iJRASET
International Journal For Research in Applied Science and Engineering Technology

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 14 **Issue:** IV **Month of publication:** April 2026

**DOI:** https://doi.org/10.22214/ijraset.2026.79664

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538*
*Volume 14 Issue IV Apr 2026- Available at www.ijraset.com*

# Secure Cloud Communication Using ECC and AES Hybrid Encryption

C. Laxmana Sai[1], V. Manognan[2], D. Adithyavardhan[3], K. Avinash[4]
[1, 2, 3, 4]*Electronics and Communication Engineering, MVSR Engineering College, Hyderabad, Telangana, India*

***Abstract:*** ***Today all our stuff is on the cloud, but it still can be breached. Most of our messaging apps claim to have encryption. This system does not really know who we are, so it does not really matter what we password are; our data can still be read by any intruder who get a hand of our cloud data. We present our own system which uses a hybrid system combined using both AES and ECC on one model. When we send a message our system encrypts the message using AES, and locks the AES key using receiver's ECC public key. Our message, along with the locked AES key are then sent on the cloud; our ECC private key, which is on the receiver's computer, is never sent out. Before we can decrypt anything we still need to identify our self using maybe a fingerprint or password. But this would not only be for messaging but any type of data stored on the cloud.***
***Keywords: Advanced Encryption Standard (AES), Elliptic Curve Cryptography (ECC), Hybrid Encryption, Authentication, Cloud.***

## I. INTRODUCTION

The era of cloud communication has led to the transmission and storage of a vast amount of personal data on the cloud. To enhance the security of data stored and transferred in the cloud, most services make use of encryption methods. However, there still remain potential vulnerabilities of impersonation, man-in-the-middle attacks, and hacking. Most systems have key management which are tied to a password or directly to our device which would not be safe once the password is revealed or the phone is compromised or stolen. We present our new secure system using a hybrid AES-ECC scheme along with biometric security. We do not transfer any of our data without it being encrypted, and will only let us decrypt our data after we identify ourselves, hence making it a zero trust system where cloud will be treated as only storage space which will not be able to access our information and if it does happen to be hacked we are still guaranteed safe access to our information.

## II. EXISTING METHODS

For security of data, our system could either use symmetric encryption, like AES for large files or asymmetric encryption such as RSA or ECC for key exchange, but both have their drawback. In symmetric encryption, a huge worry is to have effective and secure management of keys, which could potentially be a point of failure. If the key were stolen by any attacker then it could be used to read all the information stored. ECC encrypts data effectively through key exchange, but it is not ideal for large storage. Conventional system uses some kind of secure key storage, or password which could again be exploited easily by attackers if found. If password are easy to forget and are prone to hacker's attacks, their misuse if stolen or if the device is stolen is even greater. Device based authentication is just not good enough. It could always be exploited by device spoofing and attackers. The data is breached only when the system gives access to unauthorized users. Password authentication could be very useful. We should aim for data that is linked with ourself.

## III. PROPOSED WORK

Our system utilizes the AES and ECC cryptographic algorithms coupled with biometric authentication to make our system secure as even if someone manages to access our device or hack the cloud their fingerprint will never be available. It consist of a sending and a receiving module. Our architecture has the encryption layer, the storage layer, the authentication layer, and the decryption layer. When sending a message, the system generates an AES key, encrypts the message with it, and then encrypts the AES key with the receiver's ECC public key. Both are sent and received, and all these goes to the cloud, the cloud cannot really access our data since it does not have our ECC private key and only our biometric will give us access to the AES key. A user can only authenticate with their biometric, via FIDO2 or WebAuthn. And a user cannot decrypt anything unless their fingerprint is confirmed.

Secure Message Transmission: When a message needs to be sent, our system extracts the message to be sent along with the receivers ID, it is vital to do so for it enables the system to send the required encrypted data to the intended user only.

A unique 256 bit AES key is generated for each message ensuring no attacker would be able to find one message and decrypt all. The message is then encrypted using AES-256-GCM, which is good for confidentiality and integrity checking. Cipher text, nonce, and integrity tag are output by the AES encryption. The AES session key used to encrypt our message is then locked using the ECC public key of the recipient. Hence we have two layer of encryption, one to lock the message with a symmetric key, and another to lock the symmetric key with the public key of our recipient. All this data (ciphertext, nonce, integrity tag, and ECC-encrypted session key) are now stored in cloud databases, like SQLite and Firebase, and our original message is never sent across the network. Upon reception the recipient can know it instantly via a real time Socket.IO message notification.

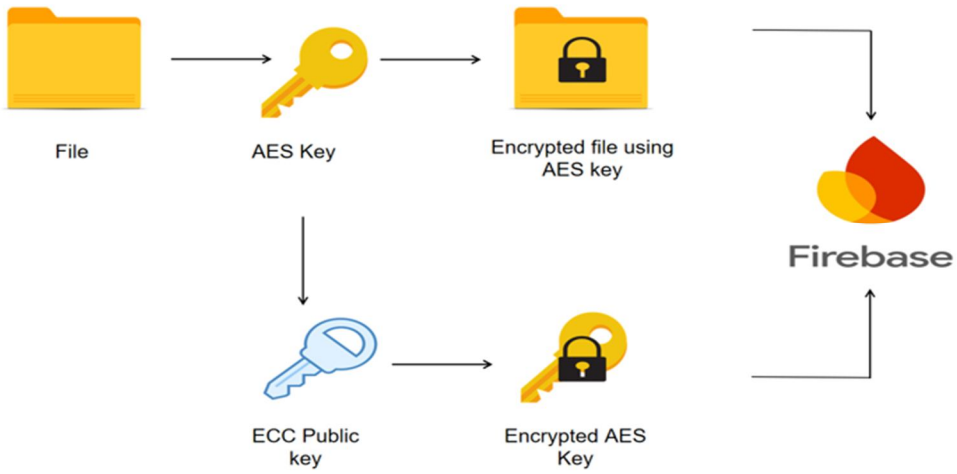



Fig. 1 Secure Message Transmission.

Secure Message Decryption: The data is to be decrypted once the receiver chooses to see the message; it prompts them for authentication, which is done by our biometric system (either through fingerprint using WebAuthn or FIDO2), only after successful authentication from the biometric system will the server trigger local decryption using our ECC private key. Since the key storage is on the client device, it will be used by our ECC private key to unlock our ECC-encrypted AES session key. Once we obtain our AES session key, we decrypt our ciphertext using the nonce and integrity tag that we obtained initially along with the ciphertext and checks for integrity. The decrypted text would then be available to us; this has achieved our goals; our data is secured and its integrity is ensured and could also be used for storage purpose in the cloud instead of messages.

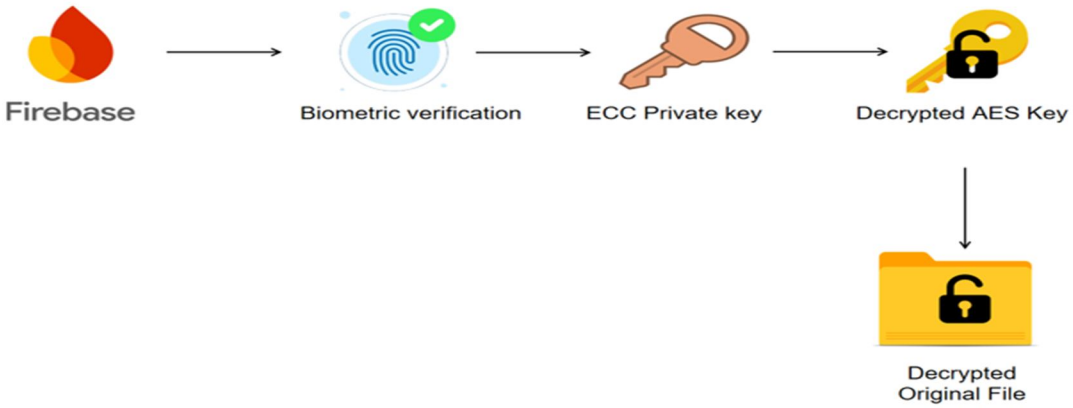



Fig. 2 Secure Message Decryption.

## IV. EXPERIMENTAL RESULTS

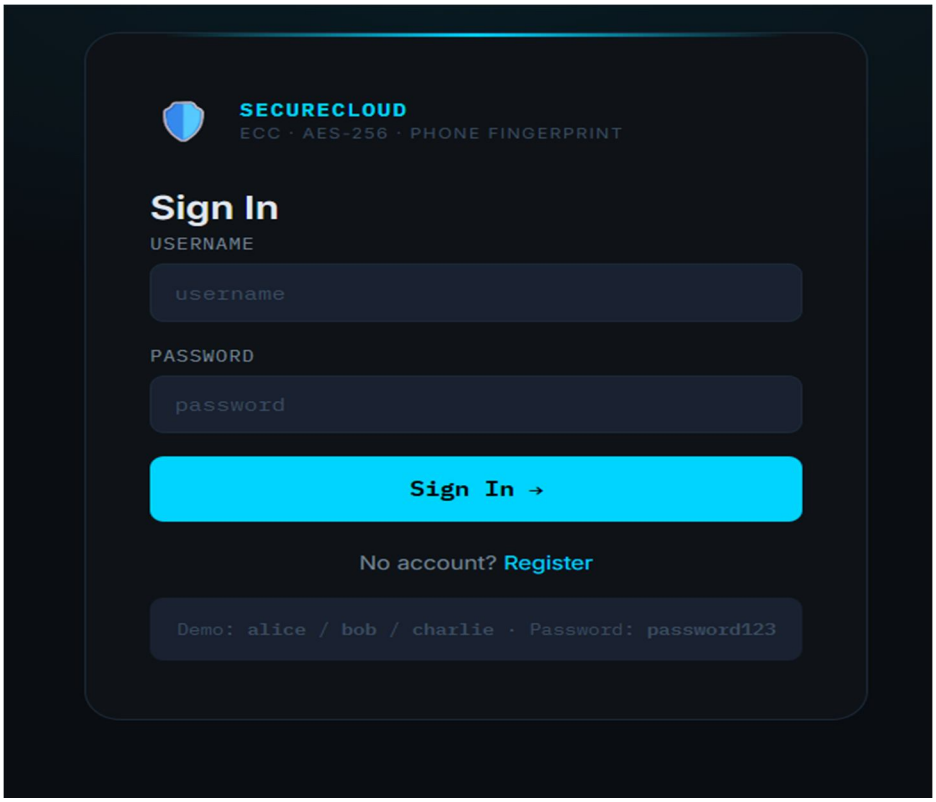



Fig. 3 Candidate Signin Page.

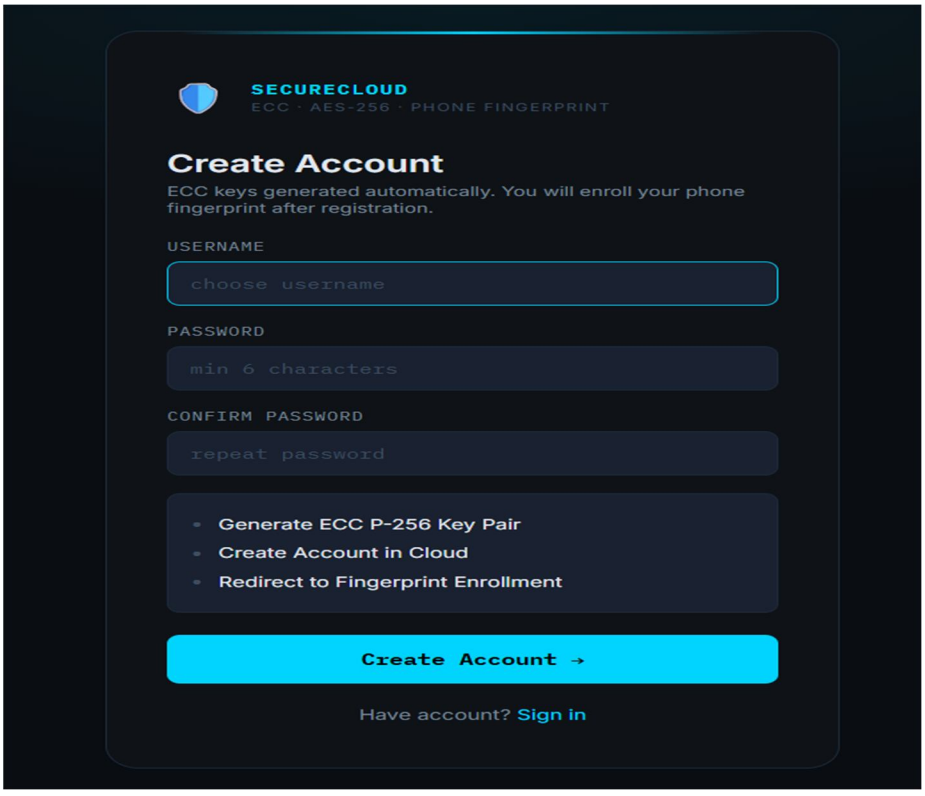



Fig.4 Candidate Registration Page.

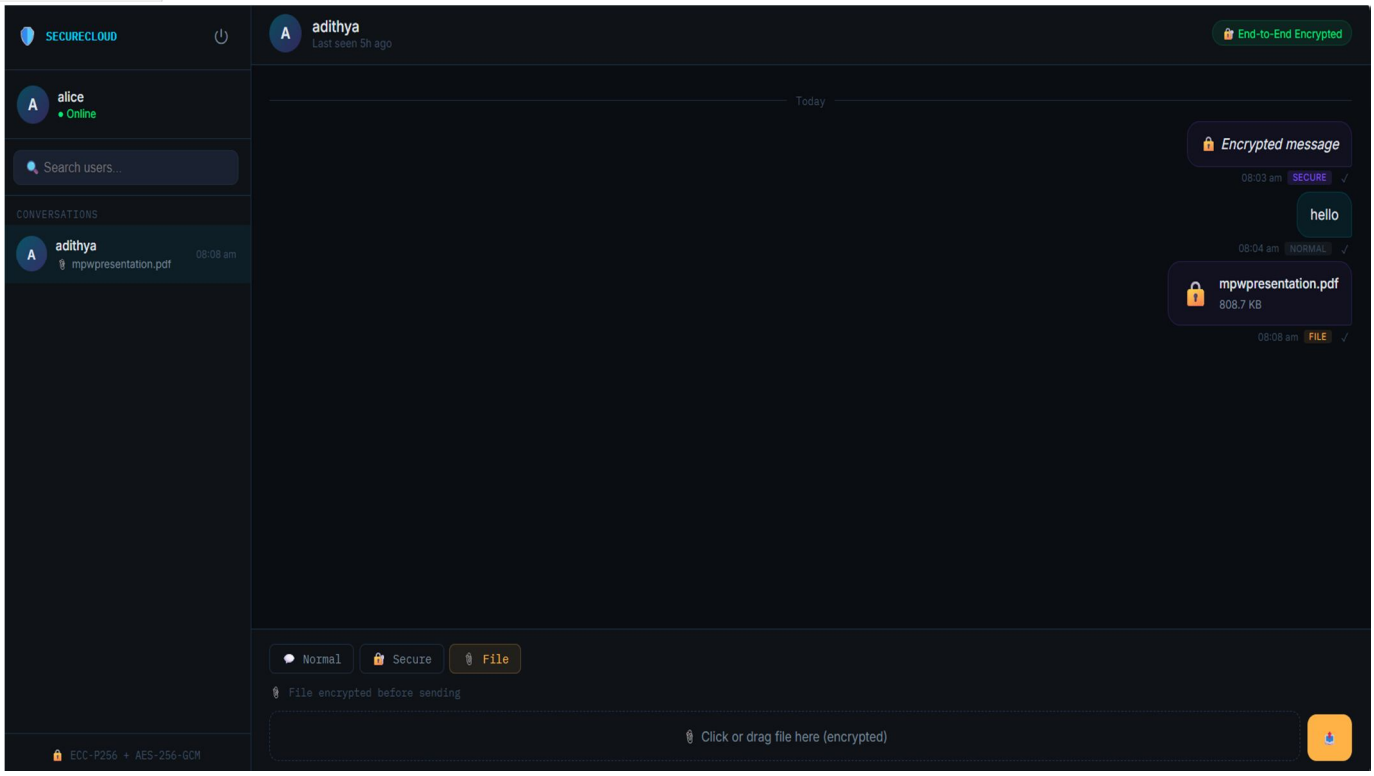



Fig. 5 Message Transmission at Sender's end.

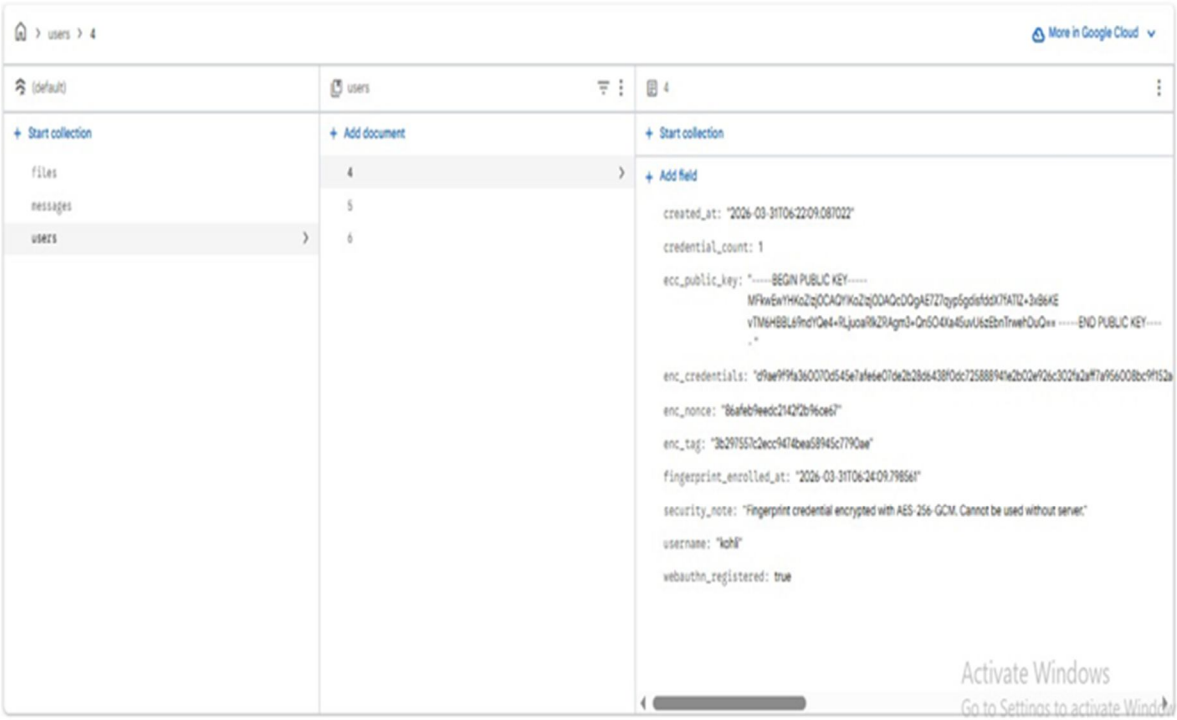



Fig. 6 User's Encrypted Credentials in cloud.

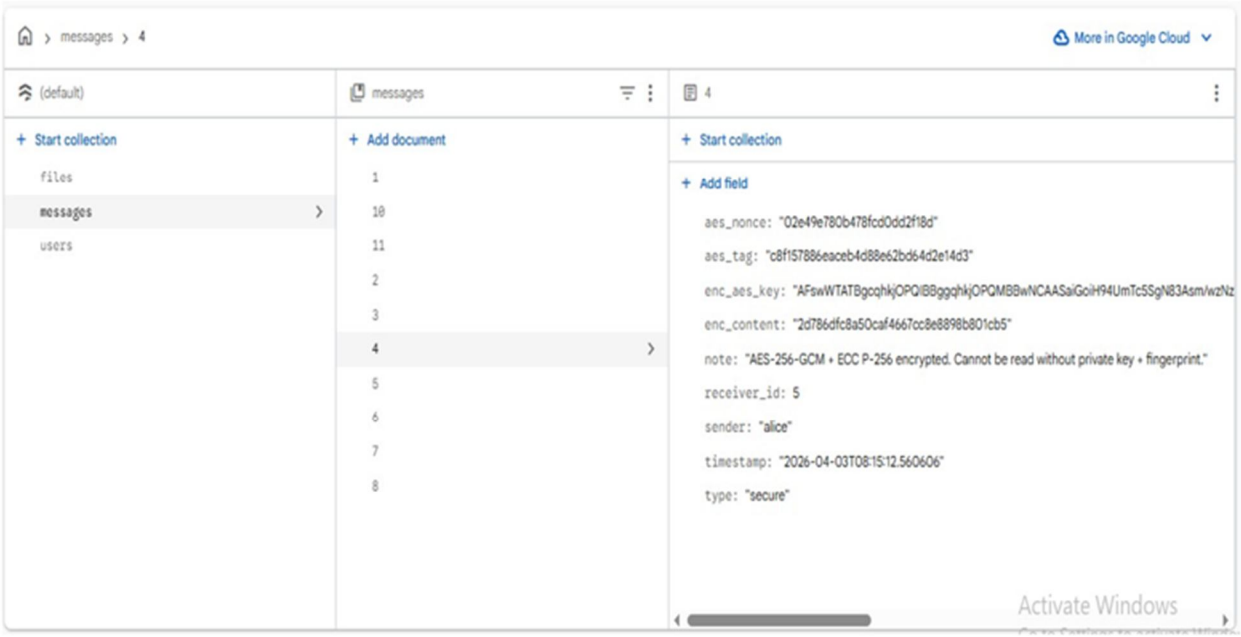



Fig. 7 User's Encrypted Messages and Files Stored in Cloud.

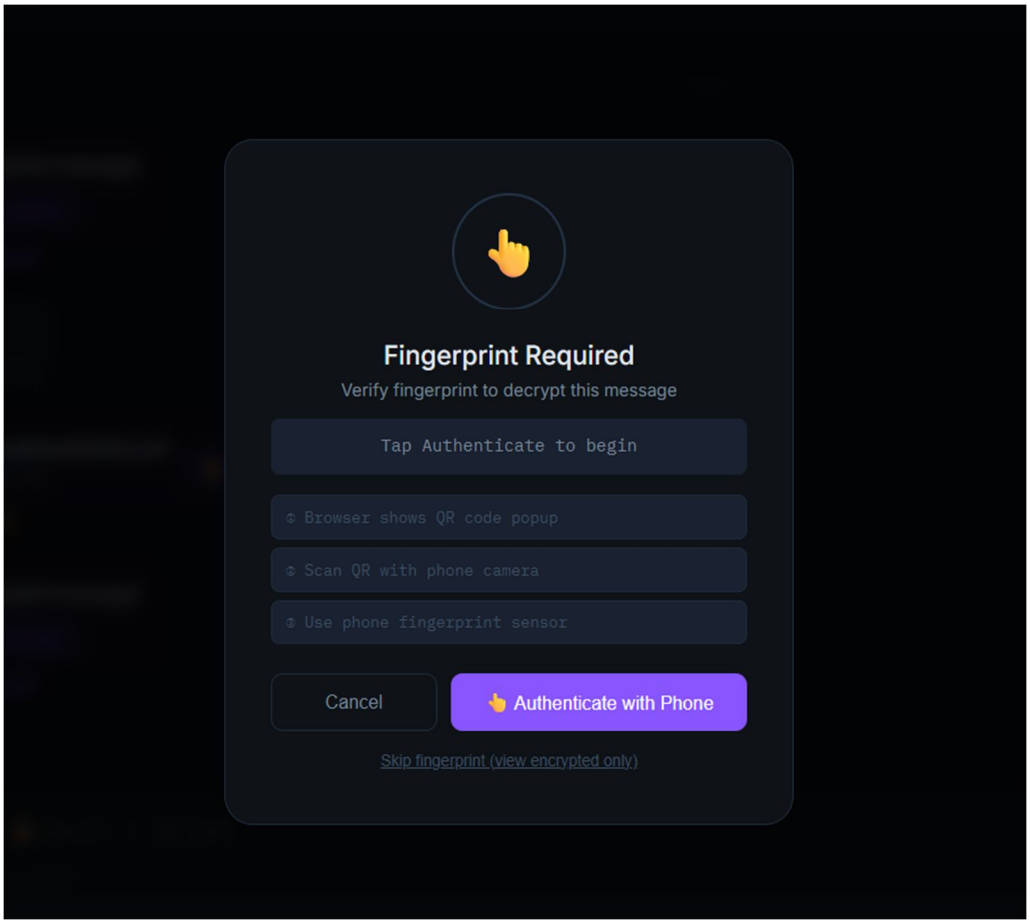



Fig. 8 Receiver's Fingerprint Authentication.

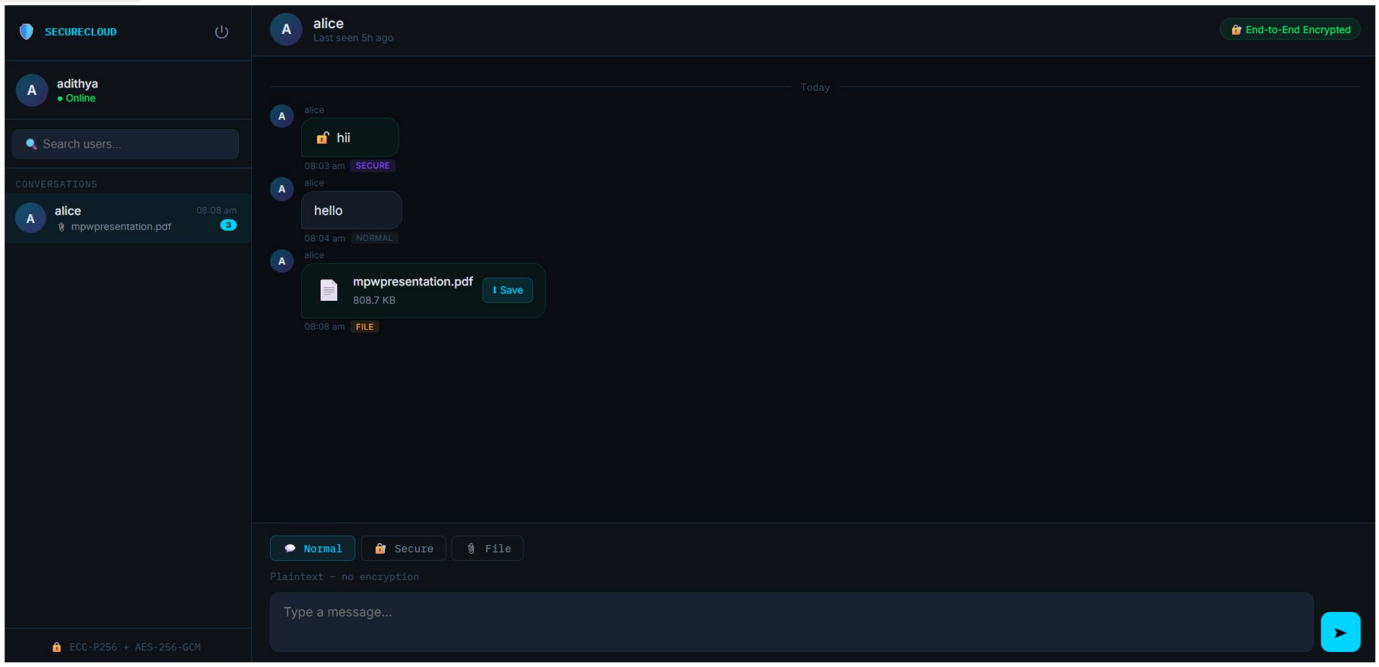



Fig. 9 Secure Message Decryption at Receiver's end.

## V. CONCLUSION

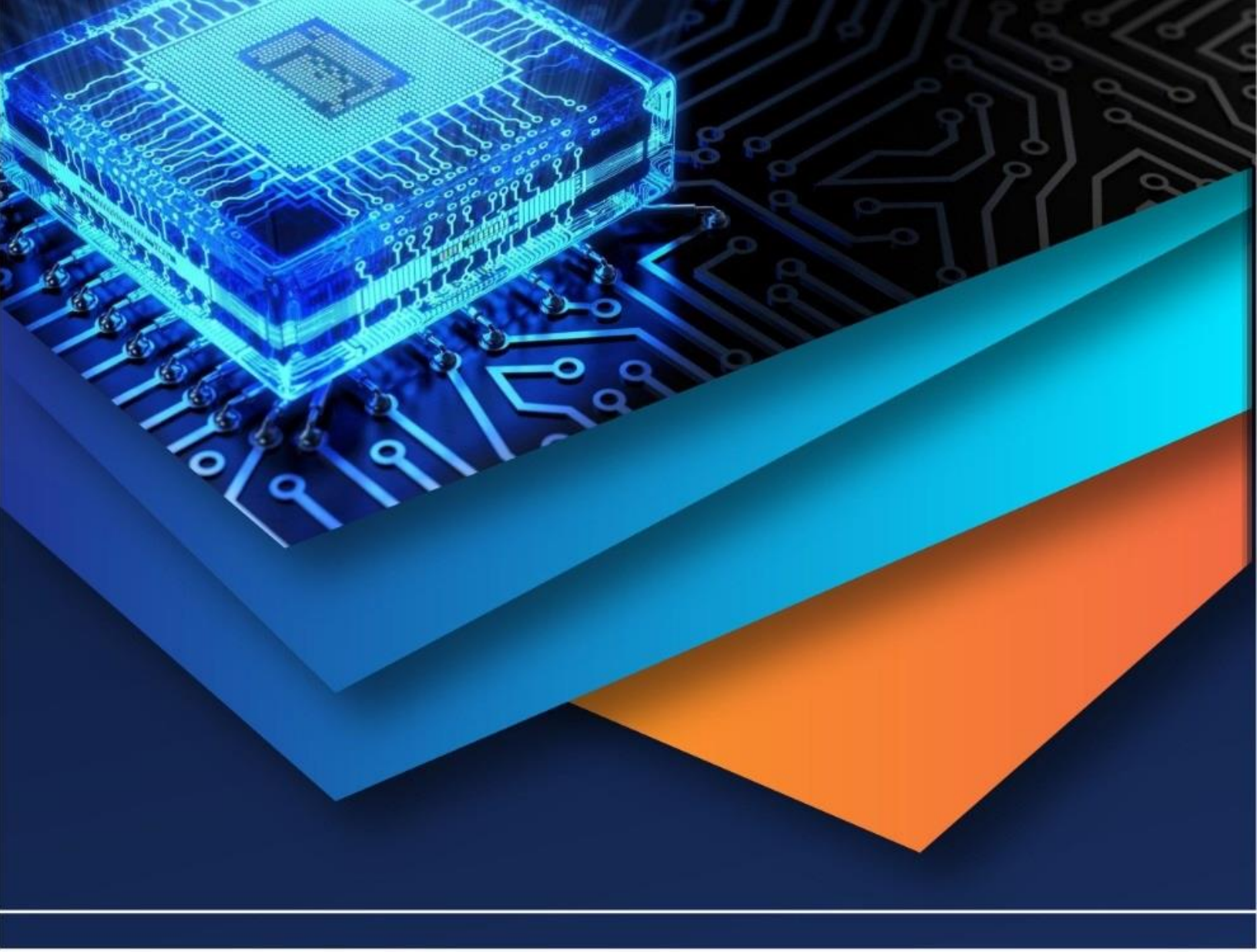
The Proposed Secure Cloud Communication using Hybrid encryption techniques and biometric based authentication addresses critical lapses in traditional approaches. By combining AES-256-GCM, ECC, and biometric identity validation under zero trust model on cloud, the system ensures confidentiality, integrity, and even in the times of cloud breaches unauthorized users cannot access plain text data. The architecture is suitable for secure cloud communication and storage protection.

## REFERENCES

[1] Y. M. A. Abualkas and D. L. Bhaskari, "Hybrid Approach to Cloud Storage Security Using ECC-AES Encryption and Key Management Techniques," International Journal of Engineering Trends and Technology (IJETT), vol. 72, no. 4, pp. 92–100, Apr. 2024

[2] A. A. Abd-Aljabbar, D. A. Hammood, and L. H. Abed, "Secure Cloud Storage Using Multi-Modal Biometric Cryptosystem: A Deep Learning-Based Key Binding Approach," Journal of Al-Qadisiyah for Computer Science and Mathematics, vol. 17, no. 1, pp. Comp 214–229, Mar. 2025.

[3] M. Manimozhi and R. K. Mugelan, "Post-Quantum AES Encryption Using ECC Points Derived from BB84 Sifted Keys," EPJ Quantum Technology, vol. 12, art. 109, 2025.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY