ISSN: 0974-8571 Vol.13 No. 2 December, 2021

International Journal of Computational Intelligence in Control

Hybrid Encryption Technology for Secure File Storage in Cloud Computing

[1] **Srinivasan Thiruvengadam**, Ph.D Research Scholar, PG & Research Department of Computer Science, Christhu Raj College (Affiliated to Bharathidasan University, Tiruchirappalli), Panjapur, Trichy, Tamilnadu. Email: sthiru81@gmail.com Mobile: 9080205842

[2]**Dr. Ramalingam sugumar**, Professor & Director, PG & Research Department of Computer Science, Christhu Raj College (Affiliated to Bharathidasan University, Tiruchirappalli), Panjapur, Trichy, Tamilnadu. Email:rsugusakthi1974@gmail.comMobile: 9944221562

Received: 26th September 2021
Revised: 19th October 2021
Accepted: 17th November 2021

Abstract: Cloud technology has been used in several fields, manufacturing and defense academies, to supply massive amounts of information. Information extracted from the cloud at the request of the customer. A number of challenges should be resolved in order to keep information in the system. To save data in the cloud, several challenges need to be addressed. A number of techniques could be used in conflict resolution. In this article, we proposed a hybrid Steganography and encryptionmethod for data security. In Internet applications, the use of an optimal solution was not suitable for high-level information protection. We introduced a new security technique on symmetric key cryptography and Steganography. Rivest cipher 6 (RC6), Advanced Encryption Standard (AES), Byte Rotation Algorithm (BRA) and blowfish techniques to provide block safety information andthe length of the technical key was 128 bits. A critical data security, Least Signification Bit (LSB)Steganography algorithm was applied. A document was allocated to eight sections. The multiprocessing method secures all of the document's sections at the same moment. Data encryption keys were built into the primary image using the LSB technique. Steganography imagewas emailed to an appropriate recipient. The Reverse Cryptography procedure should be used for document decoding. This proposed method gives more security to data, documents or files duringthe multi-processor.

Keywords: Cloud technology; Safety; Cryptography; Stego image; Least Significant Bit

1. Introduction

The encoding method converts real data into an unintelligible form. There are two types of encryption methods: symmetric code decryption and shared key encryption. One technique employs variables to transform the data into an unintelligible structure. Consequently, the authorized individual has access to the information stored on the internet platform [1]. A document was visible to everyone. International Data Encryption Algorithm (IDEA), Triple Data EncryptionStandard (3DES), AES, blowfish, BRA and Data Encryption Standard (DES) were symmetrical

key cryptography methods. The biggest problem was having the secret for the user in a multi- processor program [2-5]. The technique provides a low decoding time of information and encryption have a low level of protection. RSA and ECC algorithms are used for public key cryptography. In symmetrical encryption techniques, the public and private keys were combined. These methods provided a large amount of security, but increased the time required to encode and decode the information [6]. Steganography conceals the appearance of secretive information in a package. The availability of information is not obvious for all with this method. Information was only available to the intended recipient. Textual Steganography technology should be used to ensure data safety.

The client's private data is hidden in a message cover picture [7]. When you add text to a messagecover image, it looks like a normal text document. If an unauthorized individual discovers a Worddocument, sensitive information cannot be accessed. If an unauthorized person tries to restore actual information, considerable time was needed. Word has been encrypted and decoded using DES algorithm. Text stenography has the advantage of allowing word privacy. In contrast with image Steganography, word Steganography requires the smallest amount of space [8]. For imagingSteganography, the 3-bit LSB approach has been used [9]. Sensitive customer information was hidden behind the coverage image. It hide a large amount of information in an image using LSB cryptographic technology. The encryption algorithm [10] was executed in a high bandwidth design. AES employs symmetric keys to encrypt information. It supports three major kinds of secrets. It takes 12 turns a 192-bit key, 14 turns at a 256-bit key, and 10 turns, a 128-bit key. Cryptography or decoding timing was less than the enhanced AES method. The modified AES system was able to achieve a significant reduction in time.

It uses a specific key for decoding and encrypting messages. The key was 128 bits long. A methodology, many steps were performed arbitrarily so that an unauthorized consumer could evenassume the steps of a method [11]. One of the benefits of symmetric key cryptography techniqueswas their broadband. The enhanced DES algorithm uses a key size of 112 bits to encode and decodedata. Two keys are used for data encryption. The 128-bit result of the DES method was divided into two halves. For encrypting and decrypting, the 3DES method requires a considerable amountof time. In comparison to DES and 3DES, the enhanced DES algorithm could provide superior efficiency. One byte at a time was used for name-dependent cryptographic algorithms. It uses a personal key to encrypt and decode data [12]. The method of producing symmetric keys was used for authentication performed. It protects the privacy of the data. As it runs on a single byte per duration, this technique has a significant maximum duration to turn the information into an encrypted message. To address data processing and security problems, the author has developed aspecial security framework. Private and public cloud storage containers have been used in this strategy to enhance data security [13].

2. Related Works

In the private cloud, secure information is stored, while in the public cloud, unnecessary information is stored. As a public cloud, everyone can use it. The main motivation for it is to savemoney on storage. A private cloud has more security than a public cloud [14]. The source file is subdivided into multiple sections. Each component of the document has been encrypted and storedon a wide range of clouds. For encryption purposes, the document data was stored on a remote server [15]. If the hacker attempts to regain the word document, he would only obtain a portion ofit. To achieve a high level of protection, the Elliptical Curve Cryptography (ECC) algorithm is used. Access control and content management should be utilized to address key management issues. For encoding and decoding documents, the ECC technique computes the maximum time. The AES technique is used to transform the document into a non-detectable form. The file is encoded and stored in the cloud [16]. The AES algorithm is less secure compared to methods thatuse a shared key.

To achieve confidentiality, the AES and 3DES techniques were combined into a hybrid method. It would be more difficult for hackers to get a client's private document back. It takes several hours to convert information into decoder and encoding formats. In the current system, one method is used to encode and decrypt information. However, the use of a single method does not offer a highdegree of safety [17]. We have a security problem if they use a single symmetrical key cryptography technique since the types of technology use a separate key for encoding and decoding information. Therefore, when exchanging a key in a multi-access scenario, there is a secret communication issue. Although public key encryption techniques offer good protection, they need less time to encrypt and decode information [18]. To address the above vulnerabilities, we implemented a new security system.

The AES and Rivest–Shamir–Adleman (RSA) algorithms were combined in the optimization technique. A key is required for the AES technique. Three controls are used for the proposed methodology. Information sent over the

Internet requires an AES secret key and an RSA public key [19]. It needs an RSA secret key and AES private keys to extract information from the device.When they try to upload information to the server, the document must first be saved in a subdirectory for a short period. The AES technique is used on the document first, followed by the RSA technique for numeric information [20]. A reverse method of encryption is used. The document was decoded and stored on a remote server after the application of the keys. Data validation, security, transparency and extensibility were advantages of mixed technology. The drawback of the RSA algorithm is that it encodes and decodes long-term information. The asymmetric method would be used to code and decode fragment-level data in cloud-based technologies. It was 256 bits long. The information has undergone a rotation to ensure a high levelof protection [21]. For information safety, a hash value is generated. Hash valuesare computed after cryptography and prior to decoding. The information was accurate if the two hash codes werethe same.

Only authorized users could access cloud-based information within this security paradigm. Reliability, security and confidentiality are all advantages of a security framework. The hybrid approach is used for all three procedures. Digital signatures have been used for multi-factor management [22]. To obtain proper information secret, the Blowfish method was used. [23] This is an asymmetrical approach. The Blowfish approach takes a significant amount of time to encodeand decode. The subkey collection concept was computed using the blowfish approach. [24,25] It's a technique for encrypting data at the central level. A combination product's main purpose is to improve information security when transferring and retrieving data to the internet. Cloud servers, secrecy, or identification are all addressed by the hybrid technique.

3. Proposed system architecture

As shown in Figure 1, the cloud proprietor and cloud user are part of the network infrastructure. The information is updated on the internet platform through the internet operator. A document was separate to octets. the multiprocessing method, each component to the document was encrypted at the same duration. On a cloud platform, the encoded file is saved. The cryptographic keys were kept in the cover image. The multiprocessing scenario was proposed as an internet application. Aallows several clients to view files stored on the cloud platform. On document demand, the clientalso receives a Steganography image through email, which contains crucial data. The document was decoded using the inverse procedure.

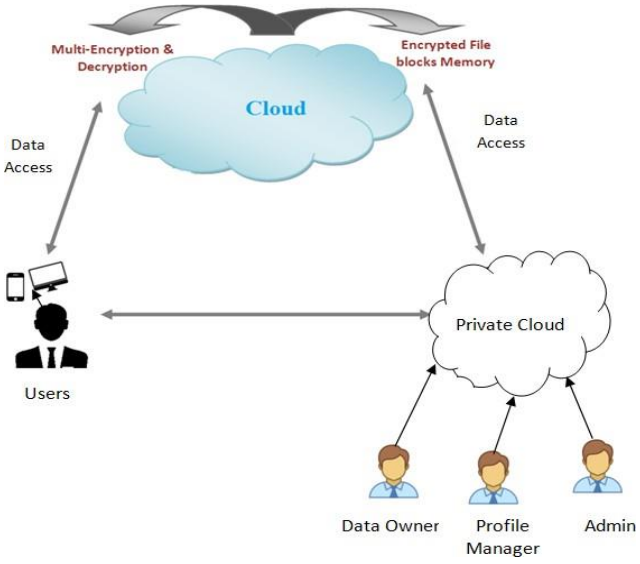


Figure 1: Overall design of the system.

3DES is a significantly improved version of DES in cryptography. DES was being used three times in the 3DES algorithm to boost secure communication. As a result, 3DES would continue to be aflexible cryptography standard in the future is shown in Figure 2.

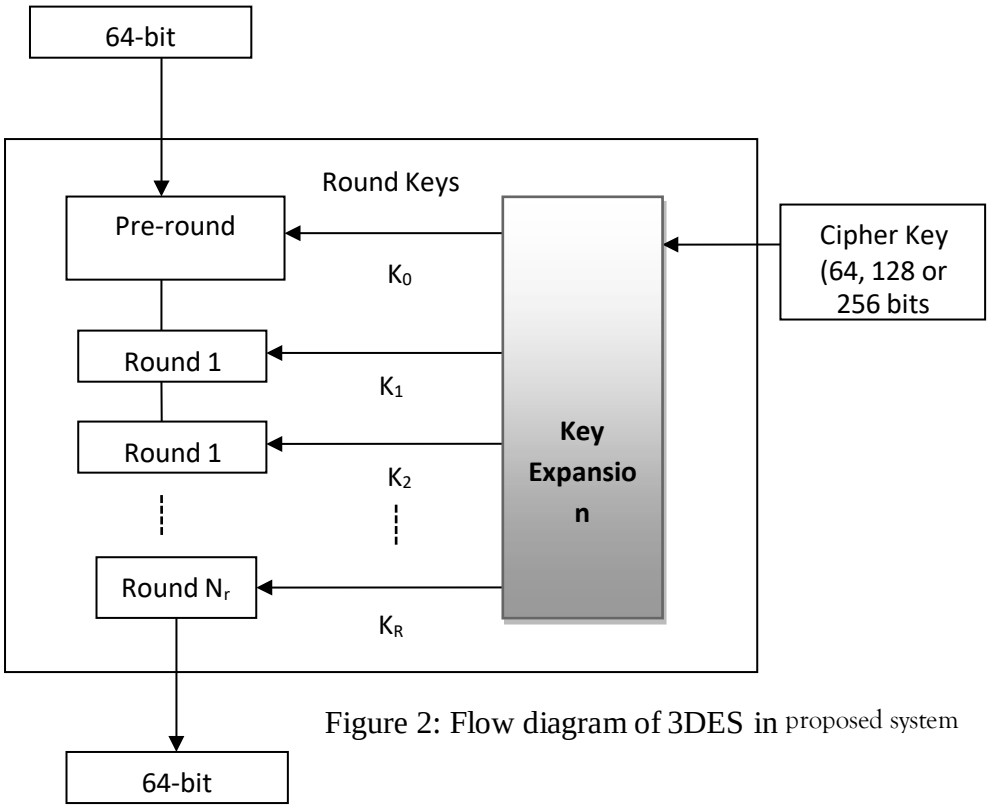
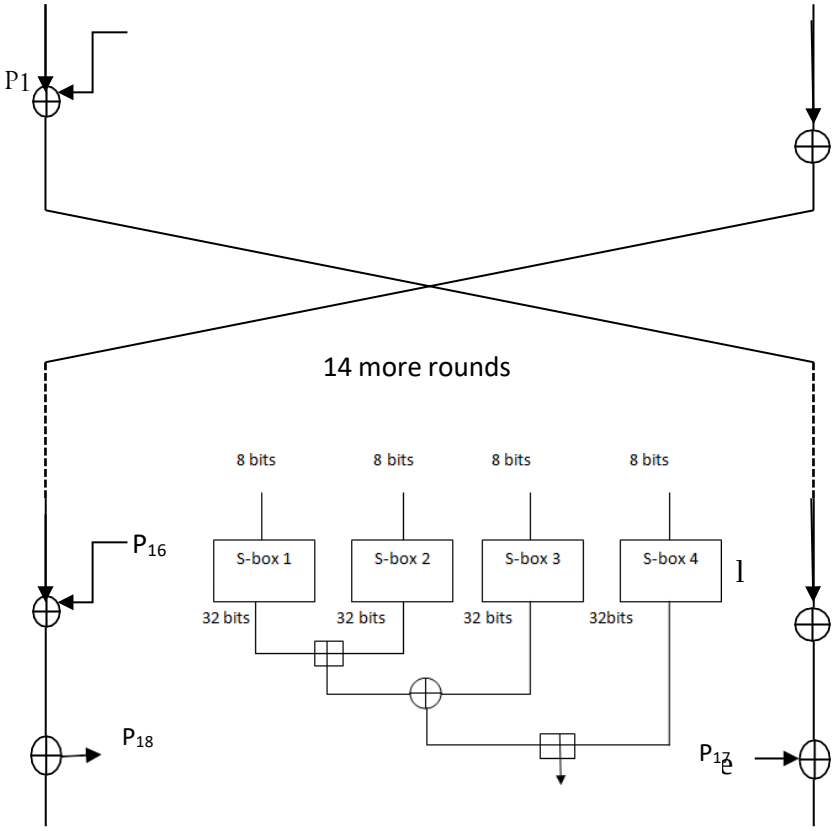


Figure 2: Flow diagram of 3DES in proposed system

After the agreement is created, the Blowfish method would be used to completely encode it to create a secure network. The Blowfish algorithm, created by Bruce Schneier in 1993, is a well- known rapid private key encryption method. This application's operation was complicated, and any attacker would have a difficult time breaking it. This should cause the system secure and safe, preventing any data breaches. Blowfish uses a 64-bit packet size and a key length that could be set anywhere between 32 and 448 pieces. For encrypting and decrypting, the technique employs a 16-round Feistel cypher and massive key-dependent S-boxes. The procedure entails the following stages shown in Figure 3.



F(XL) = ((Sl[boxl] + S2[box2]) + XOR S3[box3]) + S4[box4] (1)

P-array values are collected in each session, as well as after the last session, each half to the datablock packet was XOR of the two additional unusable P-arrays shown in Figure 4.

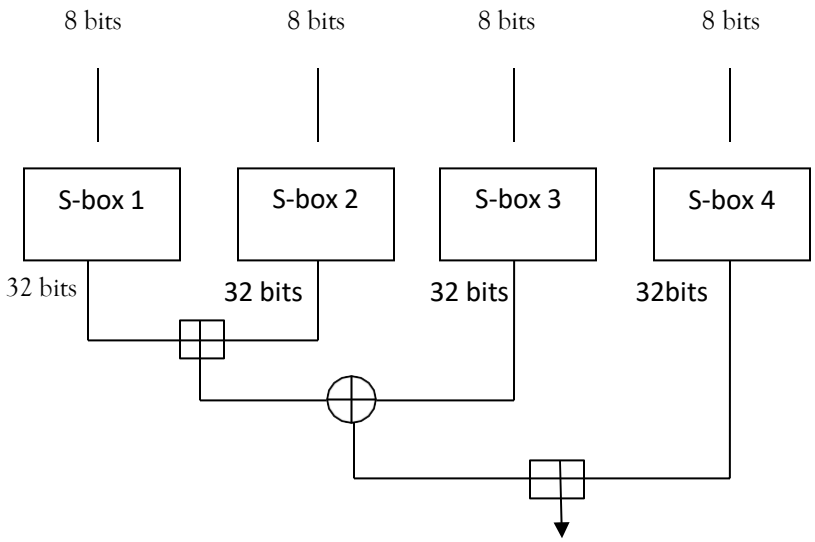


Figure 4: P-arrays architecture

Hybrid Algorithm

The proposed approach combines two techniques: RSA and Blowfish encryption. The files non- repudiation and verification are provided by RSA, while encryption and decryption were provided by Blowfish. After the contract is completed and encoded with the hybrid technique, two copies of the digital certificate were made, one for local storage and the other for uploading to the internet with the encrypted message. Documents would be deciphered using Blowfish, and digital certificates would be linked with a cloud-stored duplicate of the electronic signatures.
Step1: RSA-based key distribution method

The RSA algorithm could be used to produce the public and private keys.The stages of the
RSA method are as follows:
a.) Pick two huge arbitrary prime numbers, p, and q, at the chance. b.) Determine
n = pxq, where n is the public and private key integer.c.) Compute the Quotient:
$\phi(n) = (p-1)(q-1)$.
d.) Choose number e such that $1 < e < \phi(n)$ and e and $\phi(n)$ have no other components than 1, wheree is the public key integer.
e.) Determine d so that the equivalence connection $d \times e = 1$ modulus(n); d is the secret key integer.f.) The secret key was (n,e) and(n, d). All of the d, p, q, and phi variables must be kept hidden.
Step 2: Produce a Digital Certificate

a.) The sender uses a difficult function to construct a message digest before signing this agreement.b.) a message digest was essentially a compressed version of the original message, any hash function could be used to generate it.
Step 3: Decrypt the file.

a.) The file has become prepared to be decrypted after it has been verified.b.) The Blowfish technique is designed for cryptography.
c.) It has 16-round Feistel architecture with S-boxes that are important dependant.Step 4: Encrypt the file
Step 5: Double-checking the Digital Certificate

4. Results and Discussion

BRA, Blowfish, AES, and RC6, methods were utilized for block-wise information protection in this produced internet. A recommended network integrates Blowfish, BRA, RC6, and AES. Formal senses of the methods are symmetric-key cryptography. For document encoding and decoding, these techniques require a specific secret. The key length for all methods was 128 bits. Using the LSB method, critical information is contained in the cover picture. The proposed system is implemented using the Java programming language. Java software has been used to compute document encoding and decoding times. With a contrast of current AES and Blowfish methods, the document encodes and decode duration was determined for only text documents. The document size was provided in megabytes for the AES technique is 4 megabytes, 8 megabytes, 2 megabytes, and 1 megabyte respectively. Following file sizes are used to calculate encode and decode times for the blowfish algorithm: 200KB, 800KB, 100KB, and 400KB the time spent decoding and encoding was measured in seconds.
Figure 5 shows the proposed process for encoding the most effort-intensive files. the proposed system, a number of symmetrical key cryptographic methods are used at the same time. In comparison to the conventional method, the hybrid method uses 17-20% fewer times to process aWord document. In the cloud, a single method does not provide optimal data protection. Comparedto the hybrid approach, the current system requires 15 to 17 percent more time to encrypt documents, as shown in Figure 6. Decryption using the AES algorithm requires the least amount of effort. But data protection is compromised. As key lengths or turn counts in AES increase, the encoding and decoding time also improves.

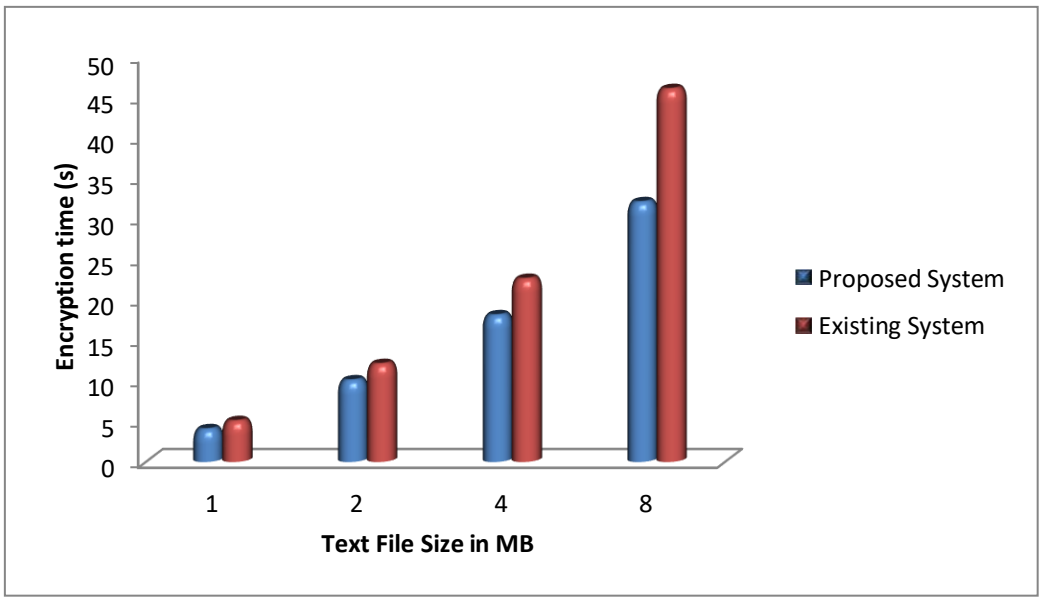
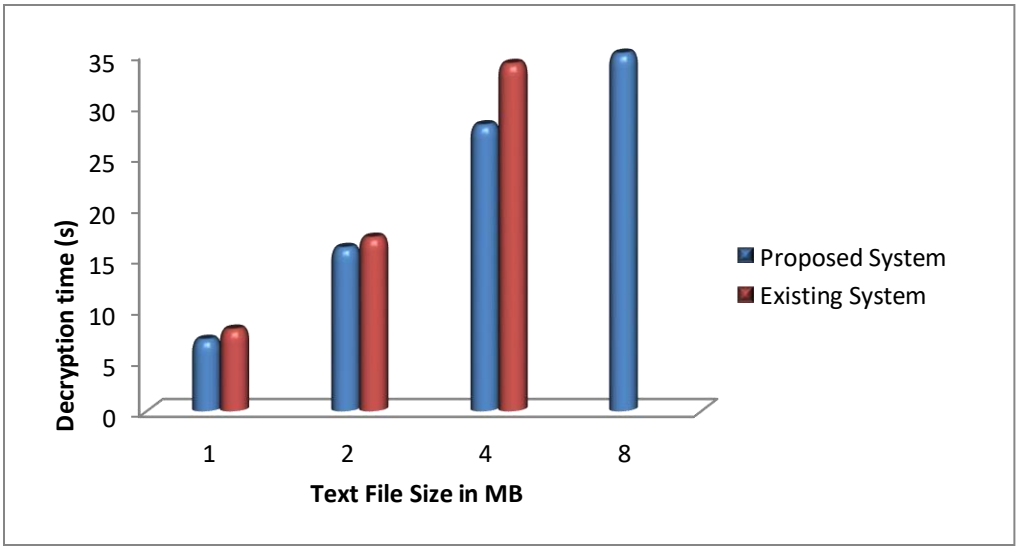


Figure 5: Encryption time comparison of Proposed with AES

Blowfish requires the shortest amount of effort to secure a document as contrasted to the AES approach. In comparison to Blowfish, the proposed technique predicts 12% to 15% short duration to code the document. The proposed mixed method encodes and decodes data with one key. Compared to Blowfish, the proposed methodology takes 10-12% less time to encrypt text files, asshown in Figure 7. Compared to encryption, decrypting documents took the longest with the proposed method. Compared to the AES approach, the Blowfish process uses the quickest time to decipher textual information. When comparing cryptography, the Blowfish method takes the most time to decipher Word documents.

Figure 6: Decryption time comparison of Proposed with AES



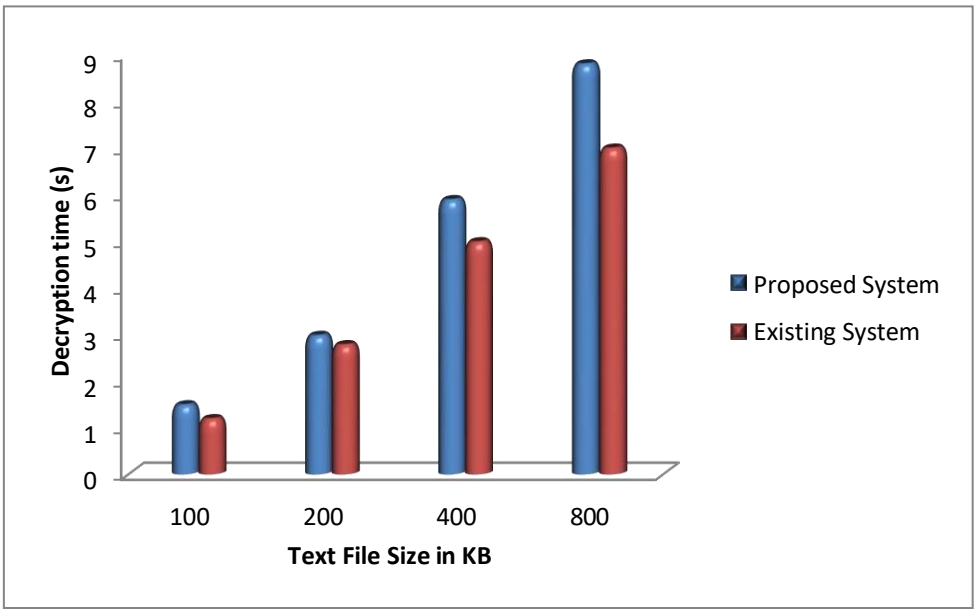


Figure 7: Encryption time comparison of Proposed with Blowfish

The method was written in Java NetBeans, and the findings were evaluated with CloudSim. For various document sizes, the following performance was achieved. The time it takes to produce digital certificates is related to the size of the file shown in Table 1. As the document size grows larger, so does the reproduction rate.

Table 1: Proposed system time taken to generate Digital signature based on file size

	Size of file (kb)	Time taken to generate the digital signature
1	20	24
2	50	24
3	100	50
4	150	110
5	200	360

The time it takes to encrypt a file using the hybrid technique is related to the file size shown in Table 2. As the size of the file grows larger, so does the time takes to decrypt it.

Table 2: Proposed system time taken to encrypt the file based on size

	Size of file (kb)	Time taken for encrypt the file
1	20	20
2	50	40
3	100	50
4	150	50
5	200	80

y -8E-07x6 + 2E-05˜˜ - 0.0003˜˜ + 0.0013˜˜ - 0.001Sx2 + 0.0009˜ + 0.7763 (2)

x represents key length of encryption and y represents encryption time in seconds

The time is taken to retrieve digital certificates was unaffected by document size shown in Table 3. It stays the same regardless of document size.

Table 3: Proposed system time taken to decrypt the file based on size

	Size of file (kb)	Time taken to decrypt the file
1	20	24
2	50	24
3	100	50
4	150	110
5	200	360

y 3E-06˜˜ - 0.0005˜˜ + 0.0594˜ - 1.433 1 (3)

x represents key length of decryption and y represents decryption time in seconds

The method that was developed would be a combination of two techniques. It may be deduced from the above data that the new Hybrid Technique was quick because it only takes a few milliseconds to encrypt and decode the message. It's also safe because the encrypted code is difficult to decipher. This is beneficial since it ensures that the new method would be both safe and speedy. Combining these two techniques offered the best of both worlds regarding public key and safety key encryption.

5. Conclusion

Cryptography and Steganography should be employed to address cloud infrastructure issues. Blowfish, RC6, BRA and AES methodologies are used to protect the data brick. LSB has been used to protect sensitive information. To ensure the integrity of the data, the SHA1 hashing algorithm is used. To find the lowest delay score, the multiple processor must be used. The proposed security protocol meets data protection, high security, minimum latency, and identification and privacy requirements. The proposal was correlated with the AES method; text document encryption

used 17-20% shorter duration. In comparison with the proposed technique, decrypting AES messages takes 15 to 17 per cent more. Compared to the recommended hybrid model, Blowfish requires 12 to 15% more to encrypt information. Compared to Blowfish's algorithm, decrypting text files using a hybrid approach takes 10% to 12% less time. In the future,combine public key cryptographic techniques to reach a tremendous level of security.

References

[1] Thabit, F., Alhomdy, S., & Jagtap, S. (2021). Security analysis and performance evaluation ofa new lightweight cryptographic algorithm for cloud computing. *Global Transitions Proceedings*, *2*(1), 100-110.

[2] Maitri, P. V., & Verma, A. (2016, March). Secure file storage in cloud computing using hybrid cryptography algorithm. In *2016 international conference on wireless communications, signal processing and networking (WiSPNET)* (pp. 1635-1638). IEEE.

[3] Venkatachalam, K., Prabu, P., Almutairi, A., & Abouhawwash, M. (2021). Secure biometric authentication with de-duplication on distributed cloud storage. *PeerJ Computer Science*, *7*, e569.

[4] Tripathi, S., Tiwari, R. K., Nigam, R., Gupta, N. K., & Verma, B. (2021, June). The Hybrid Cryptography for Enhancing the Data Security in Fog Computing. In *2021 10th IEEE International Conference on Communication Systems and Network Technologies (CSNT)* (pp. 766-771). IEEE.

[5] Arun, D. Y., Tekade, R. P., Agalave, R. K., Sanjay, S. S., & Dhage, M. R. (2021). SECURE STORAGE AT CLOUD WITH DUPLICATION-CHECKING. *INTERNATIONAL JOURNAL*, *5*(12).

[6] Pant, V. K., Prakash, J., & Asthana, A. (2015, October). Three step data security model for cloud computing based on RSA and steganography. In *2015 International Conference on Green Computing and Internet of Things (ICGCIoT)* (pp. 490-494). IEEE.Song, H., Li, J., & Li, H. (2021). A cloud secure storage mechanism based on data dispersionand encryption. *IEEE Access*, *9*, 63745-63751.

[7] Thabit, F., Alhomdy, S., & Jagtap, S. (2021). A new data security algorithm for cloud computing based on genetics techniques and logical-mathematical functions. *International Journal of Intelligent Networks*, *2*, 18-33.

[8] Garikipati, P., & Balamurugan, K. (2021). Abrasive Water Jet Machining Studies on AlSi 7+ 63% SiC Hybrid Composite. In *Advances in Industrial Automation and Smart Manufacturing* (pp.743-751). Springer, Singapore.

[9] Bharathi, P., Annam, G., Kandi, J. B., Duggana, V. K., & Anjali, T. (2021, July). Secure filestorage using hybrid cryptography. In *2021 6th International Conference on Communication andElectronics Systems (ICCES)* (pp. 1-6). IEEE.

[10] Aroulanandam, V. V., Latchoumi, T. P., Balamurugan, K., & Yookesh, T. L. (2020). Improving the Energy Efficiency in Mobile Ad-Hoc Network Using Learning-Based Routing. *Rev. d'Intelligence Artif.*, *34*(3), 337-343.

[11] Karati, A., Amin, R., Mohit, P., Sureshkumar, V., & Biswas, G. P. (2021). Design of secure file storage and access protocol for cloud-enabled Internet of Things environment. *Computers & Electrical Engineering*, *94*, 107298.

[12] Sharma, P., Moparthi, N. R., Namasudra, S., Shanmuganathan, V., & Hsu, C. H. (2021). Blockchain-based IoT architecture to secure healthcare systems using identity-based encryption. *Expert Systems*, e12915.

[13] Bermani, A. K., Murshedi, T. A., & Abod, Z. A. (2021). A hybrid cryptography technique fordata storage on cloud computing. *Journal of Discrete Mathematical Sciences and Cryptography*, *24*(6), 1613-1624.

[14] Nair, N., Jain, T., & Gada, M. (2021, July). Secured File Storage in Cloud Computing Application: Secura-Drive. In *2021 12th International Conference on Computing Communicationand Networking Technologies (ICCCNT)* (pp. 1-4). IEEE.

[15] Chinnasamy, P., Padmavathi, S., Swathy, R., & Rakesh, S. (2021). Efficient data security using hybrid cryptography on cloud computing. In *Inventive Communication and Computational Technologies* (pp. 537-547). Springer, Singapore.

[16] Gokulraj, S., Ananthi, P., Baby, R., & Janani, E. (2021). Secure File Storage Using Hybrid Cryptography. *Available at SSRN 3802668*.

[17] Tyagi, S. S. (2021, February). Secure Data Storage in Cloud using Encryption Algorithm. In *2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)* (pp. 136-141). IEEE.

[18] Kumar, S., Karnani, G., Gaur, M. S., & Mishra, A. (2021, April). Cloud security using hybrid cryptography algorithms. In *2021 2nd International conference on intelligent engineering and management (ICIEM)* (pp. 599-604). IEEE.

[19] Madhumala, R. B., Chhetri, S., Akshatha, K. C., & Jain, H. (2021). Secure File Storage & Sharing on Cloud Using Cryptography.

[20] Sindhura, S., Praveen, S. P., Syedbi, S., Pratap, V. K., & Krishna, T. B. M. (2021). Effectivesecure storage of data in the cloud using the ISSE encryption technique. *Annals of the Romanian Society for Cell Biology*, 5321-5329.

[21] Garikapati, Pruthviraju, Balamurugan, K., Latchoumi, T. P., Malkapuram, Ramakrishna (2021). A Cluster-Profile Comparative Study on Machining AlSi7/63% of SiC Hybrid Composite Using Agglomerative Hierarchical Clustering and K-Means. Silicon, 10.1007/s12633-020-00447-9

[22] Goyal, M., & Sharma, A. (2021, November). Implementation and Analysis of various Encryption Techniques with Blowfish on various Data Files. In *2021 International Conference on Technological Advancements and Innovations (ICTAI)* (pp. 541-546). IEEE.

[23] Khatal, S., Rane, J., Patel, D., Patel, P., & Busnel, Y. (2021). Fileshare: A blockchain and ipfsframework for secure file sharing and data provenance. In *Advances in Machine Learning and Computational Intelligence* (pp. 825-833). Springer, Singapore.

[24] Ezhilarasi, T. P., Sudheer Kumar, N., Latchoumi, T. P., & Balayesu, N. (2021). A secure datasharing using IDSS CP-ABE in cloud storage. In *Advances in Industrial Automation and Smart Manufacturing* (pp. 1073-1085). Springer, Singapore.