Revolutionizing Cloud Security with Elliptic Curve Cryptography

L.Pratyusha[1], Naredla Mukesh Chand[2], Rokkala Sheena[3], Vurigiti Laxmi Manasa[4], Kotta Kali Charan[5]
[12345] *Department of Computer Science & Engineering,*
Avanthi Institute of Engineering and Technology

Abstract: **Current cloud storage systems do not provide strong end-to-end encryption or secure authentication. Because of this, sensitive data is at risk of unauthorized access, data modification (tampering), and cyberattacks. Most existing systems depend on centralized security controls, which can become single points of failure and do not guarantee confidentiality, integrity, and authenticity at the same time.**

This project presents a secure cloud vault system that uses modern cryptographic techniques such as Elliptic Curve Cryptography (ECC), ECDSA, ECIES, and ECDH. The system ensures strong data encryption, secure digital signatures, safe key exchange, and protection of data during storage and transmission. The proposed system improves security, performance, and efficiency in cloud environments

Index Terms: **Cybersecurity, ECC, ECDSA, ECIES, AES-256, Cloud Security**

I. INTRODUCTION

With the rapid growth of cloud computing and online communication, secure data storage and transmission have become essential. Cyber threats such as data breaches, identity theft, and unauthorized access are increasing.

Traditional encryption methods like RSA require large key sizes and higher computational power. Elliptic Curve Cryptography (ECC) offers stronger security with smaller keys and better performance.

This project is motivated by the need to develop a secure, efficient, and modern cryptographic system that ensures confidentiality, integrity, and authenticity using ECC-based encryption and digital signatures

II. LITERATURE REVIEW

Paper 1: Elliptic Curve Cryptography for Secure Communication explains ECC fundamentals and highlights its performance and security advantages over traditional encryption.

Paper 2: Secure File Sharing using Public Key Cryptography discusses secure file transfer using encryption and digital signatures but notes performance limitations of traditional algorithms.

Paper 3: Modern Cloud Security using ECC and AES shows that combining ECC for key exchange with AES for encryption ensures strong security and better performance.

III. PROBLEM STATEMENT

Current cloud storage and file-sharing systems have several drawbacks. Most of these systems rely on traditional encryption techniques such as RSA, which require large key sizes and result in higher computational cost and slower performance. In addition, these systems do not provide an integrated approach that combines encryption, digital signatures, and secure key exchange. As a result, they are often vulnerable to unauthorized access and data tampering. Furthermore, many existing solutions lack strong authentication mechanisms and proper cryptographic verification. Another major limitation is their poor scalability and efficiency in handling modern cloud requirements. Therefore, existing systems are considered less secure and less efficient for current cloud environments.

IV. PROPOSED SYSTEM

Cipher Vault is a secure cloud vault system based on Elliptic Curve Cryptography. The system is designed to provide strong security features while maintaining efficiency and performance. It includes automatic ECC key generation, secure file encryption using ECIES and AES-256-GCM, and digital signature

generation using ECDSA. Secure key exchange is achieved through the ECDH protocol, while SHA-256 is used to ensure data integrity.

The system also provides secure authentication and encrypted communication between users. By integrating all these features into a single system, Cipher Vault ensures confidentiality, integrity, and authenticity of data in cloud environments

V. SYSTEM ARCHITECTURE

Cipher Vault follows a layered architecture to ensure secure and efficient cloud communication. The overall data flow begins with user registration or login, followed by ECC key generation. The data is then encrypted and securely transmitted to storage. On the receiver side, the data is decrypted using the private key, and the digital signature is verified to ensure authenticity and integrity. This structured flow ensures that data remains secure throughout its lifecycle

VI.METHODOLOGY

The development of the system is carried out in multiple phases. Initially, requirement analysis is performed to identify security needs and study ECC techniques. This is followed by system design, where the architecture and security modules are defined. During the development phase, encryption, digital signatures, and secure file transfer mechanisms are implemented. Testing is conducted to validate encryption, decryption, and signature verification processes. Finally, the system is deployed and evaluated for security and performance.

VII. IMPLEMENTATION

The system is implemented as a web application using modern technologies. The frontend is developed using HTML, CSS, and JavaScript to provide a user-friendly interface. The backend is built using Python with the Flask framework. Cryptographic operations are implemented using the Python Cryptography Library, including ECC with the SECP256R1 curve, AES-256-GCM for encryption, and ECDSA and ECDH for security operations.

The system uses in-memory storage with a mailbox structure to manage data, and development tools such as VS Code and Git are used for coding and version control.

VIII. MODULES

The system is divided into several functional modules. The user authentication module manages registration, login, and secure session handling. The key generation module creates ECC public and private keys automatically. The encryption module secures files using ECIES and AES-256-GCM, while the decryption module allows secure retrieval of data. The digital signature module ensures data authenticity using ECDSA, and the secure communication module handles encrypted data transfer between users.

IX. TESTING

The system is tested using multiple testing techniques to ensure reliability and security. Unit testing is performed to verify individual modules, while integration testing ensures proper interaction between components. Encryption and decryption testing validate secure data transformation, and signature verification testing confirms data authenticity and integrity. System testing evaluates the overall performance and security of the application.

X. RESULTS

The developed system successfully implements a secure cloud vault solution. It achieves secure file encryption and decryption, verifies digital signatures effectively, and establishes secure communication between users. The use of ECC ensures high performance and efficient encryption compared to traditional methods.

XI. APPLICATIONS

The proposed system can be applied in various domains requiring secure data handling. It is suitable for secure cloud storage, encrypted file sharing, and confidential communication systems. It can also be used for enterprise data protection, as well as in government, military, banking, and financial sectors where high-level security is essential.

XII. LIMITATIONS

The current system uses in-memory storage and does not include persistent database integration. It requires an active internet connection for operation and has limited scalability without distributed deployment.

XIII. FUTURE WORK

Future improvements include integrating cloud-based databases such as MySQL or MongoDB, enhancing scalability through distributed architecture, and developing mobile applications for Android and iOS platforms. Advanced security features such as blockchain integration and AI-based threat detection can also be incorporated.

XIV. CONCLUSION

Cipher Vault successfully implements a secure cloud vault system using Elliptic Curve Cryptography. The system enables secure file encryption, digital signature verification, and protected communication between users. ECC provides strong security with smaller key sizes and improved performance compared to traditional encryption methods. Overall, the system ensures confidentiality, integrity, and authenticity, making it suitable for modern secure cloud applications.

REFERENCES

[1] W. Stallings, Cryptography and Network Security, 2020.
[2] N. Koblitz, Elliptic Curve Cryptography.
[3] Hankerson et al., Guide to ECC.
[4] Liu et al., ECC for Cloud Computing.