International Journal of Scientific Research & Engineering Trends
Volume 11, Issue 5, Sept-Oct-2025, ISSN (Online): 2395-566X

Universal Encryption For Secure Cloud Storage

[1]Senthil Kumar T,[2]Mardeni Roslee, [3] Jayapradha , [4]Shubhanshu Tiwari, [5]Pranjal Mishra
[1345]Department of Computing Technologies SRM Institute of Science and Technology Chennai, India
[2]Department of Engineering Multimedia University Cyberjaya, Malaysia

Abstract- Classroom attendance tracking was a fundamental task in educational institutions, traditionally managed through manual roll calls or sign-in sheets. These methods were time-consuming, error-prone, and susceptible to manipulation. With advancements in computer vision and embedded systems, there was an opportunity to automate this process. In this research paper, a novel approach to classroom attendance management was presented, utilizing OpenCV and face recognition technologies, implemented on the ESP32-CAM microcontroller. The proposed system was designed to automatically identify and record student attendance, offering enhanced accuracy and efficiency. Comparative results demonstrated that the face recognition-based approach significantly outperformed traditional manual methods and other automated systems in terms of accuracy and processing speed. The system's architecture, implementation, and evaluation were outlined, showcasing its potential to transform attendance tracking in educational settings.

Index Terms- ECC, client-side encryption, secure storage.

I. INTRODUCTION

Encryption

The need for standardized information safety has never been more crucial than now with the always increasing digitalization of our lives, as personal and professional data now exists on cloud servers. As such, protecting this data from cyber threats has become a top priority. Cryptography is the technique by which data and information can be secured using math concepts and formulas. This ensures the integrity and confidentiality of the information as well as limits its access to certain individuals only. Two fundamental processes, depicted in Fig. 1, form the foundation of cryptography: encryption, which transforms data into a hashed format to prevent unauthorized access, which reverses this process to decrypt the data for authorized users. One cryptographic method that effectively addresses common issues is Elliptic Curve Cryptography. ECC provides security with relatively smaller key sizes compared to RSA, making it faster, especially for devices with limited resources like smartphones and IoT devices.

II. METHODOLOGY

Introduction

It is a public-private key-based cryptographic technique invented by Neal Koblitz and Victor Miller in 1985. It is based on some of the mathematical properties of elliptic curves to offer high strength for encryption and, therefore, safety and efficiency. Like other asymmetric methods of encryption, there are two keys: the public key, and the secret private key. These keys are used in the encryption/decryption processes to secure data during transit and storage. In ECC, the encryption process involves defining a curve over a finite field. For a given large prime number (p) taking mod p as Fp, the curve is expressed by the equation:

$$Y^2 \equiv X^3 + aX + b \pmod{p}$$

where a and b are constant, and the curve must satisfy the condition:

$$4a^3+27b^2 \not\equiv 0 \pmod{p}$$

Any point (x,y) that satisfies this equation lies on the curve, and the set of these points, including the point at infinity, defines the elliptic curve.

Working of ECC

The operation of ECC relies on defining elliptic curves over a finite field and exploiting their math properties to achieve robust security. Each user generates a key pair which consists of a public and private key, derived by multiplying the private key with a generator point on the curve [7]. The multiplication yields another point on the curve, which acts as the public key.

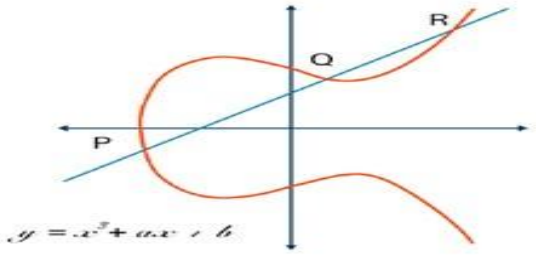

Figure1. Elliptic Curve Equation

In the above Fig-1, the general elliptic curve follows the equation:

$$Y^2 \equiv X^3 + aX + b$$

Where the red curve represents the graph of the elliptic curve, and the blue line which intersects the curve at points P, Q, and R. Given two lines on the curve which intersects the curve at points P and Q, the line will intersect at a third point R, which gives us the elliptic curve addition:

$$P + Q = -R$$

Architecture of ECC

ECC encryption involves the sender using their provided key to encrypt their data. Only users with the correct private key can decrypt the document. This asymmetric encryption provides high security, as deducing the private key is currently infeasible due to the ECDLP [8]. Additionally, ECC supports digital signatures, ensuring data integrity and authenticity. Senders sign messages with their private key, allowing recipients to authenticate them using the public key [11]. ECC is pivotal in secure cloud storage and data protection frameworks.

ECC in multi-algorithm framework

Integration of ECC with other cryptographic algorithms brings the opportunity to leverage the strengths of multiple encryption techniques, which will lead to more secure and efficient systems. One commonly implemented method is by merging ECC with other encryption algorithms like Advanced Encryption Standard. Under such hybrid models [14], ECC can be put into action for authenticated exchanging or encrypting of the symmetric keys, and AES executes fast encryptions and decryptions of big data. This ensures the protection of ECC during key exchange, while AES speeds up data handling. ECC is also employed together with hashing algorithms like SHA-256 to ensure data integrity and then develop digital signatures for protecting against tampering attacks. In multi-factor authentication systems, ECC can be adopted in combination with biometric data or password-based encryption to further enhance security. Similarly, combining ECC with quantum-resistant algorithms [25] can protect systems against emerging threats from quantum computing.

The distinctive feature of ECC is the balance it achieves in matters of security, efficiency, and optimizing resources. Also, by encompassing other algorithms, ECC is highly versatile and applicable to a wide range of secure communications and storage solutions.

III. COMPARISON ANALYSIS

Key-size Comparison

Key size has a big role in the security strength of an encryption algorithm. AES supports 128, 192, and 256-bit keys, offering a balanced trade-off between security and performance. DES, an older symmetric encryption standard, has a fixed 56-bit key, making it susceptible to brute force. Blowfish allows flexible key sizes ranging from 32 to 448 bits, though it is largely replaced by AES. RSA, an asymmetric encryption method, typically employs key sizes of 1024, 2048, or 3072 bits to ensure strong security. ECC, in contrast, achieves equivalent security levels with a relatively smaller key size, such as a 256-bit ECC key.

Encryption Time Analysis

Encryption time is crucial for performance, especially in large-scale data processing applications. AES provides the fastest encryption speeds among symmetric algorithms, making it ideal for real-time applications. DES, due to its smaller key size, is slower and less efficient. Blowfish shows slightly higher encryption times but remains competitive in speed. Among asymmetric methods, RSA encryption is significantly slower due to its complex mathematical operations, while ECC is faster as it requires smaller key sizes and lower computational overhead.

From table-1, AES effectively generates quicker results than DES and Blowfish encryption times at every size of the keys. AES specifically exhibits less speed at smaller key sizes of 64 and 128 bits, being just faster than DES and Blowfish with encryption times of 3.42s and 3.59s respectively.

Algorithm	Key Size	Encryption Time (in ms)	Decryption Time (in ms)
AES	128-bit	0.5	0.5
	192-bit	0.6	0.6
	256-bit	0.7	0.7
RSA	1024-bit	3.0	2.5
	2048-bit	6.0	5.0
	3072-bit	9.0	7.5
	4096-bit	12.0	10.0
ECC	160-bit	1.0	1.0
	224-bit	1.2	1.2
	256-bit	1.4	1.4

Table.1. Performance of various encryption algorithms with respective key-sizes.

DES has been adopted enormously in previous applications but has relatively slow encryption times for all tests, being between 3.89s and 4.34s, therefore not so ideal for today's applications,

which call for efficiency. The key sizes of Blowfish have little flexibility, but it's not quite a comfortable creature with its key size being 256 bits, slowing down to 70s significantly; this mainly represents its inefficiency at higher security levels.

IV. RELATED WORKS

With many academics and developers creating innovative solutions to improve data security, the field of secure data storage and encryption has changed significantly. Various cloud security systems have been studied using a combination of key management techniques and encryption algorithms to effectively resolve the problems connected to protecting sensitive data in digital environments. These projects' main drives are to address the shortcomings of traditional cloud storage, including dependence on server-side encryption, data transfer vulnerabilities, and the absence of user control over encryption keys.

N. Krishnaveni and C. Jayakumari [11] proposed a "hybrid framework to enhance cloud security" by combining ECC and Attribute-Based Access Control (ABAC). The goal is to improve both encryption and access control to better protect confidential data in the cloud. The framework integrates authenticated access with ABAC and enhances ECC encryption by mapping plaintext into elliptic curve points, reducing time and space requirements. This approach aims to maintain high security without sacrificing performance. However, designing an improved mapping algorithm for encoding data efficiently remains a challenge.

D Bikshapathi et al. [12] presents a technique that enhances cloud security by "combining two algorithms, namely Advanced Encryption Standard and Elliptic Curve Cryptography". AES enables fast data encryption and decryption, while ECC ensures secure public key exchange. Together, they provide a secure connection, authentication, and protection against unauthorized access. If an unauthorized user tries to access the private cloud, the system can monitor and block their IP address and device to prevent further attempts. The study also examines performance metrics such as storage, encryption, and decryption times, demonstrating that this combined approach outperforms other security algorithms. However, key management remains a significant challenge, as AES requires a secure method for distributing symmetric keys, while ECC must exchange public keys without exposing private ones.

D. Shivaramakrishna and M. Nagaratna [13] proposed "a hybrid cryptographic framework to further increase the security of data stored on servers by combining AES-OTP (Advanced Encryption Standard with One-Time Password) and RSA encryption. AES-OTP offers efficient encryption, while RSA provides secure key exchanges. The framework also features adaptive key management, which generates, distributes, and rotates keys in real time to support secure operations, and time-limited access control, which restricts data access based on predefined windows". However, the framework's complexity lies in managing multiple encryption layers and adaptive key rotation, which requires robust infrastructure.

Siva Sankaran P. and Kirubanand V. B.[19] introduced a "hybrid cryptography method using Twofish and ECC" to secure public cloud data. This approach combines Two-Fish's speed for encrypting data with ECC's strong key management for encrypting the Two-Fish key. The hybrid technique improves cloud security and user trust but may face challenges with slower encryption/decryption speeds for large data sets due to the added cryptographic steps.
Simranjit Kaur and Lokesh Jain [16] propose a hybrid encryption scheme "combining Elliptic Curve Cryptography and Triple Data Encryption Standard to enhance cloud security". This ECC-TDES method offers better protection against malicious attacks and was tested on a cloud-based web app with various file types (audio, video, image, and text). While the hybrid approach provides high accuracy (0.01% error rate), it increases encryption and decryption time compared to using ECC or TDES alone. The study focuses only on data encryption and excludes aspects like network protection or disaster management.
R. Bhagyalakshmi et al. [17] introduced a hybrid cryptographic system "combining AES and homomorphic encryption with Elliptic Wind Cryptography (ECC) to enhance data security for cloud storage. This system allows operations on encrypted data, maintains high security with reduced key sizes, and minimizes transmission and computation overhead". It also uses binary data splitting to divide files into multiple parts accessible only by the data owner, ensuring privacy. While the approach offers strong encryption and efficiency, key management and the complexity of homomorphic encryption can present challenges.

V. CONCLUSION

The increasing demand for secure data transfer today is growing faster than ever before, highlighting the importance of encryption algorithms such as Elliptic Curve Cryptography as a solution. With low computational overhead and high security, and smaller keys as compared to other algorithms like RSA and AES, it provides the general audience with a chance to securely transmit data without the worry for potential leaks.

Declarations and Ethical Considerations

Study Limitation: None.
Acknowledgments: None.
Funding Source: None.

Competing Interests: The author declares no competing interests.

Warning for Hazard: The research did not involve the use of any chemicals, procedures, or equipment with unusual hazards.

Use of Generative AI and AI-assisted Technologies in the Writing Process: During the preparation of this work, author used generative ai to re-phrase and improve the grammar content of the manuscript, The AI tool was only used to enhance clarity, not for content generation.

Ethical Approval: Not applicable. Ethical approval was not required for this study.

Informed Consent: Not applicable. No patients/participants/respondents were involved in this study.

REFERENCES

1. Gharshi, Ravi, Suresha: Enhancing Security in Cloud Storage using ECC Algorithm. SemanticScholar 2(1), 100–102 (2013).
2. Ahmad, Sadiq Aliyu, Garko, Ahmed Baita: Hybrid Cryptography Algorithms in Cloud Computing: A Review. 2019 15th International Conference on Electronics, Computer and Computation (ICECCO) (), 1–6 (2019).
3. Subrahmanyam, Vinay, Avasthi, Hanumat, Sastry, Akashdeep, Bhardwaj, G.V.B.: Security Algorithms for Cloud Computing. Procedia Computer Science 85(), 535–542 (2016).
4. Rehman, Saba, Bajwa, Nida, Shah, Munam, Aseeri, Ahmad, Anjum, Adeel: Hybrid AES-ECC Model for the Security of Data over Cloud Storage. Electronics 10(), 2673 (2021).
5. Gaikwad, Srivaramangai R., Tejaswi, Kumbhar, Rahul: Enhancing Security Using ECC in Cloud Storage. IJCRT (), 4–6 (2023).
6. Anas, Mohammad, Imam, Raza, Anwer, Faisal: Elliptic Curve Cryptography in Cloud Security: A Survey. (2022).
7. Vidhya, K., Nagarajan, B., Aisvarya, S., Anuprabha, K., Ashley, R.: Enhanced Cloud Storage Security Using Elliptic Curve Cryptography and Entity-Based Access Control. AIP Conference Proceedings 2764(1), 60011 (2023).
8. Kumar, Pawan, Bhatt, Ashutosh Kumar: Enhancing Multi-tenancy Security in the Cloud Computing Using Hybrid ECC-based Data Encryption Approach. IET Communications 14(18), 3212–3222 (2020).
9. Gupta, Daya Sagar, Biswas, G. P.: A Secure Cloud Storage Using ECC-Based Homomorphic Encryption. Int. J. Inf. Sec. Priv. 11(3), 54–62 (2017).
10. Danisha, C., Shoba Bindu, Shaik: Secure Hybrid Encryption Using ECC in Clouds. IJARCS (), (2017).
11. Krishnaveni, N., Jayakumari, C.: A Hybrid Framework to Enhance Cloud Security for Storing and Retrieving Confidential Data in Clouds. (2016).
12. Bikshapathi, D., Chethana, A., Reddy, E. Madhusudhan, Kumar, K., Babu, M. Chandra: Performance of Evaluation for AES with ECC in Cloud Environment. (2016).
13. Shivaramakrishna, D., Nagaratna, M.: A Novel Hybrid Cryptographic Framework for Secure Data Storage in Cloud Computing: Integrating AESOTP and RSA with Adaptive Key Management and Time-Limited Access Control. (2023).
14. Kashif, M., Mehfuz, S., Shkeel, I., Ahmad, S.: Employing an ECC-Based Hybrid Data Encryption Method to Improve Multitenancy Security in Cloud Computing.(2023).
15. Chen, Yijun, Liu, Hong, Wang, Bing, Sonompil, B., Ping, Y., Zhang, Z.: Threshold Hybrid Encryption Method for Integrity Audit Without Trusted Center. (2021).
16. Kaur, Supreet, Jain, Lokesh: A Hybrid Cryptographic Scheme for Improving Cloud Security Using ECC and TDES Algorithms. (2020).
17. Bhagyalakshmi, R., Roopashree, D., Shruthi, K. N.: Performance Analysis of Hybrid Cryptography System for High Security and Cloud-Based Storage. (2024).
18. Alabi, O., Thompson, A., Alese, B., Gabriel, A.: Cloud Application Security Using Hybrid Encryption. (2020).
19. Sankaran, S. P., Kirubanand, V. B.: Hybrid Cryptography Security in Public Cloud Using TwoFish and ECC Algorithm. (2023).
20. Rao, B. Ravi, Sujatha, B.: A Hybrid Elliptic Curve Cryptography (HECC) Technique for Fast Encryption of Data for Public Cloud Security. (2024).
21. Khan, Mohd, Upreti, Kamal, Alam, M., Khan, H., Siddiqui, S., Haque, M., Parashar, J.: Analysis of Elliptic Curve Cryptography & RSA. Journal of ICT Standardization 10(), (2023).
22. Christo, M. Solomon, Jesi, V., Priyadarsini, U., Anbarasu, V., Venugopal, H., Karuppiah, M.: Ensuring Improved Security in Medical Data Using ECC and Blockchain Technology with Edge Devices. Security and Communication Networks 2021(), (2021).
23. Gupta, T. Shiv, Srivastava, R.: Advanced-Data Encryption Using Three-Layered Hybrid Cryptosystem and Secured Key Storing Using Steganography. (2021).
24. Jagadeesh, S., Ali, Syed Murtuza, Selvan, S. P. Ganesh, Aljanabi, M., Gopianand, M., Hephzipah, J. P. Jasmine: Hybrid AES-Modified ECC Algorithm for Improved Data Security Over Cloud Storage. (2023).
25. Sivakumar, J., Ganapathy, S.: An Effective Data Security Mechanism for Secured Data Communications Using Hybrid Cryptographic Technique and Quantum Key Distribution. (2023).
26. Somaiya, R., Gonsai, A., Tanna, R.: Implementation and Evaluation of EMAES – A Hybrid Encryption Algorithm

for Sharing Multimedia Files with More Security and Speed. (2023).
27. Li, Xueliang, Chen, Jiayu, Qin, Danyang, Wan, Wei: Research and Realization Based on Hybrid Encryption Algorithm of Improved AES and ECC. (2010).