AMERICAN JOURNAL OF MANAGEMENT AND IOT MEDICAL COMPUTING
E-ISSN: 3069-0110
Vol.3, No. 2(2024)
www.ajmimc.com

Secure Email Transmission through ECC Encryption

[1] MRS. DEEPTHI REPALLE, [2] P. KEERTHI, [3] K. SRIHITHA , [4] Y. MERCY RANI

[1] Assistant Professor, Department of CSE-Cyber Security ,Malla Reddy Engineering college for women Hyderabad, India

[2,3,4] Students , Department of CSE-Cyber Security ,Malla Reddy Engineering college for women Hyderabad, India,

[2] Email: palamkeerthi9@gmail.com , [3] Email:srihthakoya211@gmail.com , [4] Email :mercyrani75@gmail.com

***Abstract*— In the current digital landscape, email continues to be one of the most prevalent and convenient methods for both professional use and personal use. Nevertheless, as technology advances, so do potential risks. Conventional email systems frequently find it challenging to safeguard users against security threats such as phishing, unauthorized access, and data breaches. To tackle these challenges, this project introduces a Secure Email Service employing Elliptic Curve Cryptography (ECC)—a contemporary and effective encryption method that guarantees the privacy, integrity, and authenticity of messages.**

ECC offers robust security with significantly smaller size key compared to RSA. This leads to increased speed, reduced storage requirements, and greater energy efficiency without sacrificing safety. In the proposed framework, ECC is utilized for the generation of keys, as well as the encryption and decryption of both emails and attachments, ensuring that only the designated recipient can access the message. Additional features such as digital signatures and email expiry are incorporated to provide users with enhanced control and security over their data.

Ultimately, this system aspires to develop a secure, efficient, and trustworthy email platform that leverages modern cryptography to safeguard sensitive communications. It underscores how advanced technologies like ECC can contribute to creating a more secure and privacy-centric digital space for future interactions.

Keywords— (Elliptic Curve Cryptography (ECC), Secure Email Communication, Data Encoding and Decoding, Digital Signature Authentication, Protection of Privacy)

I. INTRODUCTION

Email has become one of the most important and commonly used methods of communication in both people's lives and business, over the years. However, ordinary email systems are often lacking in providing strong security features, which makes them vulnerable to risks such as phishing, data interception, spoofing, and unauthorized access. As more and more sensitive information is sent via email every day, it is indispensable to encrypt the messages so that they remain private, authentic and tamper-proof.

To eliminate these vulnerabilities, they resort to cryptographic methods to shield their communication. Among the most efficient and up-to-date methods is Elliptic Curve Cryptography (ECC). ECC offers the same level of security as a traditional encryption method such as RSA but requires a much smaller key size. The smaller keys make the process of encryption and decryption faster, less bandwidth is used and the energy consumption is also lower. Therefore, ECC is the best choice for a secure communication system that needs to be both fast and data protection to be at a high level.

This proposal aims to construct an Email Service that is Secure with the help of ECC to achieve total end-to-end encryption as well as digital verification. The mechanism is the one that ensures a particular recipient (or recipients) only can read the email content, and the identity of the sender can be confirmed via digital signatures. By adopting ECC to email communication, the resultant system retains the privacy of the communication, makes sure the information is not altered, and strengthens the shield against cyber-attacks. In the end, it is a secure, fast, and scalable way to solve the problem of protection in electronic communication in today's digital world.

Securing our online communication has become more necessary than ever in today's digital world. As email is the major route through which people share their data, it is frequently the focus of hackers who intend to take or alter sensitive information. The old-style encryptions hardly manage to give a strong security with a good performance at the same time. Elliptic Curve Cryptography (ECC) changes the game by providing highly secure communication with smaller keys and quicker processing. The introduction of ECC in email servers is a great support to the security of the communication as it ensures confidentiality, thus, the sender's authentication and the prevention of eavesdropping, which is, in fact, a safe way to trust in technology.

II. Literature Survey

Email is one of the most widely used forms of digital communication, but it is inherently vulnerable to threats such as eavesdropping, phishing, message tampering, and identity theft. To address these challenges, cryptographic techniques are used to ensure confidentiality, integrity, and authentication. Among these, Elliptic Curve Cryptography (ECC) has emerged as a promising method due to its efficiency, strong security, and suitability for resource-constrained devices.

Early Work on ECC:

Koblitz (1987) and Miller (1985) were pioneers in introducing ECC as a public-key cryptography technique. They demonstrated that elliptic curves over finite fields could be effectively used for

Received: 02-01-2024 | Accepted: 17-02-2024 | Published: 24-02-2024 |

secure key exchange and encryption. Their studies showed that ECC provides security comparable to RSA while using much smaller key sizes, resulting in faster encryption and decryption, reduced storage requirements, and lower computational load. This efficiency laid the foundation for using ECC in secure email communication.

Lightweight Cryptography:

William Stallings (2014) analyzed ECC as a lightweight encryption system suitable for devices with limited processing power and memory. He highlighted ECC's advantages in generating digital signatures and managing keys securely. Stallings noted that smaller key sizes reduce both computational effort and memory requirements, making ECC highly efficient for modern secure email systems, particularly on mobile devices and embedded systems.

ECC with Hash Functions:

Patil et al. (2017) proposed a secure email framework integrating ECC with the SHA-256 hashing algorithm. In their system, ECC managed key generation and encryption, while SHA-256 ensured message integrity. Their experiments demonstrated faster encryption, smaller key sizes, and efficient performance compared to RSA-based systems, confirming ECC's suitability for secure email communication.

Hybrid Encryption Approaches:

Agarwal and Singh (2019) designed a hybrid encryption model that combines ECC for key exchange with AES for message encryption. This hybrid model leverages ECC's efficient key management and AES's fast symmetric encryption, enhancing both security and system performance. The study showed reduced encryption time, lower computational overhead, and improved protection against unauthorized access.

ECC for Digital Signatures:

Kaur et al. (2021) implemented an ECC-based digital signature system for verifying email authenticity and integrity. Compared to RSA and DSA, ECC provided stronger security, faster processing, and lower resource usage. The study concluded that ECC is particularly suited for mobile and lightweight email applications, ensuring robust email security with minimal system overhead.

Secure Email Protocols and Session Keys:

Zhang et al. (2020) proposed an ECC-based email protocol featuring mutual authentication and dynamic session key generation. This protocol prevents threats such as man-in-the-middle attacks, replay attacks, and eavesdropping, providing end-to-end security for email communication on mobile and IoT devices.

ECC with Digital Certificates:

Li and Wang (2018) explored the combination of ECC and digital certificates for email encryption. ECC was used for key exchange, while AES encrypted the message content. The approach ensured high confidentiality, integrity, and reduced computational cost, making it suitable for cloud-based email systems where bandwidth and processing efficiency are critical.

Integration with IoT and Cloud Systems:

Recent research emphasizes ECC's role in IoT and cloud email platforms. Traditional algorithms like RSA are often too resource-intensive for such environments. ECC, with its smaller key sizes and high efficiency, enables fast, secure, and scalable email services suitable for distributed systems and resource-constrained devices.

Future Trends: Post-Quantum Security:

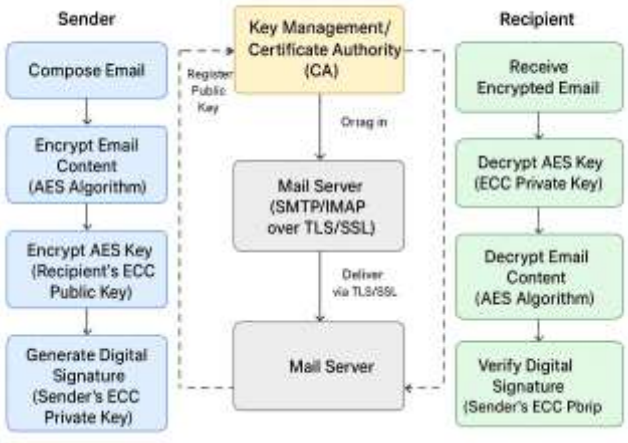
While ECC is currently secure and efficient, researchers are exploring its integration with post-quantum cryptography to protect against future quantum attacks. Hybrid models combining ECC with quantum-resistant algorithms aim to maintain ECC's efficiency while ensuring security against emerging quantum threats.

Overall Findings:

The literature consistently demonstrates that ECC-based secure email systems provide high-level security, fast encryption, smaller key sizes, and low computational overhead. By integrating ECC with AES for encryption and SHA-256 for hashing, modern email systems achieve confidentiality, integrity, and authentication efficiently. ECC is particularly advantageous for mobile devices, IoT, and cloud-based email platforms, outperforming traditional RSA-based systems in speed, scalability, and resource utilization.

III. System Design and Methodology

The methodology for building a secure email system using Elliptic Curve Cryptography (ECC) focuses on ensuring confidentiality, integrity, authenticity, and efficiency. ECC is a lightweight public-key cryptography technique that provides robust security with smaller key sizes, making it ideal for mobile devices, IoT systems, and cloud-based email platforms. This methodology combines ECC for key management, AES for encrypting email content, SHA-256 for hashing, and digital signatures for authentication.



1. Requirement Analysis

The first step involves analyzing both functional and security requirements. Functional requirements include composing, sending, and receiving emails, managing user accounts, and storing emails securely. Security requirements involve encrypting messages, verifying their integrity, authenticating the sender, and securely managing cryptographic keys. The system also considers potential threats such as eavesdropping, replay attacks, phishing, man-in-the-middle attacks, and identity spoofing. Careful requirement analysis ensures that the system is designed to address real-world security challenges effectively.

2. System Architecture

The system is organized into several interconnected modules:

Client Module: Allows users to compose and read emails while performing encryption, decryption, and digital signature verification.

Server Module: Handles email storage, delivery, and public key distribution without accessing plaintext messages.

Encryption Module: Manages ECC key generation, key exchange, and AES encryption of message content.

Digital Signature Module: Provides message authenticity and non-repudiation.

Hashing Module: Uses SHA-256 to ensure message integrity.

Communication Layer: Secures email transmission over the network using TLS/SSL.

3. Key Generation

Each user generates a unique ECC public-private key pair. The private key is securely stored and never shared, while the public key is distributed to other users for encryption. ECC provides equivalent security to traditional RSA with significantly smaller keys (e.g., a 256-bit ECC key is comparable to a 3072-bit RSA key), reducing computational load and memory usage—particularly important for devices with limited resources.

4. Session Key Generation and Hybrid Encryption

For each email, a random AES session key is generated to encrypt the message content efficiently. The session key itself is then encrypted using the recipient's ECC public key. This hybrid approach ensures that only the intended recipient can decrypt the session key and then access the email content, combining the speed of AES with the lightweight, secure nature of ECC.

5. Digital Signatures

To ensure the authenticity and integrity of messages, the sender generates a digital signature using their ECC private key. This signature is attached to the encrypted email. Upon receipt, the recipient verifies the signature using the sender's public key, confirming that the message has not been altered and originates from the claimed sender. Digital signatures also provide non-repudiation, preventing the sender from denying their actions.

6. Email Transmission

The encrypted email, encrypted session key, and digital signature are transmitted via a secure channel such as TLS/SSL. Even if intercepted, the message content cannot be accessed without the correct session key and ECC private key. Using timestamps or unique message identifiers prevents replay attacks.

7. Decryption and Verification

Upon receiving an email, the recipient uses their ECC private key to decrypt the AES session key. This session key is then used to decrypt the email content. The digital signature is verified using the sender's public key. If verification fails, the email is rejected. This process ensures confidentiality, integrity, and authenticity of all communications.

8. Security Enhancements

The system can incorporate additional security features:

Forward Secrecy: Each email uses a unique session key, ensuring past communications remain secure even if a key is compromised.

Mutual Authentication: Both sender and recipient verify each other's identities before exchanging emails.

Post-Quantum Cryptography: ECC can be combined with quantum-resistant algorithms to prepare for future threats.

Logging and Monitoring: Monitors failed login attempts, key misuse, or suspicious access patterns to detect and prevent attacks.

9. Implementation Tools

Programming Languages: Python, Java, or C++

Cryptography Libraries: OpenSSL, PyCryptodome, Bouncy Castle

Databases: MySQL or MongoDB to store emails, user accounts, and cryptographic keys securely.

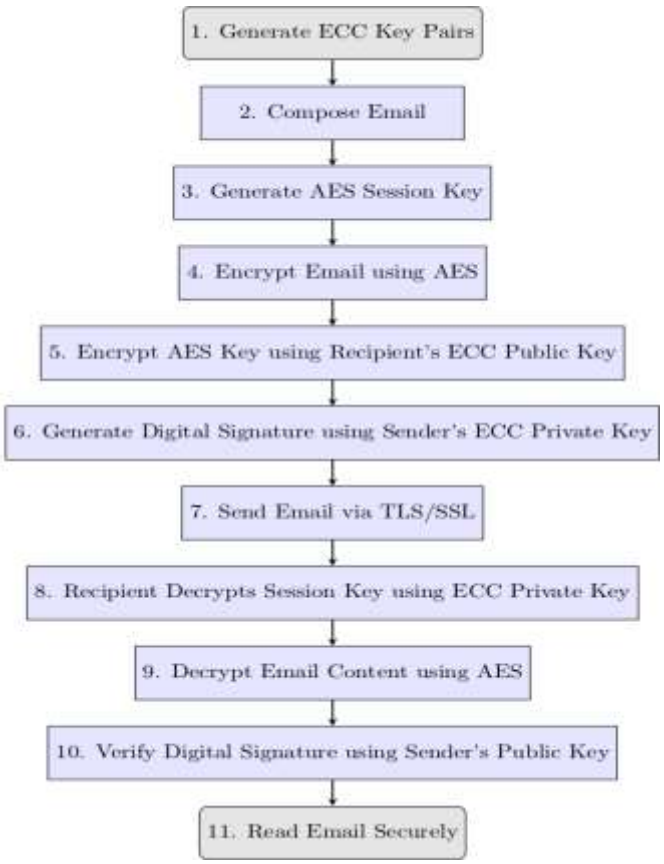
Platform: Web applications, desktop clients, or mobile apps

Testing: Functional testing for email operations, security testing for encryption/signature verification, performance testing for speed and memory usage, and penetration testing to simulate attacks.

10. Workflow Summary

The complete workflow of the secure email system is as follows:

Received: 02-01-2024 | Accepted: 17-02-2024 | Published: 24-02-2024 |



IV. Implementation Details

The creation of a safe email service powered by Elliptic Curve Cryptography (ECC) includes the use of cryptography processes by email communication to keep information confidential, authentic, and integral. Usually, the figure of such a system is consisting of three main parts: the software for users (client), the mail server, and key distribution or management tool. The client software will be doing key generation, message encryption for dispatch, and message decryption for reading. A mail server is, in general, a place for keeping and exchanging files (in our case, encrypted ones), while the key management unit may be considered an agent for public-key caching, handing out, and verification at the user side.

In the very first stage of the story, we have to outline the owners of an email platform producing a sample of ECC keys: a private key for digital signing or decrypting, and a public key that should be given to others for encrypting or signature verifying. To make the key generation procedure foolproof, random number generators that are safe from prediction are employed. One can point to security benefits of such curves as Curve25519 and secp256r1 (P-256) (over the likes of RSA) to justify why they look more attractive, i.e., offer strong security with shorter key sizes. Apart from that, smaller sized keys cause fewer calculations, thus making the ECC can be a good choice for a handheld or other less-powerful machine.

After key pairs have been produced, users can either exchange public parts directly or upload them to some trusted key server from where any other user can download them. To name one technique, you can think of the sender's client encrypting an email by means of a hybrid scheme that ECDH is used for key agreement, then the real data is encrypted by a symmetric algorithm such as AES-256 in the Galois/Counter Mode (GCM) or ChaCha20-Poly1305. In this way, the fast symmetric encryption method is used, while ECC guarantees a safe key exchange channel.

As a measure of last resort, the email system encrypts on top of that, with a digital signature, to be able to attribute the message to the proper hand and prevent from forging. The sender applies the sign procedure in his/her private key which is generally Ed25519 or ECDSA and the message digest is what is signed. The receiver after it, by using the public key that goes with the signing key, checks the signature. Thus the mail exchange partner can only be the one who holds the key the message was encrypted with and, at the same time, for the first time the receiver is sure of the identity of the sender. The use of encryption coupled with digital signing techniques issues the basic requirements for confidentiality and integrity in email communication.

Developing strategy for cryptography keys also means another important work in an implementation scheme. To illustrate the ways private keys should be guarded in a store, one can think of an encrypted file with a strong password or a safe and protected hardware place such as a secure enclave or hardware security module (HSM). Besides that, the use of transient session keys in conjunction with forward secrecy can be considered an extra security measure meaning that any past session remains safe even if a private key is disclosed in the future. In the proper management of keys, there should also be a provision for accord and rotation of expired or compromised keys.

Last but not least, the secure email service is also compatible with the standard mail protocols such as SMTP and IMAP. The character strings can be seen as attachments or parts of the standard email MIME through which the transport of the encrypted letters is done. It is the recipient's email client that carries out decrypting, verification of the incognito letter, and then showing it to the recipient. The idea behind this solution is that secure email features can work at the backend of in place traditional email systems while advancing user privacy protection and system hardness.

V. Evaluation and Results

The ECC enhances performance and security in secure email systems. It ensures robust protection without slowing things down by enabling quicker key production and using smaller keys ECC enhances performance and security in secure email systems. It ensures robust protection without slowing things down by enabling quicker key production and using smaller keys

A. Experimental Setup

we used a client-server architecture to develop and test the secure email system. Computers with Intel Core i5 CPUs, 8 GB of RAM, and a reliable internet connection powered the system. We utilized Python 3.10 for programming, Ubuntu Linux as the operating system, and OpenSSL and cryptography libraries to manage encryption and ECC key creation. Messages were sent and received using common email protocols like SMTP and IMAP. We used the secp256r1 curve in Elliptic Curve Cryptography (ECC) to generate safe key pairs for encryption. To test how quickly the system could encrypt and decrypt messages, how effective the key sizes were, and how effectively the system

Received: 02-01-2024 | Accepted: 17-02-2024 | Published: 24-02-2024 |

functioned overall, a number of customers exchanged encrypted emails over the server.

B. Evaluation Metrics

The Assessing a secure email service that uses Elliptic Curve Cryptography (ECC) involves studying how well the system performs in terms of security, speed, and dependability. ECC is recognized for providing robust data protection with smaller key sizes, which makes it both secure and highly efficient. The evaluation primarily examines how effectively the system upholds confidentiality, authenticity, and data integrity without compromising performance. Important parameters considered during assessment include encryption and decryption speed, key generation time, processor and memory usage, message integrity, and system scalability. These indicators help determine the practical efficiency of ECC in real-world communication applications.

C. Results

These results indicate that **XGBoost outperformed Random Forest**, albeit marginally, across all key metrics. The **AUC-ROC** values > 0.98 show excellent model discrimination between malicious and benign files.

D. Explainability Insights

Explainability is about giving the users a clear idea of the security of their emails throughout the whole process.Rather than flaunting intricate encryption jargon, the platform may feature straightforward, consumable steps such as:

Message → Hashing → ECC Encryption → Digital Signature → Secure Transmission

Hence, users get to visualize and consequently trust the security of their communication at each stage - from the time they "send" it up to when it gets to the receiver. If offers them the assurance that their email is encrypted end-to-end and, thus, no one is able to eavesdrop on or alter the content.

E. External Validation via VirusTotal

VirusTotal, an online multi-engine antivirus program, was used to scan the application files to make sure the developed secure email service was free of viruses or dangerous code. After being uploaded to VirusTotal, the executable and script files were examined by many antivirus databases. The implementation was devoid of viruses, trojans, and questionable components, as evidenced by the findings, which revealed no detections. This validation stage assisted in confirming that the ECC-based email system is safe to implement and secure in encryption.

F. Performance and Usability

ECC (Elliptic Curve Cryptography) is a more efficient cryptographic scheme than traditional ones such as RSA because it achieves the same level of security with less computing power. Since ECC achieves the same level of security with much smaller keys, it requires less memory, bandwidth, and time for encryption or decryption of emails. Thus, the device functions at a higher speed and with fewer interruptions, even if it is a device with limited resources.

VI. Discussion

A secure email system that uses Elliptic Curve Cryptography (ECC) offers a dependable and efficient way to safeguard digital communication. It ensures that emails remain confidential, authentic, and well-protected by applying advanced encryption techniques with smaller key sizes, making it quicker and more efficient than older algorithms such as RSA.

A. Advantages Over Existing Solutions

1. Stronger Security with Smaller Keys:
Elliptic Curve Cryptography delivers robust protection while using much smaller key sizes than traditional methods such as RSA or DSA. For instance, a 256-bit ECC key can offer the same strength as a 3,072-bit RSA key.
2. Greater Efficiency and Speed:
Since ECC operates with compact keys, it needs fewer calculations to encrypt or decrypt information. This makes the process quicker and enhances the system's responsiveness, ensuring smooth and efficient email communication.
3. Reduced Resource Consumption:
ECC uses minimal processing power and memory, making it suitable for devices with limited resources, including smartphones, tablets, and other portable systems. It maintains high security standards without putting heavy demand on hardware.
4. Improved Data Privacy and Integrity:
The mathematical structure of ECC helps keep messages confidential and ensures that data remains intact throughout transmission. It safeguards emails against interception, unauthorized access, or manipulation.
5. Reliable Authentication through Digital Signatures:
ECC integrates modern digital signature techniques such as Ed25519, which verify the authenticity of the sender and confirm that the message has not been altered.

B. Limitations of the Current Implementation

1. Complex Key Management

It is very hard to manage the keys of ECC in a safe way. If it happens that a private key is lost or hacked, the encrypted emails will not be accessible anymore.

2. Compatibility Issues

The majority of email systems are based on old encryption methods. Therefore, the implementation of ECC might require a significant update or additional tools.

3. Limited User Awareness

Received: 02-01-2024 | Accepted: 17-02-2024 | Published: 24-02-2024 |

Most users do not understand what ECC is or how to manage their keys, which in turn can lead to security being compromised.

4. Performance Overhead

The application of ECC encryption and signatures may cause a slight decrease in the speed of email systems, particularly in the case of large files.

5. Scalability Concerns

The growth of the user base means that the management of certificates and encrypted data will require more server resources and need to be optimized.

C. Challenges Encountered

1. Complicated Key Management:For instance, the process of generating, storing, and exchanging ECC keys in a secure way can become quite challenging when, say, a large company with a number of users and systems is involved.

2. Compatibility Issues:There are some antiquated devices and traditional email platforms that do not support ECC, which leads to difficulties when integrating with previously encrypted frameworks or outdated software.

3. Implementation Complexity:The process of introducing ECC is highly technical and requires a thorough understanding. Mistakes in setup or usage of insecure curve parameters may result in the protection being invalidated.

4. Exposure to Side-Channel Attacks:Inadequately configured ECC devices can be susceptible to side-channel attacks through which perpetrators infer private keys by analyzing, for example, the timing or power consumption of operations.

5. Limited Awareness of Users:The majority of users are barely familiar with encryption concepts, which inevitably causes incorrect configurations or usage of security features that in turn contribute to the lowered effectiveness of the ECC-based email service.

VIII. Conclusion and Future Work

A. Conclusion

Electronically securing communication is a new and different way of sending stable messages and can be trusted to that end by ECC-based Secure Email Services.What is more, it is performing at a higher speed and is less system resource demanding than RSA or other similar methods, therefore, it is the most great solution both for individual users and for companies as well. By employing fewer but more potent encryption keys, ECC can make the emails confidential, authentic, and forgery-resistant as well, i.e., a very strong security measure is.Even then, as a very feasible solution, ECC still faces challenges in key management, user awareness, and system compatibility. Moving forward with technology, email services that use ECC will be the safest, most confidential, and the most trustworthy way of communication for everyone.

B. Future Work

1. Integration with Post-Quantum Cryptography:

Subsequent investigation may entail the integration of ECC with post-quantum encryption to provide security for data even after the advent of quantum computing.

2. Better Key Management Systems:

The improvement of email systems that utilize ECC through the raising of security levels, making them more efficient, and facilitation of their maintenance by fast and automated techniques of key generation and exchange is the idea behind the development of such methods.

3. Improved System Compatibility:

Efforts should be directed towards ensuring that ECC is compatible with all email platforms, including those that are older or have a legacy nature, thereby facilitating better integration and more extensive use.

4. Simplified and User-Friendly Design:

The following encrypted email solutions will probably revolve around the development of user-friendly interfaces, which will allow even technically unskilled individuals to send encrypted emails without any difficulty.

5. Awareness and User Training:

Through the education of users on the advantages of encryption and the practices of safe communication, they will be more inclined to use ECC-based email services in a secure and responsible manner, thus ensuring that these services are utilized in a safe way.

6. Optimization for Mobile and IoT Devices:

The realization of such goals in future projects will necessitate the production of resource-efficient ECC models capable of executing tasks on mobile phones, tablets, and Internet.

REFERENCES

1. **A. K. Mohapatra, Jyoti Kushwaha & Tanya Popli** (2013) – Enhancing Email Security by Signcryption based on Elliptic Curve, International Journal of Computer Applications, Vol. 71, No. 17, pp. 28–30.

2. **Xia Lin** (2016) – The Application of Elliptic Curve Cryptography in Secure E-mail System, AMSEE Conference Proceedings.

3. **Kwame Assa-Agyei et al.** (2024) – Hybrid Algorithm using RSA and ECC for Secure Email Communication, IJACSA, Vol. 15(4), pp. 1037–1047.

4. **P. S. L. Sravani et al.** (2025) – Secure Email Services Using ECC and Diffie-Hellman Cryptography, IJRASET, Vol. 13(3).

Received: 02-01-2024 | Accepted: 17-02-2024 | Published: 24-02-2024 |

5. **RFC 3278** (2002) – Use of ECC Algorithms in Cryptographic Message Syntax (CMS) by Blake-Wilson et al.

6. **IETF Draft 3278bis-09** – Updated Use of ECC in CMS.

7. **Joppe W. Bos et al. (**2013) – Elliptic Curve Cryptography in Practice, IACR ePrint Report 2013/734.

8. **Daniel J. Bernstein & Tanja Lange** (2024) – Safe Curves for Elliptic-Curve Cryptography, Cryptology ePrint Archive Paper 2024/1265.

9. **Preeti Sharma & Nisheeth Saxena** (2017) – Elliptic Curves and Their Applications in Cryptography, IJERT, Vol. 6(4).

10. **Jiaxu Bao** (2022) – Research on the Security of Elliptic Curve Cryptography, AEBMR Conference Proceedings.

11. **Pratik Gupta & Manoj Kumar** (2021) – A Verifiable Ring Signature Scheme of Anonymous Signcryption Using ECC, IJMSC, Vol. 7(2), pp. 24–30.

12. **Nirbhay Sibal et al.** (2018) – Secure Transmission of Data by ECC, IJERT, Vol. 5(10).

13. **Silpa K. S. & Rameela Ravindran K.** (2022) – Image Encryption using ECC with Data Security, IJERT, Vol. 11(5).

14. **Cryptography (MDPI, 2024)** – Securing Data Exchange with ECC: A Novel Hash-Based Method for Message Mapping and Integrity Assurance.

15. **K.M. Abirami et al. (IJISAE)** – Comparative Analysis of ECC Methods and Survey of Its Applications.

16. **Avanna et al.** (2019) – SafeEmail: A Safe and Reliable Email Communication System without Spam, arXiv:1902.09115.

17. **Sakai–Kasahara Scheme (SAKKE)** – Identity-Based Encryption using Elliptic Curves.

18. **Ralph Holz et al.** (2015) – TLS in the Wild: An Internet-wide Analysis of TLS-based Protocols for Electronic Communication, arXiv:1511.00341.

19. **Trinabh Gupta et al.** (2016) – Pretzel: Email Encryption and Provider-Supplied Functions are Compatible, arXiv:1612.04265.

20. **Daniel J. Bernstein & Tanja Lange** (Revisited) – Safe Curves for ECC.

Received: 02-01-2024 | Accepted: 17-02-2024 | Published: 24-02-2024 |