Al-Rafidain Journal of Computer Sciences and Mathematics (RJCM)

www.csmj.mosuljournals.com

Applying a Hybrid Encryption Algorithm in Cloud Computing

Esraa Khalid Ahmed Alobaydi[1, *], Muna M. T. Jawhar [2]

[1, 2]Department of Computer Science, College of computer science and mathematics, Mosul University, Mosul, Iraq
Emails: esraa@uomosul.edu.iq, dr.muna_taher@uomosul.edu.iq

Article information

Article history:
Received :24/10/2023
Accepted: 17/12/2023
Available online: 25/6/2024

Abstract

The rapid digital development has led to a steady increase in the use of cloud storage as a primary means of saving and sharing data and files. This development brought major challenges in the field of security and data protection, as well as the concerns related to hacking and information theft which are constantly escalating. Hence, the importance of applying strong encryption techniques to protect data saved in cloud storage. For this reason, this study explores and presents an advanced encryption strategy that combines three of the most powerful known algorithms which are Blowfish, Paillier, and AES with the aim of increasing the level of security and privacy during uploading files to the cloud storage. This research aims to provide an overview of how this process can be implemented using these nested hybrid algorithms and the potential benefits of this multi-layered approach. While these algorithms are diverse, effective, and strong in protection, which yields the contribution significantly to increasing the level of security in the field of storing sensitive data in the cloud. The obtained results showed that the hybrid algorithm gives the ability to combine different advantages of the encryption algorithms and achieve the ideal balance between strong protection and efficient performance in the field of in-cloud data protection with minimal time consumption.

Keywords:
Cloud Computing, Cryptography, Blowfish, Paillier, AES.

Correspondence:
Author: Esraa Khalid Ahmed Alobaydi
Email: esraa@uomosul.edu.iq

1. Introduction

The current observations detect an increase in threats, attacks, and electronic crimes, especially for important private and public data. Therefore, it is necessary and imperative to follow security procedures for cloud storage users to ensure the confidentiality of the data and maintain its privacy[1]. Protecting keys in cryptographic operations is critical importance in the context of storing data in the cloud and in a variety of security and privacy scenarios. Protecting the encryption keys are essential elements in the data encryption and decryption processes, if the keys being penetrated, an attacker can access and decrypt the encrypted data[2, 3] which yields security break. In addition, a high privacy is required, such as storing data of users or customers in the cloud, keys must be kept securely to prevent violating users' privacy. As well as, protecting keys contributes to preventing any unauthorized entity from accessing encrypted data. This protects the data from any internal or external security breach.

Blowfish is a free symmetric encryption algorithm, a powerful protection tool against hackers and cybercriminals that is used in a number of products including some backup encryption devices, secure email, and password programs[4][5]. Due to the small number of rounds, the researchers confirmed that the blowfish has a relatively simple structure and is one of the strongest fast encryption tools [4, 5].

The Paillier algorithm is considered one of the most important algorithms in the field of security and privacy preservation, because it combines security strength with the ability to perform mathematical operations on encrypted data and has features that make it suitable for a variety of applications [6, 7].

AES algorithm is also one of the most famous and popular encryption systems in the world [8]. It was developed to protect sensitive data and confidential information from hacking and unauthorized access. It's used in a variety of applications and fields including secure Internet communications, email encryption, securing wireless networks, database encryption, securing logistics and government information systems, and many others [9].

The paper is organized as follows: A review of previous works of researchers is contained in Section 2. An overview of the algorithms used in this paper is taken in Section 3. In Section 4, the proposed triple encryption method is presented. In Section 5, the proposed encryption and decryption algorithms are implemented. While the results obtained are explained and compared with previous works in Section 6. Finally, the conclusion is described in Section 7.

2. Related Works

Below is a look at some previous work in which researchers have used hybrid encryption algorithms. Based on the study conducted by Kamara, S. and K. Lauter [10] a security pattern was introduced that aims to protect data stored in the public cloud environment. This style is based on basic cryptographic principles to ensure data integrity. In this context, this research reviews the benefits of storing data in the cloud environment, including aspects related to reliability, availability, and availability, data sharing and efficient retrieval that collects modern and unusual cryptographic basics for secured storage in cloud. Numbers of hybrid data encryption systems were applied using multi-encryption algorithms such as homographic encryption with blowfish encryption, RSA with Blowfish, Blowfish with ECC algorithm, RSA with DES, AES with RSA[4, 8, 9, 11, 12].
Bansal and Singh said that "a mathematical methodology was used to apply the Field Programmable Gate Array which is an effective strategy gives high level of protection with low cost" [13]. But the main issue was a big size of the key (448-bits). In the research published by [14], DES and RSA algorithms were applied to obtain higher levels of encryption for sending and higher levels of decryption for receiving sides to reduce security threats. The result of this work is that data security is maximized and reduced time spent in uploading and downloading the text file to the cloud storage compared to existing systems where different text files sizes (1-Kbytes to 10-K bytes) were tested.

Other scholars evaluated three common encryption techniques (AES, Blowfish, and GOST) for different block size [15]. Ora and Pal [19] combined RSA Partial homomorphic with MD5 (message digest algorithm) hashing algorithm. Firstly, encrypt the data by RSA Partial utilizing the multiplication of two cipher text then upload to the cloud. Secondly, calculating its hash value via MD5 hashing scheme for data backup securely.

Seth, Dalal[1] applied combination of two hybrid encryption algorithms which are: Combined encryption procedures using RSA with AES algorithms and integration the Paillier with Blowfish crypto operations. The framework consisted of 4 steps first, encrypted information Storage over the cloud using hybrid technique (RSA-AES). Secondly, the second step is to store encrypted information in the cloud using RSA-AES hybrid technology, without imposing access restrictions to combat threats. In the third, encrypted information is collected in the cloud environment using Pailier-Blowfish encryption without applying compression operations. As for the fourth, encrypted data is collected in the cloud using Pailier-Blowfish encryption, while implementing compression and blocking principles as additional measures to prevent attacks, using a firewall.

Seth, Dalal[1] applied combination of two hybrid encryption algorithms which are: Combined encryption procedures using RSA with AES algorithms and integration the Paillier with Blowfish crypto operations. The framework consisted of 4 steps first, encrypted information Storage over the cloud using hybrid technique (RSA-AES). Secondly, the second step is to store encrypted information in the cloud using RSA-AES hybrid technology, without imposing access restrictions to combat threats. In the third, encrypted information is collected in the cloud environment using Pailier-Blowfish encryption without applying compression operations. As for the fourth, encrypted data is collected in the cloud using Pailier-Blowfish encryption, while implementing compression and blocking principles as additional measures to prevent attacks, using a firewall.

According to[16] researchers reported that the files security is a method of providing security parameters through encryption. In this paper, the researchers compared between two methods (Blowfish with AES) and (AES Blowfish hybrid), which provides high productivity. The comparison resulted that the Blowfish method was faster than AES and hybrid encryption via AES with Blowfish. While the hybrid encryption via AES-encryption was better for throughput compared with AES and Blowfish was superior.

3. Overview of the algorithms

In this section, a triple encryption system was applied, which is based on three encryption algorithms: the Blowfish algorithm, the Paillier algorithm, and the Advanced Encryption Standard (AES). Here, the algorithms utilized in the proposed system will be reviewed.

3.1 Blowfish (BF)

In 1993, Bruce Schneider devised an algorithm known as the "blowfish algorithm." This algorithm is characterized by being an encryption algorithm based on a block structure, where the same secret key is used to encrypt and decrypt data. The algorithm follows the Feistel structure and is used to encrypt data blocks of 64 bits, consisting of 16 rounds. The length of the key used in the algorithm can vary between 32 bits and 448 bits [5]. According to [4, 17], this algorithm basically consists of two basic stages: the encryption of data stage and the expansion of key stage. In the phase of key expansion, a key that is typically 448 bits (56 bytes) long is converted into an array of subkeys known as a P-array.

This group consists of eighteen subkeys, each 32 bits long, summing the total data to 4168 bytes. In addition, the algorithm contains four other 32-bit boxes known as S-boxes.

The second stage of the BF process performs data encryption, which includes 16 rounds of use of the Fiestel network, in addition to the swap process and two exclusive-or. The first step is to divide the 32-bit input into 4 equal parts, with each part consisting of 8 bits, using the function F. These four values are then used to search the corresponding tables in the S-Boxs. The primary stages of the blowfish algorithm are listed as in:

a) Creating secret key:
   - Generate a secure key (32-448 bits).
   - Convert the key into a periodic array called P-array and S-boxes.

b) Basic encryption:
   - The original data is made into small block (32 bits).
   - The data is passed through consecutive stages which include mixing and interleaving using the secret key, P-array and S-boxes. This process is repeated for 16 rounds.

c) Unpack and recover data:
   - To decrypt the data, the same work as above was performed in reverse using the same secret key, P-array and S-boxes.

3.1.1 Blowfish Encryption Algorithm Characteristics

The Characteristics of the Blowfish encryption algorithm according to [4, 17, 18] are:

a. Blowfish is characterized by simple, efficiency, and ease in the processes of encrypting and decrypting data. This algorithm is fast, which makes it suitable for use in applications that require fast data processing.

b. It is also characterized by flexibility in data encryption and decryption operations image/text file.

c. Blowfish algorithm can be used to protect data on networks, software applications, and in data storage. Common uses of this algorithm are in encrypting Internet traffic, securing data in databases, and protecting sensitive data in various applications.

d. It relies on a long encryption key that can range from 32 to 448 bits. This makes it suitable for protecting data with different levels of security.

3.2 Paillier's Homomorphic Encryption (PHE)

It is a general encryption algorithm that has been successfully used in many security applications, especially in the areas of protection and privacy. It was developed by French mathematician Pascal Pierre in 1999 [19]. It is an algorithm using for homomorphic cryptosystem partly that is primarily used to protect data and enable homomorphic computing, allowing mathematical operations to be performed on encrypted data without the need for decryption [20]. Actually, information is encrypted using a public key in this system, and this key is an asymmetric key. So, users have to agree to use the public key before the encryption process can be performed. While, the private key is stay secret and is used on the receiving side of the process for decryption [18]. For the recipient, for an encryption purposes, the public key is used. The process of generating the key is done using some complex mathematical theories that limit the possibility of deducing the secret key from the public key.

The scheme of Paillier Cryptosystem is consisting of three stags based on the studies [6] [7, 21] which are :

1. Key Generation:

First, generating key by choosing large prime numbers p and q such that
gcd(pq,(p -1*q-1))=1, find n= p*q , calculate d = ƛ(n) and g = n + 1. Crating public key (n) , private key p,q,n.

2. Encryption Process:

Create diverse ciphertext for the plaintext. Start by generating the random number first, then calculating the ciphertext. C= g m * x n mod n2, where m is plain text and x is random number.

3. Decryption Process:

Obtaining plain text (m) can be via the following computation:
m =(L(cƛ(n) mod n2)) / (L(gƛ(n) mod n2)) mod n.

4. Homomorphism:

The task of the Paillier algorithm is to be able to perform mathematical operations on encrypted data. Where, the C1 and C2 being the translation of the numbers M1 and M2 respectively, and can perform the addition easily as follows: C3 = C1 * C2 mod n^2, then C3 can be decoded to get M1+M2.

3.2.1 Paillier's Homomorphic Encryption Characteristics

Paillier algorithm has some characteristics of the that make it special [20, 22] [23]:

a) It is a Semantic Security: This algorithm provides a high degree of privacy. Even if of the ability to encrypt the same value more than once, the ciphertexts will be different each time, making it difficult for attackers to deduce the original information.

b) Statistical Analysis Resistance: which can be used to reveal patterns in encrypted data, which increases the level of security.

c) Key Expansion: The ability to increase the of the public key length easily enhances security as needed.

d) (Multi-Party Computation): The Paillier algorithm is commonly used in multi-party computing, which enables more than one party to handle encrypted data without revealing it. This makes way for secure collaboration in electronic voting applications and encrypted data analysis.

e) Blind Signatures: it can be utilized to implement blind signatures, which is a type of digital signature that can be used in applications which require signature verification.

f) Paillier provides a high level of security for homomorphic computing.

3.2.2 The Advanced Encryption Standard (AES) Algorithm

AES algorithm is one of the most famous and popular encryption systems in the world. AES was published by "National Institute of Standards and technology (NIST)" in 2000 [2]. It was developed to protect sensitive data and confidential information from hacking and unauthorized access. The algorithm uses a secret key to encrypt and decrypt data and is characterized by high efficiency and security. By AES algorithm, Plain text is encrypted in blocks of 128 bits, using keys of different ranges: 128 bits ,192 bits, or 256 bits, based on the number used, which can be 10 or 12 or 14 rounds. The longer the key, the more resistant the system is to attacks. AES is certified to encrypt 128-bit (plain text) data, where the data is divided into four blocks. These blocks are organized in a 4x4 matrix and can control state, to enhance security during encryption, AES employs four distinct types of transformations in every round for each 128-bit plaintext block. These transformations include[2, 4, 8, 9, 24]:

a. Substitute Bytes Transformation (Round Addition): At this stage each byte of input data is replaced with a new value (same number of bytes) using a static replacement table (S-box) based on the key. This transformation involves applying several simple operations such as displacement and reduction.

b. ShiftRows Transformation(shorthand): The function of this stage is to change the order of bytes in each row of data (Each 4 rows of the matrix are rotating towards left). This increases the complexity and security of encrypting the data.

c. MixColumns Transformation (coefficient reduction): During this phase, bytes values are changed based on complex mathematical expressions. This stage enhances security and reduces the possibility of detecting patterns in the data.

d. AddRoundKey Transformation: At this stage, a subkey derived from the main key is added to the processed data. This process is repeated several times (number of rounds), with additional subkeys added in each round.

The algorithm repeats the previous stages for several rounds, and the number of rounds depends on the length of the key (ten rounds for a 128-bit key), (twelve rounds for a 192-bit key) , and (fourteen rounds for a 256-bit key). After the final rounds, the encrypted data is ready to be sent or stored securely.

3.3 Advanced Encryption Standard Characteristics

a. AES is considered one of the most secure and powerful encryption systems. It has been tested over the years and has shown no lack of security so far. If a strong key is used and the algorithm is implemented correctly, it is very difficult to perform attacks that break it [9].

b. AES is used in a variety of applications and fields including secure Internet communications (HTTPS), email encryption, securing wireless networks (Wi-Fi), database encryption, securing logistics and government information systems, and many others[9].

c. AES is designed to be efficient in terms of performance. It can be executed at high speed on most modern computers without causing noticeable delays in operations.

d. To increase security, the encryption key should be changed periodically. This makes it more difficult for system hacking and unauthorized access.

In short, Advanced Encryption Algorithm is one of the most important and powerful encryption systems used in the world to protect sensitive data and information. It relies on a secret key and is characterized by its security and effectiveness in performing operations related to encryption and decryption.

4. The Proposed Method

This paper presents a proposed ternary cryptography method to enhance data security in the cloud environment using a set of nested encryption algorithms. The system proposed in this study aims to increase the security level of data stored in the cloud. This comes as a result of users' increasing concern regarding data security and privacy within the cloud environment, as cloud security is considered one of the main issues facing users of cloud storage services recently. This work relies on a set of three overlapping encryption algorithms, which are blowfish encryption algorithms, Paillier Homomorphic encryption, and Advanced Encryption Standard algorithm (AES). A software tool written in Python and encryption techniques are used to enhance the level of data security in the cloud environment. "**Fig. 1**" shows the proposed ternary encryption architecture.

5. Proposed Ternary

The main steps of the proposed ternary cryptography are:

A. Initialize keys.

- Configure keys using Paillier algorithm gives (public key (PKp) and secret key (SKp)).
- Keys encryption using Blowfish algorithm gives

(public key(PKf) and secret key (SKf))

B. Data encryption

- Data encryption using Paillier algorithm gives (cipher-p).
- Re-encrypt the result using the AES algorithm gives (cipher-AES)

C. Uploading encryption file to cloud storage.

D. Data decryption

- Decrypt data (cipher-AES) using the AES algorithm.
- Decrypt data (cipher-p) using Paillier algorithm via (public key(PKf) and secret key (SKf)).

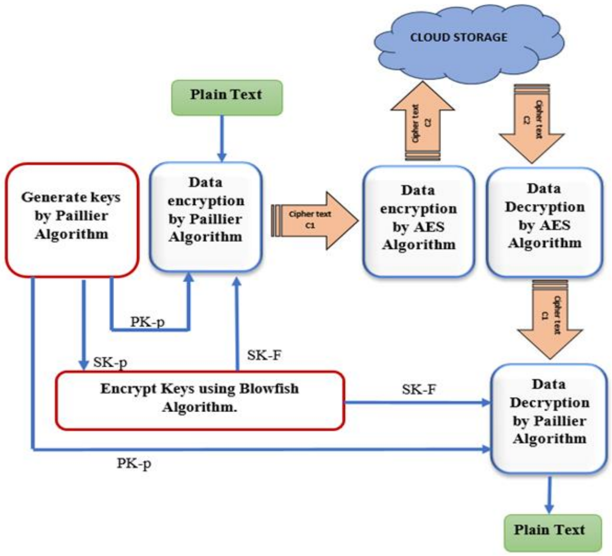
CLOUD STORAGE
Plain Text
Cipher text C2
Cipher text C2
Generate keys by Paillier Algorithm
Data encryption by Paillier Algorithm
Cipher text C1
Data encryption by AES Algorithm
Data Decryption by AES Algorithm
Cipher text C1
PK-p
SK-p
SK-F
Encrypt Keys using Blowfish Algorithm.
SK-F
Data Decryption by Paillier Algorithm
PK-p
Plain Text

Fig. 1. The Proposed Ternary Encryption Architecture.

6. Implementation

In this work, encryption and decryption algorithms are implemented using the Python programming language. Tests were conducted on a PC with a 2.60GHz Core i5 processor and 8GB of RAM. Google Drive has also been used as a cloud storage for files. In the proposed model, three overlapping algorithms were used (Blowfish algorithm, Paillier algorithm and AES algorithm) to secure data over the network utilizing encryption and decryption operations before uploading to the cloud storage and after downloading from it. When a file is sent, the data will be encrypted using the three algorithms on the sender's side. The data will be stored in encrypted form in the cloud storage to increase security, and then the same overlapping decryption algorithms are applied on the recipient's side. The following steps illustrate the nested three algorithms working procedure:

A. INITIALIZE KEYS.

1- Configure keys using Paillier algorithm.

Generate the two keys: a public key and a private key. In order to exchange these keys securely, its need to encrypt the private key using an end-to-end structure.
gcd(pq,(p -1*q-1))=1, t= p*q , calculate d = ƛ(t) and g =t + 1, public key(t) , private key p,q,t.

2- Keys encryption using Blowfish algorithm

•Generate Blowfish key: creating a 448-bit (56 byte) secret key by a random key generator.
•Encrypt (paillier-private key) by secret Blowfish key generated in the previous step to get (SkF2). Use ECB (Electronic Codebook) encryption mode to encrypt every bit of the (paillier-private key1) via a Blowfish secret key.
•Store the encrypted key (which is the output of the encryption process previous step (paillier-private key2)) securely. Store it in a secure place which is a strong password-protected file.

B. DATA ENCRYPTION

1. Encrypt plain data via Paillier algorithm.

•Before encrypted data, it converted to integers. This involves representing text data or numbers as integers.
•To encrypt data, the Paillier mathematical laws were used. This process involves as in following equations:
Ciphertext C = (g^M) * (r^n) mod n^2. r is a random integer chosen. n is the product of 2 large prime numbers.

2.Re-encrypt the Paillier' results via AES algorithm:

•Adopting GCM encryption mode which is a versatile encryption mode that combines encryption and data integrity (authentication) using an ID response code (MAC), which increases the security of the operation. GCM's mode of encryption data on the network or in wireless communications provides protection from man-in-the-middle attacks and data tampering.
•A 256-bit random key was generated. And generate an Initialization Vector (IV) as an additional value to increase cryptographic security.
•Data encryption: The data resulting from the previous encryption is divided into blocks of a fixed size (128 bits). The AES algorithm was applied to each block of data using the key generated in the previous step and IV.
•Collect all encrypted texts into one file

C. UPLOADING FILE

Uploading encryption data to cloud storage. The consumed time for this work of uploading the data is 0.1093ms

D. DATA DECRYPTION

1. ***Decrypt data (cipher-AES) using the AES algorithm.***

•Applied the same (256-bit) AES algorithm key and IV to get first decrypted file(AES-file1).

2.***Re-Decrypt data (AES-file1) using Paillier algorithm.***

•The decryption process using the privet encrypted blowfish key and public key and based on the following mathematical

rule:
M = L(C^n mod n^2) / L(g^n mod n^2) mod n.

7. Results

The proposed Hybrid Algorithm was compared to AES and Paillier using two parameters (throughput and execution time), its performance was evaluated across different data sizes, starting with 300bytes to analyze low data volume, and progressing to larger sizes (1Kbytes, 10Kbytes, and 50Kbytes).

The first evaluation conducted based on the execution time consuming in encrypting and decryption process for different data sizes, "**Fig 2,3,4** and **5**" illustrates the execution time of the proposed technique takes approximately time to that of the Paillier algorithm when it was applied singly. Where, the difference in data encryption was 6% ,15%,22% and 29% respectively with the data size of 300 B, 1 KB, 10 KB, and 50 KB per millisecond. This indicates that AES algorithm has very little impact on execution time as it is a fast algorithm. Moreover, Blowfish algorithm had no measurable impact on the execution time because it was used to encrypt the keys only. However, the time taken to decrypt the data was also close to the time taken by the Palilier algorithm where the different around 2%,3%,5% and 8% respectively with the data sizes 300B,1KB,10KB and 50KB and had a slight effect on the AES algorithm, while the Blowfish had no effect too.

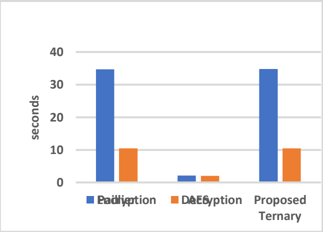

Fig. 2. Execution Time (300B) Data.

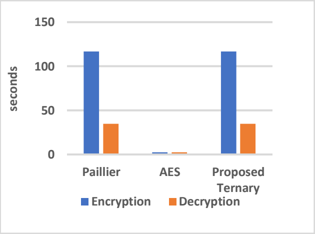

Fig. 3. Execution Time (1KB) Data.

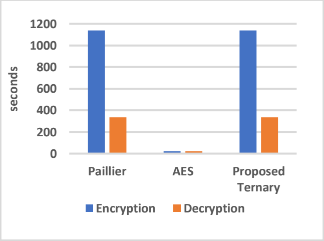

Fig. 4. Execution Time (10KB) Data.

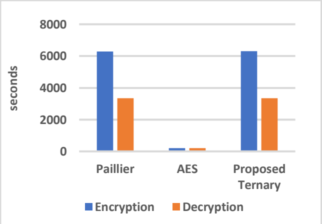

Fig. 5. Execution Time (50KB) Data.

The second evaluation is conducted based on the obtained throughputs of the proposed hybrid ternary algorithm compared to the selected techniques with the data sizes of 300 B, 1 KB, 10 KB, and 50KB per millisecond.
As is illustrated in "**Fig 6,7,8** and **9**" the throughput of the proposed technique is better than the others for the different tested data sizes.

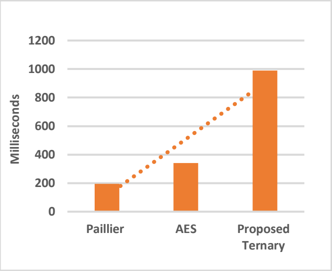

Fig. 6. Throughput with 300B Data.

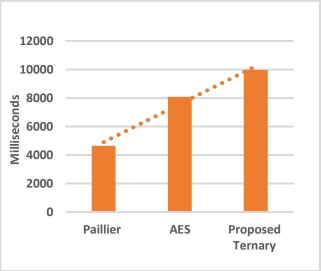

Fig. 7. Throughput with 1KB Data.

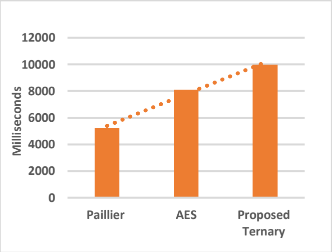

Fig. 8. Throughput with 10KB Data.

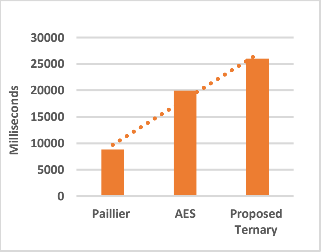

Fig. 9. Throughput with 50KB Data.

Therefore, Encryption via a ternary encryption system of overlapping algorithms (Paillier, Blowfish, and AES) can combine the advantages of these algorithms and produce multiple improvements in terms of security and privacy which resulted in more difficulty for attackers to immediately understand the encrypted data in cloud, as they must first decrypt it using AES, then decrypt the keys using Blowfish, and finally decrypting by Paillier.

Moreover, providing three nested layers of encryption increases the protection of sensitive data in Cloud Computing, but it consumes computational resources and time. " **Table 1**" shows the result compared with previous works.

Table 1. Result comparison with previous works.

Authors-year	**Hybrid encryption**	**file size**	**Findings of the study**
(Sajay, Babu et al. 2019) [11]	homographic - blowfish	64Bits	Enhance the cloud security
(Siregar 2018) [16]	Key generator: RSA - ECC Documents encrypt: AES – Blowfish	296.67-372.67 KByte	Found that the Blowfish is faster than AES and ECC method gives highest strength and faster than RSA method
(Harnal and Chauhan 2019) [9]	Asymmetric-public key over the symmetric secret key Blowfish	64 bits, 128-bits SKey	Give fast and better results in terms of performance and security
Bermani, A.K., T.A. Murshedi et al. 2021)[4]	AES-Blowfish - MD5	1MByte	Provides efficiency and speed to encryption process with
(Hussam	PRESENT -	1KB-	Improved the security of the

Authors-year	**Hybrid encryption**	**file size**	**Findings of the study**
2021) [25]	TWINE	10MB	personal data stored on the cloud
(Salem, Sabbeh et al. 2017) [12]	AES - MD5	7-22.4 Kbyte	develops availability and preserves confidentiality of data, Enhances public audibility, correctness of storage.
(Sunday and Olufunminiyi 2023)[8]	AES-RSA	22-5120 KByte	AES provides better security than all other forms of cryptography techniques, and the hybrid method results in higher security but requires more time.
Proposed ternary Cryptography in this work	Blowfish-Paillier -AES	300byte -50 KByte	-Provides a high level of security. -Double protection for keys. - enhance the cloud security. -Provides 3 nested layers of encryption increases the protection of sensitive data, but it consumes computational resources and time.

8. Conclusion

Recently, notable interest by organizations and individuals heading towards the cloud environment to store their sensitive data, but securing their data is the essential issue in the cloud. System security is not only related to data encryption alone, but also includes an important matter in protecting and managing keys. Key protection is an essential element in the security strategies of organizations and individuals. Investing in key protection can prevent serious damage and costs that can result from security breaches.

Therefore, a specific algorithm (blowfish) was applied to encrypt the keys before using them to encrypt data. In this work, a triple encryption model was applied to the data on the side of client before uploading it to the cloud server and decrypting it on the recipient region, which provides an additional layer of data security.

In this paper the results were evaluated depending in two parameters which are throughput and execution time for the proposed ternary were compared with AES and Paillier algorithm with different data size.

The improvements compared with previous works, and it was found that encrypting keys with different algorithm to the one generating the same keys followed by applying two hybrid algorithms to encrypt files gave more confidentiality and protection for sensitive data than using only hybrid algorithms for encrypting files. In future, this model of encryption can be applying using artificial intelligence techniques to add more enhancements in cloud security.

References

[1] Seth, B., et al., Secure Cloud Data Storage System Using Hybrid Paillier–Blowfish Algorithm. Computers, Materials & Continua, 2021. 67(1).

[2] Abdullah, A.M., Advanced encryption standard (AES) algorithm to encrypt and decrypt data. Cryptography and Network Security, 2017. 16(1): p. 11.

[3] Touil, H., N. EL AKKAD, and K. SATORI. Text encryption: hybrid cryptographic method using Vigenere and Hill Ciphers. in 2020 International Conference on Intelligent Systems and Computer Vision (ISCV). 2020. IEEE.

[4] Bermani, A.K., T.A. Murshedi, and Z.A. Abod, A hybrid cryptography technique for data storage on cloud computing. Journal of Discrete Mathematical Sciences and Cryptography, 2021. 24(6): p. 1613-1624.

[5] Manaa, M.E. and R.H. Jwdha, A Robust Documents Secure Approach Using Blowfish Algorithm in the Cloud Computing. Journal of Computational and Theoretical Nanoscience, 2019. 16(3): p. 823-830.

[6] Ogunseyi, T.B. and T. Bo. Fast decryption algorithm for paillier homomorphic cryptosystem. in 2020 IEEE International Conference on Power, Intelligent Computing and Systems (ICPICS). 2020. IEEE.

[7] Fazio, N., et al. Homomorphic secret sharing from paillier encryption. in Provable Security: 11th International Conference, ProvSec 2017, Xi'an, China, October 23-25, 2017, Proceedings 11. 2017. Springer.

[8] Sunday, A.E. and O.E. Olufunminiyi, An Efficient Data Protection for Cloud Storage Through Encryption. International Journal of Advanced Networking and Applications, 2023. 14(5): p. 5609-5618.

[9] Harnal, S. and R. Chauhan, Hybrid cryptography based E2EE for integrity & confidentiality in multimedia cloud computing. International Journal of Innovative Technology and Exploring Engineering (IJITEE), Scopus, 2019. 8(10): p. 918-924.

[10] Kamara, S. and K. Lauter. Cryptographic cloud storage. in International Conference on Financial Cryptography and Data Security. 2010. Springer.

[11] Sajay, K., S.S. Babu, and Y. Vijayalakshmi, Enhancing the security of cloud data using hybrid encryption algorithm. Journal of Ambient Intelligence and Humanized Computing, 2019: p. 1-10.

[12] Salem, M.Z., S.F. Sabbeh, and E. Tarek, An efficient privacy preserving public auditing mechanism for secure cloud storage. International Journal of Applied Engineering Research, 2017. 12(6): p. 1093-1101.

[13] Bansal, V.P. and S. Singh. A hybrid data encryption technique using RSA and Blowfish for cloud computing on FPGAs. in 2015 2nd international conference on recent advances in engineering & computational sciences (RAECS). 2015. IEEE.

[14] Kumar, S., et al. Cloud security using hybrid cryptography algorithms. in 2021 2nd International conference on intelligent engineering and management (ICIEM). 2021. IEEE.

[15] Wu, J., I. Detchenkov, and Y. Cao. A study on the power consumption of using cryptography algorithms in mobile devices. in 2016 7th IEEE International Conference on Software Engineering and Service Science (ICSESS). 2016. IEEE.

[16] Siregar, R. Performance analysis of AES-Blowfish hybrid algorithm for security of patient medical record data. in Journal of Physics: Conference Series. 2018. IOP Publishing.

[17] Khatri–Valmik, M.N. and V. Kshirsagar, Blowfish algorithm. IOSR Journal of Computer Engineering (IOSR-JCE), 2014. 16(2): p. 80-83.

[18] Chinnasamy, P., et al. Efficient data security using hybrid cryptography on cloud computing. in Inventive Communication and Computational Technologies: Proceedings of ICICCT 2020. 2021. Springer.

[19] Paillier, P., Public-Key Cryptosystems Based on Composite Degree Residuosity Classes. Edited by G. Goos, J. Hartmanis and J. van Leeuwen, 1999: p. 223.

[20] Crawford, J.L.H., Fully Homomorphic Encryption Applications: The Strive Towards Practicality. 2020, Queen Mary University of London.

[21] Ranjan, M., A.H. Mondal, and M. Saikia, A cloud based secure voting system using homomorphic encryption for android platform. International Journal of Electrical and Computer Engineering (IJECE), 2016. 6(6): p. 2994-3000.

[22] Patel, B., P. Tandel, and S. Sanghvi. Efficient Ballot Casting in Ranked Based Voting System Using Homomorphic Encryption. in Advances in Computing and Data Sciences: Third International Conference,

ICACDS 2019, Ghaziabad, India, April 12–13, 2019, Revised Selected Papers, Part II 3. 2019. Springer.

[23] Mohammed, S.J. and D.B. Taha. Performance evaluation of RSA, ElGamal, and paillier partial homomorphic encryption algorithms. in 2022 International Conference on Computer Science and Software Engineering (CSASE). 2022. IEEE.

[24] Gosain, A. and A. Arora, Security issues in data warehouse: a systematic review. Procedia Computer Science, 2015. 48: p. 149-157.

[25] Hussam, M., New lightweight hybrid encryption algorithm for cloud computing (LMGHA-128bit) by using new 5-D hyperchaos system. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 2021. 12(10): p. 2531-2540.