SEMARAK ILMU PUBLISHING

Journal of Advanced Research in Applied Sciences and Engineering Technology

Journal homepage:
https://semarakilmu.com.my/journals/index.php/applied_sciences_eng_tech/index
ISSN: 2462-1943

Hybrid AES-Modified ECC Algorithm for Improved Data Security over Cloud Storage

Selvaraj Jagadeesh[1,*], Sabna Machinchery Ali[2], Soundara Pandian Gnana Selvan[3], Mohammad Aljanabi[4], Manimaran Gopianand[5], John peter Jasmine Hephzipah[6]

[1] Department of Information Technology, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, India
[2] Department of IT and Security, College of computer science, Jazan University, Jazan, Kingdom of Saudi Arabia
[3] Jayaraj Annapackiam CSI college of Engineering, Nazareth, Tamil Nadu 628617, India
[4] Department of Computer, College of Education, Alirqia university, 9985+758, Baghdad, Iraq
[5] Department of Computer Applications, PSNA College of Engineering and Technology, Dindigul-624622, Tamil Nadu, India
[6] Department of Electronics & Communication Engineering, R.M.K. Engineering College, RSM Nagar, Kavaraipettai-601206, India

ARTICLE INFO

Article history:
Received 16 May 2023
Received in revised form 24 July 2023
Accepted 2 August 2023
Available online 22 August 2023

Keywords:
AES; ECC; MECC; RSA; DES; blowfish; Diffie–Hellman; Encryption, Decryption

ABSTRACT

As cloud computing has been increasingly used by businesses to address their data storage and processing needs. The private data can be stored and retrieved by the end user through remote storage using an affordable Internet connection in the cloud computing environment. The user may access the information whenever they want, from wherever. However, the data transmitted through the cloud is not always secure and data integrity and authentication may be compromised as the end user is only able to access the data through a third party. Cloud computing also enables numerous people to access information simultaneously over separate Internet connections, which might increase the risk of information loss or leakage. Several cryptographic methods like DES, 3DES, Blowfish, RSA, Diffie-Hellman have been developed to guarantee the safety and privacy of stored data. Since the business clients hesitate to adopt the cloud due to its less security. This paper suggests a method for exchanging cloud data that is both secure and efficient. The proposed method is mainly focused on higher security for the cloud computing platform by applying hybrid Modified Elliptic Curve Cryptography (MECC) method with the Advanced Encryption Standard (AES). In comparison to other methods, the hybrid ECC-AES strategy takes less time to encrypt and decode data owing to its reduced key size.

1. Introduction

Users of cloud services introduce serious vulnerabilities, such as data loss and breaches, either by accident or on purpose. Therefore, data access limits should be placed on unapproved and unauthenticated data sources. Devices may potentially contribute to data breaches if users are permitted to repurpose APIs and data. Therefore, the primary function of cryptographic approaches

* *Corresponding author.*
E-mail address: jagadeesh15.sj@gmail.com

https://doi.org/10.37934/araset.32.1.4656

is to safeguard cloud-based data using encryption/decryption procedures utilising a variety of keys. Data encryption may be done in two different ways, employing either asymmetric or symmetric keys [1]. Public-key cryptography is an alternative to symmetric-key encryption. It uses a private key and a public key to encrypt and decode information. In contrast, symmetric key encryption encrypts data using a single private key and decrypts it using the same key. Symmetric cryptographic techniques are more challenging because of the key size (which must be big enough for effective security). The AES standard, which is also based on symmetric key encryption, was supposed to replace the DES standard. The 128-bit keys used by AES make it substantially quicker than DES's 64-bit keys.

In comparison to other current cryptographic techniques like the Rivest-Shamir-Adleman algorithm (RSA), the key size required for MECC's asymmetrical key encryption is much less. MECC's use of asymmetric cryptography allows for faster processing times and simpler hardware requirements when compared to competing techniques. AES with Encryption Certificates (ECCs) was suggested by Chen *et al*., [2] as a means to strengthen system security. However, Shamir's private sharing key was also used throughout the data transmission. To protect information kept in the cloud without using an additional service, we advocated a hybrid AES-MECC method in this research. Using the suggested hybrid method, system security may be effectively maintained while relying on cloud storage.

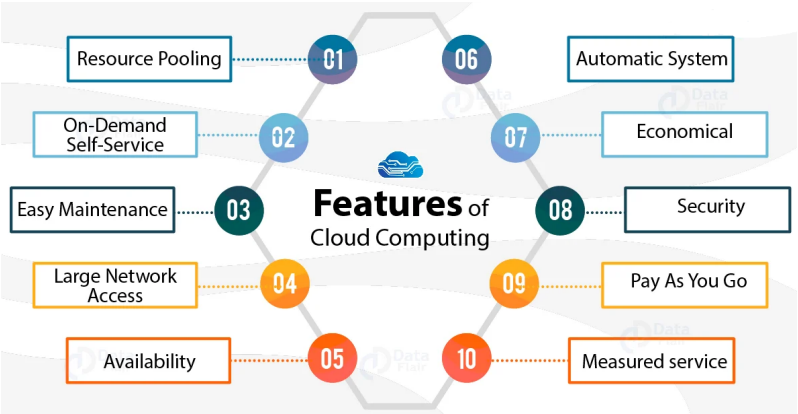

Fig. 1. Cloud Services

Figure 1 represents Current developments in cloud storage have given consumers access to a variety of services that enable experienced data encryption and decryption without the need for a mediator. This improves the system's ability to increase its security as well as the effectiveness of the storage for safe convenience and quick data retrieval. Via this service, it is simple for various user types to share cloud resources, and the use of cryptographic algorithms increases the system's capacity by securing additional storage.

In Figure 2 displays several cloud storage service types. It is clear that the data being sent back and forth between the sender and the recipient is being encrypted, decrypted and stored on a cloud server. Additionally, it stands for the safe transfer of data through cloud storage.

ECC, a sort of efficient cloud services that is utilised for data encryption and decryption, is offered. These services employ asymmetries in their data encryption and decryption. It employs RSA data encryption and decryption, which is more efficient than other methods since the key size is less than with symmetric encryption and decryption. For instance, utilising the RSA algorithm with ECC will reduce the amount of the key's data from 1020 bits to 163 bits. Additionally, ECC is better suited for network access via cellphones. Many hackers are ready to extort consumers by obtaining their

personal information or other data. Because of this, ECC is designed primarily for people who access their data through devices that aren't very secure and are therefore vulnerable to hacking.

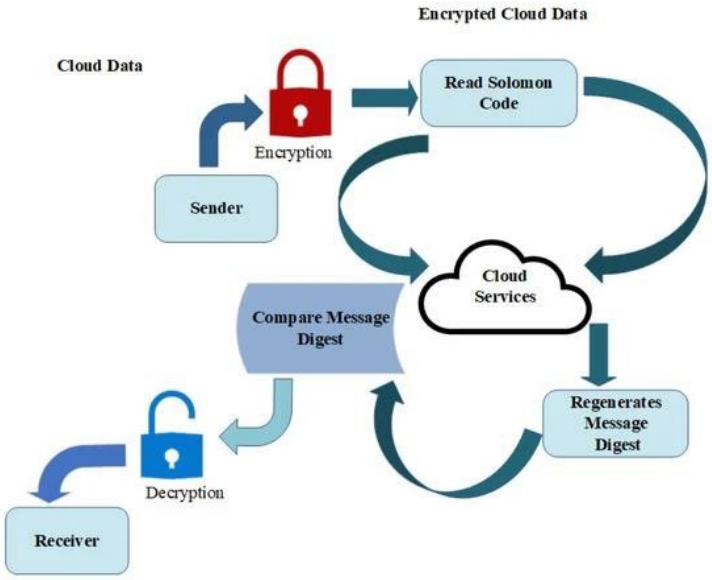

Fig. 2. Secure transmission in cloud storage

2. Literature Survey

Cloud storage is gaining popularity due to the fact that all users share resources in sync. Data owners choose cloud storage over other services because it is available around-the-clock [3]. For this reason, data integrity and data preservation should be investigated in order to increase system security. It is advised to combine AES and ECC to boost system security. Shamir's secret sharing is used to distribute and administer the system in the absence of a trusted hub. System security is improved by the combination technique that has been proposed, albeit at a high computational and time cost. The recommended method is used in conjunction with the proper algorithms, such as AES, DES, and Blowfish.

Comprehensive examination of nature-inspired cloud computing scheduling optimisation techniques. The approach increases data storage efficiency and integrity, minimising the possibility of conflicts among large user groups while maintaining the privacy of personal data for each user [4]. The service provider also coordinates and speeds up data accessibility. Cloud computing data services may also be used to assess the avalanche effect of plain text and data block size.

The security potency of RSA and ECC are connected using six data spanning 264 bits that comply with NIST requirements. The ECC technique outperforms the RSA method, as seen by this comparison of the two algorithms' performance, since it provides more secured services across lower data sizes and necessitates less storage for data accessibility [5].

Data must be encrypted and decrypted using ECC in order to provide dependable services to a variety of consumers [6]. Data is encrypted and decoded using a two-part, tiered approach. The first component reduces the size of the keys and provides rapid increments for bit additions throughout the data encryption operation. In the first layer, data is encrypted using P0, P1, P2, P3, P4, and Pn; in the second layer, a collection of elliptical curves are utilised. These procedures are used to safeguard the data throughout both the encryption and decryption processes. The previous methods were plagued by data loss and security problems. ECC is used to protect data and stop its deletion for

immoral motives in order to lessen the consequences of these issues. This asymmetric cryptography technique makes it feasible to quickly protect data and upgrade to larger datasets, enabling the fastest security service delivery. ECC offers both data access and cloud security services at the same time.

A cloud computing system based on polynomials for elliptic curve encryption. You can be sure that your clients will support and utilise the service if you employ this approach. The hybrid cloud is perfect for boosting cloud data protection because it is flexible enough to adapt to changing needs while still offering top-notch security. The primary concern is the security of the system and its users, and both polynomial hashing and the elliptical curve that follows the hybrid approach provide a significant contribution to this aim. Information is encrypted and decrypted using PHECC and given a special hash value to ensure the security of data saved in the cloud. In PHECC, an elliptical curve is utilised for both encryption and decryption, and a hash value is generated using a combination of polynomial hashing and hybrid approaches [7]. Therefore, utilising cloud services, it is feasible to safely store and transfer data.

Only the signature parts of the compressed data are sent to the elliptical curve authority for signing and digesting after the data has been compressed using a hybrid approach for RSS and ECC. ECC will sometimes use the encrypted data for this function [8]. Throughout the procedure, the same encryption technique is used. Due to their respective advantages, algorithms that employ both RSS and ECC analysis are integrated.

Different media are used to protect data encryption and decryption during transmission. In the work the secrecy, integrity and integrity of the data are discussed. When using cloud computing services via the internet, the Irondale encryption algorithm and EAP-CHAP are the technologies utilised for data authentication and secrecy.

These storage spaces store high-capacity, more sensitive data [9]. This is why data authentication is essential in various modern devices such as Internet of Things (IoT) devices. To execute cryptographic operations on this device, the processor power needs to be high. These devices use clouds to authenticate data and execute protocols. IaaS for storage provides client organisations with a suitable amount of flexibility and freedom in utilising the virtualized environment for their storage requirements. IaaS serves as the first stage for numerous sorts of administrations. The demand for capacity and data transmission determines the two other installation kinds, factors and ward. Several types of installments that rely on the capacity limit are often included in the first criterion, which is the capacity limit. As a consequence, the price of 1 GB differs depending on whether the total required is less than 1 TB or larger than 1 TB.

Services for cloud computing face substantial obstacles in terms of privacy and security [10]. We are unable to store raw data without encryption due to privacy issues, since the CSP is an unreliable third party. The suggested research talks about cross-breed cryptosystems for capacity and trustworthy data transport in the cloud. In order to increase the security of the cloud data, we may utilise symmetric and divergent encryption while concurrently enhancing the framework's classification and credibility by utilising AES and ECC. As a result, the projected model retains an efficient, powerful, and well-organized encryption technique based on AES and ECC.

The security model's ability to store and transfer sensitive information utilising public cloud technologies relies on a number of intricate components. AES is used to encrypt the message that will be delivered to the cloud, and a 256-bit decoding motor is used to decode it [11]. For quickly scrambling vast volumes of data, AES has shown outstanding performance. Steganography is one of the strategies used in information security. By hiding critical information in other data,

steganography expands the amount of data that may be kept on the cloud. These have the undesirable impact of accelerating transfer rates and decreasing cloud capacity use.

The fastest choice is AES encryption since it is also adaptable, scalable, and easy to use [12-14]. AES offers a very high level of security since keys of 128 bits, 192 bits, or 256 bits may be used. Widely varying assaults, such as square, key, key recovery, and differential, cannot succeed against it. The AES algorithm is one of the safest ones available as a consequence. Your data may be safeguarded and future attacks like smash attacks may be avoided. One of the key methods for achieving great performance and energy efficiency is approximate computing.

Researchers have suggested a two-tiered cryptographic technique and model to improve data security in cloud computing [15-17]. The model uses symmetric and uneven encryption calculation (AES and ECC) to boost privacy, respectability of the information, and time taken to perform cryptographic tasks, increasing the level of client trust in cloud computing and accelerating the use of more modest keys of ECC in the cryptographic interaction.

3. Outline of the Problem

Data security is now a key concern that may be abused by both internal and external parties. Information sent over the Internet may be encrypted in a number of ways. However, these methods have the drawback of requiring a lot of resources, such as a lot of memory and computing power, to safeguard the data. Like AES encryption, a key is created quickly after an input file is submitted. To encrypt and decode data, AES employs a technique known as symmetric key encryption, which requires the use of a single key. If a third party has knowledge of the single key, they may decrypt the input file and encrypt it again without the user ever knowing that the file was read. Asymmetric key encryption is one of the most secure algorithms. MECC uses asymmetric key encryption because it requires two keys, the public key and the private key. This means that it has a higher level of protection since it is difficult for hackers to decrypt both keys at the same time. MECC's main advantage is its smaller key size. Unlike other algorithms, it can provide the same level of security with a smaller key size. Developing a system that provides data security through the cloud with lower computational costs and faster encryption / decryption process is essential. To leverage the strengths of both, we combine them in our proposed model.

3.1 Proposed Work

- By using the two algorithms AES and MECC, we provide a hybrid paradigm in which the key generation for AES is accomplished with the aid of MECC. Simply said, we produce the key using the MECC technique rather than the AES approach because it has a smaller key size.
- A public key or private key is used for data encryption and decryption, much like in symmetric/asymmetric encryption. As a result, this method takes a lot of computer power and a big key size. By addressing the issue of key size and assisting in the reduction of computing resources for memory optimization, the suggested hybrid method (AES-MECC) helps to improve system security in a shorter amount of time.
- With our suggested framework, we also give an algorithm that explains how the MECC method is used to produce the public key and how AES is used for encryption and decryption.

3.2 Working Principle

- MECC and AES are used to produce the most modern and secure cryptographic approach for

cloud storage. Single AES takes a little longer to encrypt data than the hybrid (MECC-AES) technique because of its larger key size, but the latter offers a smaller key size and a faster security mechanism for protecting the data.

- Due to MECC's fundamental feature—its small key size—AES's use of MECC for encryption reduces the key size and improves performance. By creating protected key system standards for encryption and decryption, MECC is able to minimize key size and improve security. When using AES for encryption, MECC is the best additional protection against unauthorized access.
- Data encryption and decryption will produce cipher text once the key size has been established. AES makes use of the key that MECC produces. For the suggested method of cloud storage to obtain the protected system, the combined effects of MECC and AES are adequate. By doing this, secure data storage size may be decreased. The suggested algorithm's block diagram is shown in Figure below.

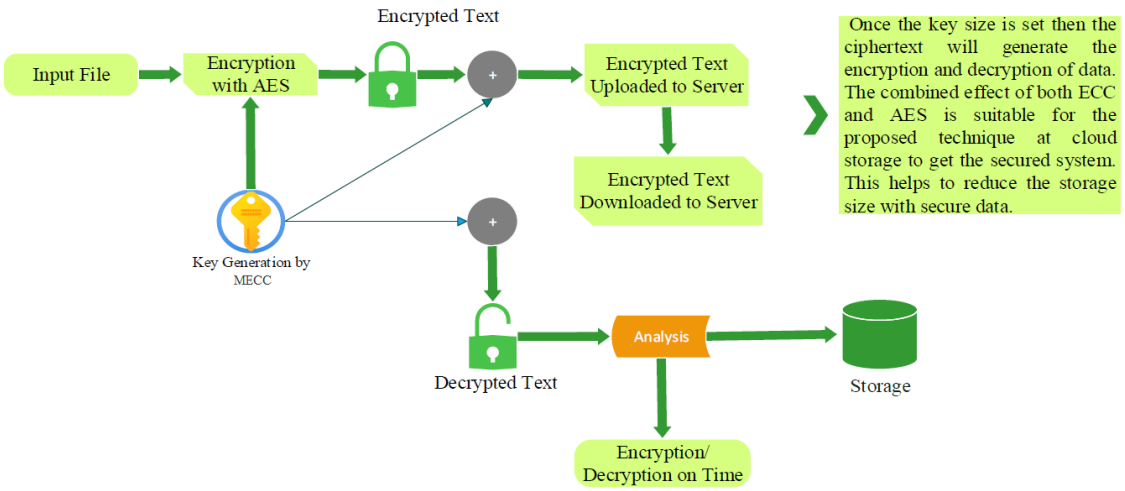

Fig. 3. Representation of AES- MECC Algorithm

The accompanying image clearly shows how AES and MECC collaborate to safely safeguard cloud-stored data. The newly presented image, which demonstrates secure user data transport to the server and afterwards storage method is even secured due to encrypted data, demonstrates how innovative the offered technique is. Moreover, innovation may be measured using the effort and expense of the computation. Attack prevention may be accomplished in the following methods, for example: in the suggested technique, the input file is turned into completely encrypted text using AES encryption once the user uploads the file. The user side can then be attacked if an attacker wishes to do so in order to steal the user's personal data or for any other reason. The user-uploaded file is therefore useless even if an attacker is successful in their attack and is able to access it because the data was already encrypted when it was posted. Similar to how an attack on one end prevents the attacker from decrypting the encrypted file, the encrypted file prevents attacks on the data.

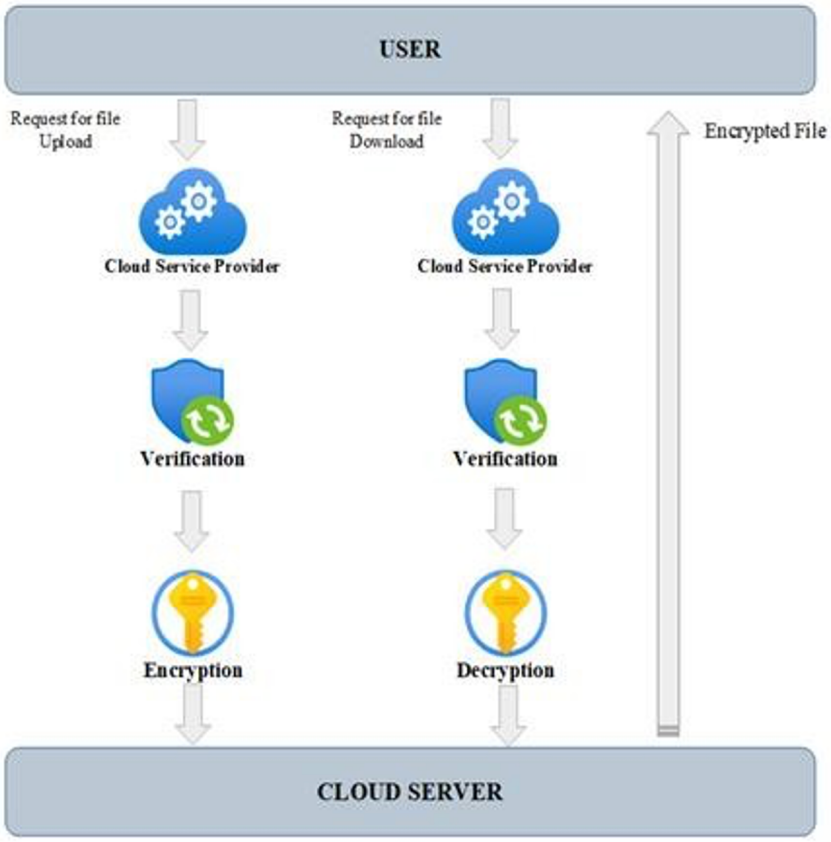

Fig. 4. Process between user and cloud server

In Figure 4, we see a user interacting with data stored on a cloud server, and we also see the actions taken by the server to fulfil the user's request in a safe and reliable manner.

3.3 The Suggested Framework's Algorithm

3.3.1 Public key generation using MECC

Step I. Select an Elliptic Curve: Choose a specific elliptic curve over a finite field. The curve equation is typically represented in the form of $y^2 = x^3 + ax + b$, where a and b are constants defining the curve and the coefficients are chosen according to certain standards.

Step II. Select a Generator Point: Choose a base point on the selected elliptic curve. This point should have a large prime order, meaning that it generates a cyclic subgroup of prime order. This point is often denoted as "G."

Step III. Determine the Order: Calculate the order of the base point G. The order represents the number of points in the subgroup generated by G. It is a large prime number, typically denoted as "n."

Step IV. Select a Private Key: Generate a random integer, often denoted as "d," such that $1 \leq d < n$. This private key will be kept secret and should not be shared.

Step V. Compute the Public Key: Instead of directly multiplying the base point G by the private key d, an improved algorithm called "Point Decompression" can be used to calculate the public key more efficiently. Here's the step-by-step process:

a. Calculate the x-coordinate of the base point G raised to the power of the private key d: X = d * Gx (where Gx is the x-coordinate of G).

b. Determine the y-coordinate of the resulting point on the elliptic curve. This requires solving the elliptic curve equation for y, given the x-coordinate X from the previous step. Depending on the curve's form, there can be two possible y-values: y1 and y2.
c. Choose the y-coordinate based on the parity of X and the least significant bit of y1 or y2. This is done to ensure the resulting point lies on the curve and maintain consistency. If the least significant bit of y1 matches the parity of X, then use y1 as the y-coordinate; otherwise, use y2.
d. The resulting point (X, y) on the elliptic curve, with the chosen y-coordinate, serves as the public key.

3.3.2 Using the AES for Encryption and Decryption

Step I. The input file
Step II. Add the MECC-generated key, which is the public key, now.
Step III. On the input file, AES encryption is carried out using the MECC-generated public key.
Step IV. After AES encryption, the encrypted file is uploaded to the server.
Step V. Following submission, the file will be downloaded from the server and translated using the MECC-provided public key to unlock the original file's encryption.
Step VI. The efficiency of the system is affected by factors like MECC and AES, which optimize storage space and increase the security of the cloud server, respectively.

4. Results and Discussion

The encryption and decryption of most of the data stored in the cloud also makes use of encrypted connections, which further distinguishes the system and improves its efficiency. This suggests that the user may get a good grasp of the original text by using these two methods. The advantages of MECC and AES over RSA are enumerated in the next section. MECC ensures the confidentiality of any cloud data. Maximizing storage space and achieving the required results may be aided by keeping data with a decreased key size. It uses the same amount of bits (3012) as Rivest Shamir Adleman (RSA). The 2 main advantages of the MECC are its reduced key size and its more efficient data encryption utilizing a public key [18]. MECC has advantages over RSA because to its use of modern mathematical techniques for data encryption and decryption and the accuracy of the decrypted data. Statistical analysis, searching, and other comparable procedures are all slowed down by AES, which limits the usefulness of cloud storage. It's a popular tactic in cloud computing for improving storage security rules. The public key may be used for encryption and decryption and is available to the public. In comparison to RSA, the benefits of MECC and AES are shown in the table.

Table 1
Key size comparison MECC, RSA

MECC(in bits)	RSA(in bits)	Key Size Comparison (in bits)
150	924	1:6
250	3012	1:12
364	7160	1:20
524	10360	1:20

As seen in Table 1, MECC demands a medium key size as opposed to RSA. It provides more security than RSA as a result. When comparing MECC-AES to other cryptographic techniques, more security is also achieved with a smaller key size. Reduced key size enhances memory efficiency and reduces computational complexity. As a result, using a medium key size can result in high levels of data security.

Table 2
Cryptographic Algorithms: An Analytical Comparison

Factors	Proposed Hybrid	Data Encryption Standard	Blowfish	Rivest Shamir Adleman	Diffie- Hellman
No. of key	1	1	1	2	Key Exchange
Key Length(in bits)	64–256	56	32–448	1024	Key Exchange
Rounds	10	16	16	1	56

Table 2 presents an analysis of numerous cryptography methods using multiple different parameters. Different cryptographic approaches have been compared and contrasted based on a variety of performance measures, including the number of keys used, the size of the keys, and the number of rounds [19].

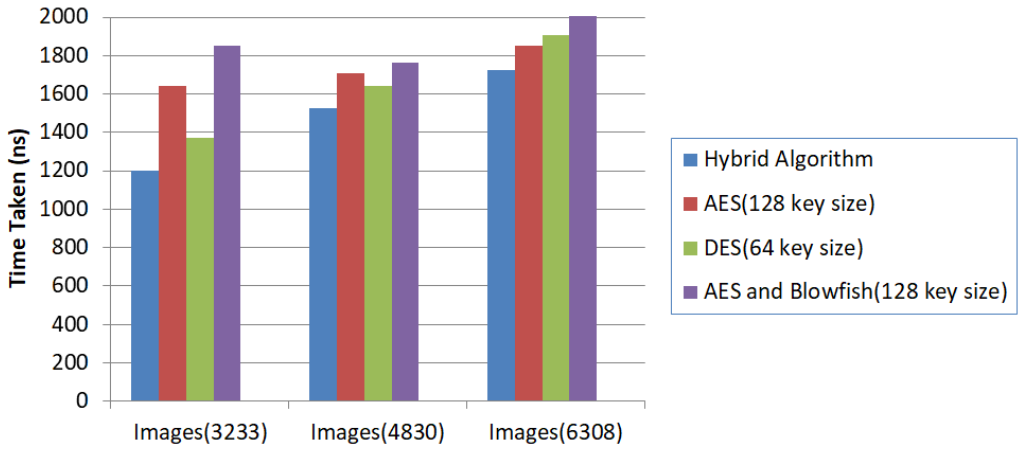

Fig. 6. Time evaluation of different encryption cryptographic algorithm

Each experiment used three image datasets (3233, 4830, and 6308) and one of four cryptographic methods (Proposed AES-MECC, AES-128, DES-64, AES, and Blowfish-128) to achieve three experimental results. Time, memory footprint, and throughput were used to evaluate the effectiveness of each approach. The time required to convert plaintext into cipher text using a certain cryptographic technique is known as the encryption time. The throughput of an encryption process may be calculated by dividing the number of bytes of encrypted plaintext by the number of nanoseconds it took to encrypt the plaintext. Figure 6 displays the outcomes of the simulated design. In contrast to competing algorithms, MECC-AES completed its processing time the quickest.

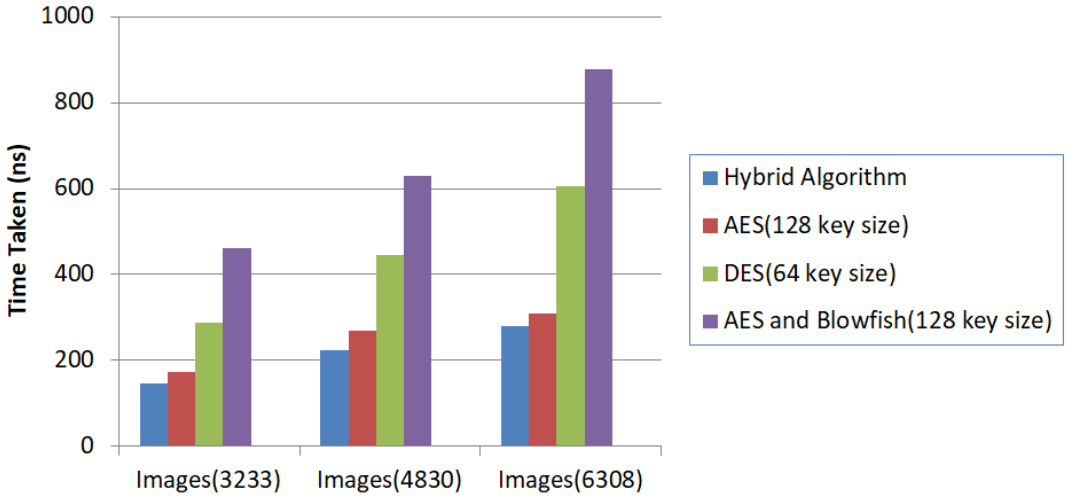

Fig. 7. Time evaluation of different decryption cryptographic algorithm

The experiments used three different image datasets (3233, 4830, and 6308) and four different cryptographic algorithms (the proposed hybrid algorithm MECC-AES, AES-128, DES-64, AES, and Blowfish-128) to generate three different sets of findings. The effectiveness of the algorithms was measured by their execution time, memory footprint, and throughput. A cryptographic algorithm's decryption time is the amount of time it takes to reverse-engineer cipher text into plain language. The throughput of a decryption operation is calculated by taking the decryption time (in ns) and dividing it by the size of the complete decrypted cipher text (in bits). The results of the simulation are shown in Figure 7. When compared to the other algorithms, the suggested MECC-AES took the least amount of time.

5. Conclusion

IT services, such as cloud computing, benefit customers even if they have a low degree of technical knowledge. Independent cloud service providers provide an interface for storing, managing, updating, and retrieving data via the Internet, making it accessible from anywhere in the world. The choices available to consumers of cloud services are flexible. Depending on the kind of cloud service, users are the ones who really make use of the service. Many customers like the low prices and convenient access to their data from any location. Since you don't need to bring your gadget with you wherever you go, any platform is open to receiving cloud services. A disadvantage of cloud services is the lack of data protection they provide, however this may be compensated for by taking extra precautions. The development of the key, in particular, may be streamlined with the help of MECC. MECC is superior to other cryptographic methods because of its small key size. Data optimization and security may be considerably improved when AES is used with MECC. Improving the safety of the hybrid method might aid future studies. Additional security measures might be included to improve the efficiency and output of the system.

Acknowledgement

This research was not funded by any grant.

References

[1] Al-Amri, Rusul Mansoor, Dalal N. Hamood, and Alaa Kadhim Farhan. "Theoretical Background of Cryptography." *Mesopotamian Journal of CyberSecurity* 2023 (2023): 7-15. https://doi.org/10.58496/MJCS/2023/002

[2] Chen, Yange, Hequn Liu, Baocang Wang, Baljinnyam Sonompil, Yuan Ping, and Zhili Zhang. "A threshold hybrid encryption method for integrity audit without trusted center." *Journal of Cloud Computing* 10 (2021): 1-14. https://doi.org/10.1186/s13677-020-00222-6

[3] Shukla, Dhirendra KR, Vijay KR Dwivedi, and Munesh C. Trivedi. "Encryption algorithm in cloud computing." *Materials Today: Proceedings* 37 (2021): 1869-1875. https://doi.org/10.1016/j.matpr.2020.07.452

[4] Yahia, Hazha Saeed, Subhi RM Zeebaree, Mohammed AM Sadeeq, Nareen OM Salim, Shakir Fattah Kak, Adel AL-Zebari, Azar Abid Salih, and Helat Ahmed Hussein. "Comprehensive survey for cloud computing based nature-inspired algorithms optimization scheduling." *Asian Journal of Research in Computer Science* 8, no. 2 (2021): 1-16. https://doi.org/10.9734/ajrcos/2021/v8i230195

[5] Khan, Imran Ahmad, and Rosheen Qazi. "Data security in cloud computing using elliptic curve cryptography." *International Journal of Computing and Communication Networks* 1, no. 1 (2019): 46-52.

[6] Agrahari, Vishal. "Data security in cloud computing using cryptography algorithms." *International Journal of Scientific Development and Research (IJSDR)* 5, no. 9 (2020): 258-260.

[7] Abdullahi Ibrahim, A., W. Cheruiyot, and M. W. Kimwele. "Data security in cloud computing with elliptic curve cryptography core." *Int. J. Comput* 26 (2017): 1-14.

[8] Manaa, Mehdi Ebady, and Zuhair Gheni Hadi. "Scalable and robust cryptography approach using cloud computing." *Journal of Discrete Mathematical Sciences and Cryptography* 23, no. 7 (2020): 1439-1445. https://doi.org/10.1080/09720529.2020.1727609

[9] Astuti, N. R. D. P., E. Aribowo, and E. Saputra. "Data security improvements on cloud computing using cryptography and steganography." In *IOP Conference Series: Materials Science and Engineering*, vol. 821, no. 1, p. 012041. IOP Publishing, 2020. https://doi.org/10.1088/1757-899X/821/1/012041

[10] S Awad, Wasan. "A framework for improving information security using cloud computing." *International Journal of Advanced Research in Engineering and Technology* 11, no. 6 (2020).

[11] Almorsy, Mohamed, John Grundy, and Ingo Müller. "An analysis of the cloud computing security problem." *arXiv preprint arXiv:1609.01107* (2016).

[12] Panimalars, Arockia, N. Dharani, R. Aiswarya, and Pavithra Shailesh. "Cloud Data Security Using Elliptic Curve Cryptography." (2017).

[13] Hosam, Osama, and Muhammad Hammad Ahmad. "Hybrid design for cloud data security using combination of AES, ECC and LSB steganography." *International Journal of Computational Science and Engineering* 19, no. 2 (2019): 153-161. https://doi.org/10.1504/IJCSE.2019.100236

[14] Mendonca, Smitha Nisha. "Data security in cloud using AES." *Int. J. Eng. Res. Technol* 7 (2018). https://doi.org/10.17577/IJERTV7IS010104

[15] Hodowu, Dickson Kodzo Mawuli, Dennis Redeemer Korda, and Edward Danso Ansong. "An enhancement of data security in cloud computing with an implementation of a two-level cryptographic technique, using AES and ECC algorithm." *Int. J. Eng. Res. Technol* 9 (2020): 639-650.

[16] Lee, Bih-Hwang, Ervin Kusuma Dewi, and Muhammad Farid Wajdi. "Data security in cloud computing using AES under HEROKU cloud." In *2018 27th wireless and optical communication conference (WOCC)*, pp. 1-5. IEEE, 2018. https://doi.org/10.1109/WOCC.2018.8372705

[17] Zhu, Yiming, Anmin Fu, Shui Yu, Yan Yu, Shuai Li, and Zhenzhu Chen. "New algorithm for secure outsourcing of modular exponentiation with optimal checkability based on single untrusted server." In *2018 IEEE International Conference on Communications (ICC)*, pp. 1-6. IEEE, 2018. https://doi.org/10.1109/ICC.2018.8422482

[18] Gharshi, Ravi. "Suresha. enhancing security in cloud storage using ecc algorithm." *International Journal of Science and Research (IJSR), India Online ISSN* (2013): 2319-7064.

[19] Rehman, Saba, Nida Talat Bajwa, Munam Ali Shah, Ahmad O. Aseeri, and Adeel Anjum. "Hybrid AES-ECC model for the security of data over cloud storage." *Electronics* 10, no. 21 (2021): 2673. https://doi.org/10.3390/electronics10212673