Received: November 1, 2023. Revised: December 28, 2023.

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Data Security in Cloud Environment by Using Hybrid Encryption Technique: A Comprehensive Study on Enhancing Confidentiality and Reliability

Susmitha Pothireddy[1] Nikhila Peddisetty[2] Pachipala Yellamma[1]* Gitanjani Botta[3] Kailash Nadh Gottipati[4]

[1]Department of Computer Science and Engineering,
Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, India
* Corresponding author's Email: pachipala.yamuna@gmail.com

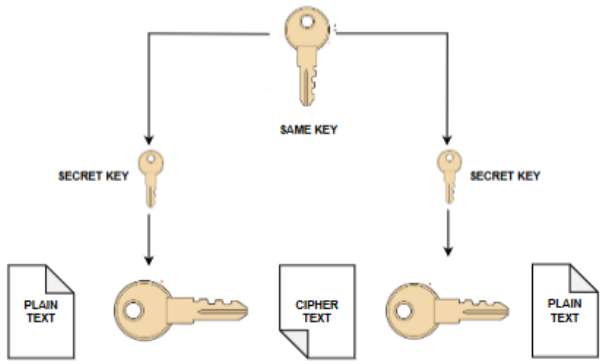
Abstract: Hybrid encryption techniques are gaining popularity in the cloud platform due to their ability to address security concerns and data storage challenges. In order to ensure confidentiality at every stage of processing, this article presents an innovative strategy that merges fully homomorphic encryption (FHE) and secure hash algorithm 3 (SHA-3), offering robust protection against cyber threats. FHE and SHA-3 offer a solution to this problem. We conducted experiments using different datasets to test the performance and security strength of this hybrid approach. Our method takes into account factors such as computational overheads, complexity requirements, key management challenges, and limited support from vendors/providers offering specialized hardware/software capable of supporting complex mathematical functions required by each technique separately before combined into a hybrid form suitable enough scaled-out horizontally across different nodes within clouds themselves today globally among end-users relying upon them heavily day-to-day tasks involving mission-critical workloads running inside virtualized machines hosted on public/private clouds ecosystems worldwide. The results show that implementing FHE together with SHA-3 can significantly improve an organization's overall cyber security posture when operating critical infrastructure components residing within cloud environments. According to the results, it performs better than other methods that are currently in used complexity of encryption and decoding, including homomorphic encryption and RSA, AES & DSA, and AES & RSA. The hybrid algorithm we are proposed using fully homomorphic & SHA3 with 2048 bits 0.789 seconds of encryption time and decryption time with 0.001 seconds and execution time with 4.25 seconds. Therefore, we conclude that our proposed hybrid encryption technique is the best approach to address cyber security risks associated with storing sensitive data in cloud computing environments.

Keywords: Hybrid encryption techniques, Cloud platform, Security concerns, Data storage challenges, Fully homomorphic encryption (FHE), Secure hash algorithm-3 (SHA-3).

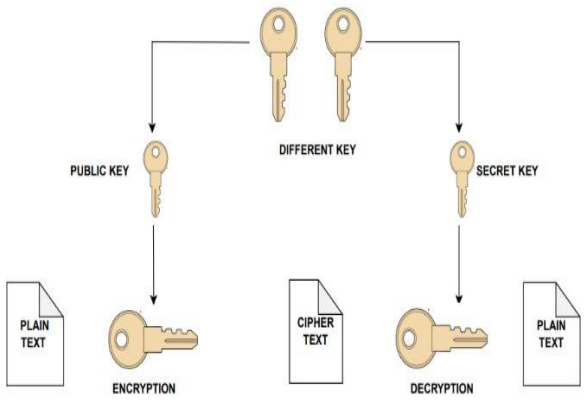
1. Introduction

Encryption and decryption are essential processes with the purpose of preserving data privacy and security. The process of converting plain text information onto cipher text which appears random and meaningless is known as encryption [1]. Decryption is the process of converting encrypted data from cipher text to plaintext, which is able to read and recognize. Symmetric key cryptography and asymmetric key cryptography are the two fundamental divisions of encryption: Symmetric key cryptography. In this method a single secret key is utilized for both the encryption and decryption of data. It is crucial that this key be kept confidential and only shared between the sender and receiver of a message [2]. However, two keys are used in asymmetric key cryptography, commonly known as public key cryptography: a public key and a private key.

Data is encrypted using the public key and decrypted using the private key [3]. While the private key needs to be kept safe, the public key can be shared freely. The utilization of data encryption is wide spread and highly effective for safeguarding data in storage a during transfer [4]. Encryption entails the conversion of data into a format that can



(a)



(b)

Figure. 1 (a) Symmetric encryption and (b) Asymmetric encryption

only be understood by authorized individuals possessing a decryption key.

1.1 About hybrid encryption schema

Hybrid encryption is a method of encryption that combines two or more encryption techniques to provide enhanced security and protection for sensitive data. In contrast, asymmetric key cryptography, also known as public-key cryptography, relies on distinct key pairs for the encryption and decryption processes [5]. Asymmetric encryption techniques include well-known methods such as RSA, the elliptic curve cryptography (ECC)-based elliptic curve digital signature algorithm (ECDSA), and the elliptic curve digital signature (ECDH) algorithm. ECC is also employed in the diffie-hellman protocol [Table 1]. To overcome the constraints of conventional encryption approaches and the hybrid encryption algorithms have been introduced.

In Figs. 1a and 1b, the combination methods for symmetric and asymmetric encryption provide different levels of enhanced security while maintaining processing efficiency. However, hybrid algorithms also have their own drawbacks. To address these limitations, a combination of fully homomorphic encryption (FHE) and secure hash algorithm-3 (SHA-3) has been proposed in this work. The combination of these two strengths results in a distinct hybrid approach. They are cryptography and hashing techniques maintaining strong security protocols is crucial to ensuring the security of data. Weak security measures can lead to the compromise of sensitive information, network congestion, loss of user trust and high recovery expenses. Therefore, it is essential to use robust encryption methods like FHE and SHA-3 to protect data in cloud computing environments.

1.2 Fully homomorphic encryption & SHA3

This method involves using multiple encryption algorithms in a layered approach to provide robust protection against cyber threats. FHE is particularly useful for protecting sensitive data in cloud computing environments, where traditional cryptographic techniques may not provide sufficient security. SHA-3, on the other hand, is a widely used cryptographic hash function that can be used to generate unique digital fingerprints of data. These fingerprints can be used to verify the integrity of data and ensure that it has not been tampered with or altered in any way. SHA-3 can be used in conjunction with FHE to provide enhanced security and ensure data protection in the cloud environment. We have taken a survey on various hybrid algorithms, taken three methods of combined encryption techniques and addressed the drawbacks and issues with those hybrid techniques. Finally, combination of hybrid encryption algorithm provides a viable answer for cloud data security.

The paper's organization of the information follows: Section 2 offers a comprehensive literature review of existing research on hybrid encryption methods. In section 3, we discuss the current methodology for secure data transmission using hybrid encryption and introduce our proposed methodology use (FHE & SHA-3) for securing data in cloud computing environments. We explain the encryption process in detail. Section 4 presents the results and comparative analysis of our proposed methodology. Finally, section 5 provides a detailed explanation of the outcomes and the ending statements of the research paper.

2. Literature review

Shahnawaz Ahmad[1], Shabana Mehfuz[2], Javed Beg[3] proposed a "Hybrid cryptographic approach to enhance the mode of key management system in cloud environment" in the year 2022 [1]. The authors proposed a hybrid cryptographic approach to

improve key management in cloud environments. The methodology involves combining symmetric encryption using advanced encryption standard (AES) with asymmetric encryption utilizing rivest-shamir-adleman (RSA). This hybrid approach aims to provide enhanced security measures for key management systems within the cloud.

The research paper titled “Cloud Computing and Security Issues” by, Dhanamma Jagli[1], Rohan Jathanna[2] in the year 2017 [2]. The concept of distributed computing is another one that offers a lot of benefits to its users. However, it also brings up a few security concerns that could limit its application. The biggest security concerns with regard to cloud processing are networks and hoarding, as this article illustrates. One of the most pressing challenges for cloud clients is virtualization, which enables several clients to share single physical servers.

The research paper titled "An Efficient Attribute-Based Encryption Scheme with Policy Update and File Update in Cloud Computing" by Jianyong Chen in the year 2019 [3]. In cloud computing contexts, the method combines attribute-based encryption (ABE) and provides functionality for updating files and policies. Further research could concentrate on improving computing efficiency and assessing scalability issues in various cloud systems. End- to-end security in a public cloud can be ensured through the ABE if an information user uploads encrypted data to the PCSP using the stated access criteria. End-to-end security in a public cloud can be ensured through the ABE if an information user uploads encrypted data using the stated access criteria.

The research paper titled "Public-Key Encryption Secure against Related Randomness Attacks for Improved End-to-End Security of Cloud/Edge Computing" by Pentagon Liu in the year 2020 [4]. The primary objective is to use public-key encryption to improve the reliability of cloud and edge computing environments. The suggestion contributed to concerns about how susceptible linked randomness attacks are to typical public-key encryption systems. Stronger security guarantees are provided for sensitive data sent between cloud and edge devices by the author's secure variant, which defends against such attacks. They demonstrated how to create an RRA secure PKE in the random oracle paradigm by using the public key and message as the rand coins for encryption.

In this research paper titled “Secured two-factor authentication, graph-based replication, and encryption strategy in cloud computing” by S. Lavanya[1], Saravanakumar[2] in the year 2022 [5]. They proposed replication and encryption methods based on graphs. In addition to username-password combinations, the methodology focuses on enhancing user authentication via a two-factor authentication mechanism. This improves protection against unauthorized access attempts by a further layer. To increase fault tolerance and high availability, the authors suggest developing a graph-based replication approach to distribute data across numerous servers in the cloud environment. Revocable- storage authentication-based encryption (RS-IBE) is a technique that can be utilized in creating an economical data-sharing system. It offers both forward and backward security.

The research paper titled "Design of Fully Homomorphic Multikey Encryption Scheme for Secured Cloud Access and Storage Environment" by Dilli Babu Salvakkam[1] and Rajendra Pamula[2] was published in the year 2022 [6]. The technique that can be used to develop a system for exchanging data that is affordable since it offers backward and forward security. It provides a secure and inexpensive way to facilitate transmission of data that permits the updating of cipher texts and identity departure simultaneously to guarantee forward and backward secrecy. The majority consider utilizing encryption to protect the privacy of data that is stored. The most important aspect of cloud storage is homomorphic multikey encryption since it permits anyone to perform specific algebraic operations on protected data. Because there are more and more scenarios where it is necessary, data sharing has gained popularity among providers of cloud-based services.

The research paper titled "A Security Model to Protect the Isolation of Medical Data in the Cloud Using Hybrid Cryptography" by Swetha Gadde[1], J. Amutharaj[2], S.Usha[3] in the year 2023 [7] March. A security approach that utilizes hybrid cryptography to secure different types of health related information preserved in cloud-based environments. The strategy brought within this research emphasizes on utilizing symmetric and asymmetric encryption methods to guarantee secure transmission as well as storage of data. This hybrid strategy strikes a balance between cryptographic security and performance efficiency.

The research paper titled "Attribute-Based Encryption Mechanism with Privacy-Preserving Approach in Cloud Computing" by Jyoti Yogesh Deshmukh[1], S.K. Yadav[2], and G.M. Bhandari3 in the year 2023 [9]. To enhance secure data storage and access in cloud computing settings while protecting privacy, the attribute-based encryption (ABE) technique is introduced in this research study. The methodology outlined in the paper places an emphasis on using ABE techniques to build user and data-related characteristics-based fine-grained access control. To safeguard private data while it is being

Table 1. Literature review on existing methodologies

S:NO	AUTHORS	TITLE	APPLIED METHODOLGY	DRAWBACKS
1	S. Ahmad, S. Mehfuz, and B. Javed	Hybrid cryptographic approach to enhance the mode of key management system in cloud environment[1]	AES & RSA	HCA-KMS sacrifices some privacy preservation compared to fully homomorphic encryption with SHA-3, potentially limiting its use in scenarios requiring robust computation on encrypted data.
2	Abhishek Prabhakar, Diksha Tiwari, Anand Singh	Performance Analysis of AES, RSA and Hashing Algorithm Using Web Technology[23]	AES&RSA	Encryption trade-offs in RSA, AES and Hashing Algorithms impact real-time processing due to the inherent tension between security and system performance.
3	Mehdi-Laurent Akkar & Christophe Giraud	An Implementation of DES and AES, Secure against Some Attacks[29]	AES&DES	The transformed masking method's drawback lies in increased computational complexity and potential vulnerabilities if the transformation process lacks adequate security measures or faces emerging attack vectors.
4	Yasmin Alkady, Fifi Farouk & Rawya Rizk	Fully Homomorphic Encryption with AES in Cloud Computing Security[30]	HOMOMORPHIC &AES	Fully Homomorphic Encryption(FHE) introduces computational overhead, hampering real-time performance in resource-intensive applications.
5	Lijuan Wang, Lina Ge, Yugu Hu, Zhonghua He, Zerong Zhao & Hangui Wei	Research on Full Homomorphic Encryption Algorithm for Integer in Cloud Environment[17]	FULLY HOMOMORPHIC	Significant drawbacks including high computational overhead and performance.
6	S. Selvi	Hyper Elliptic Curve Based Homomorphic Encryption Scheme for Cloud Data Security[28]	HYPER ELLIPTIC CURVE BASED HOMOMORPHIC	It may introduce higher computational overhead and complexity compared to other encryption schemes and potentially impacting the overall performance in the cloud computing.
7	E.K.Subramanian	Elliptic curve Diffie–Hellman cryptosystem in big data cloud security[13]	ELLIPTIC CURVE WITH DIFFIE–HELLMAN	The ECDH algorithm's improved encryption time may be offset by potential vulnerabilities. of elliptic curve with Diffie helman of cloud security.
8	Bushra Shaheen & Farheen Siddiqui	Comparison Between RSA Algorithm and Modified RSA Algorithm Used in Cloud Computing[18]	RSA	The integration of Homomorphic Encryption with RSA may introduce performance challenges, balancing enhanced security with increased computational overhead in cloud computing.

9	Chu-Hsing Lin, Jung-Chun Liu, Joy Iong-Zong Chen & Tien-Pin Chu	On the Performance of Cracking Hash Function SHA-1 Using Cloud and GPU Computing[19]	SHA	The impressive cracking capabilities of cloud and GPU systems raise ethical and legal concerns, potentially undermining encryption practices and exacerbating cyber security threats.
10	Jing Xia, Zhong Ma, Xinfa Dai & Jianping Xu	Fast Homomorphic Encryption Based on CPU-4GPUs Hybrid System in Cloud[14]	FAST HOMOMORPHIC	The CPU-4GPUs hybrid system for DGHV homomorphic encryption sacrifices some security for speed compared to fully homomorphic encryption with SHA-3.

stored and sent to the cloud, the authors also incorporate privacy-preserving methods. The attribute-based encryption approach ensures that reduplication is carried out without revealing sensitive information.

The research paper titled "Cloud Data Security Mechanism Using Lightweight Cryptography" by Zaid A. Abdulkader in the year 2022 [10]. In this article, the author studies a data security system designed for cloud computing that uses simple cryptographic methods. The proposed approach focuses an immense value on using simple cryptographic algorithms to ensure safe data Storage and transmit in a cloud context. Future studies need to concentrate on analyzing the endurance of inexpensive cryptographic algorithms against new threats while ensuring seamless interoperability with current standards and protocols used in cloud environments to progress in the area. It would also be beneficial to investigate ways to reduce critical management procedures in order to increase system efficiency generally without impacting security standards.

Finally, hybrid encryption algorithms that combine full homomorphic encryption (FHE) and secure hash algorithm 3 (SHA-3) provide a viable answer to cloud computing security problems and data storage challenges. When dealing with huge datasets hosted in the cloud, traditional cryptographic approaches may not provide acceptable security. To overcome these restrictions, a suggested system for maintaining the security of data saved in the cloud utilizing FHE and the SHA-3 algorithm has been devised. The process encrypts the data, performs completely homomorphic operations on the cipher data such as implicit addition and multiplication, and then applies the SHA-3 hashing algorithm to generate the final encrypted layer.

The table highlights the drawbacks of each methodology and limitations. The proposed hybrid approach that combines Fully Homomorphic Encryption and SHA-3 hashing algorithm offers a promising solution that can enhance security while minimizing the computational complexity and overhead associated with traditional hybrid cryptographic algorithms. This new approach shows potential for improving the security in cloud environments.

The above Table 1 provides a literature review on existing methodologies for enhancing the security in cloud computing environments. It provides a comparison of different approaches, including hybrid cryptographic algorithms, AES, RSA, hashing algorithms, homomorphic encryption, elliptic curve cryptography, and more.

3. Proposed methodology

In this section, we will discuss how to improve encryption applied to ensure cloud security. The main concern for every user is the security of their cloud data. To address this issue, the proposed system description Incorporates the use ofCloudSim is for simulating the security enhancements using fully homomorphic encryption and SHA-3 encryption. You can refer to Fig. 2 for our proposed architecture The encryption techniques to improve cloud security are described in this section.

Because security is the primary concern, the solution suggested in this study has to securethe cloud based data that every user has to deal with the homomorphic encryption of the two algorithms and the SHA-3 encryption algorithm used in this study. To improve cloud security, this study makes use of the cloud sim software tool and an encryption approach. Fig. 2 contains the proposed architecture for hybrid cryptographic approach to enhance cloud security. In this framework, the data owner uses to encrypt the data. Fully homomorphic encryption (FHE) algorithm by performing the mathematical

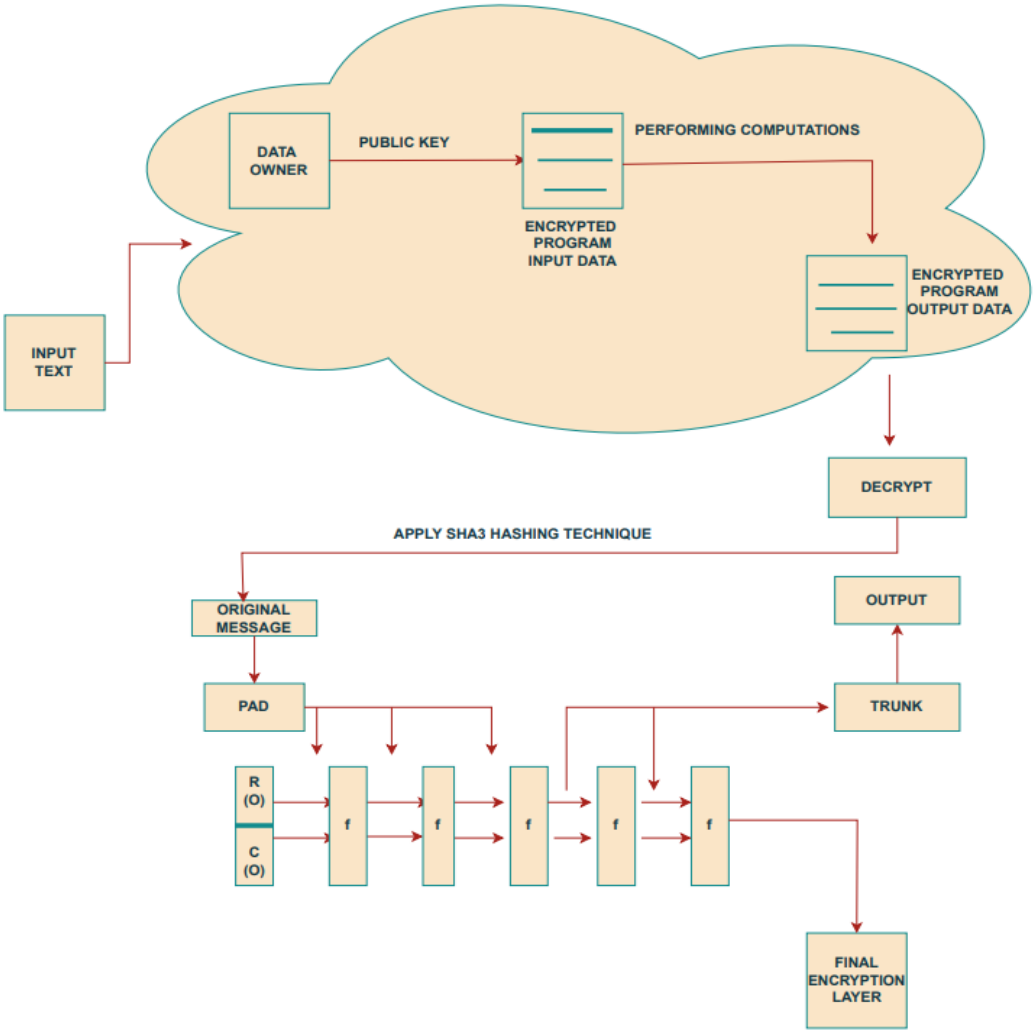


Figure. 2 A Proposed architecture for hybrid cryptographic approach to enhance cloud security -FHE&SHA-3

computations and that encrypted text combined with the SHA-3 hashing technique and the final encryption layer is formed. The entire process ensures the privacy and security of the sensitive data. Our proposed system harnesses the capabilities of CloudSim to create a secure and efficient cloud environment, where data confidentiality, integrity, and secure computation are paramount. This approach enablesus to proactively address cloud security challenges.

Algorithm used

For this investigation, the utilization of two algorithms is made, namely the fully homomorphic encryption algorithm and the SHA-3 algorithm.

Both algorithms are exampled below.

Proposed method: Enhanced encryption algorithm using FHE and SHA-3.

The combination of fully homomorphic encryption (FHE) and secure hash algorithm 3 (SHA-3) offers a robust approach to enhance cloud computing data security and privacy. In order to provide strong environments, this security solution uses a layered encryption approach that takes advantage of the characteristics of various encryption algorithms. Fundamentally, this strategy combines fully homomorphic encryption (FHE) and SHA-3, each distinct security benefits. With the aid of the state-of-the- art encryption method FHE, data can be encrypted, kept safely in the cloud, and yet be used for calculations by authorized users without the need for decryption.

Fully homomorphic encryption (FHE): Is a sophisticated encryption technique that enables calculations on encrypted data without the need for decryption. This unique capability of FHE allows for secure data processing while keeping sensitive information private.

Generation of key:

Select an odd integer 'p' from an interval [η - 1/2, η/2], where η is a parameter related to the security of the encryption scheme. This 'p' will be the public key component.

Proposed Algorithm: Hybrid Encryption and Decryption Algorithm with FHE and SHA-3 Hashing

```
def Hybrid Encryption(m, pk, sk):
 # Step 1: Encrypt the input message using the Fully Homomorphic Encryption Algorithm.
        r1 = rand (pk.max_value) # Generate a random key r1.
        c1 = (pk × m + r1) % pk # Encrypt m using the public key pk and the random key r1.
 # Step 2: Hash the encrypted message using the SHA-3 Hashing Algorithm.
         h = SHA3_Hash (c1)  # Compute the hash value h.
 # Step 3: Encrypt the hash value using the Fully Homomorphic Encryption Algorithm.
         r2 = rand (pk.max_value) # Generate a random key for encryption (r2).
        c2 = (pk × h + r2) % pk   # Encrypt h using the public key pk and the random key r2.
# Step 4: Return the final ciphertext (c2).
    return c2
# Hybrid Decryption Algorithm with Fully Homomorphic Encryption and SHA-3 Hashing
def Hybrid Decryption(c, sk, pk):
 # Step 1: Decrypt the final ciphertext using the Fully Homomorphic Decryption Algorithm.
                r2 = c % sk # Decrypt c using the private key sk to obtain the random key r2.
                h = (c - r2) // sk # Decrypt c using the random key r2 to obtain h.
# Step 2: Hash the decrypted value using the SHA-3 Hashing Algorithm.
                 c1 = SHA3_Hash (h) # Compute the hash value c1.
# Step 3: Decrypt the hashed value using the Fully Homomorphic Decryption Algorithm.
                  r1 = c1 % sk # Decrypt c1 using the private key sk to obtain the random key r1.
                 m = (c1 - r1) // sk # Decrypt c1 using the random key r1 to obtain m.
 # Step 4: Return the plaintext message m.
    return m
```

Generate a private key'd,' which remains undisclosed.

Encryption:

Given a plaintext bit 'a' ∈ {0, 1} and the public key 'p': Randomly select two integers 'f' and 'g' such that |2g| < |a/2|. These are used for noise injection and randomness.

Compute the cipher text 'C' as follows:

$$C = (a * b) + (2f) + g \quad (1)$$

'b' is the public key component 'p' from the key generation step.

The addition of '2f' and 'g' introduces randomness and noise.

Decryption:

Given a cipher text 'c' and the private key 'd': compute '(c mod p) mod 2' to decrypt the bit.

'a': Decrypted_bit = (C mod p) mod 2 (2)

This step extracts the original plaintext bit 'a'

from the cipher text 'C' and returns it.

SHA-3: Secure hash algorithm-3

(SHA-3) is a cryptographic hash function that is used to generate a unique fixed-size output (known as a hash) from input data of any size. SHA-3 works by using complex mathematical algorithms.

Generation of key:

Generate a random 64-byte string.

Hash the random string using SHA-3-512. The hash value is the private key.

Hashing Function:

Convert the message to a byte array.

XOR is the message byte array with the private key. Hash the XORed byte array using SHA-3-512(bits).

Hybrid encryption algorithm:

The hybrid encryption algorithm combines the principles of fully homomorphic encryption (FHE) and the SHA-3 hashing algorithm to ensure secure communication of sensitive information. In the first step, the plaintext message m is encrypted using FHE, introducing an additional layer of security by incorporating a random key $r1$. Subsequently, the resulting ciphertext $c1$ undergoes a hash function operation through SHA-3, producing a hash value h. The hash value is then encrypted using FHE with another random key $r2$ to generate the final ciphertext $c2$. This hybrid approach leverages the computational efficiency of FHE and the cryptographic strength of SHA-3, providing a robust encryption mechanism.

Mathematical explanation:

Let:

- m be the plaintext message,
- pk be the public key,
- sk be the private key,
- $r1$ and $r2$ be random keys,
- $c1$ and $c2$ be intermediate ciphertexts,
- h be the hash value.

Encryption:

1. Fully homomorphic encryption (FHE) for message encryption:
   $c1=(pk\cdot m+r1)\bmod pk$
2. SHA-3 hashing: $h=\text{SHA3\_Hash}(c1)$
3. Fully homomorphic encryption (FHE) for hash encryption:
   $c2=(pk\cdot h+r2)\bmod pk$

Hybrid decryption algorithm:

The hybrid decryption algorithm is designed to reverse the encryption process and recover the original plaintext message. Initially, the final cipher text $c2$ is decrypted using the FHE scheme, yielding a hash value h. Subsequently, the hash value undergoes a reverse hashing operation through SHA-3, resulting in an intermediate ciphertext $c1$. Finally, FHE decryption is applied to $c1$, using the private key sk to obtain the original plaintext message m. This two-stage decryption process ensures that the original message is retrieved accurately while maintaining the confidentiality introduced by FHE. The hybridization of FHE and SHA-3 enhances the overall security of the decryption process.

Decryption:

1. Fully homomorphic decryption (FHE) for hash decryption:
   $r2=c \bmod sk$
   $h=c-r2\div sk$
2. SHA-3 hashing:
   $c1=\text{SHA3\_Hash}(h)$
3. Fully homomorphic decryption (FHE) for message decryption:
   $r1=c1 \bmod sk$
   $m=c1-r1\div sk$

Hybrid encryption represents a pinnacle in secure data communication, seamlessly blending the strengths of fully homomorphic encryption (FHE) and the SHA-3 hashing algorithm. By encrypting the plaintext message using FHE, bolstered by the introduction of random keys; it establishes a fortified initial layer of security.

4. Result analysis

This paragraph outlines experimental findings both conventional and unique techniques. It is analyzed according to a number of performance criteria, including Time for execution, encryption, and decryption. FHE & SHA-3, AES & RSA, AES &DSA, and Homomorphic encryption & RSA are the existing techniques that were taken into consideration in this work.

Encryption time

The amount of time needed to encrypt the provided data, measured in the milliseconds, is called the encryption time and determined as homomorphic encryption & RSA, AES & RSA, AES &DSA and proposed FHE & SHA-3 in Table 2.

Here, it is examined how a linear increase in key size can result in an increase in encryption time. According to the investigation, the FHE- SHA-3 algorithm it takes a lesser duration to encrypt the

Table 2. Encryption time

S.No	Algorithms	Key Size	Encryption time
1	AES&DES[1]	128 bits	0.001 seconds
2	RSA & AES[23]	2048 bits	0.123 seconds
3	Homomorphic & AES[30]	56 bits	0.09919531 seconds
4	Fully homomorphic & SHA3	2048 bits	0.789 seconds

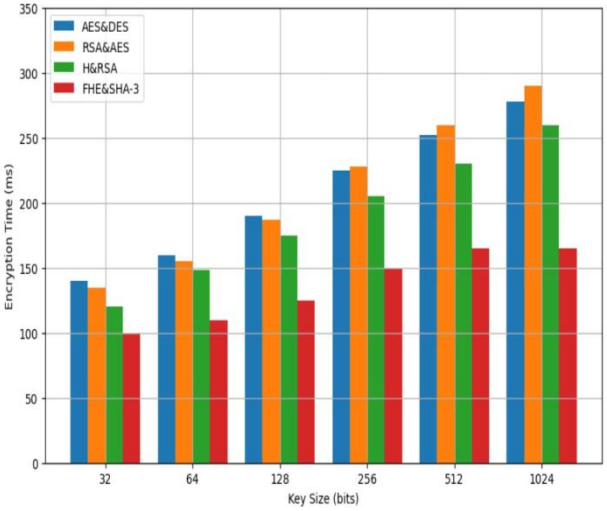


Figure. 3 Encryption time

Table 3. Decryption time

S.No	Algorithms	Key Size	Decryption time
1	AES&DES[1]	128 bits	1.234 seconds
2	RSA & AES[23]	2048 bits	0.256 seconds
3	Homomorphic & AES[30]	56 bits	0.143579162 seconds
4	Fully homomorphic & SHA3	2048 bits	0.001 seconds

data than other methods because the encrypted data is applied via homomorphic techniques in a divided

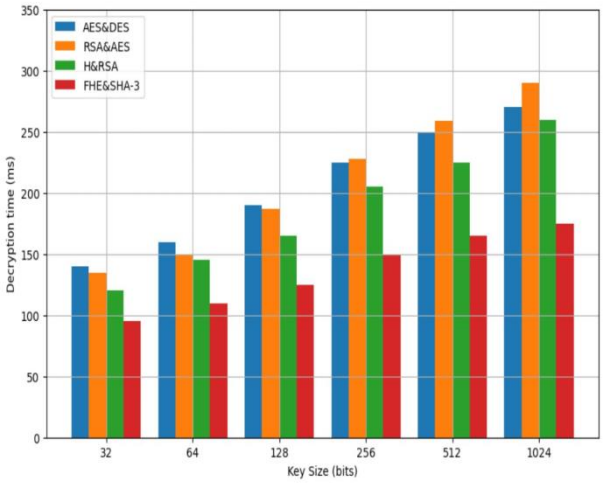


Figure. 4 Decryption time

Table 4. Execution time

S.No	Algorithms	Key Size	Execution time
1	AES&DES [1]	128 bits	0.00547 seconds
2	RSA & AES [23]	2048 bits	0.118 seconds
3	Homomorphic & AES[30]	56 bits	2.35 seconds
4	Fully homomorphic & SHA3	2048 bits	4.25 seconds

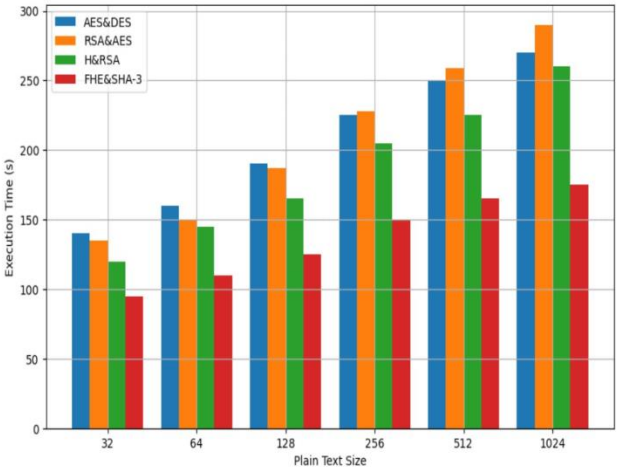


Figure. 5 Execution time

format. The existing AES & RSA, AES & DSA, homomorphic encryption & AES and suggested FHE & SHA-3 techniques to AES & RSA, AES &

DSA, homomorphic encryption & RSA and suggested FHE & SHA3 in Fig. 3.

Decryption time

The time essential for decrypting the protected Information is identified as the decryption time which is shown in milliseconds in Table 3.

The decryption times of the current AES & RSA AES &DSA, homomorphic encryption and &AES and planned FHE & SHA-3 techniques are depicted in Fig. 4 with regard to variable key size (bits). It is clear from this as key size increases linearly, decryption time increases.

Execution time

The calculation the time for cloud data storage access solutions is now another term for time. This illustrates how long it takes for the cloud system to obtain the information from the cloud server after storing it in encrypted form in Table 4.

The computation times for the current AES & RSA, AES&DSA, homomorphic encryption & AES, and suggested FHE & SHA-3, approaches based on different plots, according to the analysis, the suggested FHE technique's overall execution time (measured in ms seconds) is significantly less than that of the existing methods.

In Fig. 5, the proposed mechanism has been evaluated using several metrics, including decryption, encryption, and execution times, and it has been found to outperform existing techniques such as AES & RSA, AES & DSA, homomorphic encryption & RSA by efficiently reducing the complexity.

5. Conclusion and future work

In conclusion, hybrid encryption techniques that combine fully homomorphic encryption (FHE) and secure hash algorithm 3 (SHA-3) offer a promising solution to address security concerns and data storage challenges in cloud computing. Traditional cryptographic techniques may not provide adequate security when dealing with large datasets stored in the cloud. The proposed mechanism utilizes fully homomorphic encryption (FHE) and SHA-3 algorithm to ensure data security. The proposed mechanism has been evaluated using various execution time, encryption time, and decryption time are examples of measurements. The results indicate that it outperforms existing techniques such as AES & RSA, AES & DSA, and homomorphic encryption & RSA works to reduce the complexity of encryption and decoding.

It is suggested that we implemented fully homomorphic SHA3 with 2048 bits, an encryption time of 0.789 seconds, a decryption time of 0.001 seconds, and an execution time of 4.25 seconds. Consequently, we obtain the conclusion that the best way to handle the storing sensitive data in the cloud environments is our proposed hybrid encryption technique.

Conflict of interest

The authors declare no conflict of interest.

Author contributions

Conceptualization Susmitha; methodology, Nikhila; software, validation, Kailash; formal analysis, investigation, Gitanjani; resources, data curation, Nikhila; writing— original draft preparation, Susmitha; writing—review and editing, Yellamma and Nikhila; visualization, supervision, Gitanjani and Kailash.

References

[1] S. Ahmad, S. Mehfu, and B. Javed, "Hybrid cryptographic approach to enhance the mode of key management system in cloud environment", *The Journal of Super Computing*, Vol. 79, pp. 7377–7413, 2022.

[2] J. Rohan and D. Jagli, "Cloud Computing and Security Issues", *Journal of Engineering Research*, Vol. 7, pp. 31-38, 2021.

[3] J. Li, S. Wang, Y. Li, H. Wanng, and J. Chen, "An Efficient Attribute-Based Encryption Scheme with Policy Update and File Update in Cloud Computing", *IEEE Transactions on Industrial Informatics*, Vol. 15, pp. 6500 – 6509, 2019.

[4] P. Liu, "Public-Key Encryption Secure Against Related Randomness Attacks for Improved End-to-End Security of Cloud/Edge Computing", *IEEE Access*, Vol. 8, pp. 16750 – 16759, 2020.

[5] S. Lavanya and Saravanakumar, "Secured two-factor authentication graph-based replication and encryption strategy in cloud computing", *Multimedia Tools and Applications*, pp. 16105–16125, 2022.

[6] D. B Salvakkam and R. Pamula, "Design of Fully Homomorphic Multikey Encryption Scheme for Secured Cloud Access and Storage Environment", *Journal of Intelligent Information Systems*, Vol. 8, pp. 47144–47160, 2022.

[7] S. Gadde, J. Amutharaj, and S. Usha, "A Security Model to Protect the Isolation of

Medical Data in the Cloud Using Hybrid Cryptography", *Journal of Information Security*, Vol. 73, pp. 770–777, 2023.

[8] A. Kousalya and N. Baik, "Enhance Cloud Security and Effectiveness Using Improved RSA-based RBAC with XACML Technique", *International Journal of Intelligent Networks*, Vol. 4 , pp. 62-67, 2023.

[9] J. Y. Deshmuk, S. K. Yada, and G. M. Bhandari, "Attribute-Based Encryption Mechanism with Privacy-Preserving Approach in Cloud Computing", *Materials Today Proceedings*, Vol. 80, pp. 1786-1791, 2023.

[10] A. Z. Abdulkader, "Cloud Data Security Mechanism Using the Light Weight of Cryptography", *International Journal for Light and Electron*, Vol. 271, 2022.

[11] H. S. Murad and H. Kamel, "Implementation and performance analysis of Hybrid Cryptographic Schemes Applied in cloud computing Environment", *Procedia Computer Science*, Vol. 194, pp. 165–172, 2021.

[12] F. Thabit, A. Sharaf, and S. Jagtap, "Security Analysis and Performance Evaluation New Light Eeight of Cryptographic Algorithm for Cloud Computing", *Global Transitions Proceedings*, Vol. 2, pp. 100-110, 2021.

[13] E. K. Subramanian and L. Tamilselvan, "Elliptic curve Diffie–Hellman cryptosystem in big data cloud", *Cluster Computing*, Vol. 23, pp. 3057–3067, 2020.

[14] J. Xia and J. Xu, "Fast Homomorphic Encryption Based on Hybrid System in Cloud", *Web Information Systems and Applications*, Vol. 11242, pp. 79–90, 2018.

[15] M. K Hossen, G. Morsad, and A. C. Roy, "An approach for enhancing security of cloud data using cryptography and steganography with E-LSB encoding technique", *International Journal of Computer Science and Network Security*, Vol. 18, 2018.

[16] H. Huang and H. Zong, "Secure matrix multiplication based on fully homomorphic encryption", *Journal of Super Computing*, Vol. 79, pp. 5064–5085, 2023.

[17] L. Ge, Z. He, and H. Wei, "Research on Full Homomorphic Encryption Algorithm for Integer in Cloud Environment", *Intelligent Computing Methodologies*, Vol. 11645, pp. 109–117, 2019.

[18] B. Ahaheen and F. Siddiqui, "Comparsion Between RSA Algorithm and Modified RSA Algorithm Used in the Cloud Computing", *Inventive Computation Technologies*, Vol. 98, pp. 218–224, 2020.

[19] C. Lin, J. Liu, and T. Chu, "On the Performance of Cracking Hash Function SHA-1 Using a Cloud and GPU Computing", *Wireless Personal Communications*, Vol. 109, pp. 491–504, 2019.

[20] K. R. Sajay, S. S. Babu, and Y. Vijayalakshmi, "Enhancing the security of cloud data using hybrid encryption algorithm", *Journal of Ambient Intelligence and Humanized Computing*, Vol. 8, pp. 27–32, 2019.

[21] V. K. Veerabathiran and M. Devi, "Improving secured ID-based authentication for cloud computing through novel hybrid fuzzy-based homomorphic proxy re-encryption", *Soft Computing*, Vol. 24, pp. 18893–18908, 2020.

[22] Z. Zhang, P. Zeng, B. Pan, and K. K. R. Choo, "Large-universe attribute-based encryption with public traceability for cloud storage", *IEEE Internet of Things Journal*, Vol. 7, pp. 10314 – 10323, 2020.

[23] D. Tiwari, A. Singh, and A. Prabhakar, "Performance Analysis of AES, RSA and Hashing Algorithm Using Web Technology", *Computing Algorithms with Applications in Engineering*, Vol. 18, pp. 413–418, 2020.

[24] L. Megouache, A. Zitouni, and M. Djoudi, "Ensuring user authentication and data integrity in multi-cloud environment", *Human-Centric Computing and Information Sciences Journal*, Vol. 15, pp. 10-15, 2020.

[25] M. L. Akkar and C. Giraud, "An Implementation of DES and AES of Secure against some Attacks", *Cryptographic Hardware and Embedded Systems*, Vol. 2162, pp. 309–318, 2001.

[26] P. H. Kumar and G. S. AnandhaMala, "HMAC-R: Hash-based message authentication code and Rijndael-based multilevel security model for data storage in cloud environment", *Journal of Supercomputing*, Vol. 79, pp. 181–3209, 2023.

[27] G. Prabukanna and Vasudeva, "A fully homomorphic– elliptic curve cryptography based encryption algorithm for ensuring the privacy preservation of the cloud data", *Cluster Computing*, Vol. 22, pp. 9561–9569, 2019.

[28] S. Selvi and M. Gopi, "Hyper Elliptic Curve Based Homomorphic encryption Scheme for Cloud Data Security", In: *Proc. of International Conference on Intelligent Data Communication Technologies and Internet of Things*, Vol. 26, pp. 71-78, 2018.

[29] M. L. Akkar1 and C. Giraud2, "An Implementation of DES and AES, Secure against Some Attacks", *Cryptographic Hardware and Embedded Systems*, pp. 309–318,

2001.
[30] Y. Alkady, F. Farouk, and R. R. Rizk, "Fully Homomorphic Encryption with AES in Cloud Computing Security", In: *Proc. of the International Conference on Advanced Intelligent Systems and Informatics*, Vol. 845, pp. 370–382, 2019.
[31] S. Karimunnisa and Y. Pachipala, "An AHP based Task Scheduling and Optimal Resource Allocation in Cloud Computing", *International Journal of Advanced Computer Science and Applications*, Vol. 14, pp. 149-159, 2023.
[32] S. Karimunnisa and Y. Pachipala, "Task Classification and Scheduling Using Enhanced Coot Optimization in Cloud Computing", *International Journal of Intelligent Engineering and Systems*, pp. 501-511, 2023.
[33] V. Ganesan, M. Sobhana, G. Anuradha, P. Yellamma, O. R Devi, K. B Prakash, and J. Naren, "Quantum inspired meta-heuristic approach for optimization of genetic algorithm", *Computers and Electrical Engineering*, Vol. 94, 2021.
[34] N. Annamareddy, L. G Donepudi, L. Parvathaneni, K. B.V. B. Rao, J. Putta, and P. Yellamma "Comparison of Various Face Recognition Algorithms in ML/DS", In: *Proc. of 2nd International Conference on Sustainable Computing and Data Communication Systems*, pp. 126-131, 2023.
[35] K. V. Kousik, M. A. Tony, K. S. Krishna, S. Narisety, and P. Yellamma, "An E-Commerce Product Feedback Review using Sentimental Analysis", In: *Proc. of 6th International Conference on Inventive Computation Technologies*, pp. 608-613, 2023.
[36] A. Oppermann, A. Yurchenko, M. Esche, and J. Seifert, "Secure Cloud Computing: Multithreaded Fully Homomorphic Encryption for the Legal Metrology", In: *Proc. of International Conference on Intelligent, Secure*, Vol. 10618, 2017.
[37] K. N. Gottipati, N. Peddisetty, S. Pothireddy, G. Botta, P. Yellamma, and G. Swain, "A Study on Data Security and Privacy Issues in Cloud Computing", In: *Proc. of Third International Conference on Artificial Intelligence and Smart Energy*, 2023.