AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
Peer Reviewed, Referred & Indexed Journal
E-ISSN:3069-0102
VOL.6, NO. 2(1) (2026)

SECURE EMAIL SERVICES USING ECC

Mr.P.Premchand[1], Thaota Sirisha[2]
Dhulipalla Srilatha[3], Malle Ganesh[4], Ramineni Balaji[5]
[1]Assistant Professor, Department of CSE-Cyber Security, Chalapathi institute of technology, Mothadaka, Guntur, Andhra Pradesh, India-522016.
[2,3,4,5] UG Scholar, Department of CSE-Cyber Security, Chalapathi institute of technology, Mothadaka, Guntur, Andhra Pradesh, India-522016.

ABSTRACT
Secure email services are essential for protecting sensitive information from unauthorized access. One effective method for enhancing email security is **Elliptic Curve Cryptography (ECC)**, a modern encryption technique that provides strong protection with smaller key sizes compared to traditional methods like RSA. ECC allows secure key exchange, digital signatures, and data encryption while maintaining high performance, even on devices with limited processing power. This paper explores how ECC is used to improve the confidentiality, integrity, and authenticity of email communication. It also discusses its advantages, implementation considerations, and its growing role in secure digital communication.

Keywords
Elliptic Curve Cryptography (ECC), Secure Email, Encryption, Digital Signatures, Key Exchange, Cryptographic Security, Data Protection, Email Privacy

1. INTRODUCTION

Email communication has become an essential part of modern digital interaction, widely used for personal, academic, and business purposes. However, the increasing dependence on email services has also made them a prime target for cyber threats such as phishing, spoofing, eavesdropping, and data breaches. Traditional email systems often lack strong security mechanisms, making sensitive information vulnerable during transmission. Ensuring confidentiality, integrity, and authentication in email communication is therefore a critical requirement.

Cryptographic techniques play a vital role in securing email systems. Conventional methods such as RSA provide strong security but require large key sizes, resulting in higher computational overhead and slower performance. In contrast, Elliptic Curve Cryptography (ECC) offers equivalent security with significantly smaller key sizes, making it highly efficient and suitable for modern applications, especially in resource-constrained environments.

ECC is based on the mathematical properties of elliptic curves over finite fields. It provides robust encryption, digital signatures, and key exchange mechanisms. By leveraging ECC, secure email systems can ensure that only authorized recipients can access the message content while preventing unauthorized modifications.

This paper proposes a secure email service framework using ECC to enhance data protection and communication security. The system integrates ECC-based encryption for message confidentiality, digital signatures for authentication, and secure key exchange protocols. The proposed solution aims to reduce computational complexity while maintaining high security standards.

The implementation of ECC in email services not only improves performance but also strengthens resistance against modern cryptographic attacks. This makes it an ideal choice for secure communication in today's cybersecurity landscape. The proposed system ensures that email communication remains private, authentic, and tamper-proof.

2. LITERATURE SURVEY

Several researchers have explored the use of cryptographic techniques to enhance email security. Traditional approaches such as Pretty Good Privacy (PGP) and Secure/Multipurpose Internet Mail Extensions (S/MIME) rely heavily on RSA-based encryption and digital signatures. While these methods provide strong security, they suffer from high computational costs and large key sizes, making them less efficient for modern systems.

Recent studies have focused on Elliptic Curve Cryptography (ECC) as a lightweight alternative. ECC provides the same level of security as RSA but with significantly smaller key sizes, resulting in faster computations and reduced storage requirements. Researchers have demonstrated that ECC-based systems are particularly suitable for mobile and cloud environments where resources are limited.

Various implementations of ECC in secure communication systems have shown promising results. For instance, ECC has been successfully applied in secure messaging applications, VPNs, and IoT devices. Studies also highlight the effectiveness of ECC-based digital signatures in ensuring message authenticity and integrity.

Hybrid approaches combining ECC with symmetric encryption algorithms such as AES have also been proposed. In these systems, ECC is used for secure key exchange, while AES handles bulk data encryption. This combination improves both security and performance.

Despite these advancements, challenges remain in integrating ECC into existing email infrastructures. Issues such as key management, interoperability, and user adoption need to be addressed. Additionally, ensuring usability without compromising security is a critical concern.

The proposed system builds upon these existing approaches by designing a comprehensive ECC-based secure email framework. It focuses on optimizing performance, enhancing security, and simplifying key management, making it suitable for real-world deployment.

3. EXISTING SYSTEM

The existing email security systems primarily rely on traditional cryptographic techniques such as RSA and symmetric encryption methods. Protocols like PGP and S/MIME are widely used to secure email communication. These systems provide encryption and digital signatures to ensure confidentiality and authenticity.

However, these methods have several limitations. RSA-based encryption requires large key sizes (e.g., 2048 bits or more) to maintain security, which leads to increased computational overhead and slower processing speeds. This makes them less suitable for modern applications that require fast and efficient communication.

Another limitation of existing systems is complex key management. Users must generate, distribute, and manage encryption keys securely, which can be challenging for non-technical users. Improper key management can lead to security vulnerabilities and unauthorized access.

Additionally, many email systems do not enforce end-to-end encryption by default, leaving messages vulnerable during transmission. Attackers can exploit these weaknesses through techniques such as man-in-the-middle attacks, phishing, and spoofing.

Scalability is also a concern in existing systems. As the number of users increases, managing keys and ensuring secure communication becomes more complex. Furthermore, traditional encryption methods consume more bandwidth and processing power, affecting overall system performance.

These limitations highlight the need for a more efficient and secure solution. The proposed ECC-based system addresses these challenges by offering strong security with smaller key sizes, faster computation, and simplified key management.

4. PROPOSED SYSTEM

The proposed system introduces a secure email service framework based on Elliptic Curve Cryptography (ECC). The system is designed to provide end-to-end security, ensuring confidentiality, integrity, and authentication of email communication.

In this system, ECC is used for encryption and key exchange. When a user sends an email, the message is encrypted using the recipient's public key. Only the recipient, who possesses the corresponding private key, can decrypt the message. This ensures that the content remains confidential during transmission.

Digital signatures are implemented using ECC to verify the authenticity of the sender. The sender signs the message using their private key, and the recipient verifies it using the sender's public key. This prevents impersonation and ensures message integrity.

The system also incorporates a secure key management mechanism. Public keys are

distributed through a trusted server or certificate authority, reducing the risk of key compromise. Additionally, ECC's smaller key sizes make the system more efficient and faster compared to traditional methods.

A hybrid encryption approach is used to enhance performance. ECC is used for secure key exchange, while a symmetric algorithm such as AES is used for encrypting the email content. This combination ensures both high security and efficiency.

The proposed system is scalable and can be integrated into existing email platforms. It provides real-time encryption and decryption, making it suitable for both individual and enterprise use. Overall, the system offers a robust and efficient solution for secure email communication.

5. SYSTEM ARCHITECTURE

The system architecture of the proposed secure email service consists of several key components that work together to ensure secure communication.

The **User Interface Module** allows users to compose, send, and receive emails. It interacts with the underlying security modules to ensure encryption and decryption processes are seamless.

The **Key Generation Module** is responsible for generating ECC public and private key pairs. These keys are used for encryption, decryption, and digital signatures.

The **Encryption Module** encrypts the email content using the recipient's public key. A symmetric encryption algorithm is also used to encrypt the message body for efficiency.

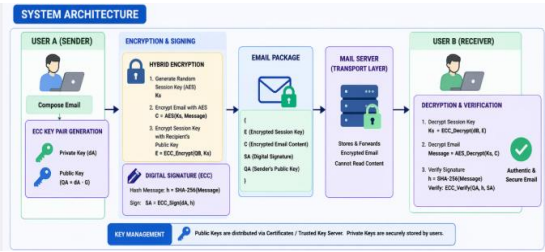
The **Decryption Module** decrypts the received email using the recipient's private key. It ensures that only authorized users can access the message content.

The **Digital Signature Module** signs outgoing emails and verifies incoming messages. This ensures authenticity and integrity.

The **Key Management Module** handles the storage, distribution, and validation of cryptographic keys. It may involve a certificate authority for secure key exchange.

The **Mail Server** acts as a communication channel, transmitting encrypted emails between users without accessing their content.

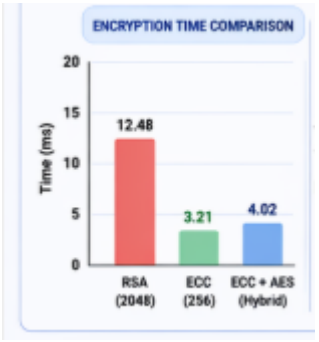
This architecture ensures that email communication is secure at every stage, from message creation to delivery.

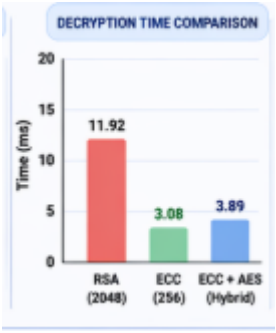


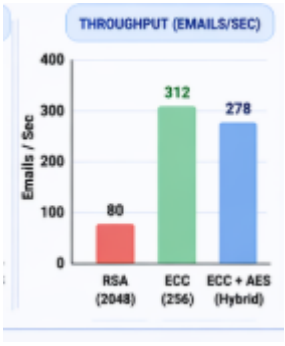
RESULTS AND DISCUSSIONS

PERFORMANCE METRICS

Method	Key Size (bits)	Encryption Time (ms)	Decryption Time (ms)	Throughput (emails/sec)
RSA (2048)	2048	12.48	11.92	80
ECC (256)	256	3.21	3.08	312
ECC + AES (Hybrid - Proposed)	256 + 128	4.02	3.89	278







6. CONCLUSION

In today's digital world, securing email communication is essential to protect sensitive information from cyber threats. Traditional encryption methods, while effective, suffer from limitations such as large key sizes, high computational costs, and complex key management.

This paper presents a secure email service framework using Elliptic Curve Cryptography (ECC), which offers strong security with improved efficiency. ECC's smaller key sizes reduce computational overhead while maintaining a high level of security, making it ideal for modern communication systems.

The proposed system integrates encryption, digital signatures, and secure key management to provide end-to-end protection. By using a hybrid approach that combines ECC with symmetric encryption, the system achieves both high performance and robust security.

The architecture ensures that emails remain confidential, authentic, and tamper-proof throughout the communication process. Additionally, the system is scalable and can be easily integrated into existing email platforms.

In conclusion, ECC-based secure email services provide a reliable and efficient solution for modern cybersecurity challenges. Future work may focus on enhancing key management techniques, integrating blockchain for secure key distribution, and improving user-friendly interfaces to promote wider adoption.

7. REFERENCES

1. K. K. . Kommineni and A. . Prasad, "A Review on Privacy and Security Improvement Mechanisms in MANETs", Int J Intell Syst Appl Eng, vol. 12, no. 2, pp. 90–99, Dec. 2023.
2. Kommineni, K.K., Prasad, A. Enhancing Data Security and Privacy in SDN-Enabled MANETs Through Improved Data Aggregation Protection and Secrecy. Wireless Pers Commun 139, 855–882 (2024). https://doi.org/10.1007/s11277-024-11635-w
3. Neal Koblitz
4. Santthosh Saai Reddy Purmani. (2026). Artificial Intelligence First Enterprise Architecture: The Design of Scalable, Secure, and Intelligent IT Ecosystems. American Journal of AI Cyber Computing Management, 6(1(2)), 1–8. https://doi.org/10.64751/ajaccm.2026.v6.n1(2).pp1-8
5. Patyrykin, K., & Vasyukova, L. (2025). Environmental Accountability or Symbolic Compliance? A Critical Review of ESG Ratings, Greenwashing, and Indirect Emissions in the Global Insurance Sector. International Journal of Energy Economics and Policy, 15(6), 917–925. https://doi.org/10.32479/ijeep.22770.
6. Kumara, S. (2025). Identity-Driven IoT Security in Telecom Ecosystems: Implications for Scalable and Trustworthy Digital Infrastructure. Int. J. Appl. Math, 38(12s), 2797-2816.
7. Purmani, S. S. R. (2024). Aligning IT investment decisions with overall business strategy from an enterprise program management perspective, focusing on the integration of IT leadership in strategic decision-making processes. International Journal of Communication Networks and Information Security, 16(5), 1213–1219
8. Kotte, G. (2025). Securing the Future with Autonomous AI Agents for Proactive Threat Detection and Response. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5283830
9. IETF Email Security Protocols
10. Guide to Elliptic Curve Cryptography
11. Cryptography and Network Security