International Journal of Engineering Trends and Technology
ISSN: 2231–5381 / https://doi.org/10.14445/22315381/IJETT-V72I4P110

Volume 72 Issue 4, 92-100, April 2024
© 2024 Seventh Sense Research Group®

Original Article

Hybrid Approach to Cloud Storage Security Using ECC-AES Encryption and Key Management Techniques

Yaser M.A. Abualkas[1], D. Lalitha Bhaskari[2]

[1,2]*Department of Computer science and systems engineering, Andhra University, India.*

[1]*Corresponding Author : yaserabualkas.gf@andhrauniversity.edu.in*

Received: 25 November 2023 Revised: 30 March 2024 Accepted: 11 April 2024 Published: 24 April 2024

Abstract - *The rising popularity of cloud storage offers convenient and scalable data storage, yet its security remains a pressing concern, given the remote storage of sensitive information. While Advanced Encryption Standard (AES) ensures secure storage, challenges arise in key distribution and management. In contrast, elliptic curve cryptography (ECC) excels in efficient key management but has data size limitations. To overcome these hurdles, a hybrid ECC-AES approach has emerged. However, optimizing and evaluating its integration into cloud storage systems is essential. This study addresses the need to develop, assess, and enhance a hybrid ECC-AES approach for secure cloud storage. By focusing on implementation and performance optimization, this research strives to bolster the security and efficiency of cloud storage systems, contributing to the advancement of secure and scalable solutions in cloud storage technology; the proposed algorithm employs a hybrid technique involving ECC-AES encryption and sophisticated key management for heightened security. It encompasses steps to generate a random AES key, encrypt it using the ECC public key, and then split and store the encrypted AES key securely. The data is encrypted with the AES key and stored in cloud storage. For decryption, the encrypted data and AES key parts are retrieved. The ECC private key decrypts the AES key parts, which are then combined to form the complete AES key for decrypting the data. The algorithm ensures secure access control and authentication mechanisms, including role-based access control and two-factor authentication, and implements key rotation for periodic AES key changes to enhance security. By combining ECC-AES encryption and advanced key management techniques, this approach aims to enhance cloud data security effectively and comprehensively.*

Keywords - *Cloud storage, Security, Hybrid approach, ECC-AES, Data encryption, Key distribution, Key management, Advanced Encryption Standard, Elliptic curve cryptography, Implementation, Performance optimization, Secure storage, Scalable solutions.*

1. Introduction

The proliferation of cloud storage has revolutionized data management, yet concerns persist over its security, particularly in the remote storage of sensitive information. While the Advanced Encryption Standard (AES) provides robust security, challenges arise in key distribution and management. Conversely, Elliptic Curve Cryptography (ECC) offers efficient key management but is constrained by data size limitations. In addressing this gap, a hybrid ECC-AES approach has emerged. However, its integration into cloud storage systems requires optimization and evaluation. This study aims to develop, assess, and enhance a hybrid ECC-AES approach for secure cloud storage. By prioritizing implementation and performance optimization, our research endeavors to strengthen the security and efficiency of cloud storage systems. The proposed algorithm employs a hybrid technique involving ECC-AES encryption and sophisticated key management, encompassing steps to generate a random AES key, encrypt it using the ECC public key and securely split and store the encrypted AES key parts. Data is then encrypted with the AES key and stored in cloud storage. For decryption, the algorithm retrieves the encrypted data and AES key parts, decrypts the AES key parts using the ECC private key, and combines them to form the complete AES key for decrypting the data. The algorithm also ensures secure access control and authentication mechanisms, such as role-based access control and two-factor authentication. It implements key rotation for periodic AES key changes to enhance security. By amalgamating ECC-AES encryption and advanced key management techniques, this approach aims to comprehensively enhance cloud data security effectively.[1]

Elliptic Curve Cryptography (ECC) stands as a groundbreaking cryptographic technique that has garnered widespread attention for its remarkable efficiency and formidable security attributes [2]. Rooted in the realm of public-key cryptography, ECC capitalizes on the distinctive mathematical properties exhibited by elliptic curves [3].

These curves, defined by mathematical equations in a finite field, underpin ECC's ability to yield heightened security levels with considerably shorter key lengths than conventional cryptographic methods. The underlying strength of ECC lies in its ability to provide robust security while demanding less computational resources. This is particularly significant in resource-constrained environments, such as embedded systems and mobile devices, where efficiency is paramount. ECC achieves this efficiency by leveraging complex algebraic operations on elliptic curves, such as point addition and scalar multiplication, which result in intricate relationships that are computationally demanding to reverse-engineer.

The application scope of ECC spans a myriad of domains, solidifying its position as a versatile cryptographic solution. In the realm of secure communications, ECC is utilized to establish secure channels for data transmission, ensuring confidentiality and integrity. Its implementation in digital signatures renders a method for verifying the authenticity and origin of digital documents, fostering trust in digital interactions. Additionally, ECC finds its prowess in data encryption, facilitating the secure storage and transmission of sensitive information [4].

Notably, ECC excels in providing strong security even in scenarios where key lengths are constrained, offering a vital advantage in a world where resource efficiency and security are of paramount concern. Its adoption continues to grow as industries recognize its potential to bolster cryptographic protocols while mitigating the resource overhead associated with longer key lengths. As the digital landscape evolves, ECC remains a cornerstone in the pursuit of safeguarding information and communications with unparalleled efficiency and robustness.

Advanced Encryption Standard (AES) stands as a pivotal milestone in the domain of symmetric encryption, celebrated for its exceptional speed, security, and extensive adoption [5]. Its design embodies a block cipher structure that underscores its efficacy in safeguarding data confidentiality and integrity across a plethora of applications. Established as a federal standard by the National Institute of Standards and Technology (NIST) in 2001 [6], AES has gained prominence as a versatile and robust encryption algorithm.

At the heart of AES lies its systematic transformation of plaintext into ciphertext, achieved through a series of well-defined steps. The core of AES's security lies in its utilization of a Substitution Permutation Network (SPN), a complex arrangement of substitution and permutation operations that ensures the data's confidentiality even when subjected to scrutiny by attackers.

The algorithm operates on fixed-size blocks of data, typically 128, 192, or 256 bits in length. The key length corresponds to the chosen block size, with AES-128, AES-192, and AES-256 utilizing 128, 192, and 256-bit keys [7], respectively. The encryption process encompasses successive rounds of operations, including the substitution of bytes through substitution boxes (S-boxes), permutation of bits, mixing columns, and adding round keys generated from the encryption key.

One of AES's most remarkable attributes is its speed, owing to its efficient structure and parallel processing capabilities. This swiftness has contributed to its wide adoption in various applications, ranging from secure communications and digital payments to cloud computing and data storage.

AES has garnered global acceptance due to its strength, performance, and standardized nature. Its symmetric encryption paradigm is particularly suitable for scenarios where the same key is used for both encryption and decryption, streamlining processes. Nonetheless, it's important to note that key management and distribution remain crucial aspects in AES implementations to ensure the algorithm's effectiveness and security.

In essence, AES serves as a cornerstone in the cryptographic landscape, offering a reliable and efficient means to protect sensitive information [8]. Its widespread use underscores its resilience and versatility, making it a stalwart choice for securing data in diverse technological ecosystems.
The Hybrid Approach to Cloud Storage Security, employing a combination of Elliptic Curve Cryptography (ECC) and Advanced Encryption Standard (AES) [9], coupled with sophisticated Key Management Techniques, has emerged as a groundbreaking solution to address the pressing security challenges associated with cloud storage systems. This approach harnesses the strengths of both ECC and AES, leveraging their individual attributes to create a robust security framework for safeguarding data stored in cloud environments.

Elliptic Curve Cryptography (ECC) brings its prowess in key distribution and management to the table. With its ability to provide strong security using shorter key lengths, ECC efficiently handles the critical task of encrypting and decrypting the encryption keys, ensuring that only authorized users can access the sensitive data. This is particularly advantageous in cloud storage scenarios, where efficient key management is paramount to maintaining data security.

On the other hand, Advanced Encryption Standard (AES) offers its speed and reliability, making it an ideal choice for encrypting the actual data blocks stored in the cloud. AES's symmetric encryption model facilitates fast encryption and decryption processes, ensuring that data remains confidential and integral during storage and retrieval operations. The synergy of ECC and AES in the Hybrid Approach provides a multi-layered defense mechanism. ECC's robust key management enhances the overall security posture, while AES contributes to efficient and secure data encryption. Moreover, the implementation of key splitting techniques further fortifies the system against potential breaches, ensuring that even if one part of the encrypted key is compromised, the data remains protected.

A significant advantage of this Hybrid Approach is its adaptability and scalability. By combining ECC and AES, organizations can tailor their security strategy to their specific needs, selecting the appropriate encryption method for different aspects of their cloud storage infrastructure [1]. This versatility allows for the optimization of security while maintaining operational efficiency.

Furthermore, the Hybrid Approach doesn't solely rely on cryptographic techniques. It also encompasses advanced key management techniques that contribute to the overall robustness of the security framework. This includes strategies like key rotation, where encryption keys are changed at regular intervals, minimizing the impact of potential key compromises.

In conclusion, the Hybrid Approach to Cloud Storage Security using ECC-AES Encryption and Key Management Techniques presents a sophisticated solution to the security challenges inherent in cloud storage systems. By capitalizing on the strengths of ECC and AES and incorporating advanced key management strategies, this approach offers enhanced data protection, efficient encryption processes, and adaptability, making it a vital component in ensuring the confidentiality, integrity, and availability of sensitive data in the cloud.

2. Literature Review

Survey on encryption techniques used to secure cloud storage system [11] This review explores various encryption techniques and security mechanisms employed in cloud storage systems. It highlights the significance of ECC and AES in enhancing data security. The study provides insights into the challenges faced and the benefits reaped by combining these techniques within a hybrid framework.

Enhancing Cloud Security with Hybrid Encryption Algorithms [12] Focusing on hybrid encryption approaches, this literature investigates the fusion of cryptographic algorithms for bolstering cloud security. It delves into the advantages of combining ECC and AES, discussing how their synergy can mitigate vulnerabilities and enhance data protection in cloud storage.

Cryptographic key management issues and challenges in cloud services [13] This review concentrates on the critical aspect of key management in cloud storage security. It evaluates the complexities associated with securely storing and distributing encryption keys. It underscores how a hybrid approach, such as ECC-AES, can address these challenges and contribute to efficient key management.

Hybrid AES-ECC model for the security of data over cloud storage [1] This study examines the performance of ECC and AES in securing cloud data. It analyzes their individual strengths and weaknesses and assesses the potential benefits of combining these techniques within a hybrid model. The review offers insights into the overall improvement in security and efficiency.

Cloud security using hybrid cryptography algorithms [10] Focusing on cryptographic techniques for cloud security, this review investigates the benefits of hybrid approaches. It discusses how combining ECC and AES can provide a comprehensive security solution for cloud storage. It highlights the advantages of harnessing the strengths of both algorithms to enhance data protection and user access control; the following is a conclusion for the surveys.

Survey on encryption techniques used to secure cloud storage system

- Evaluate the performance of encryption techniques like ECC and AES in cloud storage.
- Analyze the scalability and resource utilization of encryption methods.
- Investigate the challenges faced in optimizing performance within hybrid encryption frameworks.
- Examine the effectiveness of combining ECC and AES for enhancing data security.
- Provide insights into the benefits and limitations of different encryption techniques in cloud environments.

Enhancing Cloud Security with Hybrid Encryption Algorithms

- Assess the encryption time associated with hybrid ECC-AES approaches.
- Analyze the efficiency of hybrid encryption techniques in reducing encryption time.
- Investigate how hybrid encryption methods enhance data protection in cloud storage.
- Evaluate the complexity and effectiveness of combining ECC and AES for bolstering cloud security.
- Provide recommendations for optimizing encryption time and improving data security in cloud environments.

Cryptographic key management issues and challenges in cloud services

- Evaluate the decryption time required for managing encryption keys in cloud security.
- Analyze the efficiency of key management techniques in ensuring data confidentiality.
- Investigate the complexities associated with securely storing and distributing encryption keys.

- Assess the effectiveness of hybrid ECC-AES approaches in addressing key management challenges.
- Provide insights into the importance of efficient key management in mitigating security risks in cloud storage.

Hybrid AES-ECC model for the security of data over cloud storage

- Examine the avalanche effect of combining ECC and AES encryption techniques.
- Analyze how hybrid encryption algorithms obscure relationships between input and output data.
- Evaluate the security benefits of hybrid ECC-AES approaches for cloud storage.
- Investigate the robustness of hybrid encryption methods in protecting data confidentiality.
- Provide recommendations for implementing hybrid encryption techniques to enhance cloud security.

Cloud security using hybrid cryptography algorithms

- Assess the power consumption associated with hybrid ECC-AES encryption techniques.
- Analyze the energy efficiency of hybrid encryption algorithms in cloud environments.
- Investigate the computational overhead and resource utilization of hybrid encryption methods.
- Evaluate the advantages of hybrid cryptography approaches in minimizing power consumption.
- Provide insights into the potential of hybrid encryption techniques to improve energy efficiency and enhance cloud security.

3. Problem Statement

Cloud storage has gained widespread popularity for its convenient and scalable data storage and sharing capabilities. Despite its advantages, the security of cloud storage remains a significant concern due to the storage of sensitive data on remote servers.

Traditional encryption methods like Advanced Encryption Standard (AES) ensure security, but they exhibit limitations in terms of effective key distribution and management. Conversely, Elliptic Curve Cryptography (ECC) offers enhanced efficiency and security in key management, albeit with constraints on data size for encryption.

To overcome these constraints, a hybrid solution combining ECC and AES has been proposed. However, the successful implementation and performance assessment of such a hybrid approach within cloud storage environments necessitates careful evaluation and optimization. Thus, the central challenge lies in developing and evaluating a hybrid approach employing ECC-AES for securing cloud storage. The primary focus is on refining the implementation and optimizing performance. This research endeavor aims to not only bolster the security and efficiency of cloud storage systems but also contribute to the advancement of secure and scalable solutions for cloud storage.

4. Proposed Approach

The proposed approach would involve using ECC to encrypt the AES key, which would then be used to encrypt and decrypt the actual data. This would provide an additional layer of security since the AES key would be protected by ECC encryption. The system would also use key management techniques such as key rotation and key splitting to further enhance security.

In addition to encryption, the system would implement access control and authentication mechanisms to ensure that only authorized users could access the data. This could be achieved through the use of user accounts, role-based access control, and two-factor authentication.

The proposed hybrid approach would address the limitations of traditional encryption methods such as RSA, which require larger key sizes to achieve the same level of security as ECC. It would also provide better protection against attacks such as brute force attacks and man-in-the-middle attacks.

Overall, a hybrid approach using ECC-AES could provide a strong solution for improving the security of cloud storage systems, making them more resilient to attacks, and ensuring that data is kept secure and confidential.

5. Analysis of System Architecture and Design

The "Hybrid Approach to Cloud Storage Security Using ECC-AES Encryption and Key Management Techniques" algorithm presents an innovative solution to enhance the security of cloud-stored data. In an era where data is increasingly stored in the cloud for its convenience and scalability, ensuring robust security measures is paramount.

The algorithm takes as input the data to be securely stored in the cloud, the key for the Advanced Encryption Standard (AES), and both the public and private keys for elliptic curve cryptography (ECC). Its primary output is the encrypted data, safeguarded against unauthorized access. The algorithm employs a series of sophisticated steps to achieve this:

- It generates a random AES key to encrypt the data, ensuring a high level of security.
- This AES key is then encrypted using the ECC public key, making it secure for transmission.
- The encrypted AES key is split into two parts using a key-splitting technique. One part is stored securely.
- The remaining part of the encrypted AES key is utilized to encrypt the data using the AES encryption algorithm.
- The encrypted data is then securely stored in cloud storage.

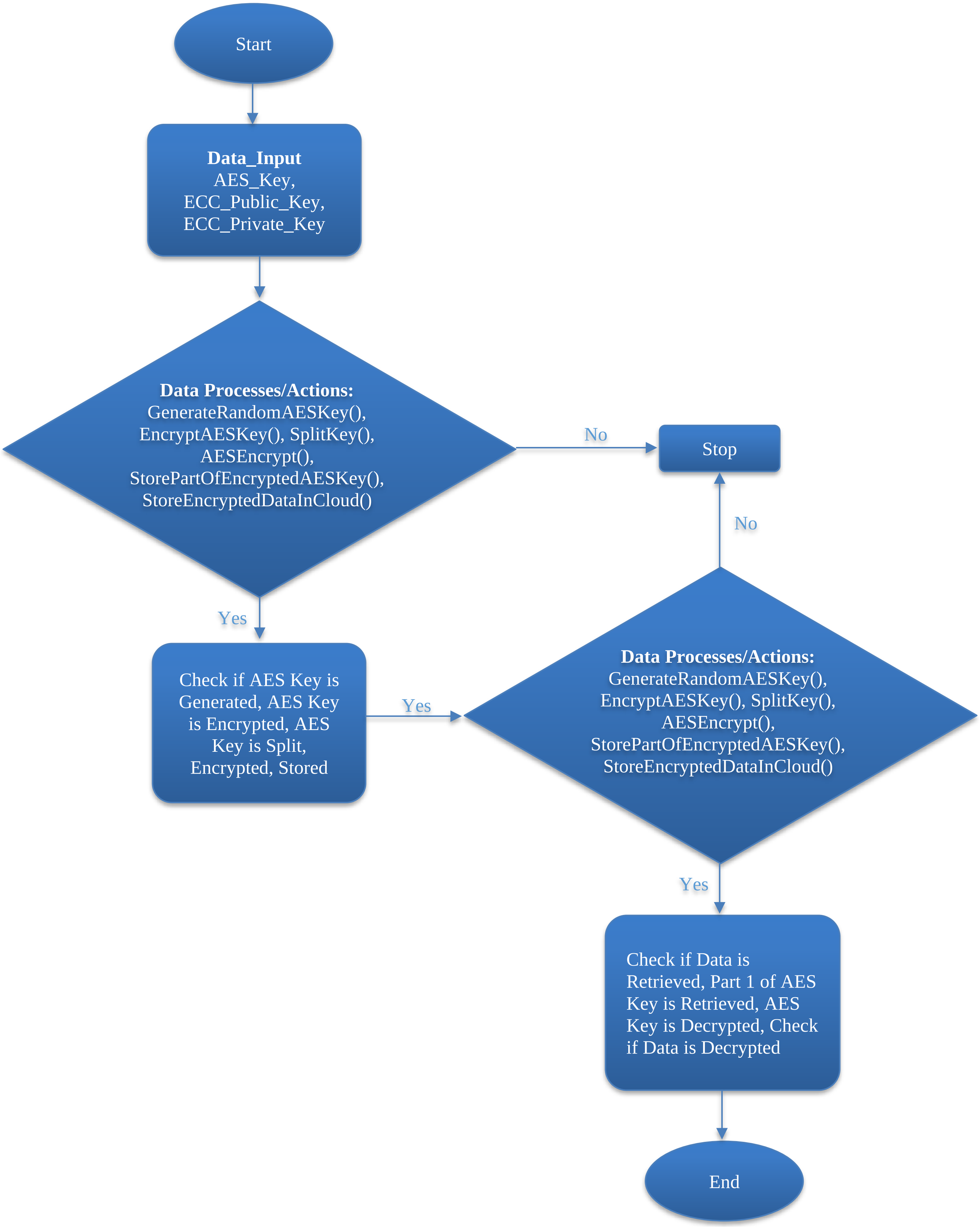
Start
Data_Input
AES_Key,
ECC_Public_Key,
ECC_Private_Key
Data Processes/Actions:
GenerateRandomAESKey(),
EncryptAESKey(), SplitKey(),
AESEncrypt(),
StorePartOfEncryptedAESKey(),
StoreEncryptedDataInCloud()
No
Stop
No
Yes
Check if AES Key is Generated, AES Key is Encrypted, AES Key is Split, Encrypted, Stored
Yes
Data Processes/Actions:
GenerateRandomAESKey(),
EncryptAESKey(), SplitKey(),
AESEncrypt(),
StorePartOfEncryptedAESKey(),
StoreEncryptedDataInCloud()
Yes
Check if Data is Retrieved, Part 1 of AES Key is Retrieved, AES Key is Decrypted, Check if Data is Decrypted
End

Fig. 1 Flowchart representation for the proposed approach

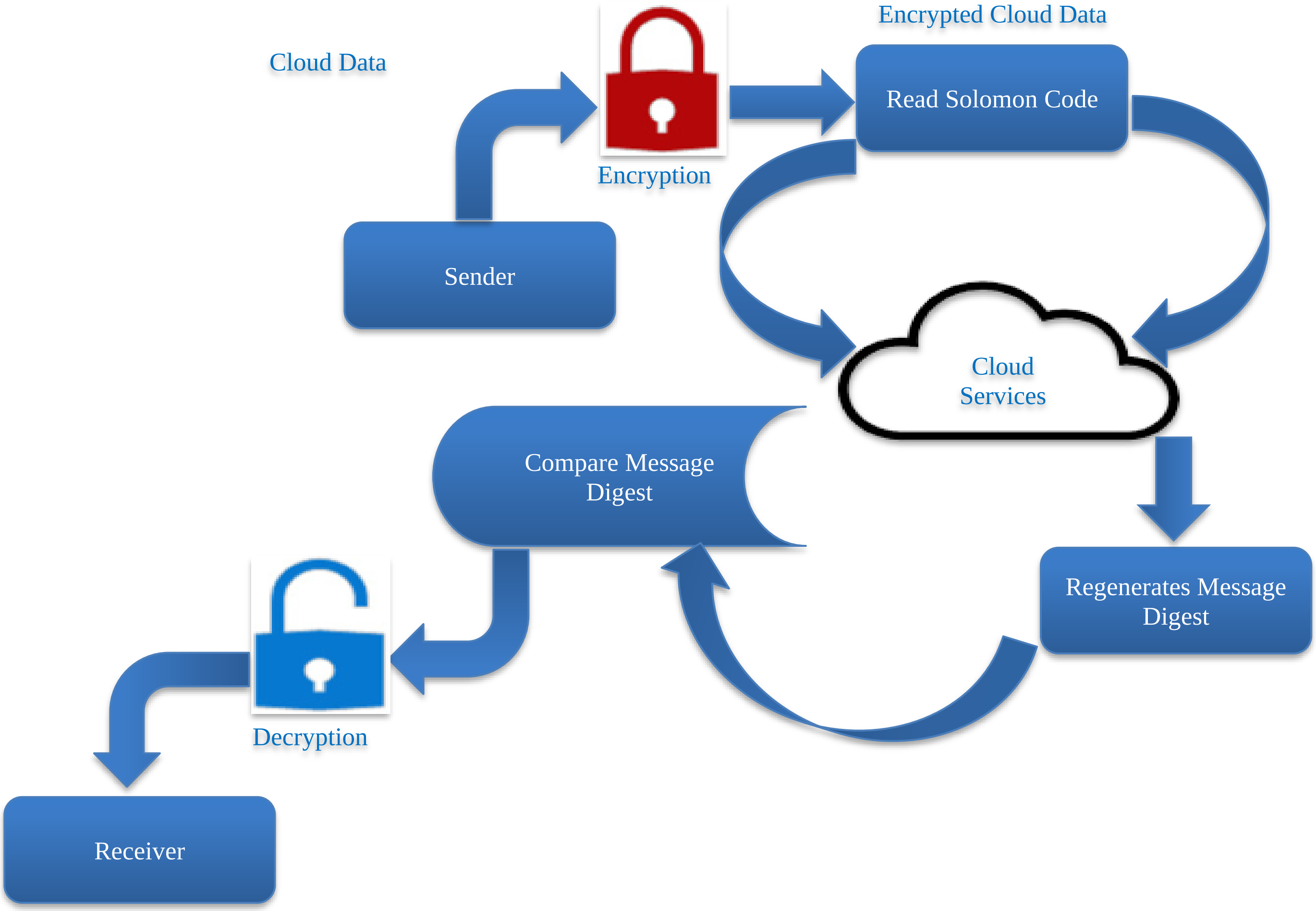

Fig. 2 Hybrid approach to cloud storage security using ECC-AES encryption

To ensure data retrieval, the algorithm includes a decryption process

- The ECC private key is used to decrypt the two parts of the encrypted AES key.
- The two parts are combined to obtain the complete AES key.
- The complete AES key is employed to decrypt the encrypted data using the AES decryption algorithm.
- Access control and authentication mechanisms, including user accounts, role-based access control, and two-factor authentication, ensure that only authorized users can access the data.
- The algorithm further enhances security by implementing key rotation techniques periodically changing the AES key.

Decryption is a crucial process for restoring encrypted data to its original form, and the algorithm provides a secure and efficient means to achieve this. It leverages the strengths of ECC and AES encryption techniques while emphasizing key management best practices.

It is important to highlight that the security of this hybrid approach hinges on the strength of the ECC and AES algorithms, as well as the robustness of the key management techniques employed. Strong and well-tested algorithms, along with meticulous key management strategies like key rotation and key splitting, contribute to the overall security of this innovative cloud storage solution. Table 1 outlines key criteria for evaluating the proposed algorithm's efficacy in securing data within cloud storage systems. Firstly, the Performance Analysis criterion scrutinizes the algorithm's efficiency and effectiveness in securely storing and retrieving data, considering factors like speed and resource usage.

Secondly, the Encryption Time metric measures the duration required for data encryption using the AES encryption algorithm and ECC public key, providing insights into encryption speed. Thirdly, Decryption Time evaluates the algorithm's efficiency in decrypting data using the ECC private key and AES decryption algorithm, shedding light on its decryption speed. The Avalanche Effect criterion gauges the algorithm's sensitivity to input changes, determining how much variations in data affect encrypted output.

Table 1. Performance metrics of the proposed algorithm

Criteria	Description
Performance Analysis	The proposed algorithm's performance is analyzed in terms of its efficiency and effectiveness in securely storing and retrieving data in cloud storage.
Encryption Time	The time taken by the algorithm to encrypt data using the AES encryption algorithm and ECC public key is evaluated.
Decryption Time	The time required for the algorithm to decrypt encrypted data using the ECC private key and AES decryption algorithm is assessed.
Avalanche Effect	The extent to which changes in the input data impact the encrypted output is measured to evaluate the avalanche effect of the algorithm.
Power Consumption	The algorithm's power consumption during the encryption and decryption processes is analyzed to assess its energy efficiency and resource utilization.

Algorithm: Hybrid Approach Using ECC_AES

```
Input:
    Data to be stored in the cloud (Data)
    Key for Advanced Encryption Standard (AES) (AES_Key)
    Public key for elliptic curve cryptography (ECC) (ECC_Public_Key)
    Private key for ECC decryption (ECC_Private_Key)
Output:
    Encrypted data (Encrypted_Data)
Begin:
    # Encryption Process
    Random_AES_Key = GenerateRandomAESKey()
    Encrypted_AES_Key = EncryptAESKey(Random_AES_Key, ECC_Public_Key)
    Split_Encrypted_AES_Key = SplitKey(Encrypted_AES_Key)
    Encrypted_Data = AESEncrypt(Data, Random_AES_Key)
    StorePartOfEncryptedAESKey(Split_Encrypted_AES_Key)
    StoreEncryptedDataInCloud(Encrypted_Data)
    # Decryption Process (If needed)
    Retrieved_Encrypted_Data = RetrieveEncryptedDataFromCloud()
    Retrieved_Part1_AES_Key = RetrievePart1OfEncryptedAESKey()
    Decrypted_AES_Key = DecryptAESKey(Retrieved_Part1_AES_Key, ECC_Private_Key)
    Decrypted_Data = AESDecrypt(Retrieved_Encrypted_Data, Decrypted_AES_Key)
    # Providing access control and authentication mechanisms is not shown in this pseudo-code.
End.
```

Lastly, Power Consumption assesses the algorithm's energy efficiency during encryption and decryption processes, illuminating its impact on resource utilization within cloud environments. Together, these criteria offer a comprehensive evaluation of the algorithm's performance and suitability for secure cloud data management. The outcomes of implementing the "Hybrid Approach to Cloud Storage Security Using ECC-AES Encryption and Key Management Techniques" algorithm are as follows:

1. Enhanced Data Security: The primary goal of this algorithm is to significantly enhance the security of data stored in the cloud. By combining the efficiency of Elliptic Curve Cryptography (ECC) and the robustness of the Advanced Encryption Standard (AES), the algorithm ensures that data is protected against unauthorized access and breaches.
2. Efficient Key Management: The use of ECC for key distribution and management streamlines the process and

reduces the risk associated with key exchange. It offers a more efficient method for securely transmitting the AES key to authorized users.

3. Protection Against Unauthorized Access: The algorithm incorporates access control and authentication mechanisms, such as user accounts, role-based access control, and two-factor authentication. These measures guarantee that only authorized users with the necessary credentials can access the encrypted data.
4. Secure Data Retrieval: The decryption process ensures that authorized users can retrieve and decrypt the data accurately. The use of ECC private keys and AES decryption ensures data integrity during retrieval.
5. Key Rotation for Ongoing Security: Implementing key rotation techniques at regular intervals enhances the security of the system over time. By periodically changing the AES key, the algorithm mitigates the risk associated with prolonged exposure to a single encryption key.
6. Scalable Cloud Storage: The algorithm is designed for use in cloud storage systems, providing a scalable and secure solution for organizations with varying data storage needs.
7. Optimized Performance: The hybrid approach balances security with performance, offering an efficient means of securing data in the cloud without compromising system responsiveness.
8. Protection of Sensitive Information: Sensitive and confidential information, including personal, financial, and proprietary data, is safeguarded from potential threats, ensuring the privacy and confidentiality of stored data.
9. Compliance with Security Standards: The algorithm aligns with established security standards and best practices, making it suitable for organizations that need to adhere to specific compliance requirements.
10. Reduced Security Concerns: By addressing key distribution and management challenges associated with traditional encryption methods, the algorithm reduces security concerns related to cloud storage and encourages wider adoption of cloud-based solutions.

6. Conclusion

In conclusion, the "Hybrid Approach to Cloud Storage Security Using ECC-AES Encryption and Key Management Techniques" algorithm holds the potential to significantly enhance the security, efficiency, and reliability of cloud storage systems. It offers a comprehensive solution that balances cryptographic strength with practical implementation, making it a promising avenue for organizations seeking to secure their cloud-stored data. The proposed hybrid approach combines the strengths of Elliptic Curve Cryptography (ECC) and the Advanced Encryption Standard (AES) to enhance the security of cloud storage systems. By encrypting the AES key using ECC and implementing key splitting and rotation techniques, the algorithm offers a robust solution to protect sensitive data stored in the cloud. Additionally, access control mechanisms and two-factor authentication ensure that only authorized users can access the encrypted data.

The future scope of the "Hybrid Approach to Cloud Storage Security Using ECC-AES Encryption and Key Management Techniques" algorithm is promising and multifaceted. It encompasses optimizing performance, ensuring scalability for larger datasets and user numbers, integrating with emerging technologies such as blockchain, addressing quantum computing threats, improving usability and user experience, seeking standardization for industry adoption, conducting continuous threat analysis, ensuring cross-platform compatibility, aligning with regulatory compliance standards, and promoting educational and awareness programs.

The algorithm's evolution will be driven by ongoing research and development efforts aimed at enhancing its efficiency, security, and applicability across diverse cloud storage environments.

Acknowledgment

I would also like to extend my thanks to ANDHRA UNIVERSITY for providing a conducive environment for research and learning.

References

[1] Saba Rehman et al., “Hybrid AES-ECC Model for the Security of Data Over Cloud Storage,” *Electronics*, vol. 10, no. 21, pp. 1-20, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[2] Turki Aljrees et al., “Enhancing IoT Security through a Green and Sustainable Federated Learning Platform: Leveraging Efficient Encryption and the Quondam Signature Algorithm,” *Sensors*, vol. 23, no. 19, pp. 1-28, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[3] Joppe W. Bos et al., “Elliptic Curve Cryptography in Practice,” *Financial Cryptography and Data Security: 18th International Conference*, Christ Church, Barbados, vol. 8437, pp. 157-175, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[4] Jianbing Ni et al., “Securing Fog Computing for Internet of Things Applications: Challenges and Solutions,” *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 601-628, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[5] Damilare Nimat Akogun, “*Enhancing Data Security in Cloud Storage Using Residue Number System and Advanced Encryption Standard*,” M.Sc Thesis, Kwara State University, Nigeria, pp. 1-24, 2020. [Google Scholar] [Publisher Link]

[6] Michael D. Garris et al., "*User's Guide to NIST Fingerprint Image Software (NFIS)*," National Institute of Standards and Technology, NIST Interagency/Internal Report, pp. 1-192, 2001. [Google Scholar] [Publisher Link]

[7] Ria Andriani, Stevi Ema Wijayanti, and Ferry Wahyu Wibowo, "Comparision of AES 128-, 192- and 256-Bit Algorithm for Encryption and Description File," *2018 3rd International Conference on Information Technology, Information System and Electrical Engineering (ICITISEE)*, Yogyakarta, Indonesia, pp. 120-124, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[8] Maroti Deshmukh, and Arjun Singh Rawat, "Secure Key Sharing Scheme Using Hamiltonian Path," *International Journal of Information Technology*, vol. 15, pp. 4141-4147, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[9] Samiksha Sharma, and Vinay Chopra, "Data Encryption using Advanced Encryption Standard with Key Generation by Elliptic Curve Diffie-Hellman," *International Journal of Security and its Applications*, vol. 11, no. 3, pp. 17-28, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[10] Sanjeev Kumar et al., "Cloud Security Using Hybrid Cryptography Algorithms," *2021 2nd International Conference on Intelligent Engineering and Management (ICIEM)*, London, United Kingdom, pp. 599-604, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[11] R. Kirubakaramoorthi, D. Arivazhagan, and D. Helen, "Survey on Encryption Techniques Used to Secure Cloud Storage System," *Indian Journal of Science and Technology*, vol. 8, no. 36, pp. 1-7, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[12] P. Kavitha Rani et al., "Enhancing Cloud Security with Hybrid Encryption," *2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC)*, Salem, India, pp. 1445-1450, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[13] Ramaswamy Chandramouli, Michaela Iorga, and Santosh Chokhani, *Cryptographic Key Management Issues and Challenges in Cloud Services*, Secure Cloud Computing, Springer, New York, NY, pp. 1-30, 2013. [CrossRef] [Google Scholar] [Publisher Link]