ISSN: 2754-6659

Journal of Artificial Intelligence & Cloud Computing

SCIENTIFIC Research and Community

Review Article

Open Access

Portable Cloud-Based Data Storage Security Using Dual Encryption

Srinivas Reddy Pulyala[1]* and Sai Teja Makani[2]

[1]Security Engineer, Smile Direct Club, USA

[2]Senior Manager-DevOps, Spotter INC, USA

ABSTRACT

Secure data transfer is a must for all cloud-based structures. Cloud infrastructure is used by many networks, including those for e-commerce, online banking, and even software programs, to move enormous amounts of important data every day. This paper primarily addresses risk factors, which are security concerns encountered when managing cloud data. This research focuses on a hybrid encryption solution for cloud privacy and security. Elliptic Curve Cryptosystem (ECC) and Advanced Encryption Standard (AES) are the two best asymmetric encryption methods and symmetric encryption technology, respectively. The AES-ECC hybrid cryptosystem combines the advantages of the AES algorithm for faster data encryption with the ECC method for symmetrical session key exchange. The proposed solution minimizes the delay factor and is computationally efficient, robust, and secure.

***Corresponding author**

Srinivas Reddy Pulyala, Security Engineer, Smile Direct Club, USA.

Received: June 03, 2022; **Accepted:** June 11, 2022; **Published:** June 22, 2022

Introduction

In the world of computer science, cloud computing is a newer area. It is large and becoming bigger daily. Instead of using the nearest server or PC, remote servers on the internet are used to store, look up, and access all data. Server purchases are no longer necessary here. For affordable services, they can only be hired from the cloud provider. Additionally, cloud servers that are rented don't require any management or monitoring. As of right present, the Cloud Services Provider (CSP) would oversee this. When anything is stored in the cloud, it is likely on web servers as opposed to a nearby PC. It's like having an additional hard disk.

The customer can access one of those whenever and everywhere there is an internet connection. Before this, the client only had a home PC with the newly announced product. The client can now take documents wherever he needs them. All praise belongs to web applications, which are cloud-based programs that operate in web browsers. It is free, does not require installation, and enables the creation of numerous different projects. This allows anyone with an internet connection to access anything created in Google Docs on any computer or device. The user can access the cloud from any connected device and carry all his multimedia files with him wherever he goes.

For instance, a user can instantaneously send his or her holiday images to friends and relatives. They don't have to be concerned about losing the images and audio-video data due to a computer breakdown because everything is kept on the cloud.

Microsoft and Google Drive, two popular cloud-based storage options, make a backup of your system. The data can be quickly moved from the storage services to another device if something goes wrong with the local PC. However, there is yet another issue with data integrity. This can be a result of the data possibly being in multiple locations. Following that, the security and privacy protection of this dispersed data may be compromised. The cloud must be secure for the data spread over so many sites.

There are various risks associated with cloud computing that affect the security of sensitive data or raw data. Cloud computing environments are used to store all of the traffic between consumer and service provider networks. Attackers can easily manipulate and access the data if they have access to the cloud network. Clients inside the same domain would typically share cross-data. The same cloud is probably holding data from various clients. Therefore, it is crucial to have a system in place for separating customer information from other information.

Because information is held in the data provider's facilities, which may provide for administrative compliance issues including confidentiality, security, and discrimination that must be handled by the provider, the conformance process in the cloud is complex. This research aims to investigate the use of Advanced Encryption Standard (AES) and Elliptic Curve Cryptography (ECC) algorithms for dual encryption in portable cloud-based data storage to provide secure and efficient data storage solutions. The proposed research will focus on designing and implementing a Portable Cloud-Based Data Storage Architecture that integrates AES and ECC encryption techniques to provide security and privacy in the cloud environment. The research will evaluate the performance of the proposed encryption scheme and compare it with existing solutions to demonstrate its effectiveness in addressing the challenges of cloud security.

The objectives of this project look at the most recent methods for secure cloud-based data management and storage, analyzes the benefits and drawbacks of AES and ECC encryption algorithms, design and implement a portable cloud-based data storage system, assess its functionality, contrast it with current solutions, and makes suggestions for further study.

Literature Review

Data security at the database server is the primary area of concern as cloud usage grows. Regarding cloud data security, various sorts of studies have been conducted and some are still ongoing.Cloud storage stability is thus the main problem in maintaining our data security. Here, we discuss some important research in this area.

Researchers Amandeep Verma and Sakshi Kaushal et al. look at security issues with new cloud computing systems [1]. Since cloud computing refers to both the infrastructures (i.e., hardware and network software in data centers) that provide the services (i.e., applications provided as services over the Internet) and the infrastructures themselves (i.e., various applications and infrastructures that pose security concerns), additional security concerns such as availability, confidentiality, honesty protection, authorization, and so forth should be taken into consideration.

K. Hajarathaiah and T. Seshu come up with a solution to deal with data loss incidents that occur during transmission [2]. They employed a third-party auditor or TPA. To restore the data and stop errors, they implement some dynamic operations such as deletion, updating, or appending.

A new hybrid model was proposed by Alakananda Tripathy et al. that allows for faster data encryption while using less RAM for key storage. ECC is utilized in their paper for key exchange between nodes [3]. Both encryption and decryption are accomplished using the RC4 symmetric key technique. We are inspired to create a fresh hybrid cryptographic algorithm as a result.

Poonam and Deepali proposed a technique in which they maintain the information's reliability at the dubious servers using the Merkle Hash tree and AES algorithm [4]. For the auditing, they utilized the term TPA, which functions for the client to check the integrity and also sends the message back to the client.

According to Snehal Rajput, J.S. Dhobi, et al., cloud infrastructure uses on-demand infrastructure services and depends on utilities [5]. The security of all of their resources, including their network, apps, infrastructure, and customer data, is the responsibility of cloud service providers. That trustworthy algorithms are used by cloud service providers to safeguard data. This essay examines several well-known encryption methods. It compares elliptical curve cryptography, single sign-on technique, DES encryption, and digital signatures in addition to RSA encryption.

A method to identify the collusion attack in the current strategy was described by Tao Jiang, Xiaofeng Chen, and Jian Feng Ma [6]. Additionally, it offers a successful public integrity technique that relies on vector responsibility and verifier-neighborhood revocation group signature for secure gathering client renunciation. Additionally, it aids users in general client verification and skilled client revocation with attributes like assurance, potency, accountability, and traceability of secure group user revocation.

The hybrid AES and RSA encryption method published by Vishwanath S. Mahalle et al. uses both the 1024-bit RSA key and the 128-bit AES secret key [7]. They recommended a structure that typically consists of two parts. The Upload Module and Download Module are those. The download element consists of two components, namely decryption, and download, whereas the upload module has four parts, including authentication, upload, key creation, and encryption. By using a special username and password, the user authenticates himself to the cloud service provider. The file will be uploaded on a secure path during the upload phase. Finally, the encryption component encrypts the file after the key generation component, as its name suggests, has generated the key. The download component of the download module again just downloads the file for the user while the decryption part extracts the plain text file from the ciphered file. In this system, a temporary directory is where the data is initially kept. It will be permanently saved in the cloud after being encrypted with the RSA and AES algorithms, as specified by the user. To store data in the cloud using this method and to retrieve data from the cloud, the user must enter the AES secret key. As a result, the hybrid (AES plus RSA) algorithm will offer great security.

A plan that uses 128-bit Advanced Encryption Standard (AES) for increased information security and classification was put forth by Babitha. M.P. and K.R. Ramesh Babu [8]. Using this method, information is first encoded using AES and then sent over a cloud. Additionally, this strategy makes use of the SMS alert system to prevent unwanted access to customer data.

The researchers are combining AES 256 (Advanced Encryption Standard), IDA (Scattering Algorithm of Information), and SHA 512 (Secure Hash Algorithm) to increase data security and privacy, according to research by Bih-Hwang Lee et al [9]. The AES 256 encryption standard is used throughout the entire process of encoding the original material; the IT manager randomly generates the encryption. To ensure the security of the data, this article uses the Heroku cloud as a platform and implements AES on the website. Python, Java, PHP, Ruby, Go, and Scala are supported by the PaaS service provider Heroku Cloud. Heroku can be operated locally via the CLI, although PHP installation is required. AES is one of the most efficient algorithms and offers improved security in addition to being important for speed. It also overcomes the AES's shortcoming of being unable to withstand brute force attacks and linear cryptanalysis.

A three-level secure approach for storing audio or video data was created by Raman Kumar and Gurpreet Singh and includes part-based authorized control, encoding, and signature confirmation [10]. The result is an enhanced, strong auditing system that allows for efficient information storage in the cloud.

According to Sandip Dutta et al., the configuration of foci that satisfies a specific numerical condition is elliptical bending. $Y2 = x3 + ax + b$ is the formula for a comparable elliptical grade bend. For aiding in the disclosure of disorganized text in an encrypted calculation, ECC employs a minimal encryption key. This short key allows for low recording power and is quicker to calculate than any other open key for native enciphering. Depending on the platform being used, a 160-piece ECC encipher key provides similar protection and is 15 times faster than a 1024-piece RSA encipher key.

Methodology

The key objective of the paper is to safeguard sensitive data from unauthorized access or malicious behavior. Basic AES and ECC are hybridized to improve data security. Previously, two

users would decide on a scheme, such as adding one to each letter of the message, when they wanted to communicate a secret message. Then, decryption was as easy as taking that one away once more. However, if someone overhears them, the entire system is destroyed. To address this issue, we developed a technique known as public key cryptography. As a result, RSA and Diffie Hellman were introduced as two distinct sets of algorithms in 1977. These enabled the creation of a public key and a private key for us. Send the public key as well. Users must then combine the message with the public key to create an encrypted message.

When the user wants to reply to the bank with that message. To retrieve the original communication, the user must utilize the private key. Now, if someone is listening in, they may see both your public key and the encrypted message. However, there is no method to determine, or perhaps we should say, it is difficult to determine, "What the private key is, and what the message is?"

ECC, often known as elliptic curve cryptography, is a form of public key cryptography that was introduced in 1985. It is based on some modular arithmetic and the esoteric subject of elliptic curves. Some implementations follow the same guidelines as the previous Diffie Hellman public key cryptosystem. However, in the domain of elliptical curves, this produces a seemingly secure system.

AES Encryption

Block cipher AES was created to replace DES and 3DES. It does not employ a Feistel structure, meaning that the encryption and decryption algorithms are not the same. Four stages make up the AES algorithm:

a. Bytes substitution operation
b. Shift rows operation
c. Mix columns operation
d. Add round key

ECC Security Algorithm

In elliptical curve cryptography, we use the equation y2 = x3 + ax + b. This is also known as the Weierstrass equation since both a and b agree that 4a2 + 27b2 6 = 0. Point multiplication is the foundation of encryption and decryption algorithms. P is the fixed base point at which point multiplication is carried out. Scalar multiplication is another name for point multiplication. The final stage includes all ECC operations. The curve's elementary operations are point addition and point doubling. In addition to the ECC algorithm, point multiplication requires the greatest time. The equation to generate these curves:

$\{(x, y) R2 \mid y^2 = x^3 + ax + b, 4a^3 + 27b^2 \neq 0\} U \{\infty\}$

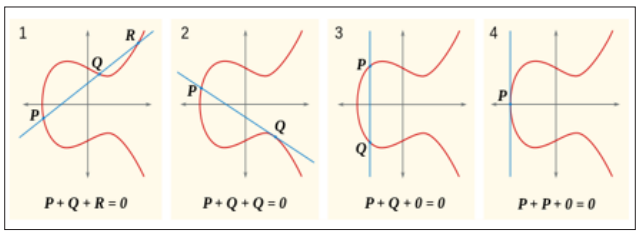

Figure 1: Some Examples of Elliptic Curves

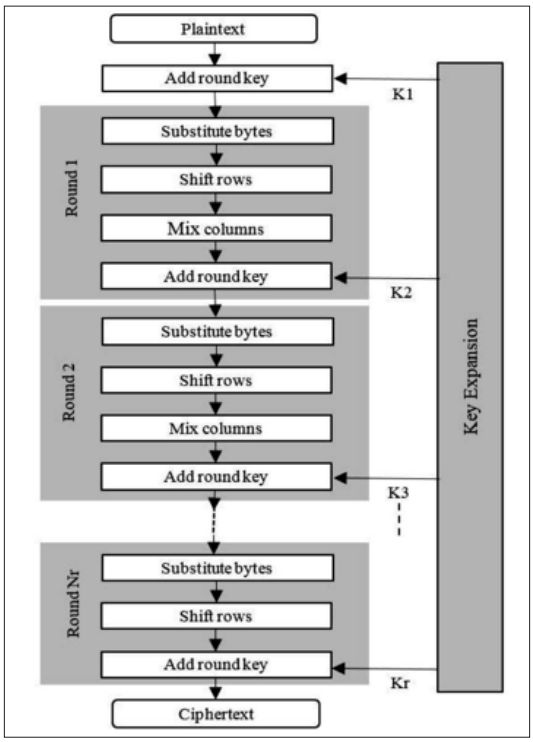

Figure 2: Flowchart of AES Encryption

Key Generation

The public key and the private key must both be generated according to the ECC Encryption's architecture. A public key is used by the transmitter to encrypt the communication, while a private key is used by the receiver to decrypt the message.

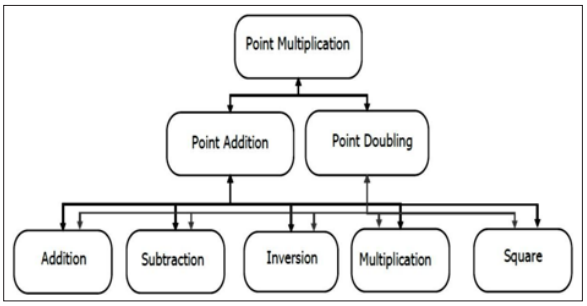

Figure 3: Pyramid of Point Multiplication

Suppose A and B want to communicate with each other. Both agree on a common elliptical curve equation and a generator Q.

Let, the Private Key of A = n_A (nA < n) and Private Key of B = n_B (n_B < n).
Similarly, the Public Key of A, is $P_A = n_A.Q$, and the Public Key of B, is $P_B = n_B.Q$.

Encryption

A want to send B a private message (PM) using B's public key. The encryption is performed using the following equation:
KQPm + KPB = Cm,
Where Cm is the ciphertext and K is a random number with a range of 1 to n-1.
An informed B of the message. When the encrypted message from A arrives at B, B uses his or her public key to convert the ciphertext into plain text and obtains the original message.
Pm = Pm + KPB nBKQ

AES - ECC Hybrid Encryption Architecture

To achieve the highest level of data security, Figure 4 demonstrates how the AES method first encrypts the plain text and then uses the ECC technique to encrypt the AES encryption key. Since the medium is unsafe, the data transformation is secure thanks to the dual encryption procedure. In this case, the AES algorithm and Ecliptic curve cryptography are coupled to produce a better ciphertext faster. These two methods are distinct from one another and possess unique qualities. The first is symmetric, while the second is asymmetric. Therefore, both the public and private keys are used here. First, the message is encrypted using both keys. But in this case, the AES is only used for one step, which is to use the private key to convert the data to hexadecimal. On the other hand, identical data is encrypted using the ECC technique. We join the two encrypted forms after that. We now have the last type of encryption. In a similar vein, we use the same technique in reverse form for the decryption step. Once the data is ready to upload, it is first encrypted using this combination of ECC-AES and then uploaded.

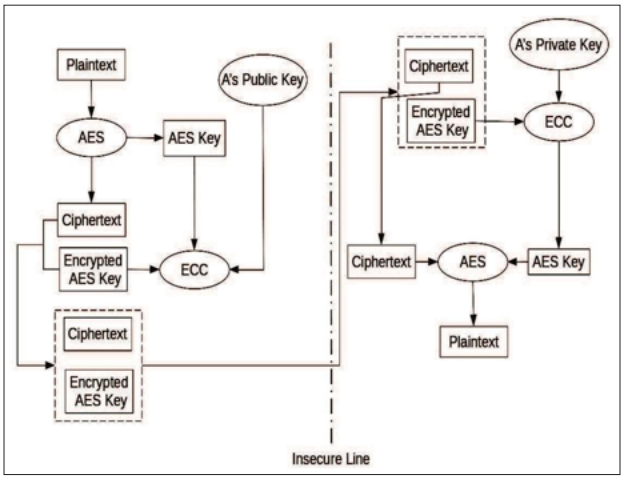

Figure 4: Hybrid Cryptosystem

Test Results

The AES-ECC cryptosystem is advantageous for both symmetric and asymmetric key methods.

File Encryption and Decryption

Figure 4 depicts the plaintext in the.txt file that will be encrypted using a dual encryption method. After successful encryption, the outcome is shown in Figure 5, which also contains the ciphertext in the a.txt file. The file is unreadable because it is encrypted.

Delay Calculation

The time between the successful run and the file reload will be used to calculate the delay.

Delay Calculation = aT – bT

where aT = Time after successful load and bT = Time before load.

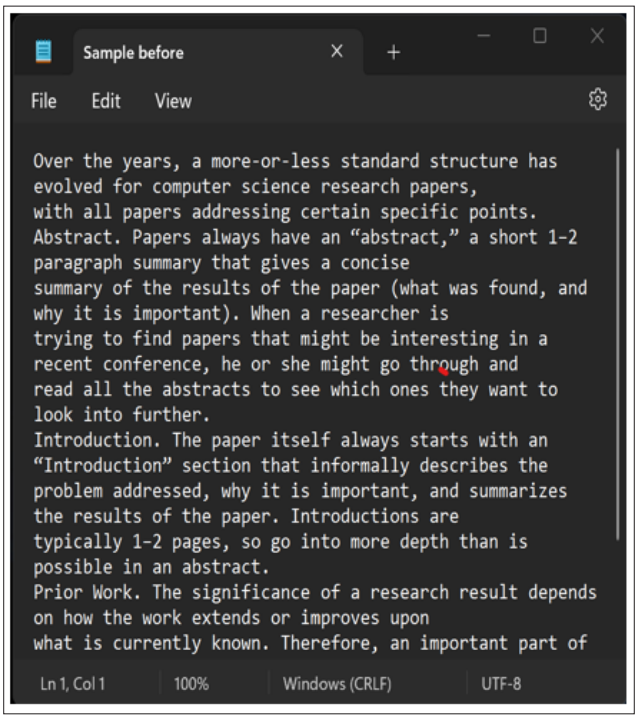

Figure 5: Plaintext

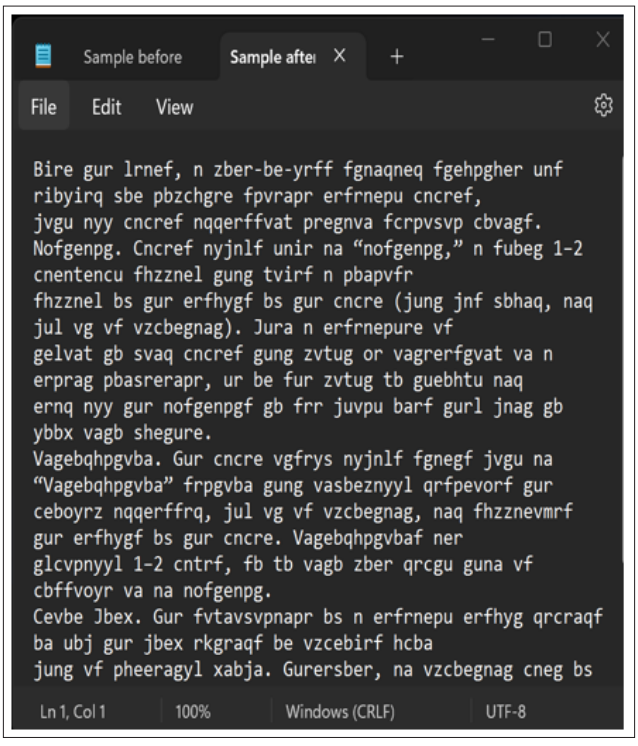

Figure 6: Ciphertext

Now, a test was carried out to compare these two methods, namely the AES algorithm and an ECC-AES combined technique. Text data was initially collected, and a key with a size of 128 was specified. This text data has been encrypted using the AES method. This encryption procedure's duration was noted. After encryption, the original text data was transformed into ciphertext. The original text data was then obtained by decrypting the encrypted data (ciphertext). Again, the length of time for this decryption procedure was documented.

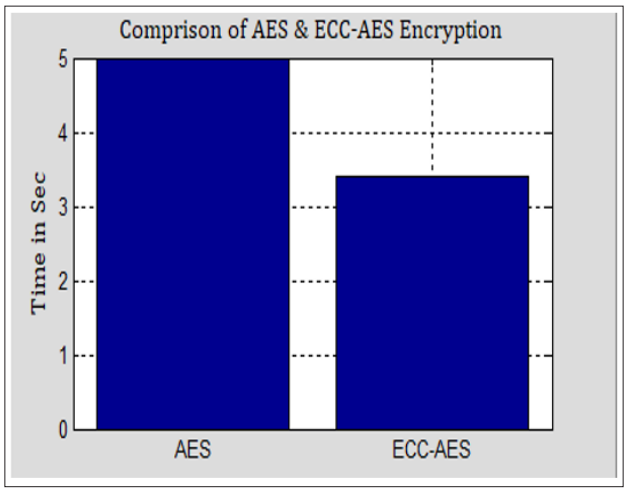

Figure 7: Comparison Time for Encryption in AES and ECC-AES

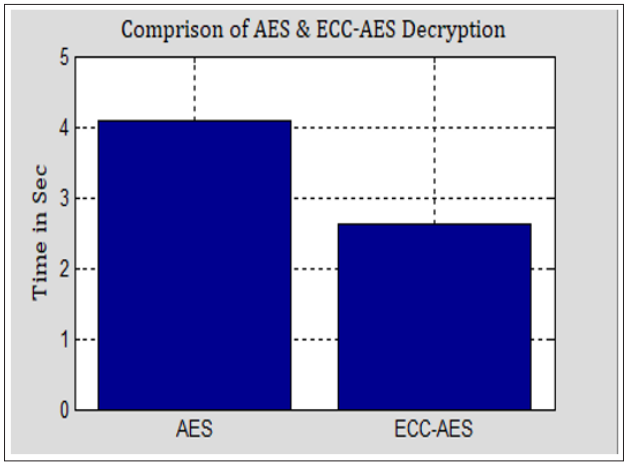

Figure 8: Comparison Time for Decryption in AES and ECC-AES

Figure 7 displays a bar graph with two bars displaying the length of time required for encryption using the AES and ECC-AES algorithms. ECC-AES uses comparably less time. Additionally, two bars in Figure 8 depict the lengths of time required to decode data using the AES and ECC-AES algorithms, respectively. The time that ECC-AES requires in this instance is also quite short.

Analysis of Test Result

The tests were conducted using several keys, including 64 bits, 128 bits, 192 bits, and 256 bits. For the final analysis of our test findings, we compare the set of results of our hybrid scheme with the already-existing scheme (AES algorithm). These keys were used to test the Hybrid ECC-AES model and the AES method for text data. The table below displays all the times required by both strategies. Additionally, for better comprehension, we can see the graph analysis of these variables here.

Table 1: Encryption Time in AES and ECC-AES

Key size (In bits)	AES encryption time (In sec)	ECC-AES encryption time (In sec)
64	-	2.43
128	3.73	2.46
192	3.67	2.47
256	3.75	2.51

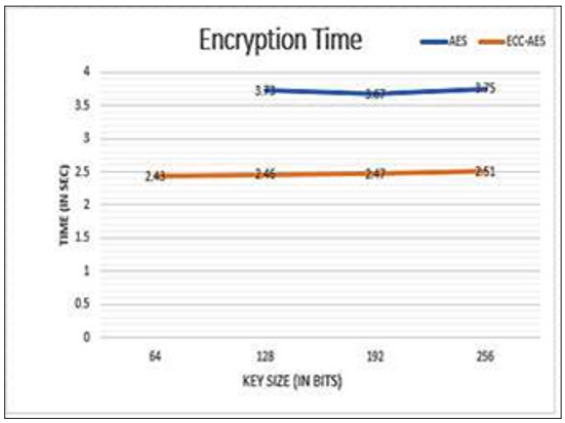

Figure 9: Comparison Chart for Encryption in AES and ECC-AES

First, as indicated in Table 1, the ECC-AES encryption process took 2.43 se conds utilizing a 64-bit key. The AES algorithm does not support the 64-bit key. AES time for the 128-bit key was recorded as 3.73 and ECC-AES time as 2.46. AES time for the 192-bit key was recorded as 3.67 and ECC-AES time as 2.47. AES time was measured at 3.75 while ECC-AES time was measured at 2.51 for the 256-bit key.

In Figure 9 the overall line graph shows how long the same text data is encrypted using AES and Hybrid ECC-AES algorithms. The hybrid ECC-AES model was found to be faster than the AES model.

Table 2: Decryption Time in AES and ECC-AES

Key size (In bits)	AES decryption time (In sec)	ECC-AES decryption time (In sec)
64	-	1.64
128	2.82	1.67
192	2.83	1.69
256	2.85	1.72

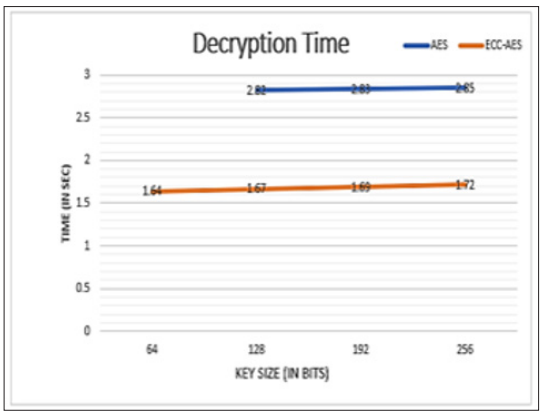

Figure 10: Comparison Chart for Decryption in AES and ECC-AES

Figure 10 illustrates the overall line chart of the time taken by AES and Hybrid ECC-AES methods to decrypt the same text input. The Hybrid ECC-AES model was discovered to be faster than the AES model.

As a result, the results demonstrated that the Hybrid ECC-AES approach takes less time to encrypt and decode than the traditional AES approach.

Conclusion

Confidentiality and security are critical concerns for cloud infrastructure data handling. Because the CSP is an untrusted third party, we cannot keep raw data without encryption due to confidentiality concerns. The proposed work discusses secure data transmission and storage in the cloud using a hybrid cryptosystem. The simultaneous use of AES and ECC helps increase the integrity and secrecy of the system, allowing us to use both symmetric and asymmetric encryption to safeguard cloud data.

As a result of combining the advantages of both, this hybrid model provides a higher level of security. The combination of these two strategies creates a more difficult system for an eavesdropper. This hybrid technique is faster than the standalone AES model for both encrypting and decrypting a file.

Future Work

Optimization of AES-ECC encryption scheme, scalability, integration of other security mechanisms, effectiveness in addressing emerging threats, applicability to other areas, the impact of network configurations, implementation of the prototype system, and comparison with other security solutions. We might also state that the "ECC" is the future of cryptography. “Its mathematical complexity and time efficiency set it apart”.

References

1. Verma S Sakshi (2011) Cloud computing security issues and challenges: a survey. In International Conference on Advances in Computing and Communications, Springer, Berlin, Heidelberg 445-454.
2. Hajarathaiah K, Seshu Chakravarthy T, Raphi G (2014) Dynamic Operation Implementation in Storage of Cloud Computing. International Journal of Science, Engineering and Technology Research (IJSETR) 3: 463-469.
3. Tripathy A, Kumar Pradhan S, Ranjan Tripathy A, Kumar Nayak A (2019) A New Hybrid Cryptography Technique in Wireless Sensor Network. International Journal of Innovative Technology and Exploring Engineering (IJITEE) 8: 121-131.
4. Poonam M Pardeshi, Deepali R Borade (2015) Improving Data Integrity for Data Storage Security in Cloud Computing. International Journal of Computer Science and Network Security 15: 61-67.
5. Rajput S, Dhobi JS, Gadhavi LJ (2016) Enhancing data security using aes encryption algorithm in cloud computing. Proceedings of First International Conference on Information and Communication Technology for Intelligent Systems 2: 135-143.
6. Tao Jiang, Xiaofeng Chen, Jian Feng Ma (2016) Public Integrity Auditing for Shared Dynamic Cloud Data with Group User Revocation. IEEE transactions on computers 65: 2363-2373.
7. Mahalle VS, Shahade AK (2014) Enhancing the data security in Cloud by implementing hybrid (Rsa & Aes) encryption algorithm. International Conference on Power, Automation and Communication (INPAC) IEEE 146-149.
8. Babitha MP, Ramesh Babu KR (2016) Secure Cloud Storage Using AES Encryption. International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT) International Institute of Information Technology (IIT) 859-864.
9. Lee BH, Kusuma Dewi E, Farid Wajdi M (2018) Data security in cloud computing using AES under HEROKU cloud. 27th Wireless and Optical Communication Conference (WOCC), IEEE 1-5.
10. Raman Kumar, Gurpreet Singh (2016) Analysis and Design of an Optimized Secure Auditing Protocol for storing data Dynamically in Cloud Computing. Materials Today: proceedings 5: 1037-1047.