Journal of Information Systems Engineering and Management
2025, 10(22s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

A Hybrid Encryption Model with Blockchain Integration for Secure Cloud Data Storage and Retrieval

Firas Mohammed Khalaf *1, Ali Makki Sagheer2

1 2 Computer Science Department, University of Anbar, Ramadi, Iraq

Emails: fir21c1014@uoanbar.edu.iq; ali_makki@uoanbar.edu.iq

ARTICLE INFO

Received: 22 Dec 2024

Revised: 31 Jan 2025

Accepted: 19 Feb 2025

ABSTRACT

Data security, privacy, sensitivity, and integrity are major concerns when using cloud-based storage solutions. In this paper, we propose a hybrid encryption model that has been integrated with blockchain technology to secure data storage in the cloud. The proposed model facilitates data encryption using a symmetric cryptography algorithm for efficient large data encryption while ensuring the encryption key can only be exchanged using asymmetric cryptography. This model utilizes the power of blockchain to manage metadata securely and associated encryption keys to ensure that records are tamper-proof, removing the need for third parties to be trusted. The security, key management, and data integrity of the proposed model are better than traditional cloud storage and existing blockchain-based approaches. The performance evaluation suggests that the model achieves a balance between security and cost efficiency, while moderate transaction speed will be witnessed owing to blockchain operations. Our proposed work aims to provide a scalable, fast, reliable, and decentralized architecture-based solution to address the challenges of cloud data security.

Keywords: Hybrid Encryption, Blockchain Technology, Cloud Data Security, Secure Cloud Storage.

INTRODUCTION

Cloud computing can provide high-performance services from a resource-sharing environment that is independent of location [1]. Cloud computing provides us with conveniences in our daily lives but also introduces security issues and cyberattacks like authentication exploitation, sniffing, spoofing, resource manipulation, etc. [2]. This sharing between resources, services, and networks makes the cloud computing environment more crucial to face such security challenges. In addition, since the user is saving data at third-party premises remotely, data security is very essential [3][4]. Thus, it is important to encrypt the data of the users in the form of ciphertext through cryptography algorithms to secure them from unauthorized access and to keep the data confidentiality and integrity. Data cryptography techniques have been used in the different deployment models of cloud computing, such as public, private, and hybrid models as well as in the different cloud service models [5].

Blockchain is a digital ledger that stores transactions shared among a distributed network of computers (nodes) [6]. When a part of data has been added to the blockchain ledger, it cannot be changed or deleted and is computationally infeasible to change or remove. All the participants in the network must approve when someone wants to add to the ledger, each of whom has a copy of the current blockchain, run the algorithm to validate the proposed transaction [7]. If most nodes agree that the new transaction appears to be valid, which means identifying information matches the history of that particular blockchain, the new transaction will be approved, and a new block will be linked to the chain. that it means only approved transactions can be added to the blockchain and reject all transactions not approved by blockchain nodes [8].

blockchain-based security approaches aim to enhance security, transparency, and efficiency in cloud computing systems by leveraging the unique features of blockchain technology. They address critical challenges in trust management and provide a robust framework for building trust-enabled cloud environments [9].

1. CRYPTOGRAPHY

Cryptography has existed for over two thousand years. It deals with the art of secure communication and provides the science of keeping communication confidential through the use of encryption techniques. The plaintext can be any data, like text messages, numeric data, or computer programming. Ciphertext is the output using the plain text with an encryption algorithm and key which results from the ciphertext. The ciphertext can then be sent to the recipient, who decrypts it with the decryption algorithm using the key to recover the plaintext [10]. There are two major types of key cryptographic symmetric key and asymmetric key cryptography.

Symmetric key Cryptography using the same key to encrypt and decrypt the data, it is known as symmetric key cryptography. The implication is that the user A and user B must agree on a key (k) named “shared secret” before they send the ciphertext owned to the other party, the key must be shared by secure channels. Symmetric key cryptography has a wide range of applications, but most widely used in secure file transfer protocols. Symmetric cryptosystems are faster compared to asymmetric cryptosystems generally, when dealing with large data [11].

There are many types of symmetric encryption algorithms, in this paper, we focus on advanced encryption standards (AES), NIST (National Institute of Standards and Technology) defines the AES algorithm as a standard. it is a symmetric block cipher; however, it isn't founded on a Feistel network. The AES in a broad sense uses a substitution-permutation network. Not only does it give more security, but it also gives more speed, the block size is fixed 128 bits and supports three keys (128 bits, 192 bits and 256 bits) according to the AES standards. AES stands for Advanced Encryption Standard and is named based on the key length: AES-128, AES-192, and AES-256 depending on the key of choice [12].

Asymmetric key cryptography, also known as key exchange or "public key cryptography," is a breakthrough introduced by Diffie and Hellman [13]. This is to solve the key distribution problem in a symmetric cryptography system using digital signatures. Asymmetric key cryptography does not remove the need for symmetric key cryptography. They typically enhance each other; one’s strengths can offset the weaknesses of the other. One of these pairs is a public key, the other a private key for the sender and receiver respectively. The Sender creates the ciphertext by encrypting the plaintext message m using the encryption algorithm E with the receiver public key, then sends the ciphertext c to the receiver. The receiver decrypts the ciphertext using decryption algorithm D and its private key to get the original plaintext. The RSA algorithm is named after Ron Rivest, Adi Shamir, and Leonard Adleman and is perhaps the most widely implemented cryptographic algorithm[14]. It relies on the fact that even though it is easy to multiply numbers together it is hard to find the prime factors of a very large composite number. That's why it is different from many classical ciphers where plaintext and ciphertext are bits. In RSA, plaintext and ciphertext respectively belong to integers in the range 0 to n-1 for some n.

The public key of the RSA scheme is a tuple (e, n), where n is known as the modulus and e is known as the public exponent. The private key then is (d, n), where n is the same modulus and d is the private exponent.

2. RELATED WORK

Various studies looked into hybrid encryption to build a security model between cloud users and service providers. Marwan Adnan Darwish et al. [15] proposed a privacy-preserving cloud storage scheme based on a hybrid encryption algorithm and blockchain technology. The system uses AES for data encryption in a symmetric way and ECC for key exchange while creating user-specific keys from user credentials and giving users client-side control over their data. Digital signatures, derived from the hash, can then be written into a tamper-proof blockchain, the experiment was done in a blockchain network using three Ethereum nodes. while the actual encrypted data sits safely in the cloud, allowing for decentralized verification of integrity. In a virtual cloud environment. The method overcomes the inherent risks of tampered records, unauthorized data access, and excessive dependencies on cloud providers for data privacy by decentralizing the trust due to the utilization of the blockchain and pre-encrypting the data before outsourcing, thus providing stronger data confidentiality, integrity, and user privacy.

In 2023, Sankar et al. [16] proposed a third-party auditing framework based on strong blockchain techniques applicable to cloud storage solutions. Using this framework, clients can store sensitive information remotely in a secure way and provide services on demand with no need to maintain it locally. It uses the RSA method of providing privacy by generating key codes based on system-specific data for authentication. The User End Generated (UEG) privacy method decreases third-party involvement while also enhancing security evaluation with the automatic logging of suspicious events. Blockchain technology enables decentralization, end-user breakdown audibility, and privacy for multi-tiered data access in networking environments.

In 2023, Geetha S. K et al. [17] proposed a framework that combines blockchain technology coupled with advanced encryption techniques to improve both the security and integrity of sensitive cloud data. Homomorphic encryption and AES are used for data, while a hybrid RSA (HE-RSA) algorithm is developed to secure cryptographic keys. Various Cloud service provider (CSP) keeps the data of clients in encrypted format, each CSP generates the hash of their data at certain time interval specified by the client. Those hashes are subsequently stored as transactions via Byzantine Fault Tolerance (BFT) on a private Ethereum blockchain in order to guarantee honest computation, as well as consensus among the CSPs. In addition, integrity is verified independently by comparing master hashes in the blockchain to those stored off-chain, which means that tampering will be detected early without having to trust CSPs. Gas fees are minimized by leveraging a private Ethereum network and clients may scale verification frequency according to their budget and data growth. The scheme presently recognizes breaches but not the specific data compromised and draws on a micro-game-theoretic analysis to establish a high degree of cost-efficient integrity confidentiality, and privacy.

Mohammad Ariff et al. [18] Proposed integration of blockchain technology with cloud data storage is a milestone in ineffective data management. This system is composed by two main components that operate to process and insert the data into the blockchain and retrieve the data from the blockchain respectively. Processing and diversion of data to the blockchain only converts raw data into the most secure ciphered data in accordance with updated methods of encryption. The very first step is inserting the raw data into the system in the text file format. Once inserted, this simple text file goes through a process to make it a binary file that only has the binary values ‘1’ and ‘0’. Its an important stage because it makes the data ready for security. Next, the processed file will be encrypted using the AES encryption algorithm in CBC mode, the algorithm used with the hashing method used is SHA-256 which was previously mentioned These encryption techniques are used to maintain the confidentiality of the data in the blockchain environment.

Mohammed Y. Shakor et al. [19] suggested new methods which can safeguard sensitive data in the cloud. The primary question concerns the vulnerability of data that is stored in the cloud, and the need for enhanced encryption and key management architectural practices.] The suggested framework consists of a two-level policy. The first level is dynamic Advanced Encryption Standard (AES) key generation, which means that a unique and ever-changing key encrypts each file. This technique provides considerable security at the file level, making it significantly more difficult for an adversary to recover multiple files if they obtain an encryption key. The next tier innovates with the integration of blockchain, effectively maintaining keys with associated metadata in a secure manner, greatly enhancing the level of security as well as the integrity of the data. In addition, the use of Elliptic Curve

Cryptography (ECC) public key encryption further improves security when data is transmitted and at storage, and supports safe file sharing. Problem Statement.

Fan Chen et al. [20] proposed a scheme that builds on AES-256 encryption and supports cloud security in a multi-tenant environment by using blockchain technology. This hybrid model leverages blockchain (utilizing Hyperledger Fabric with PBFT for consensus) for decentralized and tamper-proof logging of data transactions, combined with AES-256 for data privacy. The sensitive data are first encrypted and uploaded to the cloud storage; the Key Management system (KMS) in control of the encryption keys the hash of which is logged in the blockchain and can be verified from there. Every record of access and modification is stored in an immutable log at the blockchain layer, which speeds up breach detection (up to 10 milliseconds for complete breach detection) and ensures data integrity. Even though this is a suitable solution to providing privacy, it incurs moderate computational overhead (5-7% from encryption, 10-15ms latency per blockchain transaction and capability to scale over hundreds of proposals due to the need for consensus).

3. THE PROPOSED MODEL

This paper proposes a hybrid architecture encryption model for Secure data storage and retrieval based on blockchain shown in (Fig 1). The proposed model component comprises four primary components: the blockchain network, cloud provider, hybrid encryption approach, and the user. This model proposes to form the backbone of safeguarding the confidentiality, integrity, and security of data across its lifecycle in the cloud.

On the left side of (fig 1), can see the blockchain network composed of several hosting nodes chained together. Metadata exchange and key exchange processes can be facilitated by blockchain. Metadata exchange refers to storing information detailing the transaction-related information ownership and access and key exchange refers to securely sharing encryption keys between the participating entities. Blockchain’s decentralized and tamper-proof nature ensures these exchanges are transparent and resistant to unauthorized modifications.

The encrypted data is stored inside the level of the cloud provider which is shown at the top of the (fig 1). In the proposed model, it encrypts the data, and after that uploads it to cloud storage the data is secured so even If the cloud provider attempts to hack it,. Since no data-related metadata and encryption keys are being stored on the cloud, it is maintained using a blockchain network meaning unauthorized data access is reduced in the proposed model.

In the center the hybrid encryption model shows the combination of the symmetric and asymmetric approach for securing the data. The symmetric algorithm is the first encryption algorithm, it is stripes for a set of large, it is much faster than asymmetric. The asymmetric algorithm is the second algorithm, it is handles to send and secure symmetric keys.

The proposed model provides the interface for user to interact with and perform encryption before uploading data into the cloud, and performing decryption after retrieving the data. Blockchain ensures that the access rights and rules for decryption of a user are first verified on the network, resulting in data privacy and secure access control.

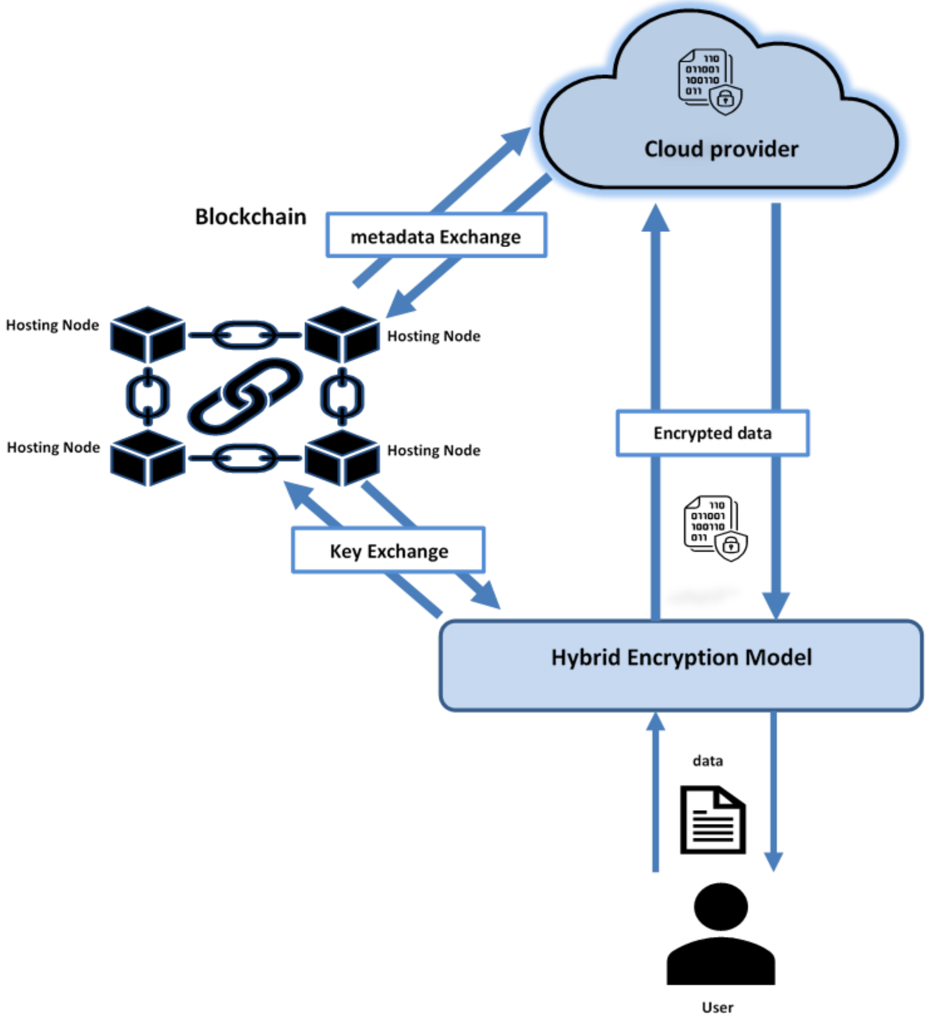

Figure 1: Proposes Hybrid Architecture Encryption Model

In this paper focused on Hybrid encryption, it is a fundamental component of the proposed model. The hybrid encryption provides the foundational security mechanisms needed to ensure data confidentiality, integrity, and authentication. The sensitive data uploaded by the User is secured by the hybrid encryption algorithm, which prepares the data for secure storage or transmission. It works closely with the Blockchain to insert cryptographic operations into blockchain transactions, making it impossible to change the data.

Serving as the security framework foundation, this hybrid encryption utilizes both symmetric encryption (AES) for encrypting larger data formats such as images and asymmetric encryption (RSA) for implementing a secure key exchange and digital signatures. It ensures that sensitive user data remains protected at all times of interaction with the model, whether that is at the point of storage within the cloud or transfer across the blockchain.

A. Key Generation and Management

Key Generation and Management in the proposed model is a core function within the hybrid encryption algorithm that ensures secure communication and data handling. As detailed in the Key Generation and Management Algorithm (1), a unique cryptographic key pair (consisting of a public key and a private key) is generated for each user used the proposed model at start point Below show why to generate the pairing key for the users:

1) Public Key: This is shared openly and used for encryption and verifying digital signatures. Anyone can use the public key to encrypt messages intended for the user.

2) Private Key: This is kept secret and is used for decryption and signing data. Only the user knows their private key, ensuring confidentiality and authenticity.

Algorithm (1): Key Generation and Management

```
Input: User ID, Password
Output: Generated Key Pair (Public Key, Private Key)
Step 1: Start
Step 2: Accept the User ID and Password if Valid.
Step 3: Generate a cryptographic key pair using an asymmetric algorithm:
    -   Call Key Generation Algorithm () to produce:
        Public Key (PK)
        Private Key (SK)
Step 4: Encrypt the private key using the user's password:
    -   Encrypted Private Key = Encrypt (SK, Password)
Step 5: Store the keys:
    -   Save the Public Key (PK) in the Blockchain layer for public access.
    -   Save the Encrypted Private Key at the user.
Step 6: Associate the key pair with the User ID in the model.
Step 7: Provide the Public Key to the user and confirm registration.
Step 8: End
```

B. Data Encryption and Decryption

Data Encryption and Decryption is a crucial process for ensuring the confidentiality and security of data stored in the proposed model. The model employs a hybrid encryption model, combining symmetric and asymmetric encryption techniques to maximize both efficiency and security.

AES (Advanced Encryption Standard) is a symmetric encryption algorithm used to encrypt user's data in the proposed model, such as images or files. Symmetric encryption is chosen for its speed and efficiency especially when dealing with large datasets.

Data Encryption Algorithm (3.3) show Hybrid encryption-based data encryption algorithm helps in secure storage of user data. In the first part, a unique AES key is created for that session, and the user data is then encrypted using AES encryption. Because AES is a symmetric encryption method, this means also have the AES key to secure; hence, encrypt it with RSA using the user public key so that, of course, only the matching private key decrypts the AES key. Finally, the encrypted data and the encrypted AES key are stored in a cloud in such a way that they can only be retrieved and decrypted by the proper users.

Algorithm (2): Data Encryption

```
Input: User Data (Data), User Public Key (Public Key)
Output: Encrypted Data (Enc Data), Encrypted AES Key (EncAESKey)
Step 1: Start
Step 2: Generate a unique AES key for this session.
    AES Key = Generate AES Key()
Step 3: Encrypt the user data using AES:
    Enc Data = AES Encrypt (Data, AES Key)
Step 4: Encrypt the AES key using RSA with the user’s public key:
    EncAESKey = RSAEncrypt(AESKey, PublicKey)
Step 5: Store Enc Data and EncAESKey securely in the cloud.
Step 6: End
```

In algorithm (3) The data decryption algorithm follows a structured process to securely retrieve the original user data. It starts by decrypting the AES key using RSA with the user's private key, ensuring that only authorized users can access the AES key. Once the AES key is decrypted, it is then used to decrypt the encrypted data using AES decryption, effectively restoring the original plaintext data. Finally, the decrypted data is returned for use. This method ensures security by combining the efficiency of AES for data encryption with the robustness of RSA for key protection, preventing unauthorized access.

Algorithm (3): Data Decryption

```
Input: Encrypted Data (EncData), Encrypted AES Key (EncAESKey), User Private Key (PrivateKey)
Output: Decrypted Data (DecData)
Step 1: Start
Step 2: Decrypt the AES key using RSA with the user’s private key:
    AESKey = RSADecrypt(EncAESKey, PrivateKey)
Step 3: Decrypt the data using AES with the decrypted AES key:
    DecData = AESDecrypt(EncData, AESKey)
Step 4: Return the decrypted data.
Step 5: End
```

4. Result and Discussion

Unauthorized access attacks occur when an attacker attempts to gain access to sensitive data, such as encrypted images or transaction details, without proper authorization. The Proposed Model mitigates this risk through robust encryption and access control mechanisms. First, sensitive data, such as images, is encrypted using AES (Advanced Encryption Standard), a symmetric encryption algorithm. The AES key itself is further encrypted using the user's RSA public key, ensuring that only the user with the corresponding private key can decrypt the data. This dual-layer encryption ensures that even if an attacker gains access to the encrypted data, they cannot decrypt it without the private key.

Man-in-the-middle (MITM) attacks involve an attacker intercepting communication between the user and the model to steal or manipulate data. The Proposed Model is designed to prevent such attacks through encryption, digital signatures, and secure communication protocols. First, all data transmitted within the model, such as transaction details and block information, is signed using the user's private key. This ensures that any attempt to modify the data in transit will result in a failed signature verification, alerting the model to the tampering.

sensitive data, such as AES keys and encrypted images, is protected using strong encryption. Even if an attacker intercepts the data, they will be unable to decrypt it without the corresponding private key. This makes the intercepted data useless to the attacker. Additionally, the model uses HTTPS for secure communication with AWS S3, ensuring that data transmitted between the user and the cloud storage service is encrypted and protected from interception.

the model's reliance on blockchain technology further mitigates the risk of MITM attacks. Since each block is cryptographically linked to the previous block, any attempt to alter the data in transit would break the chain's integrity, making the tampering immediately detectable. The combination of encryption, and secure communication protocols ensures that the model is highly resistant to MITM attacks.

A. Comparison with The Traditional Cloud

The Proposed Model was compared against traditional cloud storage methods. The comparison highlights the advantages of the Proposed Model.

Table 1 Comparison with The Traditional Cloud

Feature	Traditional Cloud	Proposed model
Data Integrity	Low	High
Data Security	Medium	High
Transaction Speed	High	Medium
Cost Efficiency	Medium	Medium

The table (1) comparing the two focuses primarily on the benefits of the proposed solution versus traditional cloud solutions. Since data integrity is guaranteed by immutability with transparency of distributed ledger technology, the Proposed Model exceeds in that area. Unlike individual cloud systems, when a traditional cloud system goes down it typically impacts multiple parties since the system is highly centralized, making it more vulnerable to a single point of failure or data corruption. In comparison, the Proposed Model leaves all data unchanged and all records verifiable, a solution in particular advantageous for sectors or applications where the accuracy and trust in data is still rather high.

But with trade-offs in areas like transaction speed, the traditional cloud remains highly performant, since all the data from cloud users can be processed in one point, and thus more quickly. The Proposed Model is medium in speed and offers increased Data efficient Security using the combination of cryptography and decentralized storage, and prevents from leakage of any sensitive information. Both systems are proven to be relatively cost-efficient, further illustrating that while the Proposed Model offers increased security and integrity, these enhancements do not always result in greater cost associated with operating the model. It is this more balanced approach that makes for a more balanced hybrid model in terms of capability and security and seems to maintain a relatively low-cost price to ability cost penalty.

B. Comparison with Related Work

The proposed model achieves better security than existing cloud storage by the integration of a hybrid encryption scheme (data AES, key RSA) with a practically useful implementation of a blockchain. This is to help maintain the confidentiality and integrity of data throughout its lifecycle. In contrast to other works, it provides a strong security basis through the use of both symmetric and asymmetric encryption. Table 2 show the Comparison with related work according to Encryption Technique Blockchain Platform Key Management Security Features and Security Features with proposed model.

Table 2 Comparison with Related Work

Research Work	Encryption Technique	Blockchain Platform	Key Management	Security Features	Limitations
[15]	AES + ECC	Ethereum	User-specific keys derived from credentials	Data confidentiality, integrity, user privacy	Ethereum gas fees, limited scalability
[16]	RSA	Not specified	System-specific key codes	Third-party auditing, privacy safeguards, automatic activity recording	Third-party auditing reliance, possible bottlenecks
[17]	AES + HE-RSA	Private Ethereum	Hybrid key management	Data integrity verification, reduced gas fees, scalability	Does not identify specific data breaches
[18]	AES + SHA-256	Not specified	Not specified	Secure data transformation and encryption	Focus on data processing, lacks detailed key management
[19]	AES (Dynamic) + ECC	Not specified	Blockchain-based key storage	Dynamic key generation, secure file sharing	Computational complexity, potential latency
[20]	AES-256	Hyperledger Fabric	Key Management System (KMS)	Immutable logging, fast breach detection	Computational overhead, blockchain transaction latency
Proposed Model	AES + RSA	Custom Blockchain Network	Blockchain-based key exchange	Data confidentiality, integrity, secure access control	Moderate transaction speed

Unlike some existing works that either lack detailed key management strategies or rely on third parties, the proposed model securely manages keys using a blockchain-based approach. This eliminates the need for external trust, reducing the risk of key compromise. Blockchain's immutability ensures data integrity, similar to the work by [17] and [20]. However, the proposed model simplifies the verification process, ensuring that data is not altered without detection. The proposed model strikes a balance between security and cost. Private blockchain networks reduce transaction fees compared to public networks like Ethereum in [15], making it more affordable for organizations. While the proposed model ensures high security, it experiences moderate transaction speeds due to blockchain operations and encryption processes. This is a common challenge observed across other hybrid encryption and blockchain-based models. The proposed model effectively mitigates unauthorized access and MITM attacks through dual-layer encryption and blockchain validation. This is comparable to the methods suggested by [19] and [16] , which emphasize encryption and secure auditing. Dynamic AES key generation enhances file-level security in the proposed model, resembling the approach by [19]. This makes it more resilient against key compromise attacks compared to static key systems.

5. CONCLUSION

this paper proposed a high-level hybrid encryption model with integrated blockchain technology, addressing cloud data encryption and retrieval securely and efficiently by employing the AES to encrypt large amounts of data into encrypted files and the RSA to exchange the key used to encrypt the big files The suggested model not only preserves confidentiality and integrity but also guarantees a secure key management mechanism as a result of the usage of a custom Blockchain, which in return, provides tamper-proof and decentralized key management with records that Gutenberg, as a system based on blockchain, can use to enhance the security of the data stored in it the new model reaches a remarkable cost efficiency to the price/security ratio compared to the other traditional cloud systems and the other existing approaches. While speeds are moderate for transactions, the value of the model providing security to sensitive data far outweighs this uneasiness. This work represents an important step towards making cloud data more secure, with a scalable and pragmatic path for organizations looking to protect their digital assets.

6. REFERENCES

[1] N. Subramanian and A. Jeyaraj, “Recent security challenges in cloud computing,” *Computers & Electrical Engineering*, vol. 71, pp. 28–42, Oct. 2018, doi: 10.1016/J.COMPELECENG.2018.06.006.

[2] H. Tabrizchi and M. Kuchaki Rafsanjani, “A survey on security challenges in cloud computing: issues, threats, and solutions,” *Journal of Supercomputing*, vol. 76, no. 12, pp. 9493–9532, Dec. 2020, doi: 10.1007/S11227-020-03213-1/METRICS.

[3] Z. Balani and H. Varol, “Cloud Computing Security Challenges and Threats,” *8th International Symposium on Digital Forensics and Security, ISDFS 2020*, Jun. 2020, doi: 10.1109/ISDFS49300.2020.9116266.

[4] A. Orobosade, T. Aderonke, A. Boniface, and A. J., “Cloud Application Security using Hybrid Encryption,” *Communications on Applied Electronics*, vol. 7, no. 33, pp. 25–31, May 2020, doi: 10.5120/CAE2020652866.

[5] V. Agarwal, A. K. Kaushal, and L. Chouhan, “A Survey on Cloud Computing Security Issues and Cryptographic Techniques,” *Lecture Notes in Networks and Systems*, vol. 100, pp. 119–134, 2020, doi: 10.1007/978-981-15-2071-6_10.

[6] I. Tyan, A. Guevara-Plaza, M. I. Yagüe, J. Alegria Quintela, and J. Gonçalves Antunes, “The Benefits of Blockchain Technology for Medical Tourism,” *Sustainability 2021, Vol. 13, Page 12448*, vol. 13, no. 22, p. 12448, Nov. 2021, doi: 10.3390/SU132212448.

[7] S. Davidson, P. De Filippi, and J. Potts, “Disrupting Governance: The New Institutional Economics of Distributed Ledger Technology,” *SSRN Electronic Journal*, Jul. 2016, doi: 10.2139/SSRN.2811995.

[8] K. Wust and A. Gervais, “Do you need a blockchain?,” *Proceedings - 2018 Crypto Valley Conference on Blockchain Technology, CVCBT 2018*, pp. 45–54, Nov. 2018, doi: 10.1109/CVCBT.2018.00011.

[9] W. Li, J. Wu, J. Cao, N. Chen, Q. Zhang, and R. Buyya, “Blockchain-based trust management in cloud computing systems: a taxonomy, review and future directions,” *Journal of Cloud Computing*, vol. 10, no. 1, pp. 1–34, Dec. 2021, doi: 10.1186/S13677-021-00247-5/FIGURES/23.

[10] B. Singhal, G. Dhameja, and P. S. Panda, “Beginning Blockchain,” *Beginning Blockchain*, 2018, doi: 10.1007/978-1-4842-3444-0.

[11] M. Stamp, *Information security: principles and practice*. John Wiley & Sons, 2011.

[12] J. Nechvatal *et al.*, “Report on the Development of the Advanced Encryption Standard (AES),” *J Res Natl Inst Stand Technol*, vol. 106, no. 3, p. 511, 2001, doi: 10.6028/JRES.106.023.

[13]W. Diffie, W. Diffie, and M. E. Hellman, “New Directions in Cryptography,” *IEEE Trans Inf Theory*, vol. 22, no. 6, pp. 644–654, 1976, doi: 10.1109/TIT.1976.1055638.

[14] R. Imam, Q. M. Areeb, A. Alturki, and F. Anwer, “Systematic and Critical Review of RSA Based Public Key Cryptographic Schemes: Past and Present Status,” *IEEE Access*, vol. 9, pp. 155949–155976, 2021, doi: 10.1109/ACCESS.2021.3129224.

[15] M. A. Darwish, E. Yafi, M. A. Al Ghamdi, and A. Almasri, “Decentralizing Privacy Implementation at Cloud Storage Using Blockchain-Based Hybrid Algorithm,” *Arab J Sci Eng*, vol. 45, no. 4, pp. 3369–3378, Apr. 2020, doi: 10.1007/S13369-020-04394-W/METRICS.

[16] S. M. U. Sankar, D. Selvaraj, G. K. Monica, and J. Katiravan, “A Secure Third-Party Auditing Scheme Based on Blockchain Technology in Cloud Storage,” *International Journal of Engineering Trends and Technology*, vol. 71, no. 3, pp. 23–32, Apr. 2023, doi: 10.14445/22315381/IJETT-V71I3P204.

[17] S. K. Geetha, R. Naveenkumaran, K. Selvaraju, C. Kishore, and A. Nagha Rathish, “Blockchain based Mechanism for Cloud Security,” *2nd International Conference on Sustainable Computing and Data Communication Systems, ICSCDS 2023 - Proceedings*, pp. 1287–1295, 2023, doi: 10.1109/ICSCDS56580.2023.10105053.

[18] M. A. Z. Bin Idrus, F. D. A. Rahman, O. O. Khalifa, and N. M. Yusoff, “Blockchain-based Security for Cloud Data Storage,” *ICSIMA 2023 - 9th IEEE International Conference on Smart Instrumentation, Measurement and Applications*, pp. 73–77, 2023, doi: 10.1109/ICSIMA59853.2023.10373457.

[19] M. Y. Shakor, M. I. Khaleel, M. Safran, S. Alfarhood, and M. Zhu, “Dynamic AES Encryption and Blockchain Key Management: A Novel Solution for Cloud Data Security,” *IEEE Access*, vol. 12, pp. 26334–26343, 2024, doi: 10.1109/ACCESS.2024.3351119.

[20] F. Chen, “Enhancing Cloud Computing Security with Blockchain: A Hybrid Approach to Data Privacy and Integrity,” *Journal of Computing and Electronic Information Management*, vol. 14, no. 2, pp. 75–79, Sep. 2024, doi: 10.54097/7QTZWC77.