conference, ICCCS 2015, Nanjing, China, August 13-15, 2015. Revised Selected Papers (Vol. 9483). Springer.
10. Wan, J., Lin, K., Zeng, D., Li, J., Xiang, Y., Liao, X., ... & Liu, Z. (2016). Cloud computing, security, privacy in new computing environments. In Proceedings of 7th international conference, cloudcomp 2016 and first international conference, SPNCE.

ISSN 2319-5991 www.ijerst.com

https://doi.org/10.62643/ijerst.2021.v14.i3.pp29-41

Vol. 14, Issue 3, 2021

11. Dang, T. K., Wagner, R., Küng, J., Thoai, N., Takizawa, M., & Neuhold, E. J. (Eds.). (2017). Future Data and Security Engineering: 4th International Conference, FDSE 2017, Ho Chi Minh City, Vietnam, November 29–December 1, 2017, Proceedings (Vol. 10646).Springer.
12. Reza, H., & Sonawane, M. (2016). Enhancing mobile cloud computing security using steganography. Journal of Information Security, 7(4), 249.