2025 5th International Conference on Mobile Networks and Wireless Communications (ICMNWC)

# Privacy-Preserving Elliptic-Curve with Proxy Re-Encryption Scheme and ABAC for Smart-Contract-based Healthcare

1st Kumar. M P
*Department of Computer Science*
*VELS Institute of Science, Technology and Advanced Studies (VISTAS)*
Pallavaram, Chennai, India
Kumarmp.mca@gmail.com

2nd Akila. A
*Department of Computer Science and Information Technology*
*VELS Institute of Science, Technology and Advanced Studies (VISTAS)*
Pallavaram, Chennai, India
akila.scs@velsuniv.ac.in

***Abstract*—In recent years, the adoption of advanced technologies in the healthcare sector and Electronic Health Records (EHRs) plays a significant role in the management of healthcare data. However, ensuring accessibility, patient privacy, and data security remains a challenge. To address these challenges, this research provides a novel privacy-preserving technique called EPPA that integrates access control, anonymization, and patient consent management by utilizing smart contracts in blockchain techniques. The proposed system employs Elliptic Curve Cryptography (ECC) combined with Proxy Re-Encryption (PRE) and a Public Key Infrastructure (PKI) is integrated to ensure data security and secure key distribution. Attribute-Based Access Control (ABAC) is employed to maintain access controls. Subsequently, PKI improves authentication and certificate management. The performance analysis shows that the proposed EPPA technique achieves lower encryption and decryption times. The proposed technique obtains an encryption time of 0.025s and a decryption time of 0.120s for 10 MB files, which shows higher efficiency and improved processing. The proposed technique provides a secure and computationally effective privacy-preserving technique for healthcare EHR data.**

***Keywords—decryption, encryption, electronic health records, elliptic curve cryptography, public key infrastructure, proxy re-encryption.***

## I. INTRODUCTION

Recently, the healthcare sector has been facing a significant paradigm shift by including advanced technologies. Electronic Health Records (EHRs) play a significant role in storing and managing patient data [1]. EHRs consist of details about patients to identify patient risk factors, validate the effectiveness of treatments, and understand disease patterns. EHR data help researchers understand more accurate and detailed views of patients than traditional paper records [2]. The EHRs are stored in a public cloud for effective access control at minimum cost and to enable multi-user accessibility. However, data security remains a major concern when cloud storage is used for EHRs [3]. To overcome the above challenges, blockchain technologies are utilized, which effectively secure patient data and ensure transparent and untampered access control. Blockchain techniques are used because of their immutable, decentralized, and secure nature [4]. Blockchain consists of various properties, such as immutability, privacy, tamper-proofing, confidentiality, traceability, and data integrity, without any third-party applications [5].

Homomorphic encryption (HE) is an effective cryptography technique that allows processing on encrypted data without any decryption process. Without any encryption or decryption process, addition and multiplication are performed in the HE technique [6]. Attribute-Based Encryption (ABE) technique is utilized to fullfill fine-grained requirements because of its one-to-many encryption characteristics and attribute-based policy control. However, ABE depends on bilinear pairing operations, which require high computational overhead and lead to bottlenecks in encryption at the end of the Data Owners (DOs). The Proxy Re-Encryption (PRE) technique is improved to delegate complex re-encryption operations to a cloud proxy server, which helps data owners perform initial encryption and reduces the burden on the data owner [7]. The Elliptic Curve Cryptosystem (ECC) is an asymmetric encryption technique, which depends on the limitation of the Elliptic Curve Discrete Logarithm Problem (ECDLP) [8]. ECC is utilized for higher security with a small key, provides better performance, and reduces resource consumption. The ECC technique has been rapidly developed and utilized in various fields, such as smart home systems, healthcare, and vehicle devices [9]. Attribute-Based Access Control (ABAC) is considered a more suitable and better solution. Access decisions in ABAC are based on environmental attributes and different subjects [10].

The main contributions of this research are described below:

- An ECC-PRE-based encryption technique is developed to minimize the re-encryption on data by converting the encryption process into a proxy environment. This integration of the PRE improves key confidentiality and prevents the exposure of private keys.
- The EPPA technique employs ABAC technique to provide flexibility and context-aware authorization. The ABAC technique dynamically validates different attributes, such as user identity, device, access time, and environment.
- A secure smart contract is employed to ensure immutable, traceable access to EHR data, which improves trust in multi-institution sharing. The smart contract provides consent rules and access policies without any third-party intervention.

The related work of privacy-preserving techniques in healthcare data is explained in Section 2. Section 3 explains the EPPA technique, and Section 4 shows the validation and results of the proposed technique with different encryption techniques. Finally, Section 5 concludes the proposed technique.

979-8-3315-5664-8/25/$31.00 ©2025 IEEE

## II. Related Works

The related works below explain the capabilities and limitations of different privacy-preserving techniques using cryptography and blockchain for EHR data.

Narendra Kumar et al. [11] developed a privacy-preservation scheme based on a decentralized blockchain for enhancing healthcare data security in the cloud. The Edward Curve Digital Signature Algorithm (EdDSA) with the SHA-256 hashing function was employed to improve authenticity. Subsequently, a modified Menezes-Vanstone-based Elliptic Curve ElGamal Encryption Scheme (MMV-ECE) was employed to secure data encryption and robust protection. Later, the Inter Planetary File System (IPFS) was utilized to store encrypted data for scalable and decentralized off-chain storage. However, the MMV-ECCE technique struggles to handle unstructured and variable network conditions in healthcare data.

Dhina Suresh and M.Lilly Florence et al. [12] introduced a User Usage-Based Encryption (UUBE) scheme for securing personal health records. UUBE was an access-control technique based on a searchable encryption scheme, and the UUBE usage was mapped as credentials with time allotment to each event. Subsequently, data users were able to decipher an event if and only if there was a match between the credential and the accreditation related to the event. However, the UUBE technique shows leakage in user-related data because of semantic clustering, and reducing overall privacy encryption.

Chandra Sekhar Tiwari and Vijay Kumar Jha [13] developed a privacy-preserving technique using smart contract creation to secure cloud data. Initially, Twisted Hessian Curve-based Digit Folding Elliptic Curve Cryptography (THC-DFECC) was utilized for securing data. Later, the DOs was utilized to create a Smart Contract (SC), and the Gini Canberra-k-anonymity (GC-k-anonymity) was utilized to protect the SC data. However, the THC-DFECC technique is limited to SSL/TLS certificate validation, which leads to reduced end-to-end communication security.

Jhuma Dutta and Subhas Barman [14] designed a blockchain and smart contract-based secure approach for securing and storing EHR data. Initially, the Inter Planetary File System (IPFS) was employed to store a large number of medical records in cloud storage. Subsequently, the Ethereum platform was used to execute transactions by utilizing smart contracts in Solidity. However, the IPFS technique generates multiple fake identities, falsifying block validation and reducing overall data trust and security.

Ganesh Kumar Mahato et al. [15] introduced a Privacy-Preserving Verifiable Federated Learning (PPVFL) technique utilizing blockchain and homographic encryption. Initially, the Elliptic Curve Digital Signature Algorithm (ECDSA) and Byzantine fault tolerance were employed to improve the system security against data tampering and malicious attacks. The enhancement in PPVFL techniques combines homographic encryption and blockchain with federated learning. However, the PPVFL technique introduces communication delays because of strict privacy-preserving operations, leading to reduction in the overall performance.

The above related works explain various cryptographic encryption techniques that are used for effective and efficient privacy-preserving techniques.

## III. Proposed Methodology

The proposed methodology explains the novel EPPA techniques used to perform operations such as, Cloud data center, DOs, and Data Users (DUs). The proposed EPPA techniques, which effectively secure cloud data, are briefly explained in this section. The EPPA technique is represented in Figure 1.

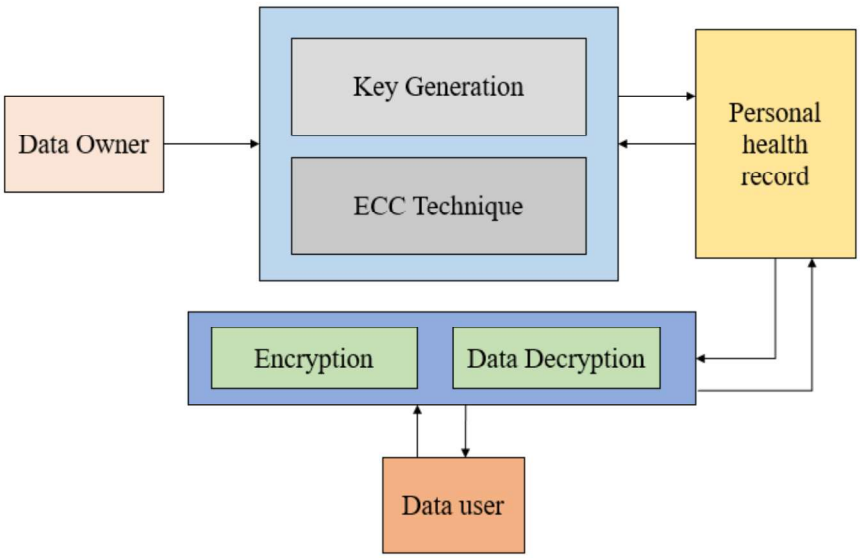


Fig. 1. Architecture of the EPPA technique, which contains the cloud data center, key generation, DOs, and Dus

### A. System model

This section explains the access control model for the three entities of the healthcare data system.

*1) Data owner:* Dos helps to store data in a cloud environment, and the healthcare data are stored in a third-party cloud server. Healthcare data are encrypted by utilizing

cryptographic encryption techniques, namely ECC encryption techniques with multi-user settings.

*2) Data user:* DUs help in creating a space for searching personal healthcare data by utilizing the institution as a key by DOs. After receiving the request from DUs, the data center computes the encrypted keyword search in the healthcare data and provides the related details as an outcome in a decrypted or encrypted form.

*3) Cloud data center:* The cloud data center is utilized to perform search, delete, and store operations in the healthcare data after access construction and key generation to construct key pairs for data encryption. A usage-based encryption technique is utilized to access data outsourced to cloud-based DUs.

## IV. Elliptic Curve Cryptography

ECC is a contemporary and effective public-key cryptographic technique, which is renowned for its efficiency and is represented in Equation (1).

$$y^2 = x^3 + ax + b \tag{1}$$

Where $a$ and $b$ are constants. ECC has various advantages when compared with other cryptography techniques such as RSA and ECC algorithms, which achieves higher security when using minimum key sizes. This characteristic in ECC makes it suitable for resource-constrained platforms, such as embedded systems and mobile devices, where storage capacity and computational power are major considerations. ECC security relies on resolving challenges in the Elliptic Curve Discrete Logarithm Problem (ECDLP). Challenges arise when determining the $k$ integer when provided with a point L on the scalar multiplication $k * L$.

### A. ECC with PRE

In this technique, PRE is performed by employing an ECC-based encryption technique, and the key intent of PRE is to preserve the integrity and privacy of healthcare data stored in the blockchain. ECC is an effective technique for public-key cryptography. This technique is implemented by considering a curve with base points and a prime number function.

The numerical expression of the ECC is given in Equation (2).

$$u^2 = c^3 + sc + n \tag{2}$$

Where the variables s and $n$ signify the integer values.

*1) Key generation:* The public key W is generated by performing scalar multiplication of the private key $J$ and base point $Q$, as shown in Equation (3).

$$W = J \times Q \tag{3}$$

*2) Encryption and decryption procedure:* During encryption, the input data $Q_m$ from sender $A$ are transferred to recipient B, and the ciphertext $Q_V$ is presented as shown in Equation (4).

$$Q_V(1H, Q_m + 1Q_B) \tag{4}$$

Where the term 1 represents a random variable and $Q_B$ represents the public key of recipient $B$, which is obtained by integrating the private key $M_B$ of recipient $B$, as shown in Equations (5) and (6).

$$Q_B = M_B H \tag{5}$$

$$Q_m + 1Q_B - (1H \times M_B) \tag{6}$$

Subsequently, at the recipient end $B$, the ciphertext $Q_V$ is decrypted to retrieve the initial data $Q_m$. Therefore, during the decryption process, the $c^{th}$ coordinate of the ciphertext $Q_V$ is multiplied by the private key of recipient $B$ and then subtracted from the $u^{th}$ coordinate of the ciphertext $Q_V$, as explained in Equation (7).

$$Q_m + 1Q_B - (1Q_B) = Q_m \tag{7}$$

Therefore, recipient $B$ securely obtains the data transferred by sender $A$. The ECC encryption technique ensures better security for transmitted data with a smaller key size key size compared to other traditional encryption techniques.

*3) Secure smart contract:* The Smart Contract (SC) is created by the DO using optimized attributes from $R$ for data in the selected file. The SC manages the transfer of digital details between the DU and DO under certain conditions. The SC data are stored and hashed for the verification process to access data by the DU, making the information more secure .

*4) Attributes extraction:* The attributes from the uploaded data are collected to construct the smart contract. Based on the domain, the attributes of the data are differentiated accordingly. Moreover, extracted attributes (F) are represented in Equation (8).

$$F = [F^1, F^2, F^3, \dots F^M], \text{ where } j = 1,2,3, \dots M \tag{8}$$

Where $F^M$ represents the $M^{th}$ attribute and $j$ denotes the attribute number. After creating the SC, SC data ($\Gamma$) are secured from attacks, which may result in a congested network that allows attackers to crash the contract.

### B. Attribute-Based Access Control (ABAC)

The ABAC technique implements policies that specify attributes such as environment, permission, subject, and resources. ABAC is a secure and flexible access-control policy computation. The ABAC policy $A = (S, R, E, P)$ contains four attributes that are utilized to define every entity utilized for authorization in ABAC. Every attribute $X$ has a key-value pair, $X = \{key: value\}$.

Where value = manager, key = role.

The attributes are described as follows:

- S = (ID, group, roles) shows the subject attribute, which contains general properties of userssuch as user roles, user group, and user ID.
- R = (device ID, MAC address) explains the resource attribute, such as the application or file that a subject wants to access. The resource data are associated with IoT device, MAC addresses, and IDs to track the stored data.

- E = (allowed IP, start time, end time) shows the environment attribute, such as an IP address or time limit of requested access. This attribute comprises three fields: allowed IP, end time (expiration time of policy), and start time (policy creation time). . The allowed IP field is utilized to protect the IP addresses outside the network from accessing system.
- P = (0 or 1) explains the permission attribute, which dictates whether the access is denied (0) or granted (1). The ABAC technique is integrated into particular situations by adding or removing attributes. Subsequently, an ABAC policy request is utilized to define the ability of the subject to access resources in a specific situation. The environment, resource, and subject are given as input parameters. When there is a request for a function call, it returns a Boolean value as output.

$$Rule: Can\ access\ (S,R,E) \leftarrow P\ (S,R,E) \qquad (12)$$

If $P = 1$, access is granted; otherwise, access is denied.

## V. Experimental Results

The performance of the proposed technique is evaluated using Python 3.2, and the system specifications include Windows 11, 128-bit OS, and Intel Core i7. The proposed method is validated through the response time, computation time, key generation time, encryption, and decryption time.

### A. Performance Analysis

Performance analysis of the EPPA technique validates the computation, key generation, decryption, and encryption times. Techniques include ABE, Homomorphic Encryption (HE), Ciphertext-Policy ABE (CP-ABE), ECC, and ECC-PRE.

TABLE I. Performance Analysis Of Encryption Time(S) With Different Techniques And Proposed EPPA For Different File Sizes In MB

| Method | File Size (MB) | | | | |
|---|---|---|---|---|---|
| | ***10*** | ***20*** | ***30*** | ***40*** | ***50*** |
| ABE | 0.831 | 1.644 | 2.486 | 3.313 | 4.139 |
| CP-ABE | 0.912 | 1.821 | 2.709 | 3.587 | 4.444 |
| ECC | 0.654 | 1.294 | 1.917 | 2.526 | 3.129 |
| HE | 1.132 | 2.284 | 2.284 | 4.515 | 5.612 |
| ECC-PRE | 0.611 | 1.231 | 1.832 | 2.439 | 3.033 |
| Proposed EPPA | 0.478 | 0.941 | 1.422 | 1.889 | 2.349 |

Table 1 presents the performance analysis of the proposed technique, which achieves lower encryption time for different file sizes. The EPPA technique is compared with existing techniques such as ABE, CP-ABE, ECC, HE, and ECC-PRE. The proposed technique shows better efficiency for large-scale encrypted data transmission in healthcare data. This improvement enhances computational efficiency and key management by utilizing ECC with PRE.

TABLE II. Performance Analysis Of Decryption Time(S) With Different Techniques And The Proposed EPPA For Different File Sizes In MB

| Method | File Size (MB) | | | | |
|---|---|---|---|---|---|
| | ***10*** | ***20*** | ***30*** | ***40*** | ***50*** |
| ABE | 0.714 | 1.417 | 2.145 | 2.853 | 3.558 |
| CP-ABE | 0.802 | 1.603 | 2.383 | 3.152 | 3.904 |
| ECC | 0.549 | 1.086 | 1.600 | 2.109 | 2.612 |
| HE | 1.009 | 2.034 | 3.027 | 4.013 | 5.002 |
| ECC-PRE | 0.512 | 1.029 | 1.517 | 2.012 | 2.506 |
| Proposed EPPA | 0.398 | 0.783 | 1.198 | 1.599 | 2.004 |

Table 2 shows the performance analysis of the proposed technique, which effectively achieves lower decryption time for all different file sizes. The proposed technique reduces computational overhead during message reconstruction by combining ECC with PRE. The ABE, CP-ABE, ECC, HE, and ECC-PRE techniques are compared with the proposed technique and this comparative analysis shows that the proposed technique obtained enhanced performance.

TABLE III. Performance Analysis Of Computational Time(S) With Different Techniques And The Proposed EPPA For Different File Sizes In MB

| Method | File Size (MB) | | | | |
|---|---|---|---|---|---|
| | ***10*** | ***20*** | ***30*** | ***40*** | ***50*** |
| ABE | 1.545 | 3.061 | 4.631 | 6.166 | 7.697 |
| CP-ABE | 1.714 | 3.424 | 5.092 | 6.739 | 8.348 |
| ECC | 1.203 | 2.380 | 3.517 | 4.635 | 5.741 |
| HE | 2.141 | 4.318 | 6.430 | 8.528 | 10.614 |
| ECC-PRE | 1.123 | 2.260 | 3.349 | 4.451 | 5.539 |
| Proposed EPPA | 0.876 | 1.724 | 2.620 | 3.488 | 4.353 |

Table 3 presents the performance analysis of the proposed technique, which obtains the lowest computational time across varying file sizes. Existing techniques show increased computation time as the file size grows. The proposed technique shows less computational efficiency for large-scale secure data processing and consists of cryptographic operations.

TABLE IV. Performance Analysis Of Key Generation Time(S) With Different Techniques And The Proposed EPPA For Different File Sizes In MB

| Method | File Size (MB) | | | | |
|---|---|---|---|---|---|
| | ***10*** | ***20*** | ***30*** | ***40*** | ***50*** |
| ABE | 0.212 | 0.214 | 0.217 | 0.220 | 0.224 |
| CP-ABE | 0.268 | 0.273 | 0.277 | 0.282 | 0.288 |
| ECC | 0.043 | 0.045 | 0.047 | 0.049 | 0.052 |
| HE | 0.905 | 0.925 | 0.948 | 0.972 | 0.997 |
| ECC-PRE | 0.057 | 0.060 | 0.063 | 0.066 | 0.070 |
| Proposed EPPA | 0.032 | 0.033 | 0.034 | 0.036 | 0.037 |

Table 4 presents the performance analysis of the proposed technique, which achieves lower key generation time across all file sizes. Techniques such as ABE, CP-ABE, ECC, HE, and ECC-PRE are used for comparison. The proposed technique generates compact keys with minimal dependency on file size and performs effectively in large-scale encryption systems. The elliptic-curve operations effectively minimize the computation of the technique.

### B. Comparative Analysis

This comparative analysis evaluates the EPPA technique with different privacy-preserving techniques to analyze the efficiency of the proposed technique.

Table 5 explains the comparative analysis of the proposed EPPA technique, which shows better performance than the UUBE technique. The proposed technique shows enhanced efficiency in handling key generation and computational processes. The proposed technique effectively manages healthcare data while maintaining high security and faster access. It shows lower decryption and encryption time of

124ms and 111ms for the 150GB dataset. For this comparative analysis, 150GB of healthcare data are used, and the EPPA technique validates and obtains the encryption and decryption time.

TABLE V. COMPARATIVE ANALYSIS WITH DATASET SIZE OF 150 GB USING THE PROPOSED EPPA

| Method | Encryption time (ms) | Decryption time (ms) |
|---|---|---|
| UUBE [9] | 180 | 160 |
| Proposed EPPA | 124 | 111 |

TABLE VI. COMPARATIVE ANALYSIS OF THE EPPA TECHNIQUE WITH THE MMV-ECE ENCRYPTION ALGORITHM

| Method | Encryption time (s) | Decryption time (s) |
|---|---|---|
| MMV-ECE [11] | 0.035 | 0.167 |
| Proposed EPPA | 0.025 | 0.120 |

Table 6 presents the proposed EPPA technique, which achieves lower encryption and decryption times of 0.025s and 0.120s, respectively. Effective key management in the proposed technique is achieved by employing EEC with the PRE technique. This comparative analysis shows the effectiveness of the proposed technique, which performs faster processing without compromising security and effectively handles large-scale healthcare data protection.

### C. Discussion

The advantages and limitations of the proposed EPPA technique are discussed in this section. The proposed technique shows better performance in securing data and computational efficiency for healthcare data security. It shows improved performance in terms of key generation, decryption, encryption, and computation times. Techniques such as ABE, CP-ABE, ECC, HE, and ECC-PRE are compared with the proposed encryption technique. The experimental results confirm that the proposed technique achieves lower encryption time and faster decryption performance. The proposed integration of ECC with PRE and ABAC provides strong cryptographic security with smaller key sizes and reduces computational overhead. The PRE technique is utilized to secure re-encryption by hiding private keys, which enhances data security and multi-user accessibility. The ABAC technique ensures fine-grained and flexible access control, enabling secure policy enforcement for healthcare data. Moreover, the proposed EPPA technique efficiently improves security strength, which is essential for handling large Electronic Health Records (EHRs) in healthcare systems.

## VI. CONCLUSION

In this research, EPPA is proposed for securing healthcare data using encryption and decryption techniques. The proposed technique consists of ECC with PRE, and ABAC is employed to ensure data security and reduce computational complexity. The experimental analysis of the proposed EPPA technique shows better performance than the existing encryption schemes such as ABE, CP-ABE, ECC, HE, and ECC-PRE in encryption, decryption, key generation, and computational time. Comparative analysis with the UUBE [9] and MMV-ECE [11] techniques obtains lower encryption and decryption times, even for larger healthcare data. The proposed EPPA technique attains an encryption time of 0.25s and a decryption time of 0.120s for 10 MB files, which outperforms existing encryption techniques. Moreover, the proposed EPPA technique provides an efficient solution for privacy-preserving healthcare data sharing. In the future, cryptographic encryption can be extended by integrating dynamic access policy updates in distributed healthcare networks to enhance adaptability and resilience.

## REFERENCES


[1] A. A. Ali, M. A. Gunavathie, V. Srinivasan, M. Aruna, R. Chennappan, and M. Matheena, "Securing electronic health records using blockchain-enabled federated learning for IoT-based smart healthcare," Clinical eHealth, vol. 8, pp. 125–133, December 2025.

[2] K. Meduri, G. S. Nadella, A. R. Yadulla, V. K. Kasula, M. H. Maturi, S. Brown, S. Satish, and H. Gonaygunta, "Leveraging federated learning for privacy-preserving analysis of multi-institutional electronic health records in rare disease research," Journal of Economy and Technology, vol. 3, pp. 177–189, November 2025.

[3] J. A. Babu, S. Patil, B. D. Parameshachari, S. Rinaldi, K. R. Balmuri, and K. L. Hemalatha, "Blockchain enabled hybrid cryptographic algorithm for security and privacy preservation of electronic health records," ICT Express, vol. 11, pp. 945–950, October 2025.

[4] S. Alahmari, A. Alshardan, F. N. Al-Wesabi, S. Sorour, O. Alghushairy, R. Alsini, A. O. Khadidos, and M. Al Duhayyim, "A decentralized and privacy-preserving framework for electronic health records using blockchain," Alexandria Eng. J, vol. 126, pp. 196–203, July 2025.

[5] A. Tomar, N. Gupta, D. Rani, and S. Tripathi, "Blockchain-assisted authenticated key agreement scheme for IoT-based healthcare system," Internet Things, vol. 23, p. 100849, October 2023.

[6] K. Saeed and M. F. Adak, "Secured cloud-based image data processing of self-driving vehicles using full homomorphic encryption," Kuwait Journal of Science, vol. 52, p. 100449, October 2025.

[7] Z. Li and G. Shi, "A CCA-secure puncturable attribute-based proxy re-encryption scheme," IEEE Internet Things J, vol. 12, pp. 47679–47690 August 2025.

[8] X. Zhang and X. Wang, "Digital image encryption algorithm based on elliptic curve public cryptosystem," IEEE Access, vol. 6, pp. 70025–70034, November 2018.

[9] Y. Jiang, J. Zhang, A. Wang, Y. Hao, J. Wang, Z. Chen, and L. Zhu, "Low-latency and area-efficient elliptic curve point multiplication architectures over Koblitz curves," IEEE Internet Things J, vol.12, pp. 27144–27159, April 2025.

[10] A. Punia, P. Gulia, N. S. Gill, U. K. Lilhore, S. Simaiya, R. Alroobaea, H. Alsufyani, and A. M. Baqasah, "QuickMedBlock: A framework for enhanced attribute-based access control using blockchain for EHR in cloud," Peer-to-Peer Networking Appl, vol. 18, p. 258, July 2025.

[11] N. Kumar, S. Kumar, R. K. Sharma, R. Sharma, and K. Tomar, "A decentralized blockchain-based privacy preservation scheme for healthcare data security enhancement in cloud," Cluster Comput, vol. 28, p. 546, May 2025.

[12] D. Suresh and M. L. Florence, "Securing personal health record system in cloud using user usage based encryption," Journal of medical systems, vol. 43, p. 171, May 2019.

[13] C. S. Tiwari and V. K. Jha, "THC-DFECC-based privacy preserved smart contract creation for cloud data security," Int. J. Inf. Technol, vol. 16, pp. 4191–4207, June 2024.

[14] J. Dutta and S. Barman, "Smart contract and blockchain-based secured approach for storing and sharing electronic health records," Multimedia Tools Appl, vol. 84, pp. 16883–16907, July 2024.

[15] G. K. Mahato, A. Banerjee, S. K. Chakraborty, and X. Z. Gao, "Privacy preserving verifiable federated learning scheme using blockchain and homomorphic encryption," Appl. Soft Comput, vol. 167, p. 112405, December 2024.