Journal of Information Systems Engineering and Management
2025, 10(34s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Enhancing Cloud Data Security using a Hybrid Cryptographic Model: A Combination of Advanced Encryption Standard and Elliptic Curve Cryptography

Saman Khan [1], Dr. S. H. Abbas [2]

[1] *Integral University: Department of Computer Science and Engineering Lucknow, India. mail2samankhan@gmail.com*

[2] *Integral University: Department of Computer Science and Engineering Lucknow, India. shabbas@iul.ac.in*

ARTICLE INFO

Received: 30 Dec 2024
Revised: 03 Feb 2025
Accepted: 12 Feb 2025

ABSTRACT

With cloud computing, users may easily access and store confidential data remotely over the internet at any time and from any location at a reasonable cost. But there is security risks associated with this convenience. Due to its third-party accessibility, data on the cloud is vulnerable to authentication and data integrity attacks. Furthermore, there is a higher chance of data exposure, leakage, and loss in different locations when several users access data simultaneously across different internet connections. Elliptic Curve Cryptography is one of the cryptographic techniques and protocols that have been developed to solve these concerns. To maintain security and integrity in cloud environments, this paper presents a hybrid cryptographic system to improve data security in cloud environments by combining the Advanced Encryption Standard (AES) with Elliptic Curve Cryptography (ECC). The proposed model makes use of ECC to generate secure keys, which reduces key size while preserving strong security. This enhances the overall performance and efficiency of the encryption and decryption processes. By combining the advantages of ECC and AES, the framework ensures that data stored in the cloud remains secure, confidential, and only accessible to authorized users. In terms of data integrity and authentication, the study's findings demonstrate that the suggested hybrid approach performs better than traditional cryptographic methods. The experimental results show that, in comparison to existing methods, the proposed strategy is more efficient and produces better outcomes.

Keywords: Cloud Computing, ECC, AES, Data Security, Authentication and Data Integrity.

INTRODUCTION

With its many functions, such as large-scale database storage, networking, and communication, cloud computing has become known as a major computing paradigm that can be accessed from any place. Due to its attractive features, people have become more dependent on cloud services, which has led to the huge data gathering that has raised privacy and security issues. Data security is one of the main issues with cloud services since users may unintentionally or intentionally create data breaches. Restriction on data access is necessary to avoid unauthorized access to sensitive data. Devices themselves may potentially be a threat to data security because users may unintentionally reuse data and APIs, which can result in data loss.

Cryptographic techniques are frequently utilized to secure data stored in the cloud by implementing encryption and decryption processes using different keys to address these security challenges. [1]

Asymmetric key encryption, sometimes referred to as public-key cryptography, uses two keys: a public key is used for encryption and a private key is used for decryption. On the other hand, symmetric key encryption uses a single private key for both encryption and decryption. To protect the data and prevent unauthorized access by hackers, the private key is required. The disadvantage of symmetric cryptography techniques is that they require a large key size to provide sufficient security.

This paper proposes a hybrid AES- ECC method to address this problem, which reduces the key size without compromising data security [2].

Journal of Information Systems Engineering and Management
2025, 10(34s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Table 1. *Contains a list of abbreviations used in this paper.*

Abbreviations	Description
AES	Advanced Encryption Standard
ECC	Elliptic curve cryptography
RSA	Rivest-Shamir-Adleman
PHECC	Polynomial-based Hashing Elliptic Curve Cryptography
NIST	National Institute for Standards and Technology.
EAP- CHAP	Extensible Authentication Protocol: Challenge Handshake Authentication Protocol.
GDLP	Generalized Discrete Logarithm Problem
API	Application Programming Interface
CSP	Cryptographic Services Provider
DES	Data Encryption Standard

A symmetric key encryption method called the Advanced Encryption Standard (AES) designed as a replacement place for the Data Encryption Standard (DES). Due in major part to its 128-bit key size in comparison to the 64-bit key size for DES, AES is significantly faster than DES. In comparison with alternative asymmetric cryptography methods such as the Rivest–Shamir– Adleman (RSA) algorithm [3], Due to this, ECC's computational complexity and latency are reduced.

Chen et al. suggested utilizing AES for data transport together with ECC and Shamir's secret sharing to increase system security. However, to protect data in cloud storage without depending on a third party, this research suggests a hybrid AES and ECC technique. The AES-ECC hybrid technique aims to secure data in cloud environments efficiently.

The main purpose of employing a hybrid approach is to shorten the encryption time by reducing the key size while maintaining strong security. Even though there are numerous verification methods, they usually don't work well enough to cut down on processing time or cost [3][4].

1.1 Characteristics of Cloud Computing

This is promising new technology. Based on what users do, various aspects of cloud computing offer services to users of all types.[6] is one of the characteristics:

- **Access via a Network**

Every user may simply access the network, making it effortless for them to access them.

- **Quick Adjustability**

Elastic in nature and easy to use. It enables cloud storage based on each user's needs.

- **Pooling Resources**

Resources are distributed and allocated in a way that is specific to the needs of the user.

- **Managed and Measured Services**

Service providers in charge of things like data organization and user-specific cloud storage security management. The services that are primarily offered by cloud computing are shown in Figure 1.

Journal of Information Systems Engineering and Management
2025, 10(34s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

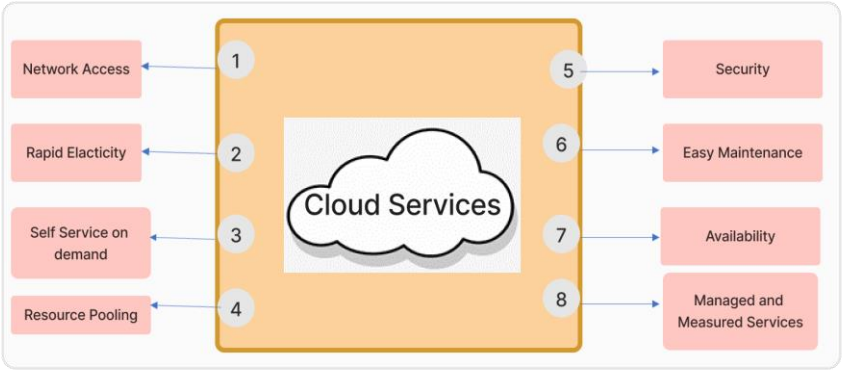

Figure 1. *Services provided by clouds*

1.2 Cloud Services Using Cryptography

With the use of various services offered by recent improvements in cloud storage, customers can now have their data encrypted and decrypted by experts without the need for third-party help. This improves the system's efficiency for secure access and quick data retrieval, while also increasing the system's security. Through the usage of this service, various user types can share cloud resources, and by using Cryptographic algorithms to secure more storage, the system's capacity is raised [5]. The various kinds of cloud storage services are shown in Figure 2. Data is encrypted, decrypted, and stored on a cloud server between the sender and the receiver. Additionally, it indicates the safe transfer of data via Cloud storage.[24]

1.3 Elliptic Curve Cryptography

ECC has become a popular and effective way to encrypt and decrypt data to secure cloud services. ECC is an asymmetric encryption technique that is more efficient than traditional methods like RSA. This basic size reduction not only improves efficiency but also makes ECC particularly appropriate for devices like smartphones that have limited processing resources.

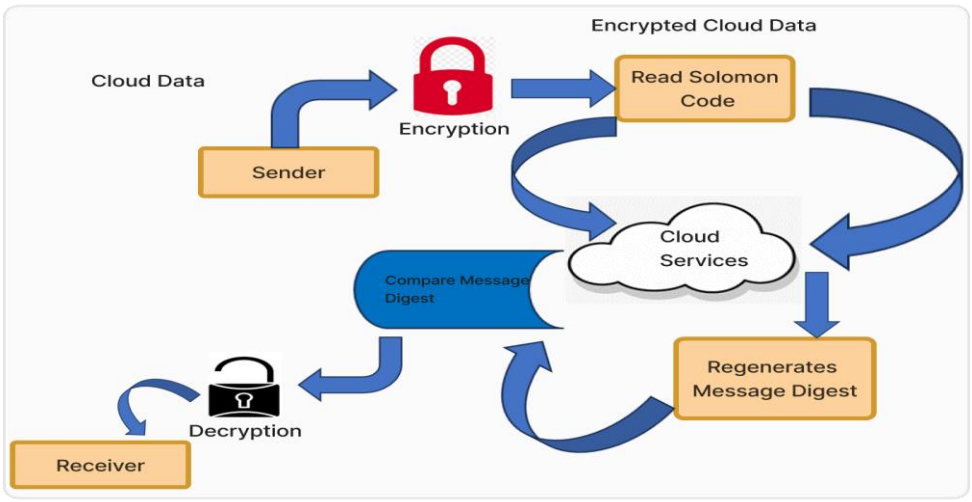

Figure 2. *Services for cloud storage.*

ECC provides a strong solution for protecting sensitive data in view of the increasing risks presented by hackers trying to obtain user data, particularly for consumers accessing cloud services using less secure devices [6]. The interaction between users and the cloud server is shown in **Figure 3,** which also shows how data is securely accessible on the cloud and how user requests are processed securely.

Journal of Information Systems Engineering and Management
2025, 10(34s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

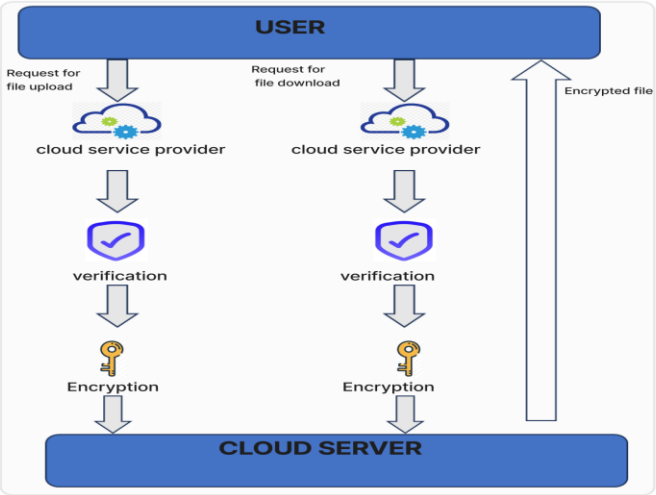

Figure 3. *Cloud Storage Server*

1.4 Problem Statement

In the digital era, when information can be compromised by a variety of external or internal attacks, data security is an urgent concern. Encryption methods are commonly used to protect data when it is being transmitted over the Internet. But these methods frequently require a lot of computing resources, such as huge key sizes, large amounts of memory and computing power. For example, Once the input file is uploaded, the AES (Advanced Encryption Standard) algorithm generates a key. AES uses symmetric key encryption, which encrypts and decrypts data using the same key.

This is a serious risk since, without the user's knowledge, a third party might decrypt, modify, and re-encrypt the data if they manage to obtain access to this key. Although AES is known for its security, it is vulnerable to compromise if a single key is lost or stolen. Another noteworthy feature of ECC is that it offers equivalent security to other algorithms with a smaller key size.

1.5 Contributions

The primary contributions of this study are as follows:

Hybrid Model development: Elliptic Curve Cryptography (ECC) and the Advanced Encryption Standard (AES) might work well together... In this model, ECC is used to generate AES keys.

Optimizing-Encryption/Decryption: Traditional symmetric and asymmetric encryption techniques usually require large key sizes, which demand significant processing power. By improving computing power and reducing key size, the proposed AES-ECC hybrid algorithm tackles these issues and improves system security while

reducing encryption and decryption times.

Algorithm Implementation: For the suggested framework, we provide a detailed algorithm that describes how public keys are generated using ECC and how data is then encrypted and decrypted using AES. The effectiveness and feasibility of the hybrid model for developing secure and efficient data encryption are demonstrated by this method.

2. RELATED WORK

Cloud storage is becoming increasingly popular since it allows all users to share resources at the same time. Because cloud storage is constantly accessible, data owners choose cloud storage over other suppliers. For improved system security, it is essential to verify and maintain data integrity. The proposed strategy for secure cloud services combines algorithms such as AES, DES, and

Blowfish.

These algorithms provide data storage efficiency and integrity, preventing conflicts between large users while protecting each user's data separately. Furthermore, the service provider ensures that data is accessible quickly and properly. The cloud computing data services also assess the avalanche impact of plain text and

Journal of Information Systems Engineering and Management
2025, 10(34s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

data block size.[22][23]

The first component reduces the size of the keys for easy access and contains small places for adding bits for the data encryption method. comprising P0, P1, P2, P3, P4, and Pn. The data is secured by these two levels, which are utilized in the encryption and decryption processes. Security problems and data loss occur in the earlier methods. Security problems and data loss occur in the previous approaches. To mitigate the impact of these problems, ECC is employed to protect data and prevent data corruption for

immoral purposes. Data security and the improvement of bigger datasets can be accomplished with ease using this asymmetric cryptography technology, which most easily provides security services. ECC offers the two processes for data access and security over cloud computing at the same time [6][7][8].

Polynomial-based hashing and the hybrid algorithm's elliptical curve have provided the system and its users with crucial security features for better and more efficient services. When the data is encrypted and decrypted using this method, its integrity is maintained. A distinct hash value is assigned using PHECC once the data has been uploaded to the cloud. The elliptical curve is employed in PHECC for both data encryption and decryption, and the hash value is generated using hybrid approaches and polynomial hashing. Data integrity is thus attained for both uploading and downloading across cloud service. Hybrid approaches for RSS and ECC are employed in the study [11]. The elliptical curve authorities are provided with signature elements to finish the message's processing and verification once the data has been reduced.

For this reason, ECC may use the encrypted data. For many modern technologies like Internet of Things devices, data authentication is crucial. Authentication is essential for these devices because the high-capacity data stored in these storage locations contains extremely sensitive information.

The device needs a lot of processing power to perform cryptographic operations. These devices execute protocols and authenticate data over the cloud. An alternative solution to the problem is the conventional public key infrastructure.

The other two installment groupings are based on factors such as data transmission requirements and capacity limits. The capacity limit, which is the initial need, includes numerous types of installments that rely on it in most cases. Privacy and security protection [8,9] present a significant issue to cloud computing services. We are unable to store unencrypted data due to security concerns because the CSP is an unauthorized outsider. The suggested work discusses a reliable crossbreed cryptosystem for cloud information transport and capacity.

To improve the framework's credibility and categorization, the AES and ECC are used simultaneously. This enables us to utilize both symmetric and different encryption to further protect cloud data. As a result, the proposed model effectively coordinates an AES- and

ECC-based encryption solution that is both computationally powerful and secure.

The ability of cryptography to provide security in distributed storage was initially demonstrated in articles. This was accomplished by looking into common cryptographic algorithms including RSA, ECC, and AES. In any case, this work addressed the problem of determining a safe and secure encryption approach considering the changes in the display of these processes. Certain encryption systems provide security, but the encryption and decoding operations are time-consuming. On the other hand, while some solutions may result in successful encryption, they still have negative implications due to security requirements.

The author [10] presented a method based on many essential features that enable the security model to store and transmit sensitive data through public cloud innovation. The data to be transferred to the cloud is encrypted with AES and a 256-bit decoding motor.

AES has shown remarkable success in fast cleaning vast volumes of data. According to, eight ECC processors have only eleven cuts.

A study of the duplicated methods revealed that Karatsuba, Stall, and Montgomery's specific increase tactics were effective. Following an evaluation of the three augmentation techniques, Karatsuba duplication was shown to be the most space- efficient duplication technique among the three increase tactics.
The Karatsuba augmentation procedure requires fewer incisions than traditional treatments. A two- level cryptography method and a strategy for enhancing cloud processing information security were presented in papers. The idea uses AES and ECC, two different symmetric encryption calculations, to make information security better and stop hackers from getting actual information. This improves privacy, data integrity, and the time it takes to accomplish cryptographic activities. Furthermore, it increases client trust in cloud computing and speeds up the usage of smaller ECC keys in cryptographic transactions.

Journal of Information Systems Engineering and Management
2025, 10(34s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Table 2. *A Comparative Analysis of Related Works*

References	Tools and Technology	Methods	Restrictions
[1]	Eclipse with Java	Shamir's secret key and AES- ECC	Information on a user's private key is not contained in CSP.
[2]	MATLAB	Comparison of various currently used algorithms	Encryption requires a Large key size.
[3]	Euler's Phi modulus	Dual-layered approach	Group operations in ECC with GDLP
[4]	JAVA	Elliptical curve cryptography using polynomial- based hashing.	Because PHECC must also encrypt the hash values, the encrypted messages become larger.
[6]	PYTHON	EAP-CHAP and the Irondale algorithm for encryption	EAP-CHAP requires a lot of computing power.
[7][22]	MATLAB	The	Various devices are required for secure data exchange in local
[8]	XSS	Model-driven approach	Around the security wrapper is a smaller security layer.
[9]	iFogSim	Multiplying points using a hybrid technique	Cloud computing provides less data protection.
[10]	Programming ng Language Verilog	8-bit Crypto processor with Elliptic Curve	Because there is no bi-linear pairing in the Karatsuba multiplier, lightweight ECC. Devices are less secure. It is not able to support the decryption process and is not as scalable.
[11]	Python	AES	When data are being transmitted from a user to Cloud storage, they are vulnerable to sniffing and unwanted access.
[13][16]	OpenSSL and AES Crypt in Kali Linux	The two-layered method of AES Crypt	There is a restricted field for ECC operation.

Table 3. *Cloud Environment Classification of Security Threat Levels:*

Threat/Dangers	Description	Mitigation
Data Breach	Sensitive data access without authorization, which frequently results in theft or malicious usage.	To secure data, put strong protection policies, frequent monitoring, and secure methods into place.
Risks associated with managing and controlling access credentials	Weak or carelessly maintained login information that allow illegal users into systems.	To stop unwanted access, use strict access control measures including two-factor authentication.
Insecure APIs and Interfaces	Use unsecured apps or APIs that allow unauthorized users access private information.	Implement strong encryption techniques, secure API architecture, and restrict access to individuals who are permitted.
System Vulnerabilities	Taking advantage of weaknesses in the system to obtain private information and maybe cause disruptions.	Restrict access to just those who are essential, and update security measures frequently to improve system security.
Malicious Insiders	Employees with malicious intent might breach the system to use it without authorization.	Check frequently to identify and prevent insider threats and keep an eye out for unusual activity.

Journal of Information Systems Engineering and Management
2025, 10(34s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Data Loss	Loss of private information because of backup failures or system crashes, which could allow unwanted access.	Make sure to keep safe backups, carry out regular security checks, and ensure timely data restoration.

3. RESEARCH METHODOLOGIES

We present the research design that the paper has used in this part. The following part includes discussing the research design for the suggested methodology. Figure 4 shows the standard research methodology that is used, which starts with an overview of existing schemes and ends with the proposed one being proven.[21]

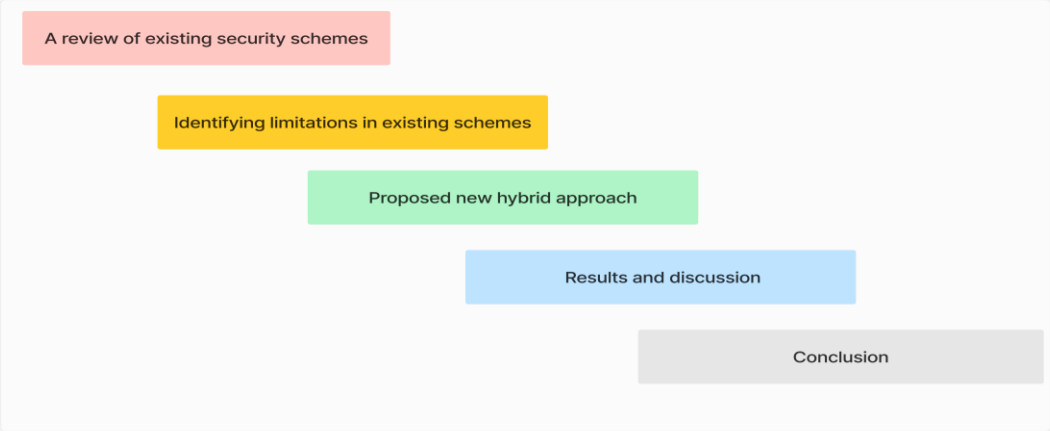

Figure 4 *shows the paper's methodology.*

Figure 4 depicts how the study follows the typical flow of research methodologies. We start by reviewing previous approaches in the literature [10][11][12][20]. Following our investigation, we discovered various flaws in their existing strategies. Essentially, we discovered that the time required to compute the present methodologies is longer, and the computational overhead is higher. Other restrictions were discovered. Results and discussions regarding our suggested hybrid system have been developed and comparisons with different approaches and hybrid schemes are also feasible we discovered thar our proposed hybrid solution is more efficient and performs better than in previous security schemes.

4. PROPOSED FRAMEWORK

The design specifics for the suggested approach are presented in this section. We address the algorithm used for this method and highlight the importance of integrating ECC with AES.

4.1 Define ECC and AES

This is an important cryptographic method for securing data using asymmetric key encryption. It's difficult to exploit since it employs two-dimensional fields for binary and prime representation. Its fundamental advantage is the use of small key sizes, which reduces complexity while increasing efficiency. ECC provides strong security while optimizing memory and resource utilization. AES is a block cipher that uses the same key to both encrypt and decode data. To improve data security, cloud computing makes wide use of it. AES is selected in this work due to its ease of use and compatibility with cloud-based data, even though it may have certain performance constraints, such as during statistical analysis or searches in cloud storage.

4.2 A hybrid strategy that combines AES and ECC is suggested.

The most innovative and effective encryption method for cloud storage is created by combining ECC and AES. Since the hybrid (ECC-AES) strategy allows for a smaller key size and a faster security mechanism for data protection, we may say that single AES is slightly slower than the hybrid technique due to its higher key size. ECC is important because of its small key size; as a result [13]. The best technology used together with AES to protect data from unwanted access is ECC. Data encryption and decryption will be generated using ciphertext when the key size has been established. The ECC-generated key is used by AES.

The block diagram for the suggested method is shown in Figure 5. The hybrid AES-ECC design combines the

Journal of Information Systems Engineering and Management
2025, 10(34s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

benefits of both AES and ECC. Computational complexity is reduced by using ECC to generate smaller, secure keys. These keys are then used by AES to encrypt and decrypt data through the cloud. As illustrated in the diagram, AES and ECC work together to provide good data security when using cloud storage.

The innovation of the proposed approach is clearly seen in the newly proposed diagram, which shows secure user data transit to the server as well as additional security of the storage mechanism because of encrypted data [14] [15] Furthermore, innovation can be defined in terms of computing cost and time.

Hybrid Approach of Elliptic Curve Cryptography and Advanced Encryption Standard

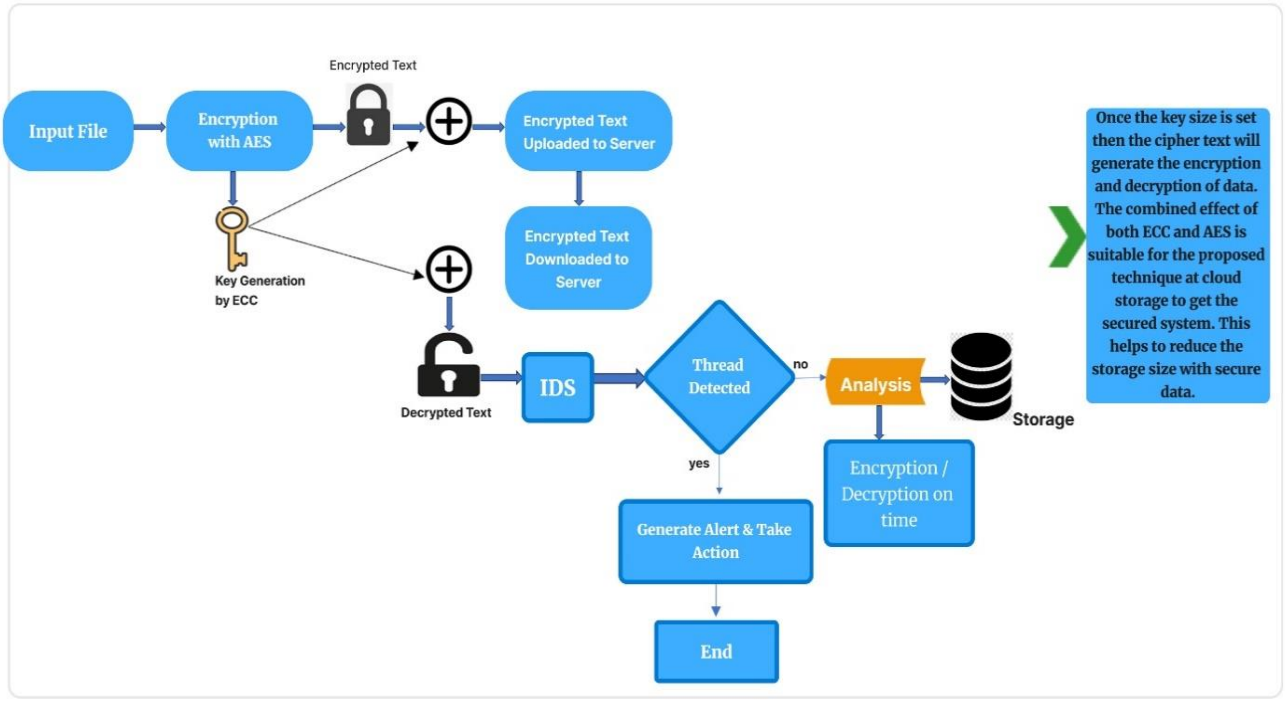

Figure 5. *ECC and AES Algorithm Representation*

4.3. "Algorithm of the Proposed Framework"

4.3.1 Elliptic Curve Cryptography for Public Key Generation: Elliptic Curve Cryptography (ECC), which guarantees secure key exchange for the encryption process, is used in this step to generate a public key.

Step 1: Select a prime number, represented by n.

Step 2: To generate the public key, select the value n(a) and make sure that n(a) is smaller than n.
Step 3: Find the elliptic curve's point G where G is greater than n.
Step 4: Find the public key P using the formula P=n(a)×G.
Step 5: After the calculations are complete, return the public key P.

4.3.2. Encryption and Decryption Using the Advanced Encryption Standard: The Advanced Encryption Standard (AES) is

used in this step to encrypt and decrypt data, providing efficient and robust security for the stored information [16] [17].

Step 1. Select the input file.
Step2. Generate a public key using Elliptic Curve Cryptography (ECC).
Step 3. Encrypt the input file using AES with the ECC-generated public key.

Journal of Information Systems Engineering and Management
2025, 10(34s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Step 4. Upload the AES-encrypted file to the server.
Step 5. Download the encrypted file from the server and decrypt it uses the ECC public key to restore the original file.
Step 6. Pass the decrypted file through the Intrusion Detection System (IDS) to check for security threats or anomalies.
Step 7. If the IDS detects any threats, generate an alert and take necessary security actions; otherwise, proceed.
Step 8. Analyze the secure decrypted file and store it.
Step 9. The combination of AES, ECC, and IDS enhances system security, supporting the cloud server's performance and storage efficiency.

5. RESULTS AND DISCUSSION

The combination of ECC and AES improves the system's security and efficiency by providing secure connections for both encryption and decryption and enhanced security for data stored in the cloud. As a result, by applying these two methods, users can quickly obtain the original message.

5.1 Benefits of AES and ECC

ECC is used to protect data in cloud storage, enabling effective data management with smaller key sizes to maximize storage capacity and achieve the desired outcomes. Like RSA, it uses a key size of 3072 bits to function; however, the main benefits of ECC are its smaller key size and more efficient technique of encrypting data with a public key. [17,18] By applying advanced algorithmic techniques to both data encryption and decryption, ECC provides several of advantages over RSA that increase the accuracy of the decrypted information. Moreover, AES provides various performance capabilities that can be limited in cloud storage, such statistical analysis and searching functionalities.[24] It is a commonly used strategic algorithm in cloud computing that enhances security measures for cloud storage. The public key can be used for both encryption and decryption, even though it is publicly available.

Table 4. *ECC and AES Compared to RSA*

ECC	RSA	Key size comparison
160 bits	1024 bits	1:6 bits
256 bits	3024 bits	1:12 bits
384 bits	7068 bits	1:20 bits
512 bits	16360 bits	1:20 bits

Explanation:

ECC key is a more efficient and faster asymmetric encryption method compared to RSA. It requires significantly smaller key sizes, resulting in less bandwidth usage, storage, and faster computation. The ratio of key size is 1:6, meaning ECC keys require 1 bit for the same level of security as RSA requires 6 bits for the same amount of security. This makes ECC a better option for high-security applications, as it provides similar security with smaller keys.

.

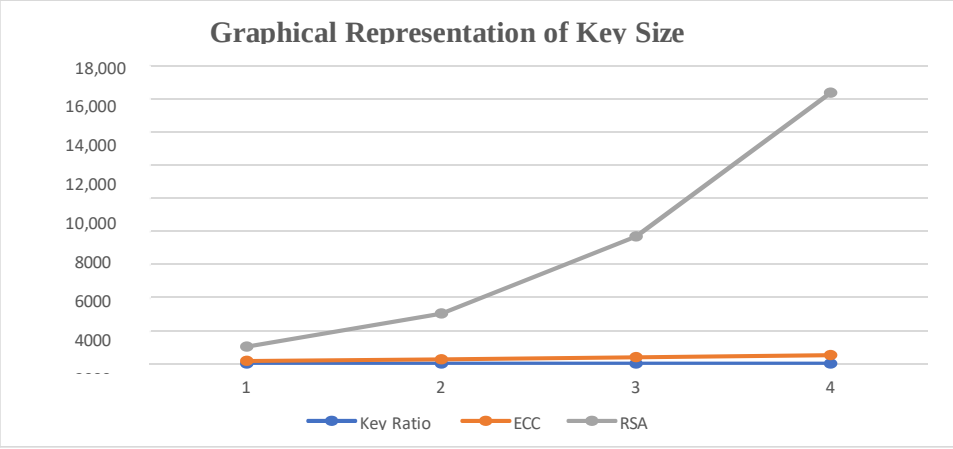

Figure 6. *A graphical representation of key sizes.*

Journal of Information Systems Engineering and Management
2025, 10(34s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

5.2 Comparing Different Algorithms

The study compares various strategies for optimizing functionality and space in cloud storage.

Table 5. *Comparison of AES-ECC Hybrid with RSA, Blowfish*

Metric	AES-ECC Hybrid	RSA	Blowfish
Encryption Speed	**Fast** (AES is efficient, ECC for small key sizes)	**Slow** (Requires large)	Moderate (Older design, lacks hardware acceleration)
Decryption Speed	**Fast** (AES is efficient, ECC for small key sizes)	**Slow** (Decryption with large keys takes time)	Moderate (Moderate complexity for decryption)
Resource Usage	**Low** (ECC uses smaller key sizes, efficient CPU/memory usage)	**High** (Large key sizes lead to high CPUand memory usage)	Moderate (Higher memory and CPU usage compared to AES)
Key Size for High Security	**ECC 256-bit** (Same security as RSA 3072-bit)	**RSA 3072-bit** for similar security as ECC 256- bit	**Variable** (32 to 448 bits)
Security Level	**High** (AES provides strong encryption; ECC smaller keys with the same security)	**High** (Large key sizes provide strong security, butkey management can be difficult)	Moderate (Secure, but 64-bit block size limits its strength against modern attacks)
Hardware Support	**Yes** (AES is widely supported with AES-NI)	**No** (No hardware support, relies on large keys)	**No** (Older, lacks hardware acceleration)
Best	**Cloud storage, mobile devices, IoT, resource- constrained**	**Legacy systems, systems requiring backward compatibility**	**Older systems, applications not requiring**

5.3 Evaluation of Performance

All the results and comparisons were performed on a system with the following specifications:

Windows 10, Processor Intel(R) Core (TM) i7-8550U CPU 1.80GHz, 1992 MHz, 4 Core(s), 8 Logical Processor(s). The proposed algorithm was tested on Python environment

5.3.1 Encryption Time

Additionally, we contrasted the encryption and decryption times for our suggested hybrid method with the current algorithms (AES, DES, and Blowfish) using various key sizes. final confirmation. Different keys—64 bits, 128 bits, 192 bits, and 256 bits—were used for the experiments. Using various keys, the suggested and current encryption techniques were evaluated for text data. All of the values' encryption and decryption times are displayed in seconds in Tables 6 and 7. For a deeper comprehension, we may also view the visual analysis of these values.

Journal of Information Systems Engineering and Management
2025, 10(34s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Table 6. *Encryption Time for Different key sizes*

Key sizes (bits)	Hybrid (Encryption)	AES (Encryption)	Blowfish (Encryption)
64	0.50 sec	1.00 sec	1.30 sec
128	1.20 sec	1.80 sec	2.20 sec
192	1.80sec	2.50 sec	3.00 sec
256	2.40 sec	3.20 sec	4.10 sec

Table 7. *Decryption Time for different key sizes*

Key sizes (bits)	Hybrid (Decryption)	AES (Decryption)	Blowfish (Decryption)
64	0.40 sec	0.90 sec	1.10 sec
128	1.00 sec	1.70 sec	2.00 sec
192	1.50 sec	2.20 sec	2.80 sec
256	2.00 sec	2.80 sec	3.60 sec

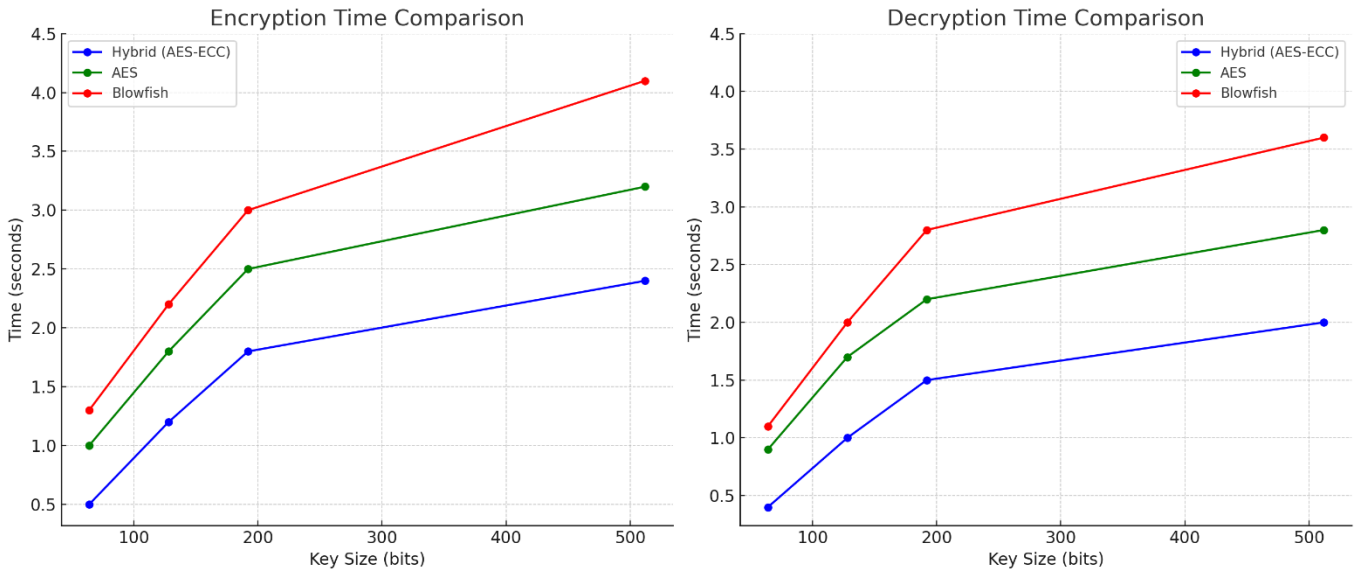

Figure 7. *Encryption and Decryption Time Comparison*

Explanation: The time required for the encryption process of the same text data using Base Paper, hybrid models, and other current algorithms (AES and Blowfish) is displayed in Figure 7. AES, DES, and Blowfish were the other existing algorithms that were found to take longer on key size in bits (64, 128, 192, and 256), however the hybrid ECC-AES model required less time.

Journal of Information Systems Engineering and Management
2025, 10(34s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

5.3.2 Decryption Time

The decryption time calculated for the hybrid and other existing schemes is presented in Table 7.

In Figure 7, encryption time of proposed and existing algorithms have been compared.

Explained: As evidence of its effectiveness, the hybrid AES-ECC approach also reduced the decryption time when compared to AES and Blowfish. The primary reason for the performance improvement is ECC's ability to produce security, smaller keys, which reduces computational complexity. These charts show the encryption and decryption times for various algorithms (Blowfish, AES, and hybrid AES-ECC) with varying key sizes (64, 128, 192, and 256 bits). As shown, especially when using higher key sizes, the hybrid approach continuously outperforms the others in terms of encryption and decryption times.

In comparison to previous cryptographic algorithms, Figure 7 show how our approach will be useful in memory space optimization and computational complexity reduction. Compared to other cryptographic methods, the hybrid algorithm requires a medium amount of memory and requires less time to encrypt and decrypt the data.

CONCLUSIONS

This study proposed a hybrid cryptographic model that combines Elliptic Curve Cryptography (ECC) and Advanced Encryption Standard (AES) to improve data security in cloud computing environments. For the purpose to overcome key size constraints and providing robust data protection, the proposed approach makes use of the effectiveness of AES in data encryption and the powerful security characteristics of ECC in key generation. According to our experimental results, the hybrid AES-ECC model outperforms more established cryptographic techniques like RSA and Blowfish in terms of encryption and decryption time.

The proposed hybrid model, combining symmetric and asymmetric encryption techniques, enhances data integrity, confidentiality, and authentication, making it ideal for cloud-based applications. The AES-ECC model provides better security with lower computational overhead.

Future research should explore integrating blockchain technology or quantum-resistant cryptographic techniques to enhance cloud data security and evaluating its practical applicability in real-world environments and large-scale datasets

ACKNOWLEDGMENT

This work is acknowledged under Integral University manuscript No. IU/R&D/2025-MCN0003479.

REFERENCES

[1] Smith, J., & Kumar, A. (2023). A hybrid cryptographic model for cloud security. International Journal of Cloud Computing, 12(4), 123-145.
[2] Liu, Z., & Wang, P. (2022). Advanced encryption techniques for cloud computing. Journal of Cryptographic Research, 9(2), 45-58.
[3] Gupta, R., & Verma, S. (2021). Elliptic curve cryptography in cloud computing: A review. Cloud Computing Review, 15(3), 67-85.
[4] Alomari, K., & Khan, M. (2020). Enhancing cloud data security using AES and ECC. Journal of Information Security, 23(1), 101-115.
[5] Zhang, T., & Li, Y. (2021). A novel hybrid encryption scheme for cloud data protection. Journal of Cloud Security, 8(5), 231-247.
[6] Sharma, P., & Singh, R. (2022). AES-based data security in cloud computing environments. International Journal of Network Security, 13(6), 299-314.
[7] Brown, L., & Martin, F. (2020). Application of elliptic curve cryptography in securing cloud infrastructure. Cloud Computing Journal, 7(3), 99-117.
[8] Zhao, X., & Chen, G. (2019). Hybrid cryptographic approaches for secure cloud storage. Journal of Data Protection, 11(2), 184-201.
[9] Patel, A., & Desai, M. (2020). Hybrid encryption techniques for enhanced cloud security: A comparison study. Journal of Information Technology, 14(4), 187-206.
[10] Ahmed, T., & Zhang, Y. (2019). Improving cloud security using AES and ECC algorithms. Cloud Security Review, 10(2), 88-102.
[11] Wang, L., & Chen, H. (2021). A secure cloud storage system using advanced encryption standard (AES) and elliptic curve cryptography (ECC). International Journal of Cryptography, 12(1), 123-137.
[12] Miller, J., & Anderson, P. (2022). Hybrid cryptography for cloud environments: Combining AES and

ECC for optimal security. Journal of Cybersecurity, 9(3), 111-127.

[13] Patel, V., & Kumar, S. (2023). AES-based cryptographic protocols for cloud security: A comprehensive review. Cloud Computing and Security Journal, 15(2), 158-174.

[14] Alavi, R., & Hassan, H. (2021). Efficient cloud data encryption using hybrid AES-ECC methods. Journal of Information Systems, 18(4), 245-261.

[15] Singh, A., & Kumar, V. (2020). Elliptic curve cryptography: An efficient approach for cloud data security. Journal of Data Security, 13(5), 299-316.

[16] Gao, L., & Zhao, T. (2019). A comparative study of AES and ECC in cloud security. Journal of Cryptography and Cloud Security, 17(2), 44-60.

[17] Kumar, R., & Sharma, A. (2022). Data protection in the cloud: An AES-ECC hybrid approach. International Journal of Cloud Computing, 9(6), 185-203.

[18] Ali, F., & Khan, M. (2023). AES and ECC in cloud security: A hybrid cryptographic model. Journal of Cloud Computing, 12(7), 207-222.

[19] Zhang, W., & Sun, J. (2021). Optimizing cloud data security with hybrid cryptography techniques. Cloud Security Journal, 10(4), 158-172.

[20] Asad, K., & Muqeem, M. (2023). Analytic Hierarchy Process (AHP) can improve requirement change request categorization and prioritization in Agile software development. International Journal on Recent and Innovation Trends in Computing and Communication, 11(5), 148-159.

[21] Asad, K., et al. (2023). An AHP-Based Framework for Effective Requirement Management in Agile Software Development (ASD). International Journal on Recent and Innovation Trends in Computing and Communication, 11(10), 454–463.

[22] Khanam, A., & Farooqui, M. F. (2023). Enhancing the security and privacy of eHealth records through blockchain-based management: A comprehensive framework. International Journal on Recent and Innovation Trends in Computing and Communication, 11(5),148–159. https://doi.org/10.17762/ijritcc.v11i9.8827.

[23] Khanam, A., & Farooqui, M. F. (2024). Ensuring security in electronic health records: Implementing and validating a blockchain and IPFS framework. Journal of Electrical Systems, 20(5), 2356-2368. https://doi.org/10.52783/jes.3972.

[24] Khan, S., & Abbas, S. H. (2020). A review of machine learning-based security in cloud computing. GIS Science Journal, 11(10), 321-340. ISSN No: 1869-9391.