International Journal of Mathematical, Engineering and Management Sciences
Vol. 11, No. 2, 896-919, 2026
https://doi.org/10.33889/IJMEMS.2026.11.2.037

An Innovative Multi-Party Authentication and Cyber Attacks Prevention Technique to Enhance the Security on Key and Data Transformation

Bilas Haldar
Department of Artificial Intelligence & Machine Learning,
St. Thomas' College of Engineering & Technology, 700023, Kolkata, West Bengal, India.
Corresponding author: bilasphd2020@gmail.com

Partha Kumar Mukherjee
Department of Computer Science and Engineering,
The Neotia University, Sarisha, 743368, South 24 Parganas, West Bengal, India.
E-mail: parthakumar.mukherjee@tnu.in

Himadri Nath Saha
Department of Computer Science,
Surendranath Evening College, Calcutta University, Kolkata, West Bengal, India.
E-mail: contactathimadri@gmail.com

(Received on May 8, 2025; Revised on August 6, 2025 & October 15, 2025 & December 25, 2025;
Accepted on December 28, 2025)

Abstract
The increasing reliance on online infrastructure and the expansion of distributed network systems have made digital communication that is an indispensable part of modern life. However, this dependence has also attracted malicious attackers' intent on intrusion, eavesdropping and compromising the security of sensitive information. This work presents an innovative approach to enhance the security in key generation, distribution and data transformation by developing a robust multi-party authentication technique. The work proposed a Modified Elliptic Curve Cryptography (MECC) technique to enhance the security for the key. The suggested approach leverages a combination of classical cryptography methods and innovative cyber attack prevention strategies to protect against unauthorized access and malicious threats. Additionally, the work introduces a novel encryption and decryption methodology for the secure transformation of key and data files using the MECC technique. Furthermore, a comparative analysis is conducted that benchmarks the performance of the proposed methodology against the traditional Elliptic Curve Cryptography (ECC) methodology. Experimental results show that MECC achieves encryption times ranging from 120.00 to 1376.99 seconds for files sized 10 to 100 MB. It is offering up to 28% faster performance and enhanced resistance to cryptographic attacks compared to traditional ECC. The applications of the suggested methodology are particularly suitable for E-banking systems that demand secure communication and real-time transactions. Furthermore, this work explores security defense strategies against Local File Inclusion (LFI) attacks in the financial sector, reinforcing the resilience of digital systems against emerging cyber threats.

Keywords- Encryption, Decryption, Modified elliptic curve cryptography, Security strategy, Local file inclusion attack, Pattern analysis attack, Chosen ciphertext attack.

1. Introduction

The security of multi-party communication systems has become increasingly crucial in the contemporary digital landscape. Particularly in scenarios involving sensitive information exchanges such as E-banking transactions, personal data sharing, and confidential communications. However, this widespread adoption has also attracted malicious actors seeking to exploit vulnerabilities for intrusion and eavesdropping. E-banking has become a fundamental service for managing financial transactions and accessing banking services via the Internet. However, securing these systems, especially in joint bank accounts that require multiple signatories to authorize transactions, present significant challenges. E-banking systems primarily rely on one-to-one message combinations for authentication, which are not sufficiently secure for joint

accounts. In such cases, only a single member may be aware of the transaction details, creating a security gap in multi-signatory scenarios. To address these security concerns, especially in multi-party authentication, robust authorization is crucial for establishing secure channels.

A hyperelliptic curve cryptography based signcryption technique was designed for E-payment systems to reduce computational costs (Devarajan and Sasikaladevi, 2020). A biometric authentication based payment protocol implemented for the improvement of security and to reduce the computational cost of electronic payment systems using elliptic curve cryptography (Malathi and Sasikaladevi, 2020). A framework based on ECC has been introduced to ensure secure financial transactions over Virtual Private Networks. This methodology incorporates Multi-Factor Authentication using authentication credentials and biometric identity to enhance transaction security through multiple layers of verification (Prabakaran and Ramachandran, 2022). A protocol developed to safeguard transaction information using a combination of ElGamal encryption, Advanced Encryption Standard, and the Chinese Remainder Theorem (Shyaa and Al-Zubaidie, 2023). However, to enhance the security of key transformations for authentication, there is a need to improve the security and efficiency of data transformation and authentication techniques.

The innovative technique presented in this work focuses on optimizing key distribution and authentication processes to safeguard against potential attacks, pattern analysis attacks, chosen ciphertext attacks, unauthorized access, and other forms of cyber intrusion. This approach aims to provide a robust framework for secure multi-party authentication to ensure confidentiality and integrity of the communication channels. A principal component of the proposed methodology is its ability to use secure key sharing and distribution mechanisms that depend on shared knowledge among participants. It ensures that any breach in one party does not compromise the entire system. Additionally, the research work introduces a novel encryption and decryption methodology utilizing MECC. It provides a more secure transformation of key and data files over the global network. The work benchmarks the performance of our proposed MECC based approach against traditional ECC methods through comparative analysis. It demonstrates the suggested MECC methodology's significant improvements in security, efficiency, and scalability. Additionally, the research presents strategies for defending against local file inclusion attacks during different types of file transformation within the financial sector. The findings highlight substantial advancements in security, efficiency, and positioning the proposed methodology as a viable solution for enhancing secure communication and transactions in the financial domain.

The principal objective of this research work is to implement an innovative robust key generation technique and cyberattack prevention strategy in the financial sector. The key objectives are as follows:

- To propose novel key generation and distribution techniques that enhance security for multi-party authentication.
- To implement innovative encryption and decryption techniques using MECC for transforming data files securely.
- To demonstrate the potential application of the proposed MECC technique in the E-banking sector that significantly improves One Time Password (OTP) as a key transformation.
- To provide a more secure and efficient framework for managing multi-signatory accounts, ensuring that all authorized participants are involved in the transaction process.
- To explore the suggested security encryption and decryption strategy against Local File Inclusion attacks.
- To perform a comparative analysis between MECC and traditional ECC based on computational efficiency and security features.

The main contributions of the given work are the invention of the new key generation and efficient authentication method based on the Modified Elliptic Curve Cryptography approach. The use of a proposed MECC method is associated with the implementation of an innovative encryption and decryption approach. The work also contributes in the creation of multi-party authentication methods to enhance data transformation security. It offers a secure and effective solution to multi-signatory systems in E-banking and other high security applications. The research further contributes in enhancing the manner in which cryptography keys are created, exchanged, and controlled in order to safeguard shared accounts and uncompromising security in the digital financial world. The work introduces security analysis of proposed methodology against pattern analysis attack, chosen ciphertext attack. Moreover, the work presents cyber-attack prevention strategy measures against local file inclusion attacks in the financial sector.

The structure of this paper is organized as follows. A comprehensive literature review relevant to the present work is introduced in Section 2. The proposed methodology with its necessary mathematical operations is presented in Section 3. The experimental results and a discussion of the suggested technique are showcased in Section 4. Additionally, Section 5 introduces a performance analysis and comparison of the proposed methodology. Moreover, security analysis and cyber-attack prevention techniques of the proposed approach in the financial sector are outlined in Section 6. The final remarks and conclusion of this work are presented in Section 7.

2. Literature Review

This section introduces a comprehensive literature review of the proposed work based on symmetric key and asymmetric key cryptography. Several researchers have contributed to the development of secure systems in E-payment and banking environments utilizing various cryptography and cyber security approaches. The selection of appropriate cryptography techniques is pivotal in addressing the security of authentication and data communication. Lawal et al. (2021) introduced an improved hybrid methodology for E-payment security using the Elliptic Curve Integrated Encryption Scheme and Provably Secure Elliptic Curve Scheme. Madje and Pande (2024) presented a framework for client authentication by using an OTP method combined with quantum-safe channel technology. A lightweight security methodology using Internet of Things and Artificial Intelligence technologies to secure banking and Automated Teller Machine systems was developed by Gowshik et al. (2024). Oo (2023) implemented a methodology that combines captcha images with Bit Plane Complexity Segmentation and visual cryptography for online banking security. Akraam et al. (2024) embarked on enhancing cryptographic robustness by devising a novel approach for generating unique secret key streams using the two-dimensional logistic map and the arnold cat map. Okediran et al. (2024) introduced a binary field elliptic curve cryptographic algorithm designed to secure the perceptual layer of IoT enabled electronic payment devices, enhancing the protection of sensitive transaction data. Braeken (2022) strongly recommends the adoption of elliptic curve cryptography in the realm of public key cryptography for data communication. However, issues are raised on the sustainability of security by ECC. Kumar et al. (2021) developed a pairing free, identity based, two party authenticated key agreement protocol where hexadecimal extended American Standard Code for Information Interchange and Elliptic Curve Cryptography are used.

Avkurova et al. (2024) identified critical factors that influence the selection of optimal methods for calculating importance coefficients, improving the objectivity and simplicity of expert assessments in cyber security. This research contributes more accurate evaluations of security events in cyberspace that facilitates better decision making. Chandrika and Perumal (2022) presented a Modified Elliptic Curve Cryptography model based on the Diffie-Hellman algorithm to provide enhanced security for alternate key generation in cloud computing. Sahoo et al. (2021) suggested a lightweight strategy using symmetric cryptography as an alternative to encryption techniques. Kavitha et al. (2019) addressed security issues with a framework that

used a public key cryptosystem based on a hyper elliptic curve. Kumar and Kumar (2024) implemented a secure hybrid cryptographic scheme that combines Advanced Encryption Standard and Elliptic Curve Cryptography to improve security of data sharing. Ganavi and Prabhudeva (2023) introduced a hybrid methodology for image files using cryptography and steganography techniques. Dawahdeh et al. (2024) presented an enhancement to the Menezes-Vanstone Elliptic Curve Cryptography methodology. The objective of the methods is to improve the encryption and decryption technique for grayscale images. Goswami et al. (2024) overcome the critical issue of healthcare data security on the Internet of Things context. The research focuses on the ASS-JFO-DHEA model that integrates the innovative hybrid Artificial Shuffle Shepherd Integrated Jellyfish Optimization algorithm with Digital Homomorphism Elgamal Algorithm encryption. The study by Nikooghadam and Amintoosi (2020) presented a new design based on two-factor authentication and key agreement that is implemented to the session initiation protocol with support of elliptic curve cryptography. Idrissi and Palmieri (2024) introduced a detailed scheme that addresses authentication and authorization dilemmas of the IoT based health care system.

Pandey and Sharma (2025) developed a new image validation mechanism at the receiver side, that is, at the low-bandwidth communication channels. The model has an excellent security that can be compared to traditional end-to-end encryption. Deshpande et al. (2024) designed light crypto schemes to secure the privacy of financial transactions like privatized content. Karim et al. (2024) explored the user authentication criteria handshakes used by large banks. It provides meaningful information on the best practices in the security of online banking accounts. Bhavsar et al. (2024) adopted an approach that incorporates the Elliptic curve cryptography and random access keys. This two-sided effort is meant to maximize data security, which will be directed toward the key exchange and mutual check security between the untrusted parties. To improve the security of Radio-Frequency Identification systems by introducing a new authentication protocol that uses ECC that is provided by Timouhin et al. (2023). Ma and Du (2022) put forward an attribute based blind signature scheme with the use of elliptic curve cryptography. The security of this scheme is evidenced through the difficulty of the brevity of the elliptic curve discrete logarithm problem. Kumar et al. (2024) introduced a new approach based on the Advanced Encryption Standard and the elliptical curve Diffie- Hellman as the measures to enhance the security of the medical record. Tiwari et al. (2023) explored a secure encryption algorithm designed specifically for safeguarding highly sensitive communications and ensuring undisturbed data transmission. Shukla and Patel (2024) contributed to the cryptographic landscape by designing a multi-factor authentication protocol based on elliptic curve cryptography for multi-server architectures, particularly focusing on cloud environments. Patnaik and Prasad (2023) introduced an enhanced Advanced Encryption Standard encryption mechanism that strengthens the confidentiality and integrity of the medical data. Haldar et al. (2024b) proposed a hybrid cryptographic approach that combines multiple encryption techniques to enhance the security of authentication keys and data files. Haldar et al. (2024c) introduced an advanced symmetric encryption and decryption methodology employing a 1024-bit key size, designed to improve data protection and resistance against cryptanalytic attacks. According to the literature review limitations of previous work are showcased in **Table 1**.

The existing literature review provided is quite extensive since it encompasses different cryptography techniques such as elliptic curve cryptography which is used to secure the banking information within the financial sectors. However, it seems that there is a significant research gaps on the use of cryptography methods in terms of multi-party authentication, security, and efficiency in the financial domain. The work project aims at the creation of a new multi-party authentication method that make the process more efficient and operational in terms of the ability to facilitate key transformation. These require more researches to come up with a more efficient, secure and universal cryptographic methodology. The technique offers protection on critical transformation, escalates encryption decryption of keys, incorporates recent multi-

party authentication algorithm, and is resistant to develop dynamic online threats. The research explores the computational time implications of key generation time, encryption time and decryption time that is involved during cryptography on E-banking systems. Additionally, the literature review raises an issue of concern about the viability of the security provided by ECC. Research gap lies in researching on the dynamic aspect of cryptography algorithms and how these evolve with the changing cyber security threats. The research would aid in the provision of effective security provisions that can be generally applied to improve the security of major transformation in the financial sector with the help of the Modified elliptic curve cryptography method.

Table 1. Limitation of previous ECC works.

Author	Used methodology	Limitation
Malathi and Sasikaladevi (2020)	Elliptic Curve Cryptography	Optimize storage space and energy without compromise security
Prabakaran and Ramachandran (2022)	Elliptic Curve Cryptography	Man in the cloud attack is possible
Madje and Pande (2024)	Quantum Cryptography	Detailed analysis of the operational feasibility
Gowshik et al. (2024)	Lightweight Cryptography	Need to minimize resource consumption of the suggested methodology
Ganavi and Prabhudeva (2023)	Elliptic Curve Cryptography with Discrete Wavelet Transform	Need to reduce encryption time
Bhavsar et al. (2024)	Elliptic Curve Cryptography and Random Access Keys	Facial recognition or iris scanning can be integrated to further strengthen the system's security
Haldar and Jha (2023)	Modified Elliptic Curve Cryptography	Vulnerable to local file inclusion and pattern analysis attacks, indicating potential weaknesses in security resilience
Trung et al. (2023)	Elliptic Curves Cryptography and Vigenère Symmetry Key	Implemented only C# programming language
Haldar et al. (2024a)	Secure Elliptic Curve Cryptography	Requires optimization to minimize encryption and decryption time, affecting real-time performance and computational efficiency

3. Proposed Methodology

The proposed methodology introduces a new approach that involves key generation and encryption and decryption procedures to improve the security of E-banking in the financial industry. The proposed algorithms are created on the foundation of advanced mathematics formulas, such as elliptic curve cryptography, modular arithmetic, prime numbers, and multiplication functions. The MECC has led in various security applications, taking advantage of its ability to offer strong cryptography properties with key-size comparatively smaller. The elliptic curve cryptography is a type of the public key cryptography, which is put strategically around the financial industry to promote safe communication, and to guarantee both integrity and confidentiality of the data. The suggested MECC methodology is designed into three parts like the key generation, encryption, and decryption. It involves the key generation process that creates several keys that are used in the data encryption and strong authentication in E-banking. Then the encryption steps follow in the encryption stage where the keys are encrypted with MECC technique and sent as email to all authenticated users. The key objective of this methodology is to ensure privacy, accuracy, and legitimacy of the financial data. Decryption process entails conversion of unintelligible keys into the readable ones, whereas the authentication process consists of regeneration of a key between a group of keys. It is a match between the re-generated key and the original key that determines the success of authentication. Otherwise, the authentication is considered to fail. The E-banking system passes into the operative phase on the successful authentication in the financial sector. The keys to the proposed methodology include a session management aspect of the keys in order to improve security of E-banking.

The underlying techniques hinge on the fundamental elliptic curve equation $y^2 = x^3 + a \times x + b$ here constraints *'a'* and *'b'* define the curve's shape. Point addition, a geometric operation on the curve, entails drawing a line through two points and identifying the third point where the line intersects the curve. This process is associative and crucial for the associativity of elliptic curve cryptography operations $(P + Q) +$

$R = P + (Q + R)$. Scalar multiplication involves adding a point to itself a certain number of times, resulting in a new point on the curve, which becomes the public key. The suggested MECC security relies on the difficulty of the discrete logarithm problem, making it computationally infeasible to derive the private key from the public key. A random function generates a secret number, and the result of scalar multiplication of the generator point on the elliptic curve by the private key is obtained. The algorithm employs specific terms such as PN_{user} represents the private key for the user, PN_{ebank} indicates the private key for the financial sector, P_{mecc} denotes points on the curve with coordinates (x, y), Q_{user} indicates the public key of users, Q_{ebank} represents the public key of financial server, and N_{max} represents the maximum order of the base points KGP_{mecc}.

3.1 Key Generation using Modified Elliptic Curve Cryptography

The key generation phase assumes a central role in establishing the multi-party authentication of E-banking within the financial sector by crafting both the public key and the private key. It generates a key pair of private and public key using MECC. These keys are the foundation on which the securing of communications, maintenance of data integrity, and performance of authentication in a financial system can be achieved. The purpose of the public key is that of encrypting messages which produces unintelligent ciphertext. The decryption of the message is through the use of the private key. The key generation technique is expounded in Algorithm 1.

Algorithm 1: Key generation using modified elliptic curve cryptography

Require: Prime number Q_{mecc}, Integer numbers a_{mecc}, b_{mecc}
Ensure: N_{max} represents the maximum order of base points KGP_{mecc}
1: Generate a prime number Q_{mecc} and points on the elliptic curve in KGP_{mecc}
2: Select two constant integer numbers such as a_{mecc} and b_{mecc}
3: $I = 0$
4: **while** $I < Q_{mecc}$ **do**
5: $RES_{right} = (I^3 + a_{mecc} \times I + b_{\text{mecc}}) \% Q_{mecc}$
6: $LES_{left} = I^2 \% Q_{mecc}$
7: $LHS_{user}.append(LES_{left})$
8: $RHS_{user}.append(RES_{right})$
9: $I = I + 1$
10: **end while**
11: $I = 1$
12: **while** $I \leq Q_{mecc}$ **do**
13: $K = 1$
14: **while** $K \leq Q_{mecc}$ **do**
15: **if** $(LHS_{user}[I] = RHS_{user}[K])$ **then**
16: $KGP_{mecc}.append([I, K])$
17: **end if**
18: $K = K + 1$
19: **end while**
20: $I = I + 1$
21: **end while**
22: Select random point P_{mecc} = random.choice(KGP_{mecc})
23: $PN_{user} \in (1 < PN_{user} < N_{max})$ // Randomly generate private key for user
24: $PN_{ebank} \in (1 < PN_{ebank} < N_{max})$ // Private key for financial server
25: $Q_{user} = PN_{user} \times P_{mecc}$ // Generate a public key for user
26: $Q_{ebank} = PN_{ebank} \times P_{mecc}$ // Generate a public key for financial server
27: Return PN_{user}, PN_{ebank}, Q_{user}, Q_{ebank}
28: Exit

The MECC key generation algorithm suggested has a number of new features that are more flexible, secure and have diversity of computations than the classical ECC key generation algorithms. Traditional ECC normally makes use of pre-defined curves that have fixed base points and parameters. Nevertheless, the proposed MECC algorithm generates dynamically the points of elliptic curves depending on a chosen prime number Q_{mecc} and constants a_{mecc}, b_{mecc}, as opposed to using constant parameter sets. This brings another dimension of variability and unpredictability which has the potential to trim away certain known curve specific vulnerabilities. Random selection of the base point adds a layer of randomness and personalization to the key generation process, making it significantly harder for attackers to guess or reuse base points across sessions or users. The generation of the valid point set is decoupled from the scalar key generation, meaning that even with a known curve structure, the actual point set used in the MECC system can vary significantly depending on input parameters and random selections. The algorithm is designed to support two-party secure communication by generating independent private and public key pairs for both entities from a shared curve context. This built-in dual key structure streamlines secure session establishment without requiring separate agreement protocols. The proposed MECC provides a more adaptable, randomized and possibly light weight substitute to traditional ECC key generating mechanisms. Its unique point matching operation, as well as random choice of base point, provides an extra dimension of unpredictability and customizability, and as such its operation is especially suited to current secure communication systems with stringent performance or security requirements.

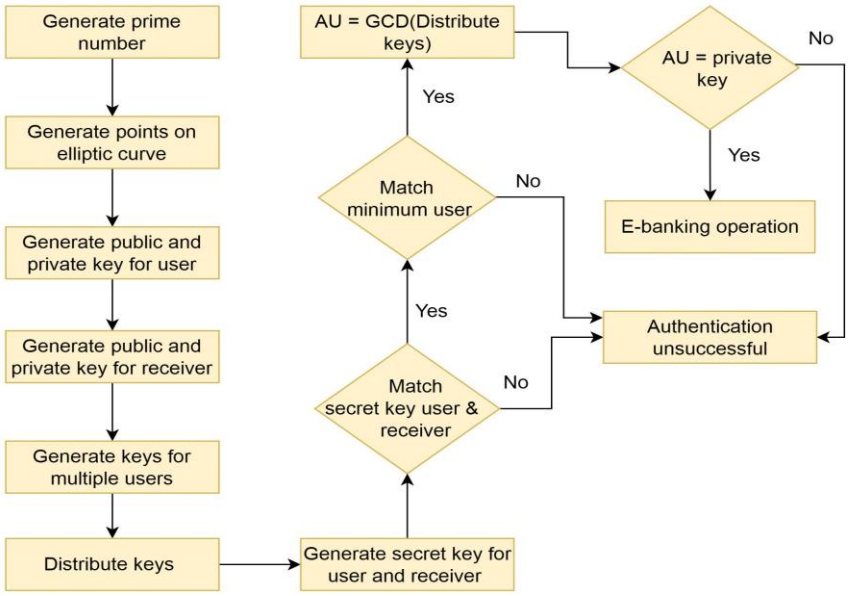

Figure 1. Process flow diagram of key generation and multi-party authentication technique.

The functionality of the proposed process flow diagram illustrates in **Figure 1** is a secure cryptographic technique used in multi-party authentication systems, particularly for E-banking or digital identity verification applications. The methodology is based on MECC and involves multiple stages are key generation, distribution, secret key matching, and authentication. A large prime number is generated to define the finite field over which the elliptic curve is constructed in key generation phase. The proposed key generation methodology is employed to generate keys for both authentication and encryption purposes within the context of E-banking in the financial sector. This methodology encompasses the generation of both private and public keys. Public keys are distributed among the communicating parties. Private keys are

securely stored by the respective users. The process involves the generation of a secret key for user authentication. The system verifies if the secret keys generated on both sides match. If the secret keys match between the sender and the receiver, then system process to the next steps. If it fails to match, then authentication is unsuccessful. The suggested model ensures that a minimum required number of authenticated users have valid secret keys. A secure authentication unit is derived using the greatest common divisor of distributed keys, a technique likely used to ensure uniqueness or consensus. The final verification step checks if the derived authentication key denotes 'AU' matches the expected private key. Once authentication is confirmed, E-banking gains authorization to initiate operations within the financial sector. It enhances security by ensuring that both parties share a derived secret, and that the final authentication relies on cryptographic and mathematical validation.

3.2 Encryption using Modified Elliptic Curve Cryptography

Encryption is simply the act of ciphering a message to be able to protect data, such that only authorized entities can access it. In financial sector E-banking which involves the utilization of advanced technologies to streamline financial practices. Encryption can play a significant role in ensuring the security of E-banking data communications. This tactical implementation of encryption is very important in the maintenance of confidentiality and integrity of sensitive information in the financial sector. The base points of the elliptic curve are calculated using the prime numbers that are used to form the basis of cryptographic operations.

Algorithm 2: Encryption using modified elliptic curve cryptography

Require: Input data file V_{dat}, Public key for encryption
Ensure: Base points on the elliptic curve in KGP_{mecc}
1: Input data file V_{data}
2: Fetch the user public key of the Q_{ebank}
3: Fetch the base point P_{mecc} from KGP_{mecc}
4: $FilePm$ = ConvertASCII (V_{data})
5: Len = length ($FilePm$)
6: $KI = 1$
7: **while** $KI \leq Len$ **do**
8: KP_{user} such that ($1 < KP_{user} < N_{max}$) // Generate a random number
9: **if** $KP_{user} > N_{max}$ **then**
10: Goto step 8
11: **end if**
12: Calculate $C1_{user} = KP_{user}[KI] \times P_{mecc}$
13: Calculate $C2_{user} = FilePm[KI] \times Q_{ebank}$
14: $KI = KI + 1$
15: **end while**
16: Return ($C1_{user}$, $C2_{user}$)
17: Exit

The encryption algorithm proposed in MECC based encryption scheme introduced in Algorithm 2 contains a number of important innovations in comparison to conventional ECC based encryption techniques. These improvements are mainly in terms of flexibility, randomness, data level granularity, and increased immunity to known cryptanalytic attacks. The classical ECC encryption protocols usually process bulk encrypted data or value on the key level. However, proposed MECC encrypts each character or byte of the input data file separately. This character level fine grained encryption adds more randomness and offers better resistance against frequency analysis or chosen plaintext attack. The algorithm uses a dynamically generated random integer KP_{user} for each data character during encryption. Unlike conventional ECC, where

a single ephemeral key may be reused across a session, this per-character randomness enhances forward secrecy and makes cryptanalysis significantly harder, especially when applied to streaming or real-time data. MECC generates two ciphertext components for each data unit $C1_{user}=KP_{user}[KI] \times P_{mecc}$ and $C2_{user}=FilePm[KI] \times Q_{ebank}$ in encryption process. This two-part encryption resembles the ElGamal-style structure but is implemented with a customized elliptic curve and dynamic ephemeral keys, providing forward secrecy and non-deterministic encryption across multiple sessions.

3.3 Decryption using Modified Elliptic Curve Cryptography

Decryption within the field of cryptography refers to the inverse procedure of encryption. In this process, ciphertext transforms back into plaintext through the application of specific algorithms. The suggested decryption methodology for E-banking security in the financial sector involves implementing a secure process to reverse the encryption applied to sensitive financial data.

Algorithm 3: Decryption using modified elliptic curve cryptography

Require: Encrypted data file $C1_{user}$, $C2_{user}$, private key for decryption
Ensure: Base points on the elliptic curve in KGP_{mecc}
1: Fetch ciphertext message $C1_{user}$, $C2_{user}$
2: Retrieve the receiver's private key PN_{ebank}
3: $C1C2_{user}$ = length ($C1_{user}$, $C2_{user}$)
4: **while** K in $C1C2_{user}$ **do**
5: $V_{datax} = C1_{user}[K] \times PN_{ebank}$
6: $V_{datax} = KP_{user}[K] \times P_{mecc} \times PN_{ebank}$
7: $V_{datax} = C2_{user}[K] - V_{datax}$
8: $V_{datax} = convertdecimal(V_{datax})$
9: **end while**
10: **if** V_{data} match with $FilePm$ **then**
11: print ("Accepted data files")
12: **else**
13: Print("Reject data files")
14: **end if**
15: Exit

The MECC decryption procedure introduces in Algorithm 3 several innovative features that enhance security, efficiency, and integrity verification beyond what is available in standard ECC decryption routines. Traditional ECC decryption algorithm recovers data (m) from ($C1, C2$) = (kG, mQ) by computing $m = C2 - d \times C1$ where d is the private key. Whereas proposed MECC decryption algorithm leverages the fact that computing $C1[K] = KP_{user}[K] \times P_{mec}$ *and* $C2[K] = mK \times Q_{ebank}$. The computing $V_{dataxK} = C2[K] - PN_{ebank}$, $(C1[K]) = mK \times Q_{ebank} - PN_{ebank} \times KPuser\,[K] \times P_{mecc}$ operations directly cancels the per-symbol random scalar without separate inversion or complex pairing operations. This dual multiplication approach internally aligns both ciphertext components for a single subtraction step. After recovering each numeric plaintext unit V_{dataxK} (*convertdecimal)*, the algorithm immediately compares the reassembled message sequence against the original ASCII sequence *(FilePm).* Any mismatch triggers rejection of the entire data file. This embedded consistency check simplifies integrity verification without extra cryptographic primitives. The decryption loop processes each ciphertext pair independently, allowing the algorithm to stream decryption and validation for arbitrarily large files or data streams.

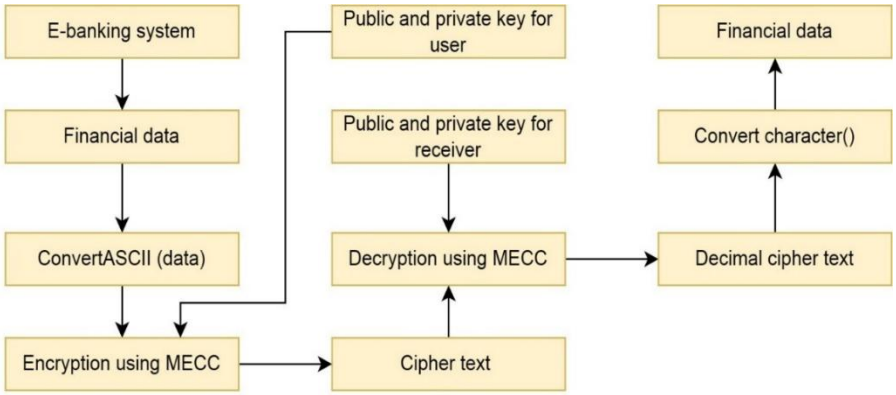

Figure 2. Process flow diagram of encryption and decryption technique using MECC.

The proposed model provides a safe encryption and decryption model of relaying financial information in E-banking system through Modified Elliptic Curve Cryptography in **Figure 2**. It has a user and receiver part that employs a pair of keys, which is public and private and a set of transformation phases. The process can be divided into the following steps:

1) Data Generation and Preprocessing
- **E-banking System:** The system generates financial data that needs to be transmitted securely.
- **ConvertASCII(data):** The financial information is translated into its ASCII form in order to be encrypted. The transformation is compatible with the encryption algorithm.

2) Encryption Using MECC
- **Public and Private Key for User:** The user is issued with a key pair. These keys find their application in MECC to encrypt the data in ASCII form.
- **Encryption using MECC:** The user and the receiver communicate on the basis of their public key and his private key with the ASCII data, which is then encrypted to produce cipher text.

3) Transmission
- **Cipher Text:** The message in the encrypted form is safely sent to the receiver. It is coded and a numeric value is obtained, denoted as being in the form of a decimal cipher text following the decryption.

4) Decryption Using MECC
- **Public and Private Key for Receiver:** The receiver uses their private key and the sender's public key to decrypt the cipher text.
- **Decryption using MECC:** MECC decrypts the cipher text into its numeric form (decimal cipher text).

5) Post-Processing and Data Reconstruction
- **Convert Character():** The numeric values are converted back to characters, reversing the ASCII transformation.
- **Financial Data:** The original financial data is reconstructed and delivered to the receiver.

The Proposed model enhances data confidentiality and integrity on the transmission. It can withstand typical cryptographic attacks and reduce unnecessary workload and it is best suited to secure and real time financial applications. Scalable key sizes and flexible level of security offered in MECC structure enables an upgrade in the cryptographical strength in the future, without paradigm shift. The addition of curve adaptation and parameter diversification to MECC add more complexity, rendering it more invulnerable to changing attack strategies, such as attack as a quantum threat in the future. These enhancements ensure that MECC offers greater resistance to both classical and emerging threats, thereby addressing the longevity concerns that

have been raised in recent ECC related literature. The proposed network model for data transformation is presented in **Figure 3**.

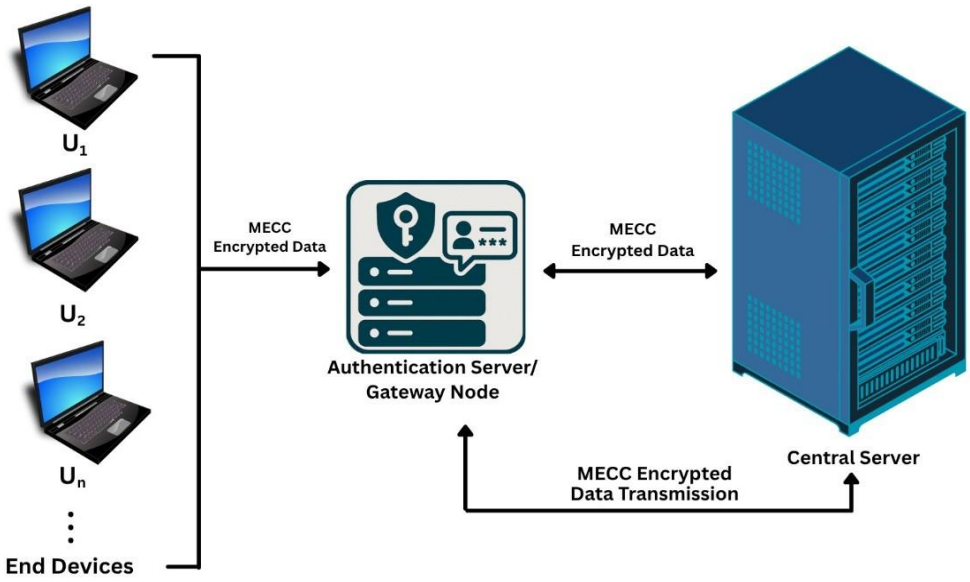

Figure 3. Network model for data transformation using MECC.

4. Results and Discussion

This section showcases the outcomes derived from the implementation of the suggested methodologies. Our proposed method delivers an exceptionally high level of data protection using the proposed modified elliptic curve cryptography techniques. Furthermore, it ensures a peak level of security for key generation, encryption, and decryption processes of E-banking in the financial sector. The suggested method has been applied to several kinds of larger file sizes. It has presented encryption time using suggested algorithms on text, image, audio, pdf, and exe files with a variety of sizes. The unique feature of this approach is that the encryption time is different for every kind of file regardless of the key size and number of values of private keys. The proposed encryption and decryption techniques significantly improve the security of data transformation in the financial sector. In the following tables, it has been listed the estimated key generation time, encryption time, and decryption time.

Table 2 presents the key generation and regeneration times of the proposed MECC methodology based on the number of prime numbers. The first column of the table denotes the value of private keys which varies from 10 to 160. The key generation time using the proposed MECC technique showcases the second column from the left in the same table. This interval has been fluctuating with a range of 0.15423 to 0.78613 seconds. The critical time of regeneration commences at 0.14780 seconds when the private key value is 10 and the regeneration time rises to 0.45182 seconds when the private key value is 160. The results indicated that key regeneration time is shorter as compared to key generation time. It has been noticed that increasing the value of n that affect the degree of the security of the proposed key generation process and higher values imply higher levels of security.

Table 2. Key generation time of the proposed MECC methodology.

Value of private key 'n'	Key generation time (Second)	Key regeneration time (Second)
10	0.15423	0.14780
25	0.19919	0.13944
40	0.23943	0.14157
55	0.27025	0.14707
70	0.30848	0.15109
85	0.34903	0.16006
100	0.40483	0.21348
115	0.45911	0.23343
130	0.49620	0.28032
145	0.60226	0.39233
160	0.78613	0.45182

Table 3. Encryption and decryption time of the proposed MECC methodology.

File name	File size (MB)	Encryption time (Second)	Decryption time (Second)
Data1.txt	10	120.0045	232.8955
Data2.txt	20	205.4000	480.9111
Data3.pdf	30	260.2212	955.5817
Data4.jpg	40	404.0674	1227.4551
Data5.png	50	455.4815	1205.3194
Data6.pdf	60	674.4603	1542.1693
Data7.docx	70	756.0506	1612.1334
Data8.docx	80	908.5239	1958.1408
Data9.mp3	90	1159.9653	2376.5878
Data10.exe	100	1376.9948	2749.7066

Table 3 contains the results of the encryption timings of various files and sizes when using the novel modified elliptic curve cryptography method. **Table 3** contains the various of file sizes as measured in megabytes in the second column, and the corresponding time of encryption with the proposed MECC technique as the mandatory and optional number in the column next to it. The results of the experiment show that the time range of encryptions is between 120.0045 and 1376.9948 seconds. In addition, the decryption time of the MECC methodology is depicted in the last column of the table. The analysis shows that decryption of the data files will take between 232.8955 to 2749.7066 seconds. The MECC methodology shows a growing complexity of computation in both encryption and decryption methods as the files grow in size. This complication appears to increase more on the decryption approach rather than the encryption approach. It proposes that the decryption algorithm is associated with a tight security and computation.

Experimental setup

The proposed algorithms that were developed on the MECC technique were implemented in Python version 3.11. It was all tested and simulated on a 64-bit operating system of Microsoft windows 11 to make sure that the modern development tools and libraries can work with it. The hardware used in the experiments was the Intel find the Intel® Core™ i5-10210U CPU with a base frequency of 1.60 GHz and a peak boost frequency of 2.11 GHz. The system was equipped with 8 GB of RAM, providing sufficient processing and memory resources to support the cryptographic operations and the handling of moderately sized financial datasets. This setup provides a workable context to test the efficiency and robustness of the MECC based cryptographic model in the real-world E-banking context in terms of computational efficiency and security.

5. Performance Analysis and Comparison

This section shows the analysis of the performance of the given approaches to generating keys, encrypting, and decrypting processes. It introduces the ECC and proposed MECC approach as they are the two approaches that compared in terms of execution time. The tables and graphs give an overview of their corresponding performance in the different types of data used and the size of files used. The numerical data in **Table 2** is presented in **Figure 4** through a continuous solid line and dotted line that indicates the visual representation. The solid line is used to represent key generation time, and the dotted line is used to represent key regeneration time. The graph illustrates the relation of the random generation of private keys. The analysis observed that increasing the number of prime numbers corresponds to a gradual increase in key generation time. The methodology randomly selected elliptic curve points from the generated points in the key generation process, which affects the key generation time.

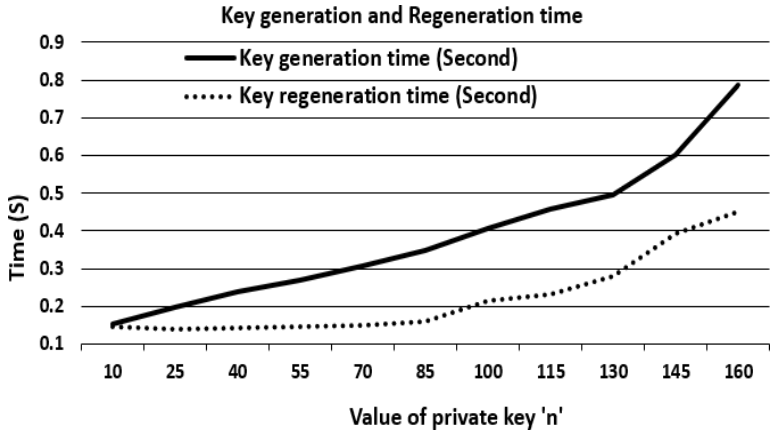

Figure 4. Key generation and regeneration time of proposed MECC methodology.

The elliptic curve points addition and multiplication operations are performed in the key generation process. The different complex mathematical operations are used for the same coordinate points and different coordinate points on the elliptic curve. This approach increases the hardness of the key so that it is difficult for an attacker to break. The regenerated keys improve the strength of the decryption process. It provides robust security for the conversion of data from ciphertext to plaintext.

The graphical depiction in **Figure 5** corresponds to the data presented in **Table 3** employing both continuous solid and dotted lines. The solid line is a representation of encryption time and the dotted line is a representation of decryption time as shown in the framework of proposed MECC methodology. The graph analysis shows that the decryption time is not constant and instances of increase and decrease are observed. This variability is dependent on the randomly generated key private values as seen in the graph. In addition, the encryption time increases gradually whereas the decryption time is exponentially growing as size of file increases. It is worth noting that, the time it takes to decrypt the message after some time is a big problem, the decryption time is much more than the encryption time. This attribute adds the high security of the proposed methodology because unauthorized decryption might be made difficult.

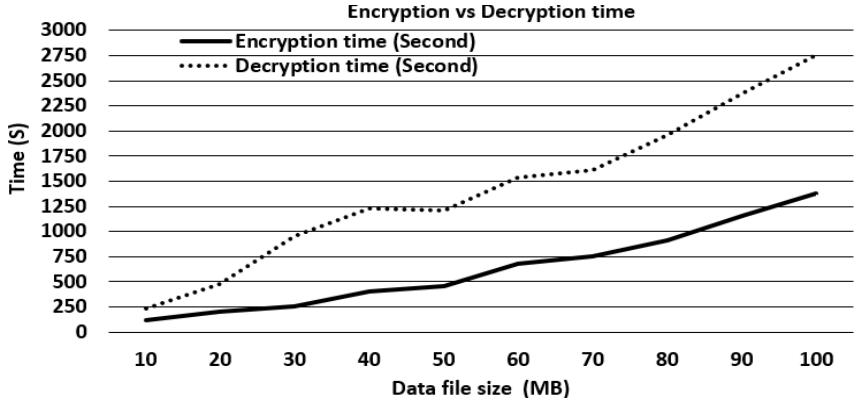

Figure 5. Encryption and decryption time of the proposed MECC methodology.

Table 4. Comparison of encryption time in proposed MECC and traditional ECC methodology.

File name	File size (MB)	Proposed MECC (Second)	Traditional ECC (Second) (Haldar et al., 2024a)
Data1.txt	10	120.0045	579.4000
Data2.txt	20	205.4000	463.5200
Data3.pdf	30	260.2212	695.2800
Data4.jpg	40	404.0674	927.0400
Data5.png	50	455.4815	1158.8000
Data6.pdf	60	674.4603	1390.5600
Data7.docx	70	756.0506	1622.3200
Data8.docx	80	908.5239	1854.0800
Data9.mp3	90	1159.9653	2114.6000
Data10.exe	100	1376.9948	2451.2320

Table 4 shows the comparison of encryption time of proposed MECC and traditional ECC (Haldar et al., 2024a) methods. In the third column is the encryption time with the proposed MECC methodology that is ranging between 120.0045 to 1376.9948 seconds. The left most column is an indication of time taken to encrypt a block using a conventional ECC algorithm. It has a range of 579.4000 to 2451.232 seconds on the 10 to 100 megabyte files. The MECC approach shows a high and steady increase in the speed of encryption with different file sizes. The MECC is 3.8 times quicker than conventional ECC on the 10 MB file. This aspect of enhancement advances with the size of files but is substantial through it all and demonstrates the effectiveness of MECC methodology.

The analysis of the results of **Table 4** in the form of graph is presented in **Figure 6**. Blue bars indicate the time it takes to encrypt the proposed MECC methodology. The time of encryption of the former ECC method is represented by the orange bars. The column graph indicates that the time of encryption is lower under the proposed MECC methodology, than the traditional encryption time of ECC methodology. The outcome of the proposed methodology determines that MECC is quicker than the conventional approach to methodology. The implication of the MECC method on the practical use is the speed of the encryption in the context of application that needs an efficient and effective method of data encryption. It enhanced the security of data transformation and improved the efficiency of system performance. It is useful for large volumes of data that need to be encrypted quickly.

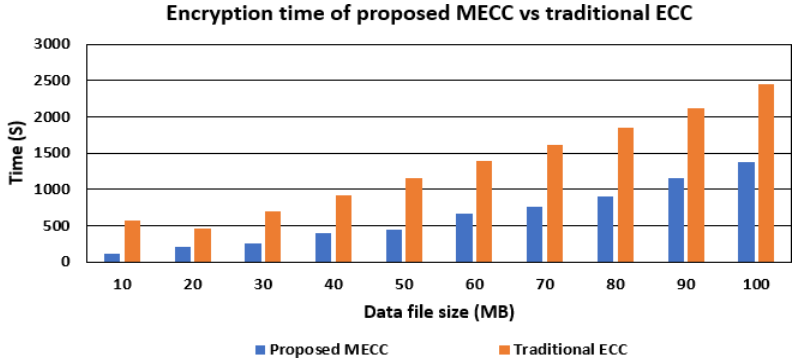

Figure 6. Comparison analysis of encryption time between proposed MECC and traditional ECC.

Table 5. Comparison of decryption time in the proposed MECC and traditional ECC.

File name	File size (MB)	Proposed MECC (Second)	Traditional ECC (Second) (Haldar et al., 2024a)
Data1.txt	10	232.8955	470.7667
Data2.txt	20	480.9111	676.6133
Data3.pdf	30	955.5817	1064.9200
Data4.jpg	40	1227.4551	1753.2267
Data5.png	50	1205.3194	1941.5333
Data6.pdf	60	1542.1693	2129.8400
Data7.docx	70	1612.1334	2618.1467
Data8.docx	80	1958.1408	3106.4533
Data9.mp3	90	2376.5878	3636.9000
Data10.exe	100	2749.7066	4015.7852

The comparison of decryption time between proposed MECC and traditional ECC (Haldar et al., 2024a) techniques is present in **Table 5**. It is essential for the performance analysis of the decryption technique of the proposed MECC methodology. The decryption time of the proposed MECC methodology is introduced in the third column. It varies between 232.8955 to 2749.7066 seconds for different sizes of files. The first column from the right indicates the decryption time using a traditional ECC algorithm. The decryption time varies from 470.7667 to 4015.7852 seconds. This trend of reduced decryption time with MECC persists across various file types such as txt, pdf, jpg, png, docx, mp3, exe. and even becomes more pronounced with larger files.

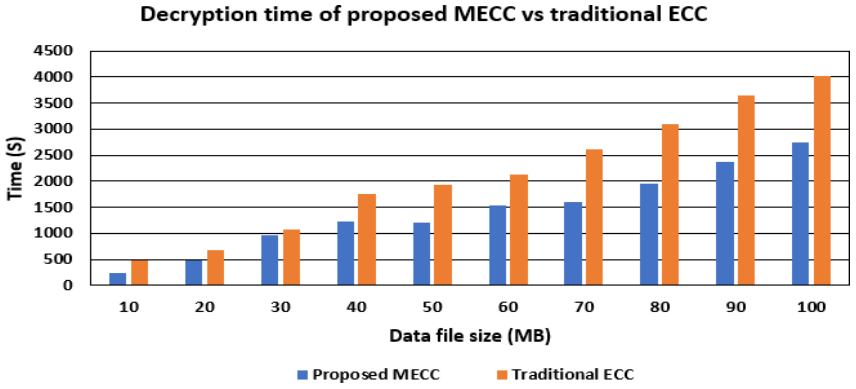

Figure 7. Comparison analysis of decryption time between proposed MECC and traditional ECC methodology.

The performance analysis of the decryption time is shown in **Figure 7**. The orange bars denote the decryption time of the traditional ECC techniques. The decryption time of the suggested MECC methodology is denoted through blue bars. It has been observed from the column graph that the proposed MECC methodology takes less decryption time compared to the decryption time of the traditional ECC methodology. The result of the MECC technique ensures that it is faster than the traditional methodology. The complex decryption process provides more robust security of the data decryption than traditional methodology. It demonstrates that the MECC decryption is more effective and needs less computational time to take the process of decryption. MECC has a similar communication cost as or somewhat less that of standard ECC techniques, owing to optimized prime based base points and smaller ciphertext sizes. The benefits of reduced computation time of MECC in terms of overall performance are not actually confined to the reduced transmission size but also have a positive impact on performance reductions in bandwidth limited systems. The MECC has increased trade-off in between computation and communication especially when dealing with big data or multiple parties as a result of lesser encryption and decryption times.

Table 6 presents a comprehensive comparison of the proposed Modified Elliptic Curve Cryptography technique with Secure Elliptic Curve Cryptography (Haldar et al., 2024a) and Modified Elliptic Curve Cryptography (Haldar and Jha, 2023). The suggested MECC method identifies the key size with reference to the maximum order of the base points, which is more flexible and scalable than the reliance to a private key value (Haldar and Jha, 2023) and bit length of prime numbers (Haldar et al., 2024a). The proposed MECC is much more scalable to large data sets in comparing the performance of encryption and decryption. Whereas a single encryption of 11 MB data takes Secure ECC 167.1245 seconds, MECC encrypts 10 MB data only in 120.0045 seconds. Similarly, decryption is faster in MECC than in Secure ECC (Haldar et al., 2024a) (282.8755 seconds) only with the more expeditious Modified ECC (Haldar and Jha, 2023) on small datasets. In the area of security, MECC complies with the highest rating since it provides an extreme rating as opposed to the better and moderate ratings of the earlier methods. Also, MECC considers some of the attack vectors that were not taken into account in former techniques. It gives preventive measures to Local File Inclusion and pattern analysis attacks, which had no previous works addressed or mentioned. Moreover, MECC presents defence to ciphertext attacks of choice, which is a great leap forward in security ability, in comparison to both previously mentioned schemes. Thus, the suggested MECC offers a sound trade-off in terms of performance, scalability, and enhanced security execution and therefore represents a better solution to the modern cryptographic based apps that involve high performance and ability to combat the emerging threats. The proposed MECC has a mean enhancement of about 56.83% and 32.08% of encryption and decryption time per MB than the standard ECC respectively.

Table 6. Comparison among proposed MECC technique with previous works.

Evaluation factors	**Modified elliptic curve cryptography (Haldar and Jha, 2023)**	**Secure elliptic curve cryptography (Haldar et al., 2024a)**	**Proposed MECC technique**
Key size	Depends on value of private key	Depends on number of bits of prime numbers	Depends on maximum order of base points
Key generation time (second)	0.07986	0.2410904	0.15423
Encryption time (second)	0.23401 for 110 byte data	167.1245 for 11 MB data	120.0045 for 10 MB data
Decryption time (second)	1.51237	282.8755	232.8955
Security level	Better	Moderate	Extreme
Efficiency	Moderate	Better	High
Protection against Local File Inclusion Attack	Not presented	Not mentioned	Prevention possible
Protection against pattern analysis attack	Not presented	Not mentioned	Prevention possible
Protection against chosen ciphertext attack	Not presented	Not presented	Prevention presented

6. Security Analysis and Cyber Attack Prevention

The security of the MECC methodology is to be analyzed in order to give certainty on the robustness and reliability of the proposed methodology. The new MECC method has high security and uses comparatively minimal key sizes as opposed to the conventional methodology. Key generation, encryption, and decryption involve hard mathematical operations such as modular arithmetic, point generation on elliptic curves, prime numbers and random functions. The MECC relies on mathematical calculations of addition and scalar multiplication of coordinate points on elliptic curves to enhance hardness of the offered methodology. Additionally, the security of the techniques strongly relies on building of prime number referred to as Q_{mecc}. The methodology is strengthened by the fact that the field size of the elliptic curve is based on the utilisation of a prime number. The algorithm picks a random point (P_{mecc}) of the curve out of the produced set of points (KGP_{mecc}). The security of the suggested methodology is enhanced by the randomization of the points used in the proposed research. The authentication method is based on multiuser authentication that improves the security of the proposed methodology because the users who have a chance of authentication know the transformation of information that occurs across the communication networks. This is the complexity of the key generation process to make it resistant to cyber attacks like pattern analysis attacks, chosen ciphertext attacks, unauthorized access control and local file inclusion attack.

6.1 Prevention Technique of Local File Inclusion Attack

A Local File Inclusion attack is a form of security vulnerability that takes place when an application can enable an attacker to add files on a server via web browser. This hacking in an E-banking system can be a serious security risk. It takes advantage of vulnerabilities in an application on the web where the input of the user is not correctly tested and used as a means of adding files on the server. This vulnerability allows attackers to gain access to configuration files which could have encryption keys, database credentials and other sensitive user data. Attackers read session files to hijack user sessions, gaining unauthorized access to E-banking accounts. It leads to executing malicious scripts on the server if attackers manage to include a file with executable code. If an E-banking application stores authentication mechanisms in files, then LFI may allow attackers to bypass login mechanisms and gain administrative access. It exposed sensitive data about user transactions, bank balances, and account details.

Preventing local file inclusion attacks for E-banking in the financial sector is crucial to safeguard financial data and ensure the correct distribution of authentication keys. It has proposed a security encryption strategy for an E-banking system for key distribution in Algorithm 4. It is needed to validate user inputs to ensure that only legitimate and expected data is processed. This helps prevent attackers from injecting malicious payloads. Use secure communication protocols to encrypt data transmitted between the E-banking system and central servers. This helps protect sensitive information during transit. Implement robust user authentication using secure authentication methods to ensure that only authorized users can access the financial data. This work suggested a security decryption strategy to prevent local file inclusion attacks in the financial sector.

The cyber security encryption strategy of E-banking system for data and key distribution is presented in Algorithm 4. The MECC involves a set of mathematical operations on elliptic curves to provide secure encryption and decryption. The E-banking generates an MECC key pair, consisting of a private key and a corresponding public key. The public key is shared securely with the central control system or any entity that needs to communicate with the E-baking. When the E-banking system needs to send financial data, it uses the recipient's public key to perform MECC based encryption on the data files.

Algorithm 4: Security encryption strategy for multiparty authentication

Require: E-banking Data Files (MDF_{user}), Financial Database Server (HDS_{ebank})
Ensure: Used MECC key generation and encryption methodology
1: Select the number of users as N_{user}
2: Get KEY_{user} from users // Input keys from the users
3: Get MDF_{user} from users // Input E-banking data files from users
4: **if** $N_{user} < 2$ **then**
5: Goto step 1;
6: **else**
7: $I = 1$
8: **while** $I \leq N_{user}$ **do** then
9: KEY_{priv}, KEY_{Pub}, = Keygeneration() //Call Algorithm 1
10: EN_{key}= Encryption ($KEY_{user}[I]$, KEY_{Pub}) // Call Algorithm 2
11: EN_{data}= Encryption ($MDF_{user}[I]$, KEY_{Pub}) // Call Algorithm 3
12: $HDS_{ebank}[I] = KEY_{priv}$; $HDS_{key}[I] = EN_{key}$; $HDS_{data}[I] = EN_{data}$;.
13: **end while**
14: **end if**
15: $Flag$ =0
16: **while** KEY in N_{user} **do**
17: **if** $KEY \neq KEY_{original}$ **then**
18: $Flag$ =1
19: Goto step 22
20: **end if**
21: **end while**
22: **if** $Flag == 0$ **then**
23: Print("Authentication successful for financial data transformation")
24: Return Decryption(); //Call Algorithm 3 to decrypt data files
25: **else**
26: Print("Authentication unsuccessful")
27: **end if**
28: Exit

In Algorithm 4 and Algorithm 5, the variable MDF_{user} is employed to symbolize the E-banking Data File. KEY_{user} is utilized as a representation for the keys belonging to users, and HDS_{ebank} denotes the financial database server. The variable N_{user} is used to denote the number of users entering the keys. The Keygeneration() method is implemented to generate both private and public keys essential for the encryption and decryption processes. The variable KEY_{priv} represents the private key, while KEY_{Pub} signifies the public keys. The Encryption() method is utilized for encrypting keys and data files, with EN_{key} representing the encrypted key stored in the financial database server (HDS_{key}). Similarly, EN_{data} stands for the encrypted data files stored in the financial database server. Decryption, as a technique, is applied to decrypt data files and keys. Following the decryption process, original data files are generated, enabling E-banking to commence the delivery of data and keys to authorized users within the financial system.

The financial database server receives the encrypted data files and keys. The MECC based decryption of the received ciphertext with their own private key by the central financial system to extract the original plaintext message. The decrypted message is processed securely by the financial system for key distribution. This suggested security encryption and decryption for E-baking security in multiparty authentication systems can provide a strong foundation for protecting against local file inclusion attacks and ensuring secure communication.

Algorithm 5: Security decryption strategy of financial data transformation

Require: Encrypted keys (HDS_{key}), Encrypted data files (HDS_{data}),
Ensure: Used MECC key generation and decryption methodology
1: Get N_{user} from the requesting HDS_{ebank}
2: Get HDS_{key} from the requesting HDS_{ebank}
3: Get HDS_{data} from the requesting HDS_{ebank}
4: **if** $HDS_{key} == NULL$ **then**
5: Print("Access ignored to the HDS_{ebank}")
6: Goto step 1;
7: **else**
8: $I = 1$
9: **while** $I \leq N_{user}$ **do** then
10: Retrieve $KEY_{P\,riv}$[I] from the requesting HDS_{ebank}
11: KEY_{user} = Decryption (HDS_{key} [I], $KEY_{P\,riv}$) // Call Algorithm 3 12: MDF_{user} = Decryption (HDS_{data}[I], $KEY_{P\,riv}$) // Call Algorithm 3 13: **end while**
14: **end if**
15: $Flag$ =0
16: **while** MDF_{user} in HDS_{ebank} **do** 17: **if** $MDF_{user} == NULL$ **then**
18: $Flag$ =1
19: Goto step 22
20: **end if**
21: **end while**
22: **if** $Flag == 0$ **then**
23: Print("Financial sector read uploaded data files");
24: Return "Transfer data files in the financial sector"
25: **else**
26: Print("Corrupted data file, E-banking system discard data files")
27: **end if**
28: Exit

6.2 Pattern Analysis Attack

A pattern analysis attack is a form of cyberattack where an attacker attempts to uncover valuable information by analyzing patterns in data transmission or user behavior. The attackers rely on analyzing traffic or behavior patterns to infer details about sensitive information instead of directly breaking encryption or bypassing security measures. The proposed MECC methodology introduces randomness at various stages of the key generation and encryption processes to prevent pattern analysis attacks over the networks. Key elliptic curve parameters a_{mecc} and b_{mecc} are selected randomly to ensure the unpredictability of the key generation process. A larger value of N_{max} is chosen to resist pattern analysis in key distribution, making it harder for attackers to infer the structure of the cryptographic keys. The value P_{mecc} is chosen randomly from the elliptic curve points pool KGP_{mecc} using a secure random random.choice(KGP_{mecc}) function. This step enhances security by introducing further randomness into the point selection for key generation. Private keys for both the user and the bank are generated using a random number generator. The private key of the user is generated using ($PN_{user} \in (1 < PN_{user} < N_{max})$) and for bank using ($PN_{ebank} \in (1 < PN_{ebank} < N_{max})$). This process makes it nearly impossible for an attacker to predict private keys based on observable data. The user's public key is generated as $Q_{user} = PN_{user} \times P_{mecc}$. and the bank's public key is generated as $Q_{ebank} = PN_{ebank} \times P_{mecc}$. The public keys for the user and E-bank are both unique and unpredictable by using random private keys and a random point on the elliptic curve. The creation of a random number KP_{user} of each block *(KI)* of the data file has placed a component of unpredictability that is

important in cryptography security in encryption algorithms. The randomness techniques guarantee different encrypted output ($C1_{user}$, $C2_{user}$) are produced even when the same block of data is encrypted more than once. It offers protection against attacks of pattern analysis. The use of random elliptic curve parameters, the creation of unpredictable and undetectable private and public keys and the use of random encryption keys to each block of data means that an adversary cannot use recurring or forecastable patterns in the process of key generation and encryption.

6.3 Chosen Ciphertext Attacks

An attacker selects ciphertexts and retrieves their corresponding plaintexts through a decryption mechanism in a chosen ciphertext attack. The attacker targets vulnerabilities in the decryption process to compromise the security of the encryption methodology. The key generation, encryption, and decryption techniques of the MECC integrate randomization, unpredictable private and public keys, and random elliptic curve parameter selection to protect against chosen ciphertext attack. The data values are secured using the equations the $C1_{user} = KP_{user}[KI] \times P_{mecc}$ and $C2_{user} = FilePm[KI] \times Q_{ebank}$ in the encryption process. The random generation of $KP_{user}[KI]$ and $FilePm[KI]$ ensures that identical plaintexts produce different ciphertexts with each encryption, making it significantly harder for attackers to exploit chosen ciphertext attack techniques. The use of the receiver's public key (Q_{ebank}) for encryption ensures that only the holder of the corresponding private key can decrypt the encrypted data ($C2_{user}$). It provides confidentiality of data transformation. The elliptic curve point multiplication ($C1_{user}[K] \times PN_{ebank}$) and ($KP_{user} \times P_{mecc} \times PN_{ebank}$) used in the decryption process is computationally infeasible to reverse without the private key. The additional elliptic curve operation $C2_{user}[K] - V_{datax}$, makes predicting the data exceedingly difficult, thereby strengthening the security of the data transfer. Additionally, the algorithm processes each block of ciphertext ($C1_{user}$, $C2_{user}$) individually that help to prevent chosen ciphertext attacks. The complex mathematical operations involved in the MECC algorithm, particularly in key generation, encryption, and decryption, introduce an extra layer of difficulty. It makes the proposed MECC technique highly resistant to chosen ciphertext attacks. This harder mathematics computation includes more complexity of the proposed technique. It is quite difficult to break the suggested technique through the chosen ciphertext attack.

6.4 Justification and Informal Security Analysis

- MECC strengthens security using large prime numbers and a modified elliptic curve structure, making it resistant to brute-force, lattice-based, and side channel attacks.
- The encryption process introduces non-determinism and diffusion properties, which significantly reduce the chances of pattern recognition and ciphertext manipulation, even under chosen ciphertext scenarios.
- The dynamic key generation mechanism, based on the maximum order of base points, provides forward secrecy and prevents key recovery, even if part of the session is compromised.
- MECC significantly enlarges the key space, making it computationally infeasible for attackers to predict or reverse keys by utilizing dynamically generated prime numbers and varying elliptic curve base points.
- Additional analysis has been added to demonstrate MECC's effectiveness against Local File Inclusion vulnerabilities during key exchange.

- **Proposition 1:** The proposed key exchange protocol ensures forward secrecy under the assumption that the Elliptic Curve Discrete Logarithm Problem (ECDLP) is hard.
- **Proposition 2:** Ciphertext indistinguishability under chosen ciphertext attack is preserved by incorporating randomization and message integrity checks.
- **Proposition 3:** Resistance to pattern analysis is achieved through key dependent transformation and randomized encryption parameters.

Table 7. Comprehensive table of notations.

Notation	Description
PN_{user}	Private key for the user
Q_{user}	Public key of user
PN_{ebank}	Private key for the financial sector
Q_{ebank}	Public key of financial server
P_{mecc}	Point on the curve with coordinates (x, y)
N_{max}	Maximum order of the base points
Q_{mecc}	Prime number
V_{data}	Input data file
$C1_{user}$	Ciphertext components
$C2_{user}$	Ciphertext components
MDF_{user}	E-banking Data Files
HDS_{ebank}	Financial Database Server
N_{user}	Number of users
KEY_{user}	Keys from the users
HDS_{key}	Encrypted keys
HDS_{data}	Encrypted data files
KGP_{mecc}	Set of points generated on the curve

Table 7 presents the definitions of the symbols that are to be employed in the suggested algorithms. This is in notations of cryptographic operations, keys, input, output parameters and of intermediate values.

7. Conclusion

This research has introduced an innovative multi-party authentication technique designed to significantly enhance data security and provide robust protection against cyber attacks. The suggested technique takes advantage of altered cryptography protocols and new key distribution techniques to deal with the weaknesses of legacy authentication systems. The proposed method provides protection to sensitive information within distributed networks where unauthorized access and malicious activities are widespread. The work introduces a new approach to key generation that is based on the Modified Elliptic Curve Cryptography technique. The methodology offers effective protection of key generation and transformation towards authentication. It presents a strong encryption and decryption algorithms based on MECC to enhance the security of the transformation of data. Additionally, the MECC approach is compared with the classical ECC approach. The findings of the comparison reveal that the proposed methodology is less time consuming and safe compared favorably to the traditional ECC methodology. This novel methodology has been a success to strengthen the security backups of the multiparty authentication and data transformation in the financial domain.

Moreover, the proposed security plan plays an important part in enhancement of security of financial sectors. The cryptanalysis of the suggested methodology guarantees that there are no pattern analysis attacks and chosen ciphertext attacks in MECC techniques. Furthermore, the proposed security strategy focuses on the secure delivery of keys within the financial sector. The security strategy of encryption and decryption prevents local file inclusion attacks in the financial sector. This includes a proactive strategy to mitigate local file inclusion attacks, ensuring comprehensive protection of financial data against diverse threats. One of the possible future paths of the research is looking at how a dynamic security measure can be developed through the lens of a machine learning based approach. It has the capability to evolve automatically to meet the developing threat levels and the dynamic work environment within the financial authentication systems. It is possible to strengthen the proposed MECC technique with the emerging security paradigms, including blockchain technology, zero knowledge proofs, and post quantum cryptography. Such integrations have the

promise of reinforcing the system in a substantial manner in terms of resilience, scalability and resistance to future and highly advanced threats.

Conflicts of Interest
The authors confirm that this article's contents have no conflict of interest.

Acknowledgments
The authors would like to acknowledge there are no financial support funds.

AI Disclosure
The author(s) declare that no assistance is taken from generative AI to write this article.

References

Akraam, M., Rashid, T., & Zafar, S. (2024). A novel and secure image encryption scheme based on two-dimensional logistic and Arnold Cat map. *Cluster Computing, 27*(2), 2029-2048. https://doi.org/10.1007/s10586-023-04084-w.

Avkurova, Z., Gnatyuk, S., Abduraimova, B., & Makulov, K. (2024). Targeted attacks detection and security intruders identification in the cyber space. *International Journal of Computer Network and Information Security,16*(4), 144-153. https://doi.org/10.5815/ijcnis.2024.04.10.

Bhavsar, R., Dave, M., Shah, P., Joshiyara, H.A., &, Patel, C. (2024). Enhancing data security in banking: the power of hybrid algorithm-based solutions. *Journal of Electrical Systems, 20*(10), 1093-1102. https://doi.org/10.52783/jes.5208.

Braeken, A. (2022). Public key versus symmetric key cryptography in client–server authentication protocols. *International Journal of Information Security*, *21*(1), 103-114. https://doi.org/10.1007/s10207-021-00543-w.

Chandrika, S.U., & Perumal, T.P. (2022). Modified ECC for Secure data transfer in multi-tenant cloud computing. *International Journal of Computer Network and Information Security*, *14*(6), 76-88. https://doi.org/10.5815/ijcnis.2022.06.06.

Dawahdeh, Z.E., Almaiah, M.A., Alkhdour, T., Lutfi, A.W., Aldhyani, T.H.H., & Bsoul, Q. (2024). A new modified grayscale image encryption technique using elliptic curve cryptosystem. *Journal of Theoretical and Applied Information Technology*, *102*(7), 3225-3239.

Deshpande, V., Khubalkar, D., Dhablia, A., Pasha, M.J., Dhabliya, D., & Gandhi, Y. (2024). Enhancing financial transaction security with lightweight cryptographic algorithms. *Journal of Discrete Mathematical Sciences Cryptography, 27*(2-B), 741-751. https://doi.org/10.47974/JDMSC-1924.

Devarajan, M., & Sasikaladevi, N. (2020). A secured signcryption scheme for e-payment system using hyper elliptic curve. *Journal of Intelligent & Fuzzy Systems: Applications in Engineering and Technology, 39*(6), 8237-8247. https://doi.org/10.3233/JIFS-189144.

Ganavi, M., & Prabhudeva, S. (2023). Two-layer security of images using elliptic curve cryptography with discrete wavelet transform. *International Journal of Computer Network and Information Security, 12*(2), 31-47. https://doi.org/10.5815/ijcnis.2023.02.03.

Goswami, C., Selvi, P.T., Sreenivas, V., Seetha, J., Kiran, A., Talasila, V., & Maithili, K. (2023). Retracted article: securing healthcare big data in industry 4.0: cryptography encryption with hybrid optimization algorithm for IoT applications. *Optical and Quantum Electronics, 56*(3), 366. https://doi.org/10.1007/s11082-023-05672-1.

Gowshik, M., Kumar, V.P.A., Muthukumaran, N., Boopathy, K.A., & Gokulnath, D. (2024). Lightweight security system for bank and ATM. In *2024 International Conference on Science Technology Engineering and Management* (pp. 1-5). IEEE. Coimbatore, India. https://doi.org/10.1109/ICSTEM61137.2024.10561138.

Haldar, B., & Jha, P.K. (2023). Securing mobile robots multi-party authentication technique using modified elliptic curve cryptography. In *2023 International Conference on Advanced Computing & Communication Technologies* (pp. 104-109). IEEE. Banur, India. https://doi.org/10.1109/ICACCTech61146.2023.00025.

Haldar, B., Jha, P.K., & Mukherjee, P.K., (2024a). An efficient multiuser authentication and data transformation technique for smart agriculture using cryptography. *International Journal of Intelligent Systems and Applications in Engineering, 12*(4), 3087-3100. https://ijisae.org/index.php/IJISAE/article/view/6802.

Haldar, B., Mukherjee, P.K., & Saha, H.N. (2024b). A robust security strategy using hybrid cryptography approach to protect data in the financial sector. *International Journal of Computer Networks and Application, 11*(6), 749-773. https://doi.org/10.22247/ijcna/2024/46.

Haldar, B., Mukherjee, P.K., & Saha, H.N. (2024c). An approach of modified IDEA with 1024 bits key to enhance security and efficiency of data transmission in the healthcare sector. *International Journal of Mathematical, Engineering and Management Sciences, 9*(6), 1453-1482. https://doi.org/10.33889/IJMEMS.2024.9.6.078.

Idrissi, H., & Palmieri, P. (2024). Agent-based blockchain model for robust authentication and authorization in IoT-based healthcare systems. *The Journal of Supercomputing, 80*(5), 6622-6660. https://doi.org/10.1007/s11227-023-05649-7.

Karim, N.A., Khashan, O.A., Kanaker, H., Abdulraheem, W.K., Alshinwan, M., & Al-Banna, A.K. (2024). Online banking user authentication methods: a systematic literature review. *IEEE Access, 12*, 741-757. https://doi.org/10.1109/ACCESS.2023.3346045.

Kavitha, S., Alphonse, P.J.A., & Reddy, Y.V. (2019). An improved authentication and security on efficient generalized group key agreement using hyper elliptic curve based public key cryptography for IoT health care system. *Journal of Medical Systems, 43*(8), 260. https://doi.org/10.1007/s10916-019-1378-2.

Kumar, D., & Kumar, M. (2024). Hybrid cryptographic approach for data security using elliptic curve cryptography for IoT. *International Journal of Computer Network and Information Security, 16*(2), 42-54. https://doi.org/10.5815/ijcnis.2024.02.04.

Kumar, K.P., Prathap, B.R., Thiruthuvanathan, M.M., Murthy, H., & Pillai, V.J. (2024). Secure approach to sharing digitized medical data in a cloud environment. *Data Science and Management, 7*(2), 108-118. https://doi.org/10.1016/j.dsm.2023.12.001.

Kumar, V., Ray, S., Dasgupta, M., & Khan, M.K. (2021). A pairing free identity based two party authenticated key agreement protocol using hexadecimal extended ASCII elliptic curve cryptography. *Wireless Personal Communications, 118*(4), 3045-3061. https://doi.org/10.1007/s11277-021-08168-x.

Lawal, O.M., Vincent, O.R., Agboola, A.A.A., & Folorunso, O. (2021). An improved hybrid scheme for e-payment security using elliptic curve cryptography. *International Journal of Information Technology, 13*(1), 139-153. https://doi.org/10.1007/s41870-020-00517-6.

Ma, R., & Du, L. (2022). Attribute-based blind signature scheme based on elliptic curve cryptography. *IEEE Access, 10*, 34221-34227. https://doi.org/10.1109/ACCESS.2022.3162231.

Madje, U.P., & Pande, M.B. (2024). A conceptual model of quantum cryptography techniques used to provide online banking transactions security. In *2024 International Conference on Trends in Quantum Computing and Emerging Business Technologies* (pp. 1-5). IEEE. Pune, India. https://doi.org/10.1109/TQCEBT59414.2024.10545237.

Malathi, D., & Sasikaladevi, N. (2020). Biometric based three-factor mutual authentication scheme for electronic payment system using elliptic curve cryptography. *Malaysian Journal of Computer Science*, *2020*(1), 39-60. https://doi.org/10.22452/mjcs.sp2020no1.4.

Nikooghadam, M., & Amintoosi, H. (2020). A secure and robust elliptic curve cryptography-based mutual authentication scheme for session initiation protocol. *Security and Privacy, 3*(1), e92. https://doi.org/10.1002/spy2.92.

Okediran, T.M., Vincent, O.R., Abayomi-Alli, A.A., & Adeniran, O.J. (2024). Securing the perceptual layer of E-payment-based internet of things devices using elliptic curve cryptography over binary field. *The Journal of Supercomputing, 80*(15), 21592-21614. https://doi.org/10.1007/s11227-024-06270-y.

Oo, L.L. (2023). Development of online banking system based on secure captcha image using visual cryptography. In *2023 IEEE Conference on Computer Applications* (pp. 232-236). IEEE. Yangon, Myanmar. https://doi.org/10.1109/ICCA51723.2023.10181735.

Pandey, K., & Sharma, D. (2025). Digital content security by butterfly and elliptic curve cryptography with channel optimization. *International Journal of Mathematical, Engineering and Management Sciences, 10*(1), 76-91. https://doi.org/10.33889/IJMEMS.2025.10.1.005.

Patnaik, A., & Prasad, K.K. (2023). Secure authentication and data transmission for patients healthcare data in internet of medical things. *International Journal of Mathematical, Engineering and Management Sciences*, *8*(5), 1006-1023. https://doi.org/10.33889/IJMEMS.2023.8.5.058.

Prabakaran, D., & Ramachandran, S. (2022). Multi-factor authentication for secured financial transactions in cloud environment. *CMC-Computers, Materials & Continua, 70*(1), 1781-1798. https://doi.org/10.32604/cmc.2022.019591.

Sahoo, S.S., Mohanty, S., & Majhi, B. (2021). A secure three factor based authentication scheme for health care systems using IoT enabled devices. *Journal of Ambient Intelligence and Humanized Computing, 12*(1), 1419-1434. https://doi.org/10.1007/s12652-020-02213-6.

Shukla, S., & Patel, S.J. (2024). A design of provably secure multi-factor ECC-based authentication protocol in multi-server cloud architecture. *Cluster Computing, 27*(2), 1559-1580. https://doi.org/10.1007/s10586-023-04034-6.

Shyaa, G.S., & Al-Zubaidie, M. (2023). Utilizing trusted lightweight ciphers to support electronic-commerce transaction cryptography. *Applied Sciences, 13*(12), 7085. https://doi.org/10.3390/app13127085.

Timouhin, H., Amounas, F., & Azrour, M. (2023). New ECC-based IoT authentication protocol for securing RFID systems. *SN Computer Science, 4*(6), 785. https://doi.org/10.1007/s42979-023-02220-2.

Tiwari, D., Mondal, B., Singh, S.K., & Koundal, D. (2023). Lightweight encryption for privacy protection of data transmission in cyber physical systems. *Cluster Computing, 26*(4), 2351-2365. https://doi.org/10.1007/s10586-022-03790-1.

Trung, M.M., Do, L.P., Tuan, D.T., Tanh, N.V., & Tri, N.Q. (2023). Design a cryptosystem using elliptic curves cryptography and Vigenère symmetry key. *International Journal of Electrical and Computer Engineering*, *13*(2), 1734-1743. https://doi.org/10.11591/ijece.v13i2.pp1734-1743.