Indonesian Journal of Electrical Engineering and Computer Science
Vol. 32, No. 2, November 2023, pp. 1105~1114
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v32.i2.pp1105-1114

A multilayer model to enhance data security in cloud computing

Wid Akeel Awadh[1], Ali Salah Alasady[2], Mohammed S. Hashim[3]
[1]Department of Computer Information Systems, Collage of Computer Science and Information Technology, University of Basrah, Basrah, Iraq
[2]Department of Computer Science, University of Basrah, Basrah, Iraq
[3]Department of Computer Science, Education College for Pure Sciences, University of Basrah, Basrah, Iraq

Article Info

Article history:

Received May 29, 2023
Revised Jul 30, 2023
Accepted Aug 13, 2023

Keywords:

Cloud computing
Compression
Cryptography
Data security
Steganography

ABSTRACT

Cloud computing has introduced substantial advancements to the field of information technology, offering businesses enhanced features, flexibility, reliability, scalability, and a wide range of services. However, it also presents security challenges like data theft and manipulation. To minimize the risks associated with these threats, a model that depends on encryption and steganography is proposed with the aim of applying a security model in a cloud environment. The proposed cloud security model utilizes a multi-layer model that includes a Rivest-Shamir-Adleman (RSA), advanced encryption standard (AES), identity-based encryption (IBE) methods, least significant bit (LSB) method, and the Brotli method. This comprehensive approach effectively safeguards data integrity, confidentiality, and privacy against potential intruders. In addition, it enhances the flexibility and efficiency of the cloud by enabling the secure storage and transmission of large amounts of data.

Corresponding Author:

Wid Akeel Awadh
Department of Computer Information Systems, Collage of Computer Science and Information Technology
University of Basrah
Basrah, Iraq
Email: wid.jawad@uobasrah.edu.iq

1. INTRODUCTION

Cloud computing has emerged as a powerful technology for delivering on-demand internet-based computing services [1], [2]. Industries across various sectors, including banking, healthcare, and education, are increasingly adopting cloud computing to leverage its benefits, such as cost-efficiency, accessibility, high performance, hassle-free maintenance, reliable backup and recovery, scalability, and expansive storage capacity [3], [4]. Prominent examples of cloud computing services include Microsoft Azure, Amazon web services (AWS), and Google cloud platform, offering a wide array of cloud-based services like virtual machines, databases, analytics, and storage [5]–[7].

However, the adoption of cloud computing can also lead to concerns regarding confidentiality, data protection, and information security [8]. Unauthorized access by internal personnel remains a significant issue, as existing prevention techniques have proven insufficient [9]. Data breaches resulting from such unauthorized access not only erode trust but also lead to financial setbacks for organizations relying on cloud computing services. Cyberattacks and eavesdropping further amplify the risks of data leakage and exposure to confidential information [10]. While encryption algorithms have been employed in private clouds to secure sensitive information during storage and transmission, they alone have proven inadequate in ensuring comprehensive data security in the cloud [11], [12]. A holistic security framework could be based on distributed computing architecture, computation approaches, or access control mechanisms.

Cloud security and privacy breaches have far-reaching consequences for various industries, including IT and Academia. Multiple stakeholders, such as organizations, clients, employees, IT administrators, and cloud service providers, are affected by these issues. Therefore, implementing robust security measures is crucial to mitigate these risks [13]. Another challenge in cloud computing is the efficient transfer of large amounts of data between users and cloud providers, which can lead to network congestion, increased latency, and slower data transfer rates. These issues negatively impact performance, and user experience, and incur additional costs in terms of data transfer fees [14]. To address these challenges, cloud providers offer solutions like content delivery networks, and organizations can optimize their cloud services by managing data transfer requirements and utilizing compression techniques to reduce data volumes [15]. The proposed model [16] combines cryptography and steganography but lacks the ability to compress data before hiding it. Therefore, an additional layer is necessary to enhance data security in the cloud by incorporating information compression.

This paper presents an innovative multi-layer cloud security model that integrates cryptographic algorithms, least significant bit (LSB) steganography techniques, and data compression technology. This approach sets itself apart from existing data security models that predominantly rely on cryptography and steganography algorithms, with few incorporating compression techniques. Furthermore, after reviewing existing security frameworks, it becomes evident that none provide a definitive solution for securely sharing data while considering the size of hidden data. This study aims to offer insights and answers to fundamental questions in cloud security. The first question is, "How can we provide a robust approach to optimize the security and privacy of sensitive information in the cloud?" This question will be addressed by combining cryptography and steganography methods. The second question is, "How can we optimize the performance of cloud environments?" this question will be answered by employing compression methods.

The aim of this research is to improve the security of the proposed cloud security model by addressing privacy and security concerns in cloud computing while minimizing the size of hidden data. The specific objectives of this study are as follows: i) Improve the cloud computing security model by integrating cryptography with steganography methods. ii) Enhance the performance of cloud computing by employing compression methods. Consequently, the proposed model is a multi-layered data security model that employs encryption algorithms in the first layer, compression in the second layer, and steganography techniques in the third layer. This multi-layered approach provides an additional layer of security to provide data confidentiality, protection, and availability of cloud data.

The rest of the article is organized as follows: Section 2 discusses the background of the research. Section 3 presents related work. Section 4 describes the research methodology. Section 5 explains the results and discussions, and the final section provides the conclusion.

2. RELATED WORK

Ghuge *et al.* [17] proposed a model for software as a service (SaaS) application hosted in a private cloud environment. The model involved dividing the application into two microservices. The first microservice implemented an application layer firewall to detect malicious activity and prevent unauthorized access. The second microservice focused on securing sensitive data transfer within the private cloud using the advanced encryption standard (AES) encryption algorithm. Ghuge also suggested the use of a hidden Markov model (HMM) layer for probability-based intrusion detection. Additionally, the author proposed a novel approach that employed the LSB technique to hide sensitive data within video covers, thereby enhancing security and protecting data confidentiality, privacy, and integrity.

Kumar and Badal [18] leveraged the performance advantages of private key encryption and proper key management of public key encryption in Bluetooth technology. They proposed a hybrid encryption scheme utilizing the AES and Rivest-Shamir-Adleman (RSA) algorithms. The authors found that AES encryption with a 256-bit key in 14 rounds proved effective for cloud computing. Their approach also incorporated fully homomorphic encryption, enabling more content to be encrypted and providing multiplicative homomorphism.

Chinnasamy *et al.* [9] emphasized the significance of encryption as a technique to ensure high levels of security for data transfer and storage across unsecured networks. They proposed a hybrid cryptography technique combining elliptic curve cryptography (ECC) and Blowfish algorithms. This approach addressed the limitations of traditional symmetric and asymmetric techniques and achieved confidentiality, integrity, and availability (CIA) property. The proposed method demonstrated better security and confidentiality for patient data compared to existing hybrid methods.

Denis and Madhubala [19] highlighted the benefits of combining encryption with steganography methods to enhance data security in cloud computing. They proposed an efficient model using a hybrid encryption approach with the AES and RSA algorithms. The model secured data by embedding it in a cover image using the LSB technique. To improve the LSB embedding process, they employed the adaptive genetic algorithm-based optimal pixel adjustment (AGA-OPAP) method, which ensured high embedding capacity and security. The proposed model also integrated the 2D-discrete wavelet transform (2D-DWT-2L) method for blockwise concealing to enhance embedding efficiency.

Reynaldo *et al.* [20] addressed the challenges posed by limited media storage capacity and increasing data size by proposing the use of the Brotli compression algorithm. They implemented the algorithm as a plugin developed in Java and PHP for a Moodle-based UMN e-learning server. The successful compression and decompression of data using the Brotli compression algorithm indicated its successful implementation in the study.

3. BACKGROUND

3.1. Cloud computing service models

Cloud computing encompasses three primary service models: SaaS, infrastructure as a service (IaaS), and platform as a service (PaaS). In the SaaS model [21], cloud-hosted software applications are accessible to users via the Internet. These applications can be reached using a web browser or client application. Noteworthy SaaS examples encompass Gmail, Office 365, Salesforce, and Dropbox. In the IaaS model [8], the provider of service provide users virtualized computing resources like, servers, networking and storage. Users can then deploy and run their own software applications on these resources. instances of IaaS involves Google compute engine, Microsoft Azure, and AWS [21]. In the PaaS model [8], the cloud provider provides a platform enabling developers to create, deploy, and manage software applications sans concerns about the underlying infrastructure. This platform includes essential tools, libraries, and frameworks for application development and deployment. Illustrative PaaS instances encompass Heroku, Google App Engine, and Microsoft Azure App Service [21].

3.2. Cryptography

Cryptography is the practice of studying secure communication techniques to prevent unauthorized access to private data, information, or messages [11]. It encompasses methods for ensuring secure communication, data confidentiality, integrity, and authentication [22]. The significance of encryption in the context of cloud computing has been widely acknowledged and explored in various studies [9]. Shakir and Yassir [23] emphasized the importance of data security in cloud computing to mitigate the risks of unauthorized access and ensure that only authorized users can retrieve data. The accessibility of cloud computing via the internet and the management of sensitive data make cloud computing security a critical concern [24]. By employing cryptography, data security in the cloud can be enhanced, offering benefits such as improved data integrity, privacy, confidentiality, flexibility, performance, and redundancy while protecting against unauthorized access [16]. Several hybrid encryption and decryption algorithms, such as AES, RSA, and identity-based encryption (IBE) algorithms, are available to secure data in the cloud environment [8].

3.3. Encryption methods

There are two primary types of encryption algorithms used to secure data: symmetric encryption and asymmetric encryption. Symmetric encryption utilizes a single key for both encryption and decryption, necessitating that both the sender and receiver possess the same key [25]. Conversely, asymmetric encryption employs two separate keys-public and private-for encryption and decryption operations. The public key serves encryption purposes, while the private key handles decryption tasks [25]. Asymmetric encryption is considered more secure than symmetric encryption due to the use of separate keys for encryption and decryption. However, symmetric encryption is faster and more efficient [25]. To address the challenge of key exchange in symmetric encryption, asymmetric encryption was developed. Asymmetric encryption eliminates the need for a shared secret key by utilizing both the public and private keys in the encryption process.

3.4. AES

The AES is a widely adopted encryption algorithm that employs symmetric-key cryptography to safeguard sensitive data. With a fixed block size of 128 bits, AES supports key sizes of 128, 192, or 256 bits [26]. It is regarded as one of the most secure encryption standards and finds application in various domains, including cloud computing, electronic transactions, and wireless communication networks [27]. The operation of AES involves dividing the data into fixed-size blocks and subjecting each block to a series of mathematical operations using the encryption key. This process transforms the data into ciphertext, which appears random and is virtually impossible to decipher without the correct decryption key [26]. While AES is highly secure, it does have certain considerations. It may entail a higher computational overhead compared to some other encryption algorithms, impacting processing efficiency. Additionally, AES requires longer key lengths, which might pose practical challenges for specific applications [27].

3.5. RSA

The RSA algorithm is widely acknowledged as a prominent technique for encryption and decryption. It relies on prime factorization and modular arithmetic to facilitate secure data transmission. While RSA provides robust security, it is slower compared to symmetric encryption algorithms and necessitates larger key sizes to ensure adequate security. This increased key size contributes to a higher computational load and greater memory requirements [28]. To enhance both security and efficiency, developers often employ a combination of RSA with other encryption schemes. This approach ensures that only the intended recipient can decrypt the message using their private key, rendering decryption virtually impossible without the corresponding key. Thus, combining multiple encryption and decryption algorithms has become a standard and effective solution for improving both security and efficiency [29].

3.6. IBE

IBE is a variant of public-key encryption where a user can generate a public key based on a unique identifier, such as an email address [30]. In an IBE system, the public key generator (PKG) generates both the public and private keys for users, with the public keys derived from their identities. The private keys are generated by the PKG based on user identities, while the PKG retains a master private key. Once the public key is computed, encrypted messages can be securely sent to the intended recipient/entity associated with the identity-ID [30]. The main advantage of IBE over traditional public-key encryption is the elimination of the need for a public key infrastructure to distribute and manage public keys. This feature makes IBE particularly useful in scenarios where key distribution is challenging, such as wireless networks or situations involving a large number of users [30]. By leveraging unique identifiers as the basis for key generation, IBE simplifies the encryption process and enhances the practicality of encryption in challenging environments.

3.7. Compression

Compression is a process that encodes data in a manner requiring fewer bits to represent the same information, resulting in reduced storage space and transmission time over networks or on devices [31], [32]. There are two primary types of compression: lossless and lossy. Lossless compression algorithms, such as ZIP and Brotli, retain all the original data, while lossy algorithms like JPEG and MP3 discard some data to achieve higher compression ratios [31].

In the proposed model, the Brotli algorithm [33] is utilized due to its optimization for web content and superior compression ratios compared to other algorithms like Deflate and Gzip, while still maintaining reasonable decompression speeds. Brotli employs a combination of context modeling, a static dictionary, Huffman coding, and a range encoder. It also boasts a larger dictionary size of up to 128 Mb, allowing for enhanced compression of long repetitive strings typically found in text-based files. Brotli proves especially beneficial for mobile networks as it reduces the volume of data transferred, saving bandwidth and enhancing performance.

3.8. LSB

The LSB refers to the bit in a binary number that represents the smallest power of two and is the rightmost bit in the binary representation [25]. In the context of image processing and steganography, the LSB denotes the lowest bit of each pixel in an image. This bit represents the least significant information of the pixel's color value, and modifying it has minimal visual impact on the image [25]. The LSB's inconspicuous nature makes it an appealing choice for hiding information within an image, as changes made to the LSB are unlikely to be noticeable to the human eye.

Steganography involves concealing confidential data within innocent carriers, such as images, audio files, or text documents, without arousing suspicion. The LSB technique is a steganographic method that involves modifying the LSB of pixel values in a digital image to hide information. By replacing the LSB of each pixel value with a bit of hidden information, it is possible to embed data within the image file without significantly affecting its appearance or quality [16]. However, it should be noted that while the LSB technique is a simple and effective way to hide data, it can be detected by certain analysis techniques. To enhance the security of this method, data can be encrypted before embedding it into the cover file using well-known cryptography methods, such as RSA and AES [25].

In the proposed method, a combination of steganography, cryptography, and compression is employed to enhance security and speed. The message is encrypted using RSA and AES, ensuring its confidentiality. Before being hidden using LSB steganography, the encoded information is compressed using the Brotli algorithm, which reduces its size and enhances efficiency. This comprehensive approach integrates multiple techniques to provide improved security while maintaining speed and performance.

4. METHOD

This paper proposes a cloud security model that enhances data security and performance by utilizing a multi-layer model that involves cryptography, compression, and steganography techniques as follow: In the first layer, the proposed security model involves the utilization of cryptography to improve data security in the environment of cloud. To address the challenge of securely transmitting a secret key to multiple recipients without the risk of discovery, in this layer, a hybrid encryption approach is utilized, combining the security features of the AES and the RSA methods for encryption. The goal of this stage is to harness the rapidity and effectiveness of symmetric encryption (AES), while upholding the confidentiality and security advantages of asymmetric encryption (RSA) and techniques from steganography. As AES functions as a symmetric encryption technique, both the encryption and decryption procedures necessitate the utilization of the same key. However, securely distributing this shared key to multiple recipients poses a significant challenge. By combining AES and RSA encryption [34], this step provides a graceful solution to the key distribution problem. This hybrid technique eliminates the requirement for a shared secret key. Instead, the sender simply requires the recipient's public key, reducing the risk of information leakage [34]. This approach ensures that the transmitted data remains confidential and only accessible to the intended recipients, preserving data security in the environment of cloud.

The second layer of the proposed security model involves the utilization of the Brotli compression method. The goal of this layer is to enhance the overall security and efficiency of the system by compressing the encoded information before it is hidden using the LSB steganography technique. By employing Brotli compression, the size of the data is reduced, resulting in minimized storage requirements and faster data transmission.

In the third layer, the AES key, which is necessary for decryption, is encoded using the LSB technique. This process enables the AES key to be concealed within the cover object without significantly altering its visual appearance or quality. This approach provides the confidentiality and integrity of the data during transmission and storage in the cloud environment.

As part of the proposed security model, a redundant copy of the data is stored in a separate location to ensure that data can be restored in the event of data loss. The backup strategy employed may vary depending on the user's preferences and settings. This can include different types of backups such as full backups, incremental backups, or other backup methodologies. By implementing an appropriate backup strategy, the model ensures that data can be recovered and restored effectively, minimizing the risk of permanent data loss and ensuring data availability and continuity. The proposed methodology, illustrated in Figure 1 (see in Appendix), involves several steps, which are explained as follows:

- In the sender stage, the AES key is generated.
- Encrypt the secret text using the generated (AES) key.
- Encrypt the cipher text and generated (AES) key using The Rivest-Shamir- Adleman (RSA) key.
- Compress the cipher text using the Brotli method.
- Hide the encrypted AES key and compressed cipher text in a cover image.
- The stego image is backed up by any backup methodologies.
- The stego image is sent to the receiver.
- In the receiver stage, the cipher text is extracted from the stego image.
- Decompress the ciper text.
- Using (RSA) key to decrypt the (AES) key.
- Using the (AES) key to decrypt the secret text.

5. RESULT AND DISCUSSION

Our evaluation strategy for assessing an artifact is an ex-ante evaluation, which involves assessing the artifact prior to its use and without testing it in a real-world context. This approach uses hypothetical or theoretical scenarios rather than practical experiences to evaluate the artifact [15]. Access time and the processing speed rate of the AES and Rivest–Shamir–Adleman algorithms were utilised to evaluate the proposed model. To perform encryption and decryption, it was necessary to install various Python libraries, like AES, NumPy, RSA, CV, Cryptodome, PIL and Matplotlib, which provided the required helper algorithms. These libraries were installed using pip, and installing them enabled us to access the necessary functions and algorithms to carry out the encryption and decryption processes effectively.

In our proposed model, we had to hold the text message in an image file, from where we could encrypt a text message using AES and RSA techniques. Next, we applied the Brotli compression technique to compress the encrypted message before using LSB steganography to embed the compressed data back into the image. This process allowed us to transmit the message securely while concealing it within the image, thus providing an additional layer of security to the communication.

Our approach involved implementing AES encryption as the first step in our process. By using this technique, we were able to generate ciphertext from the text message, effectively converting it into an unreadable form. After the encryption stage, the result was the generation of an AES ciphertext. Decryption of this ciphertext is only possible through the use of the secret AES key. This condition ensured that the encrypted message remained secure and protected from unauthorised access until the correct key was used to decrypt it.

The proposed model employs the AES-256 encryption algorithm, which undergoes 14 conversion rounds. Unlike RSA, AES only requires a single secret key for both encryption and decryption, which results in lower computational demands and faster execution. This makes AES a more efficient choice for the proposed model. As part of the cryptography process, the secret information was encrypted using the public key of the RSA, and the corresponding private key was utilised to decrypt the encrypted information. The RSA encryption algorithm is slower than AES due to its computationally intensive asymmetric approach and the need to perform complex mathematical operations such as prime factorisation. By contrast, AES is designed to use a symmetric key and has been optimised for both hardware and software implementations, resulting in faster and more efficient encryption and decryption of large quantities of data.

The RSA encryption algorithm is reliant on the challenge of factoring large integer numbers since the equation $n = p * q$ most holds, where p and q are prime numbers and n is a shared component of the public and private keys, as shown in (1):

$$n = p * q \tag{1}$$

with the public keypair (n, e) provided, it is feasible to compute the corresponding private keypair (n, d), as shown in (2):

$$d = e^{-1} \, mod \, \phi \, (n) \tag{2}$$

the formula used to convert plain text into a cipher message is as shown in (3):

$$C = M^e \, mod \, (n) \tag{3}$$

likewise, the formula used to convert a cipher message back to plain text is as shown in (4).

$$M = C^e \, mod \, (n) \tag{4}$$

After attempting to encrypt our confidential text message using RSA, we received an error message indicating that the message was too long. To address this issue, we decided to encrypt the already encrypted text using another encryption method, that is, AES. Upon further investigation, we found that the RSA encryption process was taking longer than expected, likely due to the larger message size. Given that increasing the security level typically requires more time for both encryption and decryption, we opted for a hybrid encryption approach that combines both AES and RSA encryption as part of our overall security architecture.

To resolve the problem of the large message size, we proposed to add a compression layer using Brotli method to reduce the size of the message and thus improve the performance of the model. It is designed to provide better compression ratios while still maintaining fast decompression speeds. Brotli works by identifying and eliminating redundancy in the data being compressed. For example, it will use information about the frequency of characters and character sequences to optimise the encoding process. Once the dictionaries and context models have been created, Brotli uses a combination of Huffman coding and a static arithmetic coder to compress the data. The compressed data are then split into a series of blocks and written to the output stream. During decompression, the compressed data are read from the input stream and the reverse process is used to reconstruct the original data. Static and dynamic dictionaries are used to optimise the decoding process.

To increase the level of encryption, we opted to conceal the message by distributing it across different distinct images, each having different sizes and colour scales. We hid the message within the image pixels using the LSB steganography method. Each pixel is comprised of three values: Red, Green and Blue. Histograms of the encoded and decoded images were generated to analyse any changes in the RGB pixel values.

Tables 1-3 collectively provide a comprehensive performance analysis of the proposed system. In Table 1 outlines the time spent on encryption, compression, and steganography in the sender stage, Table 2 elaborates on the time required for decryption, decompression, and steganography in the receiver stage. Table 3 summarizes these findings, presenting an integrated view of response times across both sender and receiver stages, effectively capturing the temporal behavior for each cover image.

Table 4 displays histograms of cover and stego images, showing minimal distortion and identical histograms. The histograms of both types of images are almost identical, indicating that the embedding process did not result in significant distortion. The difference between the histograms is also minimal and not detectable by the human eye. To achieve this, we first generated a histogram of the cover image without any data being embedded. Next, we encrypted and compressed a secret message using our proposed model and embedded the resulting compressed message in the LSB of the cover image. The histograms for the cover image, stego image and the difference between them are presented in Table 4.

Table 1. Response time of the proposed system performance (sender stage)

Cover image	Size of cover image	Encryption time		Compression time	Steganography time	Total time
		AES time	RSA time	Brotli time	LSB time	
CoverImage1	1.5	0.02189	0.49240	0.165	0.09	0.76929
CoverImage2	2.3	0.12583	0.52639	0.202	0.09	0.94422
CoverImage3	9.2	0.31721	0.82310	0.621	0.10	1.54410

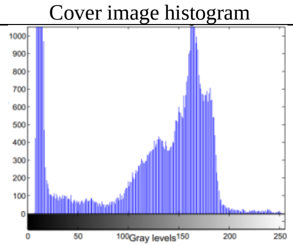
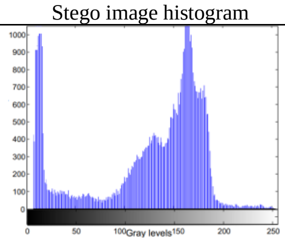
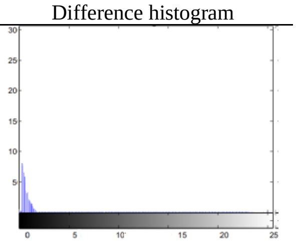
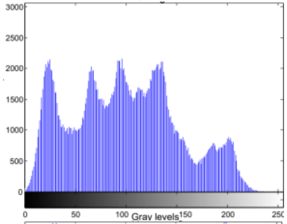
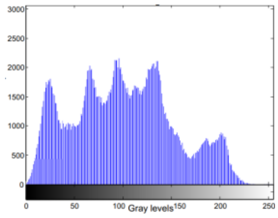
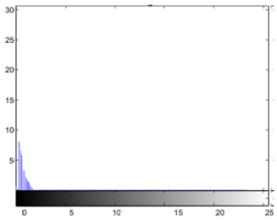
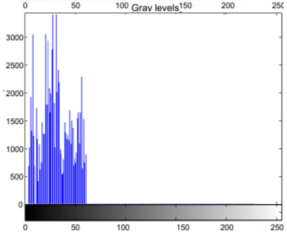
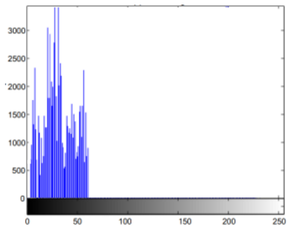
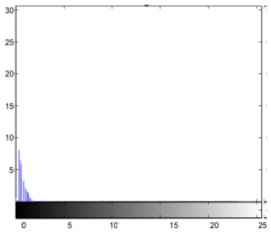
Table 2. Response time of the proposed system performance (receiver stage)

Cover image	Size of cover image	Decryption time		Decompression time	Steganography time	Total time
		AES time	RSA time	Brotli time	LSB time	
CoverImage1	1.5	0.00126	0.00281	0.001	0.09	0.09507
CoverImage2	2.3	0.00289	0.00438	0.003	0.09	0.10027
CoverImage3	9.2	0.08281	0.09330	0.008	0.10	0.28411

Table 3. Total response time of the proposed system performance

Cover image	Size of cover image	Time of sender stage	Time of reciver stage	Total time
CoverImage1	1.5	0.76929	0.09507	0.86436
CoverImage2	2.3	0.94422	0.10027	1.04449
CoverImage3	9.2	1.54410	0.28411	1.82821

Table 4. Histograms of cover and stego images and difference of the histograms

Cover image	Cover image histogram	Stego image histogram	Difference histogram
			
			
			

6. CONCLUSION

The combination of encryption and steganography techniques presented in this study has effectively improved the security of cloud-stored data. The proposed model consists of multiple layers and utilises both AES symmetric and RSA asymmetric encryption algorithms to enhance the efficiency and security of the data.

Additionally, the Brotli compression algorithm is utilised to improve the efficiency of data transmission in cloud, followed by concealing the compressed data within an image using the LSB steganography technique. Results demonstrate that compared to data concealment without compression the proposed model significantly increases the amount of data that can be hidden within an image using LSB while minimising image distortion. The suggested model is highly adaptable, flexible and efficient in securing cloud data, thus preserving the confidentiality, privacy and integrity of the data. Overall, this study achieves its security objectives of protecting cloud data. However, further research is necessary to enhance the amalgamation of methods and bolster security protocols for multimedia data in the coming years.

APPENDIX

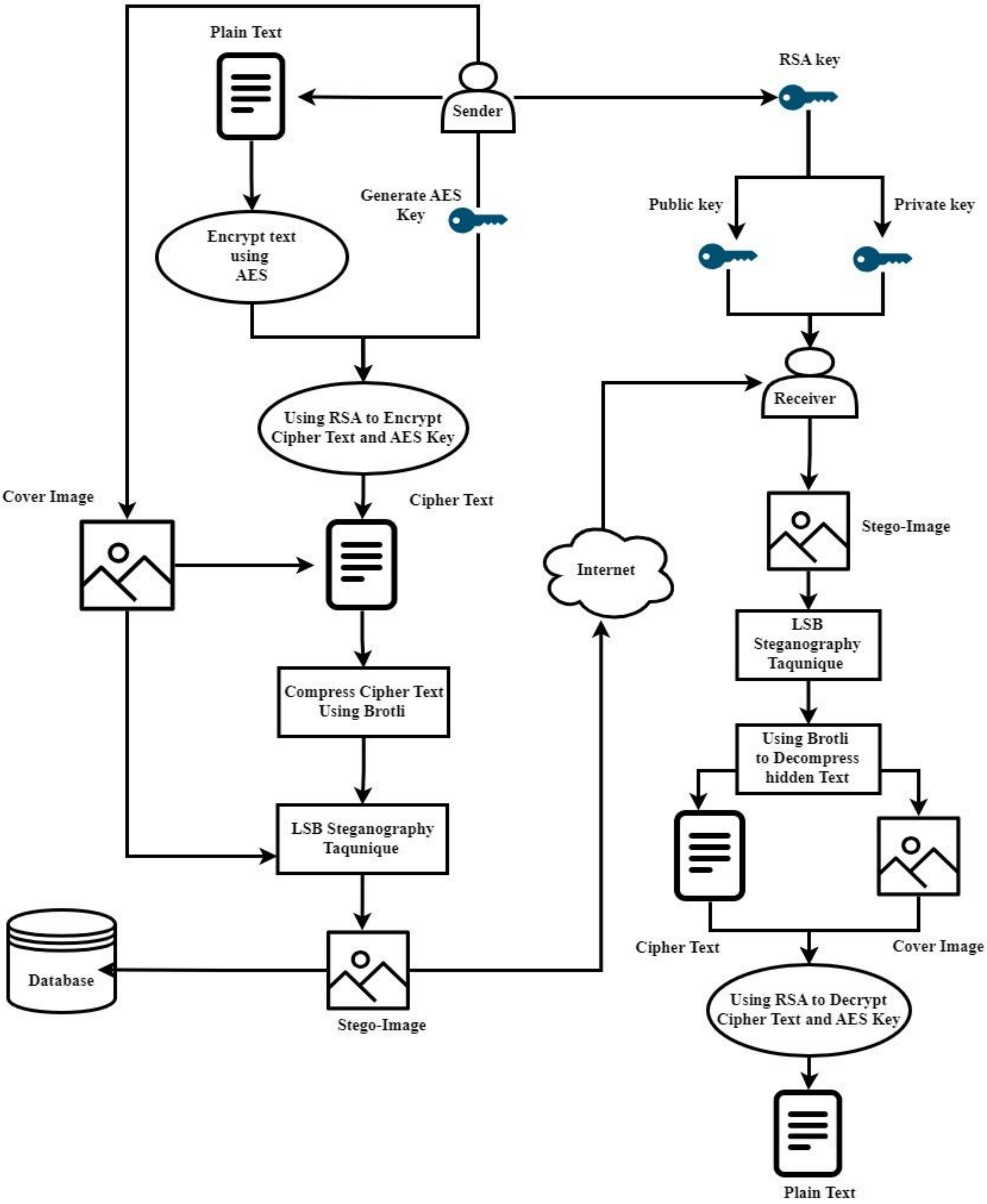

Plain Text
Sender
RSA key
Generate AES Key
Public key
Private key
Encrypt text using AES
Receiver
Using RSA to Encrypt Cipher Text and AES Key
Cover Image
Cipher Text
Stego-Image
Internet
LSB Steganography Taqunique
Compress Cipher Text Using Brotli
Using Brotli to Decompress hidden Text
LSB Steganography Taqunique
Cipher Text
Cover Image
Database
Stego-Image
Using RSA to Decrypt Cipher Text and AES Key
Plain Text

Figure 1. Proposed method

REFERENCES

[1] K. Hamid, M. W. Iqbal, Q. Abbas, M. Arif, A. Brezulianu, and O. Geman, "Cloud computing network empowered by modern topological invariants," *Applied Sciences (Switzerland)*, vol. 13, no. 3, p. 1399, Jan. 2023, doi: 10.3390/app13031399.

[2] W. A. Awadh, A. S. Hashim, and A. K. Hamoud, "A review on internet of things architecture for big data processing," *Iraqi Journal for Computers and Informatics*, vol. 46, no. 1, pp. 11–19, Jun. 2020, doi: 10.25195/ijci.v46i1.245.

[3] W. A. Awadh, A. S. Hashim, and A. Hamoud, "A review of various steganography techniques in cloud computing," *University of Thi-Qar Journal of Science*, vol. 7, pp. 113–119, May 2019, doi: 10.32792/utq/utjsci/vol7/1/19.

[4] I. A. Najm *et al.*, "OLAP mining with educational data mart to predict students' performance," *Informatica (Slovenia)*, vol. 46, no. 5, pp. 11–19, Mar. 2022, doi: 10.31449/inf.v46i5.3853.

[5] M. K, M. Laxmaiah, and Y. K. Sharma, "A comparative study on Google app engine Amazon web services and Microsoft Windows Azure," *International Journal of Computer Engineering and Technology*, vol. 10, no. 1, Jan. 2019, doi: 10.34218/ijcet.10.1.2019.007.

[6] B. Gupta, P. Mittal, and T. Mufti, "A review on Amazon web service (AWS), Microsoft Azure and Google cloud platform (GCP) services," *In Proceedings of the 2nd International Conference on ICT for Digital, Smart, and Sustainable Development, ICIDSSD 2020, Jamia Hamdard, New Delhi, India,* 2021, doi: 10.4108/eai.27-2-2020.2303255.

[7] M. O. Ogbole, E. A. L. Ogbole, and A. Olagesin, "Cloud systems and applications : a review," *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, pp. 142–149, Feb. 2021, doi: 10.32628/cseit217131.

[8] S. M. J. Islam, Z. H. Chaudhury, and S. Islam, "A simple and secured cryptography system of cloud computing," in *2019 IEEE Canadian Conference of Electrical and Computer Engineering, CCECE 2019*, May 2019, pp. 1–3, doi: 10.1109/CCECE.2019.8861845.

[9] P. Chinnasamy, S. Padmavathi, R. Swathy, and S. Rakesh, "Efficient data security using hybrid cryptography on cloud computing," in *Lecture Notes in Networks and Systems*, vol. 145, 2021, pp. 537–547, doi: 10.1007/978-981-15-7345-3_46.

[10] A. Sanghi, S. Chaudhary, and M. Dave, "Enhance the data security in cloud computing by text steganography," in *Lecture Notes in Networks and Systems*, vol. 18, 2018, pp. 241–248, doi: 10.1007/978-981-10-6916-1_22.

[11] A. Sarkar, S. R. Chatterjee, and M. Chakraborty, "Role of cryptography in network security," in *Lecture Notes in Networks and Systems*, vol. 163, 2021, pp. 103–143, doi: 10.1007/978-981-15-9317-8_5.

[12] W. A. Awadh, A. S. Alasady, and A. K. Hamoud, "Efficiently secure data communications based on CBC-RC6 and the overflow Field of Timestamp option in an IPv4 packet," *Informatica (Slovenia)*, vol. 46, no. 6, pp. 125–133, Sep. 2022, doi: 10.31449/inf.v46i6.4005.

[13] R. Shanthakumari and S. Malliga, "Dual-layer security of image steganography based on IDEA and LSBG algorithm in the cloud environment," *Sadhana - Academy Proceedings in Engineering Sciences*, vol. 44, no. 5, p. 119, May 2019, doi: 10.1007/s12046-019-1106-0.

[14] C. L. Stergiou, A. P. Plageras, K. E. Psannis, and B. B. Gupta, "Secure machine learning scenario from big data in cloud computing via internet of things network," in *Handbook of Computer Networks and Cyber Security: Principles and Paradigms*, Cham: Springer International Publishing, 2019, pp. 525–554.

[15] P. Kumar and R. Kumar, "Issues and challenges of load balancing techniques in cloud computing: A survey," *ACM Computing Surveys*, vol. 51, no. 6, pp. 1–35, Nov. 2019, doi: 10.1145/3281010.

[16] R. Adee and H. Mouratidis, "A dynamic four-step data security model for data in cloud computing based on cryptography and steganography," *Sensors*, vol. 22, no. 3, p. 1109, Feb. 2022, doi: 10.3390/s22031109.

[17] S. S. Ghuge, N. Kumar, S. Savitha, and V. Suraj, "Multilayer technique to secure data transfer in private cloud for SaaS applications," in *2nd International Conference on Innovative Mechanisms for Industry Applications, ICIMIA 2020 - Conference Proceedings*, Mar. 2020, pp. 646–651, doi: 10.1109/ICIMIA48430.2020.9074969.

[18] L. Kumar and N. Badal, "A review on hybrid encryption in cloud computing," in *Proceedings - 2019 4th International Conference on Internet of Things: Smart Innovation and Usages, IoT-SIU 2019*, Apr. 2019, pp. 1–6, doi: 10.1109/IoT-SIU.2019.8777503.

[19] R. Denis and P. Madhubala, "Evolutionary computing assisted visually-imperceptible hybrid cryptography and steganography model for secure data communication over cloud environment," *International Journal of Computer Networks and Applications*, vol. 7, no. 6, pp. 208–230, Dec. 2020, doi: 10.22247/ijcna/2020/205321.

[20] V. Reynaldo, A. Wicaksana, and S. Hansun, "Brotli data compression on moodle-based E-learning server," *ICIC Express Letters, Part B: Applications*, vol. 10, no. 11, pp. 963–970, 2019, doi: 10.24507/icicelb.10.11.963.

[21] C. M. Mohammed and S. R. M. Zeebaree, "Sufficient comparison among cloud computing services: IaaS, PaaS, and SaaS: a review," *International Journal of Science and Business*, vol. 5, no. 2, pp. 17–30, 2021.

[22] B. Seth, S. Dalal, V. Jaglan, D. Le, S. Mohan, and G. Srivastava, "Integrating encryption techniques for secure data storage in the cloud," *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 4, Apr. 2022, doi: 10.1002/ett.4108.

[23] H. R. Shakir and S. A. Yassir, "Image encryption-compression method based on playfair, OTP and DWT for secure image transmission," in *Communications in Computer and Information Science*, vol. 1487 CCIS, pp. 95–113, 2021, doi: 10.1007/978-981-16-8059-5_7.

[24] M. Kaur and V. Kumar, "A comprehensive review on image encryption techniques," *Archives of Computational Methods in Engineering*, vol. 27, no. 1, pp. 15–43, Jan. 2020, doi: 10.1007/s11831-018-9298-8.

[25] Q. Zhang, "An overview and analysis of hybrid encryption: The combination of symmetric encryption and asymmetric encryption," in *Proceedings - 2021 2nd International Conference on Computing and Data Science, CDS 2021*, Jan. 2021, pp. 616–622, doi: 10.1109/CDS52072.2021.00111.

[26] O. Hosam and M. H. Ahmad, "Hybrid design for cloud data security using combination of AES, ECC and LSB steganography," *International Journal of Computational Science and Engineering*, vol. 19, no. 2, pp. 153–161, 2019, doi: 10.1504/IJCSE.2019.100236.

[27] M. M. Yahaya and A. Ajibola, "Cryptosystem for secure data transmission using advance encryption standard (AES) and steganography," *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, pp. 317–322, Dec. 2019, doi: 10.32628/cseit195659.

[28] H. T. Sihotang, S. Efendi, E. M. Zamzami, and H. Mawengkang, "Design and implementation of Rivest Shamir Adleman's (RSA) cryptography algorithm in text file data security," *Journal of Physics: Conference Series*, vol. 1641, no. 1, p. 012042, Nov. 2020, doi: 10.1088/1742-6596/1641/1/012042.

[29] R. Yudistira, "AES (Advanced Encryption Standard) and RSA (Rivest–Shamir–Adleman) encryption on digital signature document: A literature review," *International Journal of Information Technology and Business*, vol. 2, no. 2, pp. 26–29, 2020.

[30] J. Wei, W. Liu, and X. Hu, "Secure data sharing in cloud computing using revocable-storage identity-based encryption," *IEEE Transactions on Cloud Computing*, vol. 6, no. 4, pp. 1136–1148, Oct. 2018, doi: 10.1109/TCC.2016.2545668.

[31] A. Gupta and S. Nigam, "A review on different types of lossless data compression techniques," *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, pp. 50–56, Jan. 2021, doi: 10.32628/CSEIT217113.

[32] W. A. Awadh, A. S. Alasady, and A. K. Hamoud, "Hybrid information security system via combination of compression, cryptography, and image steganography," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 12, no. 6, pp. 6574–6584, Dec. 2022, doi: 10.11591/ijece.v12i6.pp6574-6584.

[33] R. N. Aher and M. Pande, "Analysis of lossless data compression algorithm in columnar data warehouse," in *2022 6th International Conference on Computing, Communication, Control and Automation, ICCUBEA 2022*, Aug. 2022, pp. 1–4, doi: 10.1109/ICCUBEA54992.2022.10010925.

[34] A. Jan, S. A. Parah, M. Hussan, and B. A. Malik, "Double layer security using crypto-stego techniques: a comprehensive review," *Health and Technology*, vol. 12, no. 1, pp. 9–31, Jan. 2022, doi: 10.1007/s12553-021-00602-1.

BIOGRAPHIES OF AUTHORS

Wid Akeel Awadh was born in Basrah, Iraq in 1984. She earned a bachelor's degree in Computer Science from Basrah University in 2006 and a master's degree in the same area from the same university in 2012. She is working as a lecturer in the Department of Computer Information Systems, Computer Science and Information Technology College, Basrah University, Iraq. She has sixteen papers in the field of computer science (information security and data mining cloud computing). She can be contacted at email: wid.jawad@uobasrah.edu.iq.

Ali Salah Alasady was born in Basrah, Iraq in 1985. He earned a bachelor's degree in Computer Science from Basrah University in 2007 and a master's degree in the Information Technology field from the Tenaga University, Malaysia in 2014. He is working as a lecturer in the Department of Computer Science, Computer Science and Information Technology College, Basrah University. He has sixteen papers in the field of computer science (information security and data mining and cloud computing). He can be contacted at email: alis.hashim@uobasrah.edu.iq.

Mohammed S. Hashim was born in Basrah, Iraq in 1995. He earned a bachelor's degree in Computer Science from Basrah University in 2017 and a master's degree in the same area from the same university in 2023. He is working as a lecturer in the Department of Computer Science, Education College for Pure Sciences, Basrah University. He has three papers in the field of computer science (data mining and artificial intelligence). He can be contacted at email: moh.salah@uobasrah.edu.iq.