Journal of Computer Science

Original Research Paper

Block chain based Privacy-Preserving Authentication and Key Verification using PBDS Framework

M. P. Kumar [1], A. Akila[2]

[1] *Department of Computer Science, VELS Institute of Science, Technology and Advanced Studies (VISTAS), Chennai, India;*
[2] *Department of Computer Science and Information Technology, VELS Institute of Science, Technology and Advanced Studies (VISTAS), Chennai, India.*

Article history
Received: 14 November 2025
Revised: xx August 20xx
Accepted: xx September 20xx

*Corresponding Author: M. P. Kumar, *Department of Computer Science, VELS Institute of Science, Technology and Advanced Studies (VISTAS), Chennai, India*;
Email:Kumarmp.mca@gmail.com

Abstract: The blockchain based Industrial Internet of Things (IIoT) system enables secure data sharing by preserving user privacy through decentralization and cryptographic methods. It provides privacy by protecting data during transmission and by allowing only authorized entities to communicate with IIoT networks. However, ensuring security and privacy in IIoT remains challenging. Traditional methods typically address only authentication and privacy, while static block chain consensus mechanisms introduce significant overhead and lack adaptive access control in dynamic environments. To overcome these challenges, this research proposes Password Based Key Derivation Function2 (PBKDF2) integrated with Blowfish Encryption (BE) and Hash Message along with Digital Signature named as PBDS. This method is associated with block chain, Zero Knowledge Proof (ZKP) are employed to prevent unauthorized access and ensure secure data sharing. PBDS provides adaptive and fine-grained access control, enabling various untrusted entities to flexibly and securely manage resources based on contextual information and policy rules. Experimental results show that the proposed PBDS achieves lower Encryption Time (ET) and Decryption Time (DT) of 6.4513s and 5.9836s respectively.

Keywords: Authentication; Block chain; Blowfish Encryption; Digital Signature; Hash Message Authentication Code; Zero Knowledge proof.

Introduction

Industrial Internet of Things (IIoT) devices include processors, software, transmitters and receivers for data processing and exchange over the Internet and communication channels (Alsuqaih et al., 2023). The Internet of Things (IoT) refers to a network in which various objects are connected for business applications without human intervention in digitized environment (Padma and Ramaiah, 2025). In healthcare, IoT-based medical equipment assisted in gathering of the patient information, automate workflows, generate an insight into disease patterns and indications while providing patients with better control over their health and medication (Tawfik et al., 2025). IIoT systems typically connect devices across multiple domains and platforms, transmitting data through different networks (Rao and Deebak, 2024). This complexity introduces cross domain access control challenges and increases vulnerability to attacks (Usman et al., 2024). Although traditional centralized security architectures in IIoT systems provide resilience against attacks and handles threats such as data breaches, network intrusions or identity spoofing, the efficiency of existing security solution remains limited (Luong and Park, 2023). IIoT and IIoT-enabled medical devices that monitor patient health conditions and have improved healthcare quality by enabling the transmission of health data to physicians via Internet (Liu et al., 2023). These IIoT devices are generally classified into low-level and high-level devices (Zhang et al., 2024).

In recent years, the convergence of blockchain technology and healthcare has shown a significant potential to reform how patients' Electronic Health Records (EHRs) data are managed, shared and utilized (Duggegowda and Rama moorthy, 2024). Block chain is

Science Publications

a decentralized technology that enables distributed authentication and mitigates security threats by eliminating the need for Centralized Authority (CA) (Vishwakarma et al., 2025). Its transparency and traceability further enhance the reliability of identity management (He et al., 2024). Smart healthcare systems extensively leverage communication technologies and interconnected electronic devices to improve healthcare service delivery and support automated healthcare processes (Liu et al., 2023). However, the sensitive and private nature of healthcare information demands advanced security mechanisms beyond traditional blockchain approaches to ensure integrity, confidentiality and patient-centric control (Morales et al., 2024). Existing cryptographic schemes such as Advanced Encryption Standard (AES) and asymmetric encryption have limitations in data sharing scenarios in medical records (Yin et al., 2022). These schemes often require a private-key exchange or full-record decryption to access specific data fields, which reduces overall system efficiency (Li et al., 2022). Blockchain-based distributed identity infrastructures facilitate digital identity management across providers (Wang et al., 2023). For privacy-preserving access to personal data, robust authentication mechanisms are required to prevent data forgery within supply chains while enabling secure communication among systems and entities (Bao et al., 2022). Blockchain platforms are therefore considered as a suitable foundation for privacy-preserving and secure data sharing due to their decentralization, auditability and unforgeability properties (Vatambeti et al., 2023). Despite these advantages, current e-healthcare systems still compromise patient privacy to achieve high quality medical services, especially in environments involving portable devices privacy requirements are increasing (Das et al., 2023).

The main contributions of this research are described in below:

- The proposed Password Based Key Derivation Function2 (PBKDF2) integrates with Blowfish Encryption (BE) and Hash Message along with Digital Signature named as PBDS which method is associated with block chain, Zero Knowledge Proof (ZKP) are used for privacy preserving authentication and verification in IIoT system.
- ZKP combined with HMAC-SHA 256 is used to preserve patient privacy while verifying entities, this integration ensures data integrity and confidentiality during the identity-checking process.
- Blowfish encryption is employed to secure Electronic Health Records (EHRs), providing fast encryption and decryption performance, which reduces processing time and support secure communication transmission.

The remainder of this paper is organized as follows: the next section presents the literature review of existing works, followed by a section describing the proposed methodology. This is then followed by a section discussing the experimental results, and finally, the concluding section summarizes the work.

Literature Review

Haritha and Anitha, (2023) implemented multi-level security in an e-healthcare system by integrating Lattice Based Access Control (LBAC) with a blockchain-based smart contract framework. LBAC provided multi-level protection by enforcing access control restrictions, while smart contracts were utilized to validate transaction procedure in a decentralized environment through agreements between users and parties. An Ethereum Virtual Machine (EVM) was employed to execute the smart contract to evaluates each user while accessed an authentication procedure in an envisioned model. In a blockchain, the patient e-health details were stored and accessed as immutable blocks.

Sharma et al., (2023) developed a Transient Key Congruential Generator- based Elliptic Curve Cryptography (TKCG-ECC) and a Dual-Keyed Cipolla Extended Euclidean (DKCEED)-based Lattice Cryptosystem (LC) for protecting a registered data. To manage the Block Chain Network (BCN), the gateway verified authorized users by employing a key-based Zero-Knowledge Proof (ZKP) and an Approximation Fully Homographic Encryption Neural Network (AFHENN)-based BCN.

Rao and Sujatha, (2023) introduced Hybrid Elliptic Curve Cryptography (HECC) for public-cloud security. The proposed HECC generated a key using a lightweight Edwards curve. A key-minimization procedure was applied to shorten the keys, and this process was further enhanced using the Advanced Encryption Standard (AES). In addition, a Diffie-Hellman key-exchange mechanism was performed for public key exchange.

Sharma et al., (2023) implemented a blockchain-based IoT architecture to improve the security of healthcare data by using an Identity Based Encryption (IBE) algorithm. The IoT-based distributed architecture relied on blockchain to protect large amounts of healthcare data. IBE was used to store healthcare information securely, while blockchain was

applied to handle EHR data manipulation or modification. In addition, smart contracts determined the core functions of the healthcare system, which were beneficial to all stakeholders.

Xiang and Zhao, (2022) introduced a blockchain-assisted Searchable Attribute Based Encryption (SABE) scheme for e-health systems. SABE was employed to achieve data authenticity, confidentiality, and fine-grained access control, while its integration with blockchain supported hidden access policies. In addition, a rigorous security-proof scheme was provided, which demonstrated security even under keyword-attack conditions.

Deebak et al., (2023) developed a Cloud-Assisted Decentralized Privacy-Preserving Framework (CA-DPPF) using block-chain along with Key Agreement (KA) mechanisms to achieve secure data privacy and storage. The in-depth security analysis ensured the operations of Healthcare Supply Chain Management (H-SCM) such as data immutability, integrity and traceability.

Proposed Methodology

In this research, the proposed PBDS scheme is used for privacy-preserving authentication and key-agreement-based access control in blockchain. In this research, EHR data (hospital clinicians, laboratory, pharmacy, and health-insurance data), public keys, private keys, hash functions, ciphertext, digital signing, and verification operations are connected within the block chain through secure data exchange. The proposed PBDS scheme operates in five phases, namely system model, PBKDF2, HMAC-SHA256, DAA, and Blowfish encryption. These phases are described in this section. Fig. 1 illustrates secure EHR data exchange using blockchain, PBKDF2 encryption, and HMAC-SHA-256 verification.

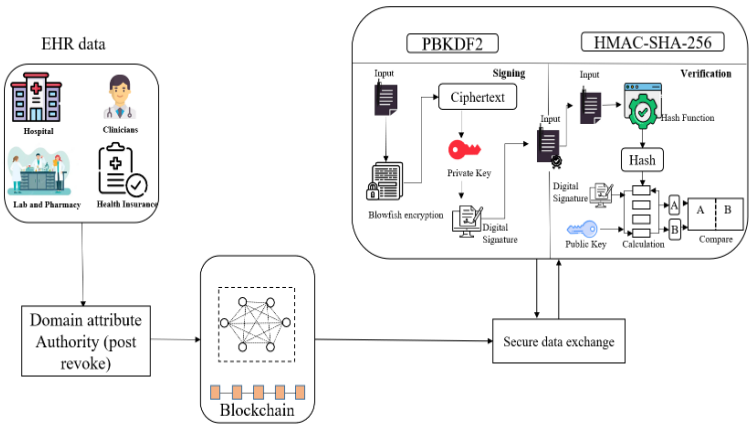

Fig. 1. Block chain enabled secure EHR sharing with blow fish encryption, digital signatures and HMAC-SHA 256 based verification

System Model

In this research, the proposed PBDS primarily functions within a signature scheme, which plays a crucial role in establishing the security framework of EHR. As healthcare data enhances, the cryptographic demand also improves, ensuring that the patient data remains significant within EHR and is protected from unauthorized access.

Workflow

In the primary stage, healthcare entities such as hospitals, laboratories, and pharmacies, health-insurance providers, and clinicians generate and register EHR data. The DAA handles user access and revocation, ensuring that only authenticated users are allowed to participate. PBKDF2 is used for secure cryptographic key derivation and Blowfish encryption is applied to convert EHR data into cipher text. A digital signature is generated to produce a private key and to establish secure connections within the system. Blockchain provides secure storage and transaction processing, where the encrypted EHR data associated with digital signatures are documented in the blockchain. Secure data storage prevents unauthorized access. For integrity verification, HMAC-SHA256 generates hash values that are compared against the original document during the data exchange. The blockchain framework ensures secure data transactions and enables trusted access control for data verification and exchange in authorized users. Public-key operations are combined with the HMAC-SHA256

hash function to evaluate digital signatures; by comparing the calculated hash results with the stored records, ensuring the validity and authenticity. This mechanism not only secures healthcare transactions but also protects against unauthorized access, thereby enabling secure data sharing.

Block chain

Blockchain is a decentralized system that records and manages transactions across multiple computers, where each block store transaction data. By using a decentralized model, blockchain enables secure data sharing for EHR data and patient information. In the healthcare domain, blockchain technology supports user access control, increases security, preserves data integrity and stores patient healthcare data. In this healthcare system, block chain is utilized to retrieve and manage data, and its adoption in healthcare applications highlights significant concerns regarding the security and privacy of patient information. Zero-Knowledge Proof (ZKP) protocols in blockchain allow one party, known as the prover, to prove to another party, known as the verifier, to verify that a statement is true or not without revealing any underlying information. This mechanism enhances privacy, security, and scalability in decentralized systems. ZKPs ensure that sensitive data, such as transaction amounts or identities, remain undisclosed while still validating correctness. In blockchain platforms, ZKP protocols such as zk-SNARKs and zk-STARKs are widely used in privacy-centric cryptocurrencies (e.g., Zcash) as well as in layer-2 scaling solutions. These protocols reduce on-chain data storage, improve computational efficiency, and facilitate confidential transactions, secure voting, identity verification, and trustless smart-contract execution without disclosing private details.

Digital Signature

A digital signature is a cryptographic model known as a signature scheme that ensures the integrity and authenticity of messages and prevents the sender from denying the transmission of a message. A confidential key which is held by the signer is utilized to generate a digital signature for a given message. The corresponding public key of the signer which is accessible to all parties, permits anyone to verify the validity of the signature. The digital signature operates through one-way cryptographic functions; however, each execution of the signing algorithm requires the signer's secret key, ensuring that each generated signature is unique. Any modification of the message is detected by the receiver. The signer alone receives a secret code which is required to evaluate the signature, enabling the receiver to confirm that the message was delivered to the sender. HMAC-SHA 256 protocol is used to ensure both message authentication and integrity in the key generation model. HMAC-SHA 256 allows the receiver and sender to share a secret key which is utilized to generate a Message Authentication Code (MAC) signature for the transmitted message. At the sender side, the EHR data generates an HMAC signature using private key and SHA-256 functions as the one-way hash function. The message is hashed using SHA256 then HMAC signature is evaluated with public key. During key-generation, the EHR data is combined with the HMAC signature, enabling the model to verify the data, authenticate the message, and compare the message. HMAC-SHA 256 not only handles the shared secret key but also provides a lightweight authentication mechanism while ensuring message security and integrity. By comparing the calculated HMAC values with the received HMAC values, it is determined whether the key is accepted or rejected. This verification process strengthens security by ensuring proper key authentication and preventing unauthorized users from generating fake secret keys. Therefore, HMAC-SHA 256 protocol confirms message authenticity, handles key secret, and reduces computational overhead. The fig. 2 shows the architecture of HMAC-SHA 256 digital signature.

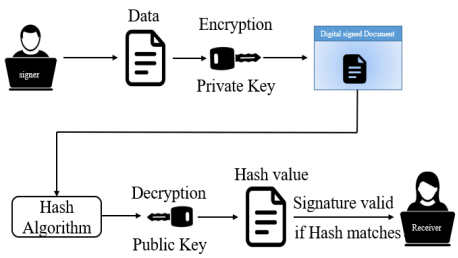

Fig. 2. Architecture of HMAC-SHA 256 digital signature

Blowfish Encryption

After the registration phase, the input data is encrypted using Blowfish Encryption (BE), which is a cryptographic model. Blowfish operates on 64-bit block sizes with variable key lengths ranging from 32 to 448 bits. It employs a P-array and four 32-bit S-boxes, where each S-box receives an 8-bit input and produces a 32-bit output. The BE includes two primary phases, namely key expansion and encryption procedure. The encryption procedure is based on 16-round Feistel network, where each round performs key dependent substitution and permutation operations. These operations combine 32-bit words using XOR operations and BE to improve data security. BE consists of the following steps such as key generation, s-box initialization, encryption and decryption. For illustration, consider the plain text value 123456abcd132536.

Key Size Generation: The encryption and decryption procedures require 18 sub keys, and same key is used in both the processes. These sub-keys are stored in S-array, where each element is a 32-bit input value. Initially, the entries of the S-array are initialized with digits of $S_i[X]$. After initialization, each sub key is modified according to the input keys.

Initialize the S-box: Blowfish uses four substituting boxes $\{S^b[1], S^b[2], S^b[3], S^b[4]\}$ in both encryption and decryption procedures. Each S-box contains 255 entities $\{S^b[i][0], S^b[i]\,[1], \ldots, S^b[i][255]\}$ with 32 bits.

Encryption: Blowfish uses 16 rounds of encryption. The 64-bit input data block X is divided into 64 halves, denoted as xL and xR are presented in Eqs. 1 and 2. Then, for each round i= 1 to 16.

$$xL = xLXORS_i \tag{1}$$

$$xR = F(xL)XORxR \tag{2}$$

xL and xR are swapped. After the sixteenth round, the halves xL and xR are swapped again to undo the final swap which is given as $xR = xRXORS_{17}$ and $xL = xLXORS_{18}$. Finally,xL and xR are reintegrated to find the cipher text.

Decryption: In the decryption process, an already encrypted input is decrypted using the same key that was used during encryption. The decryption procedure follows the same sequence of operations as the encryption stage, except that the decryption s$\{S[1], S[2], \ldots., S[18]\}$ are performed in reverse order.

PBKDF2

PBKDF2 is a key derivation function that is utilized to minimize vulnerabilities by resisting brute-force attacks through intensive operations. In the cryptographic algorithm, PBKDF2 uses HMAC to integrate an input value with a salt value to generate a derived key. In cryptography, HMAC is a message-authentication code based on a hash function and a secret key, which is applied to verify the integrity and authenticity of a transmitted message. For PBKDF2, HMAC uses the SHA256 hash function, which consists of three main stages: padding, block decomposition and hash computation. During this procedure, the input message is padded and divided into N blocks of 512 bits, and then each block is processed through block decomposition and hash computation to produce the final hash value.

Pseudocode of the proposed PBDS algorithm:

1. Device Bootstrap
- Derive symmetric key $K_{bf} \leftarrow PBKDF2$ (salt, iterations)
- Produce key pair $(SK_{dev,}PK_{dev})$
- Construct DID from PK_{dev}
- Store $\{DID, SK_{dev,}PK_{dev}, K_{bf,}salt, iterations\}$ securely.

2. Device Registration
- Submit $\{DID, SK_{dev}\}$to blockchain.
- Wait for consensus confirmation.

3. Attribute Issuance
- DAA issues credential AU = {role, context, expiry}.
- Store hash of AU on blockchain.
- Deliver AC securely off-chain.

4. Access Request
- Device generates nonce n_r
- Create ZKP proving AU satisfies policy P
- Construct message $M = \{DID, n_r, proof, policyHash, resource\ R\}$
- Generate Digital Signature:
  - Sig = HMAC_SHA256 $(SK_{dev,}Hash\ (M))$
- Send request $\{M, sig, PK_{dev}\}$

5. Verification
- Verifier retrieves commitments/revocation state from blockchain.
- Verify ZKP validity.
- Verify digital signature:
  if HMAC_SHA256$(SK_{dev,}Hash\ (M)) = sig \rightarrow Authentic$
- Evaluate policy P and context.
- Decision = Permit or Deny.
- Log decision hash on blockchain.

6. Secure Data Exchange
- If Permit:

a) Encrypt payload: $C = Blowfish_{CBC}(K_{bf}, plain\ text)$

b) Compute Integrity Tag: MAC = HMAC_SHA256$(k_{bf}, IV \parallel C)$

c) Send {IV, C, MAC, Sig}

- Receiver verifies MAC and Sig before decryption

7. Revocation

- DAA posts revocation deltas to blockchain.
- Verifiers periodically sync revocation state.

End Algorithm

Experimental Results

The proposed PBDS is simulated using python 3.8 or any other suitable software, the details of the system configuration are given below:

System Configuration

- Intel Processor: i7
- RAM: 16 GB
- GPU: 6GB
- SSD: 1TB
- Operating System: Windows 10

The proposed method is estimated via different evaluation metrics such as encryption time, decryption time, processing overhead, delay and computation time are used to analyze the model performance and its descriptions are discussed in below:

Performance Analysis

Fig. 3 shows the performance analysis of the security level based on the signature size, The X-axis represents the security level (KB) ranging from 100 to 700, and the Y-axis denotes the signature size (KB). As the security level increases, the signature size also increases for all approaches. However, the proposed PBDS consistently achieves higher signature value across all security levels. For example, at a security level of 700 KB, the PBDS attains a signature value for 90 KB, which is higher compared to the existing models such as ECDSA and RSA-SHA 256. This result indicates that PBDS produces a higher storage overhead, scalability and a larger signature size, which is more suitable for high security applications.

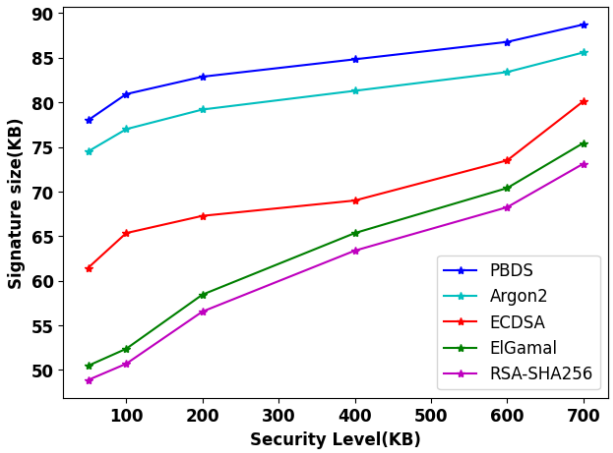

Fig. 3. Graphical representation shows various signature sizes of cryptographic methods across enhancing security levels are compared with proposed PBDS

Fig. 4 demonstrates that the proposed PBDS model consistently achieves a lower communication cost compared to RSA-SHA256, ElGamal, ECDSA and Aragon 2 as the number of messages increases. The proposed model achives lower cost because it minimizes cryptographic complexity and message processing overhead while enhancing the security of the messages. The traditional models involve tough key operations and offer limited scalability while PBDS provides a light weight and scalable framework. The proposed PBDS achieves higher value through transmitting faster communication with decreased cost which is suitable for the secure system.

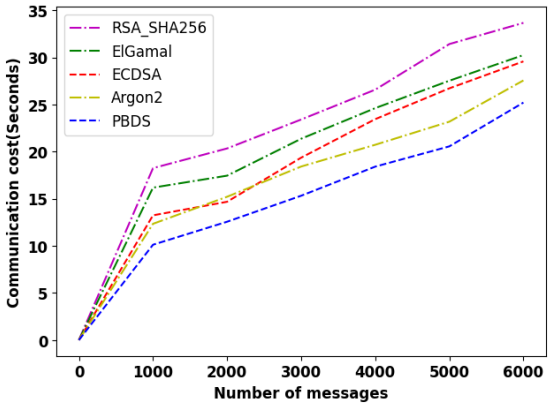

Fig. 4. Graphical representation of communication cost showing PBDS obtains lowest overhead compared with other algorithms.

Fig. 5 illustrates the signature creation time (seconds) for various models. Among all the models, the proposed PBDS achieves the minimum signature creation time of 0.1934 seconds, whereas RSA-SHA26 records the highest value of 0.5238 seconds. This improvement is achieved due to reduced computational operations and optimized key processing, enabling faster execution process without compromising security. Although ECSDA and Argon2 reduce overhead compared to RSA, which remain lower than PBDS. Therefore, PBDS not only reduces processing delay but also ensures quick authentication security.

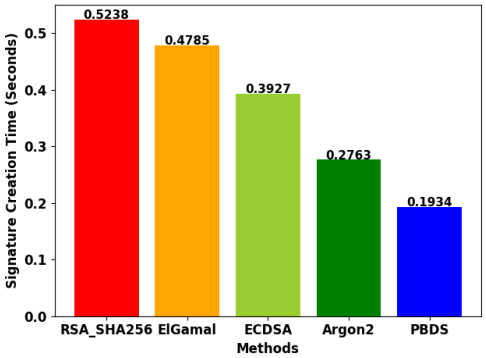

Fig. 5. Graphical analysis of signature creation time, highlighting PBDS attains fastest performance between models

Fig. 6 illustrates the performance evaluation of average latency with different throughput levels. As throughput increases, the average latency also increases showing direct correlation. Among the estimated algorithms, the proposed PBDS consistently achieves the lowest latency values, whereas RSA_SHA256 incurs the highest delay. ElGamal and ECDSA show moderate performance but still remain higher than PBDS, while Argon2 performs better than these traditional models but still falls short of PBDS. The minimized latency of PBDS is due to effective message processing, making it suitable for high-throughput applications.

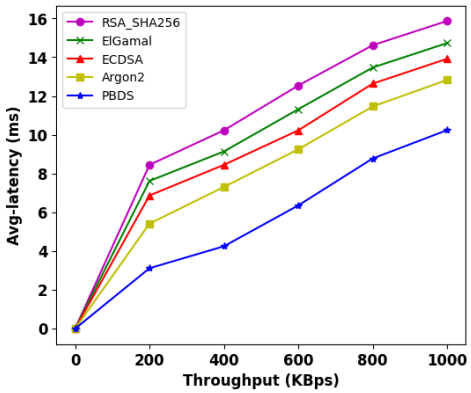

Fig. 6. Performance analysis of throughput (KBps)

Fig. 7 illustrates that the proposed blockchain-based model significantly minimized data transfer compared to the traditional client/server model. While the client/server model showed an increase, reaching 6.91 GB for 6000 records, only 5.43 GB was required to the block chain-based data transfer for the same number of records. This improvement was achieved due to blockchain's distributed architecture, where only authentication and verification metadata were exchanged instead of repeatedly transmitting the entire health record content. Consequently, the proposed model attained better scalability, lower bandwidth consumption, and improved network efficiency, outperforming both centralized and hybrid models by reducing redundancy and ensuring secure and efficient health data management.

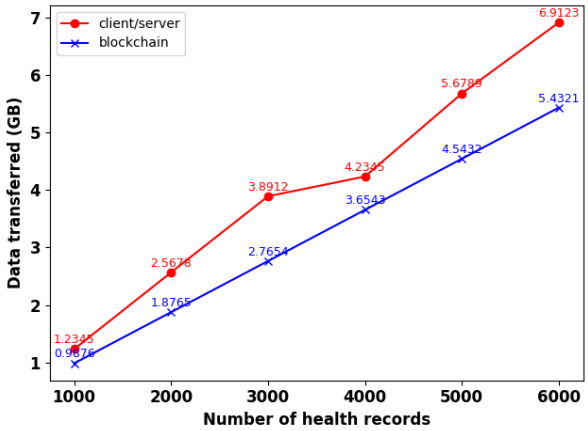

Fig. 7. Performance analysis of data transferred based on number of health records

The execution time analysis in Fig. 8 demonstrated that the blockchain-based model consistently outperformed the traditional client/server approach. Although the execution time increased with the number of health records in both models, the blockchain model achieved faster processing with 180.16 seconds for 10,000 records compared to 185.25 seconds in client/server model. This improvement was attributed to blockchain's distributed architecture where validation and storage were shared, thereby decreasing central server bottlenecks and enabling more efficient parallel processing.

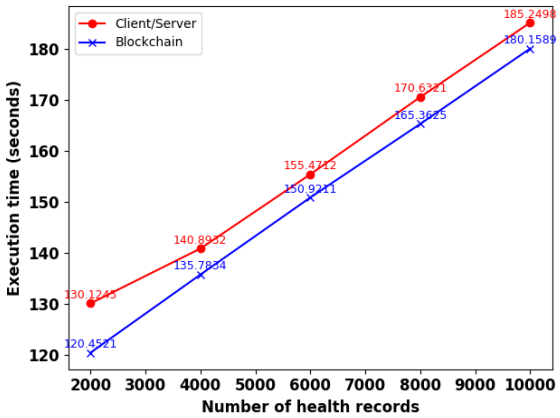

Fig. 8. Performance analysis of execution time based on number of health records

Fig. 9 compared the encryption and decryption times across various cryptographic methods. Traditional schemes such as RSA_SHA256 and ElGamal exhibited higher computational overhead, while ECDSA and Argon2 achieved average efficiency. In contrast, the proposed PBDS model attained the lowest encryption 6.45 s and decryption 5.98s, demonstrating superior performance. The proposed PBDS model delivered faster execution while handling strong security, making it highly suitable for IIoT and healthcare access environment.

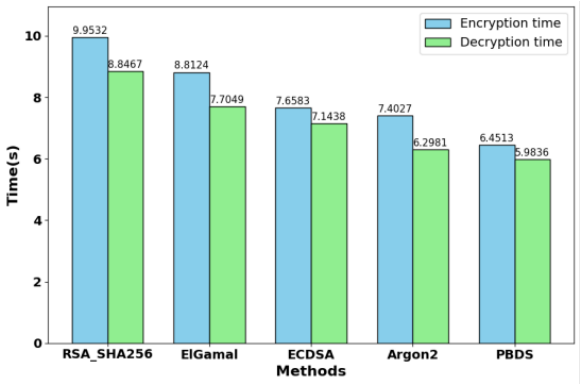

Fig. 9. Performance analysis of encryption and decryption times comparison

Comparative Analysis

In the comparative analysis section, the existing approaches like AFHENN-BCN (Sharma et al., 2023), HECC (Rao and Sujatha, 2023), IBE (Sharma et al., 2021) and CA-DPPF (Deebak and Hwang, 2023) are compared with proposed PBDS. Table 1,2,3 and 4 denotes the comparative analysis of existing approaches are AFHENN-BCN (Sharma et al., 2023), HECC (Rao and Sujatha, 2023), IBE (Sharma et al., 2021) and CA-DPPF (Deebak and Hwang, 2023) with proposed PBDS with metrics such as Encryption Time (ET), Decryption Time (DT), Throughput, Packet Delivery Ratio (PDR).

Table 1. Comparative performance of AFHENN-BCN (Sharma et al., 2023) and the proposed PBDS in terms of throughput, PDR and execution time across all nodes

Methods	Metrics	Number of Nodes			
		100	200	300	400
AFHENN-BCN (Sharma et al., 2023)	Throughput	312	334	351	343
	PDR (%)	88.98	85	84	82
	Execution Time (ms)	7.102	7.278	7.423	7.509
Proposed PBDS	Throughput	348	375	393	386
	PDR (%)	92.5	89.6	88.2	86.4
	Execution Time (ms)	6.41	6.57	6.68	6.74

Table 2. Comparative performance of the HECC (Rao and Sujatha, 2023) and the proposed PBDS in terms of encryption, decryption, and key generation time

Methods	Metrics	Input File Sizes (KB)				
		3	5	8	12	16
HECC (Rao and Sujatha, 2023)	Encryption Time (s)	0.007998	0.008244	0.008463	0.008599	0.008649
	Decryption Time (s)	0.006944	0.007997	0.008014	0.008245	0.008318
	Key Generation Time (s)	0.000014	0.000021	0.000019	0.000016	0.000032
Proposed PBDS	Encryption Time (s)	0.0069	0.0071	0.0073	0.0075	0.0076
	Decryption Time (s)	0.0060	0.0069	0.0070	0.0072	0.0073
	Key Generation Time (s)	0.000012	0.000018	0.000017	0.000014	0.000028

Table 3. Comparative analysis of IBE (Sharma et al., 2021) and the proposed PBDS in terms of computation time and delay

Methods	Metrics	Number of Transactions				
		200	400	600	800	1000
IBE (Sharma et al., 2021)	Computation Time (s)	0.95	1.28	1.64	1.96	2.31
	Delay (s)	2.1	2.6	3.0	3.3	3.6
Proposed PBDS	Computation Time (s)	0.83	1.10	1.42	1.70	2.02
	Delay (s)	1.85	2.30	2.65	2.95	3.20

Table 4. Comparative analysis of CA-DPPF (Deebak and Hwang, 2023) and the proposed PBDS in terms of execution time and latency

Methods	Metrics	Number of Transactions				
		1000	2000	3000	4000	5000
CA-DPPF (Deebak and Hwang, 2023)	Execution Time (s)	1.35	1.38	1.14	1.44	1.47
	Latency (s)	0.143	0.146	0.148	0.150	0.152
Proposed PBDS	Execution Time (s)	1.22	1.25	1.27	1.30	1.32
	Latency (s)	0.129	0.132	0.134	0.136	0.138

Table 1 denotes the performance of the proposed PBDS method AFHENN-BCN (Sharma et al., 2021) in terms of PDR, execution time and PDR across all nodes, while PBDS attains high throughput and PDR because of the validation in blockchain and effective data transmission. Table 2 shows that the proposed PBDS outperforms HECC (Rao and Sujatha, 2023) by attaining a lower ET, KGT and DT in all file sizes such as 3,5,8,12 and 16, the proposed PBDS optimize a cryptographic procedure, light weight key management and minimized computational overhead. Table 3 illustrates that the proposed PBDS model attains a lower computation time and delay compared to IBE (Sharma et al., 2021) in all transactions. The results show that the minimized computational overhead and reduced delay made the PBDS model more scalable and effective than IBE framework. Table 3 output determines that the proposed PBDS model has more effectiveness compared to CA-DPPF (Deebak and Hwang, 2023) and showed lower execution time and latency. The proposed PBDS ensures faster transaction processing with lower latency and improved scalability compared to CA-DPPF.

Conclusion

In this research, the PBDS model is proposed for privacy preservation and authentication to securely encrypt the message by blockchain which relies on healthcare data in IIoT environment. The ZKP is integrated with blockchain to improve privacy and authentication, where ZKP allows the verification of patient data and access without revealing any information, thereby ensuring confidentiality and

protecting against unauthorized access of EHR. HMAC-SHA256 is used in the digital signature process, while efficiently prevents interfering, establishes trust among entities and attains lower computational overhead, making it suitable for healthcare access systems. Blowfish encryption model is applied after the registration phase to encrypt the input data, the cipher text is then transmitted to the receiver, and the decryption restores the original data which reduces the delay, minimizes complexity, and improves the effectiveness of healthcare data access and storage. The experimental results show that the proposed PBDS achieves lower ET and DT values of 6.4513s and 5.9836s respectively. In the future, hybrid encryption method will be considered for privacy preservation and better authentication performance.

Acknowledgement

The authors express their sincere gratitude to the Department of Computer Science and the Department of Computer Science and Information Technology, VELS Institute of Science, Technology and Advanced Studies (VISTAS), Chennai, India, for providing the necessary facilities, support, and encouragement to carry out this research. The authors also thank all colleagues and reviewers whose valuable feedback contributed to improving the quality of this manuscript.

Funding Information

The authors declare that no external funding was received for the preparation of this manuscript

Author's Contributions

M. P. Kumar: Conceptualization, Methodology, Data Collection, Formal Analysis, Writing – Original Draft, Writing – Review & Editing.

A. Akila: Supervision, Validation, Resources, Writing – Review & Editing, Project Administration.

Ethics

The authors affirm that this manuscript is an original piece of work and has not been published or submitted elsewhere. All data used in the study has been obtained, processed, and presented ethically. There are no conflicts of interest, and no ethical issues are anticipated after the publication of this manuscript.

References

Alsuqaih, H.N., W. Hamdan, H. Elmessiry and H. Abulkasim. 2023. An efficient privacy-preserving control mechanism based on block chain for E-health applications. Alexandria Engineering Journal, 73: 159-172. https://doi.org/10.1016/j.aej.2023.04.037

Bao, Z., D. He, M.K. Khan, M. Luo and Q. Xie. 2022. PBidm: Privacy-preserving blockchain-based identity management system for Industrial Internet of Things. IEEE transactions on industrial informatics, 19(2): 1524-1534. https://doi.org/10.1109/TII.2022.3206798

Das, S., S. Namasudra, S. Deb, P.M. Ger and R.G. Crespo. 2023. Securing IoT-based smart healthcare systems by using advanced lightweight privacy-preserving authentication scheme. IEEE Internet of Things Journal, 10(21): 18486-18494. https://doi.org/10.1109/JIOT.2023.3283347

Deebak, B.D. and S.O. Hwang. 2023. Healthcare applications using blockchain with a cloud-assisted decentralized privacy-preserving framework. IEEE Transactions on Mobile Computing, 23(5): 5897-5916. https://doi.org/10.1109/TMC.2023.3315510

Duggegowda, D. and U. Rama moorthy. 2024. MedAccess HBPF: A Privacy-Preserving Hybrid-Block chain Framework for Secure and Efficient Cloud-Based Electronic Health Record Sharing. SN Computer Science, 5(8): 1018. https://doi.org/10.1007/s42979-024-03343-w

Haritha, T. and A. Anitha. 2023. Multi-level security in healthcare by integrating lattice-based access control and block chain-based smart contracts system. IEEE Access, 11: 114322-114340. https://doi.org/10.1109/ACCESS.2023.3324740

He, B., T. Feng, C. Liu and C. Su. 2024. CD-BISHAC: Cross-Domain Scheme for Blockchain-Based Industrial Internet of Things Security Hybrid Access Control. IEEE Internet of Things Journal, 12(6): 7164-7179. https://doi.org/10.1109/JIOT.2024.3492279

Li, T., H. Wang, D. He and J. Yu. 2022. Blockchain-based privacy-preserving and rewarding private data sharing for IoT. IEEE Internet of Things Journal, 9(16): 15138-15149. https://doi.org/10.1109/JIOT.2022.3147925

Liu, S., L. Chen, G. Wu, H. Wang and H. Yu. 2023. Block chain-backed searchable proxy signcryption for cloud personal health records. IEEE Transactions on Services Computing, 16(5): 3210-3223. https://doi.org/10.1109/TSC.2023.3272770

Liu, S., L. Chen, H. Yu, S. Gao and H. Fang. 2023. BP-AKAA: Blockchain-enforced privacy-preserving authentication and key agreement and access control for IIoT. Journal of Information Security and Applications, 73: 103443. https://doi.org/10.1016/j.jisa.2023.103443

Luong, D.A. and J.H. Park. 2023. Privacy-preserving identity management system on block chain using Zk-SNARK. IEEE Access, 11:1840-1853. https://doi.org/10.1109/ACCESS.2022.3233828

Morales, D., I. Agudo and J. Lopez. 2024. Toward a Framework for Cost-Effective and Publicly Verifiable Confidential Computations in Blockchain. IEEE Communications Magazine, 63(2): 96-102. https://doi.org/10.1109/MCOM.001.2300839

Padma, A. and M. Ramaiah. 2025. Lightweight privacy preservation blockchain framework for healthcare applications using GM-SSO. Results in Engineering, 25:103882.https://doi.org/10.1016/j.rineng.2024.103882

Rao, B.R. and B. Sujatha. 2023. A hybrid elliptic curve cryptography (HECC) technique for fast encryption of data for public cloud security. Measurement: Sensors, 29: 100870. https://doi.org/10.1016/j.measen.2023.100870

Rao, P.M. and B.D. Deebak. 2024. Lightweight two-factor authentication framework with privacy preserving for smart eHealth. Peer-to-Peer Networking and Applications, 17(1): 373-396. https://doi.org/10.1007/s12083-023-01596-5

Sharma, P., N.R. Moparthi, S. Namasudra, V. Shanmuganathan and C.H. Hsu. 2021. Blockchain-based IoT architecture to secure healthcare system using identity-based encryption. Expert Systems, 39(10): e12915. https://doi.org/10.1111/exsy.12915

Sharma, P.C., M.R. Mahmood, H. Raja, N.S. Yadav, B.B. Gupta and V. Arya. 2023. Secure authentication and privacy-preserving blockchain for industrial internet of things. Computers and Electrical Engineering, 108: 108703. https://doi.org/10.1016/j.compeleceng.2023.108703

Tawfik, A.M., A. Al-Ahwal, A.S.T. Eldien and H.H. Zayed. 2025. PriCollabAnalysis: privacy-preserving healthcare collaborative analysis on blockchain using homomorphic encryption and secure multiparty computation. Cluster Computing, 28(3): 191. https://doi.org/10.1007/s10586-024-04928-z

Usman, M., M.S. Sarfraz, M.U. Aftab, U. Habib and S. Javed. 2024. A block chain based scalable domain access control framework for industrial internet of things. IEEE Access, 12: 56554-56570. https://doi.org/10.1109/ACCESS.2024.3390842

Vatambeti, R., E.P. Krishna, M.G. Karthik, and V.K. Damera. 2023. Securing the medical data using enhanced privacy preserving based block chain technology in Internet of Things. Cluster Computing, 27(2): 1625-1637. https://doi.org/10.1007/s10586-023-04056-0

Vishwakarma, L., S.A. Saji and D. Das. 2025. CuraFrame: a patient-centric secure and privacy preserving medical framework with zero-leak using block chain. Peer-to-Peer Networking and Applications, 18(4): 231. https://doi.org/10.1007/s12083-025-02061-1

Wang, Z., Q. Chen and L. Liu. 2023. Permissioned blockchain-based secure and privacy-preserving data sharing protocol. IEEE Internet of Things Journal, 10(12): 10698-10707. https://doi.org/10.1109/JIOT.2023.3242959

Xiang, X. and X. Zhao. 2022. Blockchain-assisted searchable attribute-based encryption for e-health systems. Journal of Systems Architecture, 124: 102417.https://doi.org/10.1016/j.sysarc.2022.102417

Yin, J., Y. Xiao, Q. Pei, Y. Ju, L. Liu, M. Xiao and C. Wu. 2022. SmartDID: A novel privacy-preserving identity based on blockchain for IoT. IEEE Internet of Things Journal, 10(8): 6718-6732. https://doi.org/10.1109/JIOT.2022.3145089

Zhang, Y., L. Xiong, F. Li, Y. Hao and Z. Liu. 2024. Block chain-based privacy-preserving authentication with hierarchical access control using polynomial commitment for mobile cloud computing. IEEE Internet of Things Journal, 11(10): 18266-18280. https://doi.org/10.1109/JIOT.2024.3361506.