

A PRIVACY-AWARE ENHANCEMENT OF PROOF OF ELAPSED TIME (PPOET)
FOR HEALTHCARE BLOCKCHAIN SYSTEMS

S. Kanagasankari, J. Remy, M. Preethi and T. Idhaya
Department of Computer Science, St. Xavier's College, India

Abstract

The healthcare sector faces persistent challenges in ensuring data security, privacy, and regulatory compliance, as traditional systems remain vulnerable to breaches and unauthorized access. Blockchain technology offers decentralization, immutability, and transparency. Its effective adoption in healthcare requires consensus mechanisms tailored to domain-specific requirements. Existing approaches such as Proof of Elapsed Time (PoET) provide scalability and energy efficiency but offer limited support for privacy awareness and healthcare-oriented data management. This paper presents a privacy-aware enhancement of the Proof of Elapsed Time (PPoET) consensus mechanism for healthcare blockchain systems. The proposed approach introduces asynchronous wait-time generation to reduce latency and improve system responsiveness, along with ECDSA-based authentication and SHA-512 hashing to strengthen transaction integrity and trust. Unlike conventional PoET implementations that rely on hardware-based Trusted Execution Environments (TEE), the proposed model adopts a software-based cryptographic approach, enabling practical deployment without specialized hardware. Experimental results demonstrate that PPoET achieves reduced transaction latency and stable resource utilization while maintaining acceptable throughput under healthcare workloads. The proposed framework supports secure and efficient management of Electronic Health Records (EHRs) and provides a scalable and reliable solution for healthcare blockchain applications.

Keywords:

Blockchain, Consensus Mechanism, Proof of Elapsed Time (PoET), Privacy-Aware PPoET, Elliptic Curve Digital Signature Algorithm (ECDSA), Electronic Health Records (EHR), SHA-512

1. INTRODUCTION

The healthcare industry is undergoing rapid digital transformation, driven by the need to enhance data security, interoperability, and efficient information sharing [1]. Traditional healthcare systems remain vulnerable to data breaches, unauthorized access, and limited transparency, compromising patient confidentiality and the integrity of Electronic Health Records (EHRs) [2] [3] [4]. In this context, blockchain technology has emerged as a promising solution due to its decentralized architecture, immutability, and transparency, enabling secure and trustworthy data management [5] [31]. Despite these advantages, the effective adoption of blockchain in healthcare depends on the design of suitable consensus mechanisms [6] [7] [8]. Conventional algorithms such as Proof of Work (PoW) and Proof of Stake (PoS) are often unsuitable due to high energy consumption and scalability limitations [5] [6]. Proof of Elapsed Time (PoET), implemented in platforms such as Hyperledger Sawtooth and provides an energy-efficient alternative by enabling fair leader selection [8]. Existing PoET-based approaches offer limited support for healthcare-specific requirements, including controlled data access, system responsiveness, and efficient handling of concurrent transactions. To address these limitations, this paper proposes a privacy-aware enhancement of the Proof of Elapsed Time (PPoET) consensus mechanism for healthcare

blockchain systems. The proposed approach introduces asynchronous wait-time generation to reduce blocking delays and improve system responsiveness. ECDSA-based authentication and SHA-512 hashing are integrated to strengthen transaction integrity and ensure secure validation [13]. Unlike conventional PoET implementations that rely on hardware-based Trusted Execution Environments (TEEs), the proposed framework adopts a software-based cryptographic approach, enabling practical deployment without specialized hardware. This design improves scalability and efficiency while maintaining secure and reliable consensus operations in healthcare environments.

1.1 IMPORTANCE OF CONSENSUS IN
HEALTHCARE BLOCKCHAIN

Consensus algorithms play a crucial role in ensuring the correctness and consistency of transactions in blockchain-based healthcare systems [32]. They validate transactions, maintain ledger integrity, and enable secure data sharing among distributed participants [4] [12]. In healthcare environments, consensus mechanisms must also support low latency, energy efficiency, and secure handling of sensitive patient data. PoET-based systems provide a practical foundation for meeting these requirements in permissioned blockchain settings [10] [15].

1.2 CHALLENGES IN
BLOCKCHAIN

The adoption of blockchain in healthcare is constrained by several challenges, including data privacy, regulatory compliance, scalability, and efficient transaction processing. While PoET improves energy efficiency and fairness, it does not fully address issues such as high transaction volume handling and fine-grained access control for sensitive healthcare data [11]. These limitations highlight the need for enhanced consensus mechanisms that improve responsiveness and reliability while maintaining security. The Table.1 presents a structured mapping between healthcare challenges, limitations of PoET, and the corresponding enhancements introduced in the proposed PPoET framework.

Table.1. Challenges Vs Proposed Solution

Healthcare Challenge	PoET Limitation	Proposed Solution	Evidence
Data integrity	No external validation	ECDSA-based verification	Section 4
Scalability	Blocking wait times	Asynchronous execution	Section 6
Trust dependency	TEE-only trust	Cryptographic validation	Section 4
Security	No signed wait time	Wait certificate (W,H,σ)	Algorithm

1.3 RESEARCH CONTRIBUTIONS

This work presents a privacy-aware enhancement of the Proof of Elapsed Time (PPoET) consensus mechanism tailored for healthcare blockchain systems. The novelty of the proposed approach lies not in the individual cryptographic primitives, but in their architectural integration within the consensus layer. Unlike conventional PoET, where correctness relies solely on Trusted Execution Environments (TEEs), the proposed model introduces externally verifiable consensus validation through signed wait-time certificates and hash commitments, thereby shifting the trust model from hardware dependency to cryptographic verification. The proposed PPoET integrates asynchronous wait-time execution with consensus validation, reducing blocking delays and enabling concurrent processing during block selection. Experimental evaluation demonstrates that PPoET achieves lower transaction latency compared to conventional PoET, while maintaining competitive throughput and stable resource utilization under varying workloads. From a theoretical perspective, the use of ECDSA signatures ensures the authenticity and non-forge ability of consensus parameters, while SHA-512 provides integrity through collision-resistant hashing [14]. These properties enable verifiable and tamper-resistant consensus without relying entirely on trusted hardware. The proposed PPoET represents a system-level enhancement that improves transparency, robustness, and scalability. Unlike finance or supply chain systems, healthcare applications require strict privacy, auditability, and regulatory compliance. The proposed framework supports these requirements by ensuring verifiable transaction integrity and controlled access validation, which are essential for secure Electronic Health Record (EHR) management.

1.4 ORGANIZATION

This manuscript is organized as follows. Section 2 reviews related work and highlights existing approaches to blockchain consensus in healthcare. Section 3 presents the background concepts, including cryptographic foundations and the Elliptic Curve Digital Signature Algorithm (ECDSA). Section 4 introduces the proposed methodology, detailing the design of the Privacy-Aware Proof of Elapsed Time (PPoET) algorithm, including asynchronous wait-time generation and enhanced cryptographic mechanisms. Section 5 discusses the integration of ECDSA within the PPoET framework to strengthen security and authenticity in healthcare applications. Section 6 presents the experimental results and performance analysis, and Section 7 concludes the paper by summarizing the key findings and outlining future research directions.

2. LITERATURE REVIEW

Research on blockchain-based healthcare data management has gained considerable momentum, with scholars exploring various dimensions including architecture design, cryptographic techniques, consensus mechanisms, and privacy-aware frameworks.

Several studies have focused on leveraging consortium blockchain architectures to manage Electronic Health Records (EHRs) securely. Shunrong Jiang *et al.* [16] proposed an

Ethereum-based system enabling patients to control the storage of EHR hashes on a blockchain, with cryptographic primitives supporting authorization and access control; they also improved block deletion through transaction categorization. Similarly, Weiquan Ni *et al.* [17] introduced HealChain, a decentralized mobile healthcare data management system featuring a three-layer hierarchical architecture that addresses security and privacy requirements while supporting optimal mining node decision-making. Randhir Kumar and Rakesh Tripathi [18] complemented these efforts by combining consortium blockchain with IPFS for on-chain and off-chain storage, successfully prototyping a decentralized framework that eliminates intermediaries and ensures equitable access for authorized peers. However, a common shortcoming across these studies is the lack of attention to consensus-level efficiency, latency optimization, and cryptographic validation of consensus parameters.

The challenge of designing effective consensus mechanisms for blockchain has been separately addressed in the literature. Yanjun Jiang and Siye Ding [19] proposed the HPBC algorithm targeting asynchronous Byzantine networks, overcoming limitations of the Proof-of-Work (PoW) algorithm with minimal overhead. A broader survey by Giang-Truong Nguyen and Kyungbaek Kim [27] categorized consensus algorithms into proof-based and vote-based paradigms, describing how nodes demonstrate sufficient computational work to append transactions and receive corresponding rewards. While these works advance understanding of consensus design, neither proposes healthcare-specific enhancements nor incorporates privacy-aware consensus validation. Kanagasankari and Vallinayagi [35] addressed this gap partially by proposing a patient-centered framework using Hyperledger Fabric with an Improved Practical Byzantine Fault Tolerance (IPBFT) consensus, which outperforms traditional PBFT in efficiency and scalability; however, it still does not incorporate time-based or privacy-aware consensus mechanisms.

Cryptographic techniques form another major thread of inquiry. Ashok Kumar Yadav [20] and Elif Hilal Umucu [21] provided theoretical and mathematical foundations of Elliptic Curve Cryptography (ECC), with the former comparing ECC to RSA in blockchain contexts and the latter analyzing cryptographic methods used in cryptocurrency key design. Joppe W. Bos *et al.* [24] offered a practical reference on ECC implementation, covering secure parameter selection, though without application to consensus validation. Anubis Graciela de Moraes Rossetto *et al.* [25] took a more applied approach, evaluating the impact of RSA, ECC, and AES on computational effort, memory, and execution time in a decentralized health data network, albeit focusing solely on the data layer. Muhammad Rashid *et al.* [30] further proposed a hardware-optimized shared key generation architecture using ECDH and Karatsuba multiplication with FSM-based controllers, though this remains inapplicable to software-based consensus environments.

The integration of encryption into healthcare record systems has also been explored. Yen-Liang Lee *et al.* [22] designed a combined encryption-decryption architecture for medical records, establishing a decentralized EMR repository with blockchain storage of encrypted hash values. Kundan Munjal and Rekha Bhatia [23] examined homomorphic encryption for secure healthcare record analysis, including genetic data, though the

approach suffers from high computational overhead and has not been integrated with blockchain consensus mechanisms.

A number of studies have adopted Hyperledger Fabric as a practical platform for healthcare blockchain deployments. Sudeep Tanwar et al. [28] demonstrated optimized latency, throughput, and Round Trip Time for EHR systems using Hyperledger Fabric with access control, while Wanbing Zhan et al. [29] implemented a secure EMR model exchange system using Hyperledger Fabric with ECDSA and Attribute-Based Access Control (ABAC), improving data security and stakeholder trust. In both cases, however, cryptographic mechanisms such as ECDSA remain confined to the transaction layer and are not extended to consensus-level validation or wait-time authentication.

More recent contributions have sought to broaden the scope of blockchain healthcare architectures. Aniruddha Bhattacharjya et al. [26] proposed a trusted blockchain architecture for the Internet-of-Medical-Things (BIoMT) ensuring real-time secure communication through a CIA model, while S. Nekkalapudi et al. [33] demonstrated how smart contracts and decentralization can reduce data siloing and improve transparency in healthcare systems, though scalability and consensus optimization remain unaddressed. A. Bratu et al. [34] introduced a blockchain bridge architecture for cross-chain verification of verifiable credentials, enabling trustless interoperability between healthcare institutions with reduced administrative overhead, though scalability and regulatory adaptability require further investigation.

Recent dual-architecture and fog-assisted approaches have also emerged. Soubhagya Ranjan Mallick et al. [36] proposed a fog-assisted blockchain framework for IoMT environments with role-based access control that reduces latency and improves scalability, while the same group [38] developed a dual blockchain architecture separating patient and provider data, integrating IPFS for distributed storage and ECDSA for improved energy efficiency. In both works, however, ECDSA is restricted to data security purposes and is not extended to the consensus layer or wait-time certificate validation. Taken together, while the existing literature has made substantial advances in blockchain-based healthcare data management, cryptographic techniques, and consensus mechanism design, a persistent gap remains: the absence of privacy-aware, time-validated consensus mechanisms specifically optimized for real-time healthcare blockchain environments. The present work aims to address this gap.

A critical analysis of existing literature reveals that most healthcare blockchain solutions primarily focus on cryptographic techniques such as encryption and digital signatures to ensure data security and privacy [22][23][25], while comparatively less attention is given to optimizing consensus mechanisms for healthcare-specific requirements [27] [28]. Conventional consensus algorithms often suffer from high computational overhead, increased latency, and limited scalability, making them less suitable for real-time healthcare applications [19] [27]. Although Proof of Elapsed Time (PoET) improves energy efficiency and fairness, it lacks support for asynchronous execution and system-level optimizations required to handle high transaction volumes in healthcare environments. Furthermore, existing studies tend to address either cryptographic security or consensus efficiency independently [29] [36], with limited efforts toward integrating both aspects within a unified framework. Current PoET-based implementations also restrict ECDSA to the

transaction layer [29] [38] and do not incorporate verifiable consensus validation mechanisms alongside efficient asynchronous execution strategies. Motivated by these observations, this work proposes a privacy-aware enhancement of the PoET consensus mechanism (PPoET), integrating asynchronous wait-time generation with ECDSA-based authentication and SHA-512 hashing to improve transaction integrity, scalability, and overall system performance in healthcare blockchain environments.

3. EXISTING METHODOLOGY

3.1 PROOF OF ELAPSED TIME CONSENSUS (POET)

The Proof of Elapsed Time (PoET) consensus algorithm serves as the foundation for the proposed approach, offering an energy-efficient alternative to traditional consensus mechanisms. In PoET, participants rely on Trusted Execution Environments (TEEs) to generate secure and random wait times that determine block creation, ensuring fairness and unpredictability in the selection process [9]. PoET operates through three main phases. In the initialization phase, each participant establishes a secure enclave within the TEE, where a random wait time is generated. This ensures that all nodes begin the consensus process under equal and tamper-resistant conditions. In the wait-time phase, each node activates a timer based on the assigned wait duration, which runs securely inside the enclave. Nodes remain idle until their timer expires, creating a lottery-like selection mechanism without requiring intensive computation. In the block creation phase, the node whose timer expires first is selected to generate the next block, which is then broadcast to the network for validation and inclusion in the blockchain. PoET ensures fairness, decentralization, and reduced energy consumption through the use of secure enclave operations and randomized wait times, in contrast to Proof of Work (PoW) and Proof of Stake (PoS). Its dependence on hardware-based TEEs introduces significant deployment limitations. Specialized hardware such as Intel SGX incurs additional infrastructure costs and is not universally available across healthcare institutions. Furthermore, TEE-based trust is implicit and cannot be externally verified, reducing transparency in the consensus process. These constraints restrict the practical adoption of conventional PoET in resource-limited and large-scale healthcare environments, motivating the need for a software-based cryptographic alternative. Fig.1 illustrates the three-phase PoET consensus flow, showing TEE-based attestation, random wait-time assignment to each node, and block creation by the first-expiring node, followed by network-wide verification before blockchain inclusion.

3.2 ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM (ECDSA)

The Elliptic Curve Digital Signature Algorithm (ECDSA) is a widely adopted public-key cryptographic scheme based on the mathematics of elliptic curves over finite fields [20] [24]. Compared to RSA, ECDSA achieves equivalent security with significantly shorter key lengths, reducing computational overhead and making it well-suited for resource-constrained environments such as healthcare blockchain systems. ECDSA

operates through three main procedures. In key generation, each node produces a private key sk and a corresponding public key pk derived from a base point on the elliptic curve. In the signing procedure, given a message m , the node computes a digital signature $\sigma \leftarrow \text{ECDSA}.\text{Sign}(sk, m)$, binding the message to the signer's identity. In the verification procedure, any receiving node can confirm authenticity by computing $\text{ECDSA}.\text{Verify}(pk, m, \sigma) \rightarrow \{\text{true}, \text{false}\}$, ensuring the message has not been altered or forged. In the proposed PPOET framework, ECDSA is extended beyond its conventional role in transaction authentication to the consensus layer, enabling cryptographic validation of wait-time certificates and ensuring tamper-resistant node selection.

3.3 SHA-512 HASHING

SHA-512 is a cryptographic hash function belonging to the SHA-2 family, producing a fixed-length 512-bit digest from an arbitrary input [14]. It provides three essential security properties: pre-image resistance, second pre-image resistance, and collision resistance, ensuring that the original input cannot be recovered from its hash and that no two distinct inputs produce the same digest. SHA-512 is preferred over SHA-256 in the proposed framework due to its longer digest length, which offers a stronger security margin for sensitive healthcare data. In the proposed PPOET mechanism, SHA-512 is applied to a cryptographically generated random value R to derive a secure and verifiable hash $H = \text{SHA-512}(R)$. This hash serves as the basis for wait-time derivation, ensuring unpredictability and integrity throughout the consensus process. The combination of SHA-512 hashing with ECDSA-based signing provides a dual-layer cryptographic foundation for the proposed framework. To address these limitations, the proposed PPOET framework replaces hardware-dependent TEE operations with a software-based cryptographic approach using ECDSA and SHA-512, as detailed in Section 4.

4. PROPOSED METHODOLOGY

The proposed Privacy-Aware Proof of Elapsed Time (PPOET) enhances the conventional Proof of Elapsed Time (PoET) consensus mechanism by introducing cryptographic validation, asynchronous execution, and integrity-preserving techniques tailored for healthcare blockchain environments. In traditional PoET, the correctness of wait time generation relies on Trusted Execution Environments (TEEs), which provide implicit trust without enabling external verification. This limitation reduces transparency in the consensus process. To address this issue, PPOET introduces a verifiable consensus mechanism in which the wait time-serving as the core decision variable-is digitally signed using the node's private key. The resulting signed wait certificate is attached to the block and broadcast to the network. Participating nodes verify this certificate using the corresponding public key, ensuring that the wait time has not been altered or forged. This approach establishes a cryptographic validation layer that enhances trust, fairness, and transparency in node selection, while reducing reliance on implicit trust assumptions.

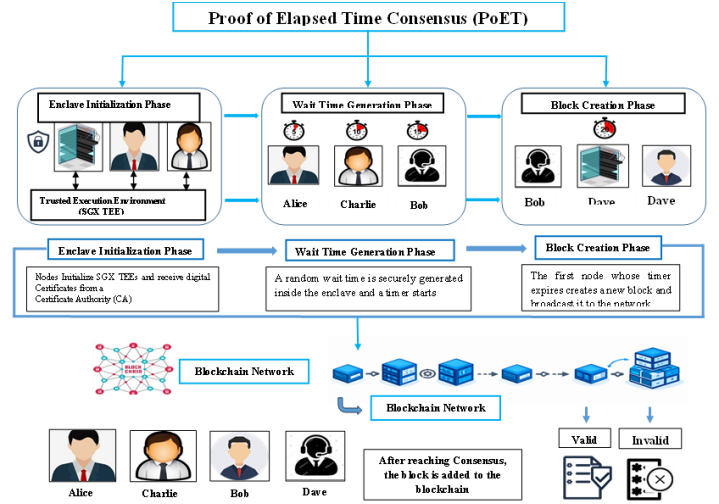


Fig.1. Proof of Elapsed Time Consensus in Blockchain

4.1 ECDSA-BASED WAIT TIME AUTHENTICATION

The proposed methodology integrates the Elliptic Curve Digital Signature Algorithm (ECDSA) into the consensus process to ensure the authenticity and integrity of wait time generation. In this approach, each node generates a random wait time within a software-based secure execution environment, eliminating the need for specialized hardware such as Intel SGX. The generated wait time is digitally signed using the node's private key, producing a verifiable wait certificate. Formally, given wait time W and hash H , the signature is computed as

$$\sigma \leftarrow \text{ECDSA}.\text{Sign}(s_k, W \parallel H), \text{ and verified as } \text{ECDSA}.\text{Verify}(p_k, W \parallel H, \sigma) \rightarrow \{\text{true}, \text{false}\}$$

This certificate is included in the block and broadcast to the network. Upon receiving the block, other nodes verify the certificate using the corresponding public key before accepting the block. This mechanism ensures that wait times are tamper-resistant and prevents manipulation by malicious participants. Also, it enables independent verification of the consensus decision, improving transparency and reducing reliance on trusted hardware assumptions.

4.2 SHA-512-BASED INTEGRITY ASSURANCE

To strengthen the integrity of the consensus process, the proposed model incorporates SHA-512 as a cryptographic hashing mechanism. Rather than generating randomness, SHA-512 is used to derive a secure and verifiable representation of the generated values:

$$H = \text{SHA-512}(R)$$

where R denotes the cryptographically generated random value and H represents the derived hash value. This transformation ensures immutability and resistance to tampering during transmission and verification. The integration of hashing with wait time validation enhances the reliability and consistency of the consensus process while preserving the unpredictability provided by the underlying random number generation mechanism.

4.3 ASYNCHRONOUS WAIT TIME GENERATION

The proposed PPoET introduces an asynchronous wait time generation mechanism to improve system responsiveness and scalability. In conventional PoET implementations, wait time computation may block execution, limiting concurrency and resource utilization. In contrast, the proposed approach performs wait time execution asynchronously using non-blocking timers or parallel task scheduling, allowing nodes to process transactions concurrently while awaiting timer expiration. The wait time is defined as:

$$W = \text{SecureRandom}(0, T_{\max})$$

where W represents the generated wait time and $T_{\max}$ denotes the maximum allowable wait duration. In the proposed prototype implementation, $T_{\max}$ is configurable based on network size and transaction load, set experimentally to support varying workload conditions as described in Section 6. This asynchronous design reduces idle blocking and improves throughput, particularly under high transaction loads, making it well-suited for real-time healthcare blockchain environments.

4.4 PPOET CONSENSUS ALGORITHM

The PPoET consensus algorithm integrates secure enclave execution, cryptographic validation, and asynchronous processing to ensure fairness, integrity, and efficiency.

Algorithm 1 Privacy-Aware Enhancement of Proof of Elapsed Time (PPoET)

```

1: Input: Pending transactions, Maximum wait time  $T_{\max}$ 
2: Output: Validated block appended to blockchain
3: Initialize software-based secure execution environment
4: Generate secure random value  $R$  using cryptographic RNG
5: Compute hash  $H \leftarrow \text{SHA-512}(R)$ 
6: Convert  $H$  to integer value  $I$ 
7: Derive wait time  $W \leftarrow (I \bmod T_{\max}) + 1$ 
8: Generate signature  $\sigma \leftarrow \text{Sign}_{\text{sk}}(W \parallel H)$  // sk = private key
9: Start asynchronous timer for duration  $W$  //non-blocking execution
10: if timer expires first among competing nodes then
11:     Create new block from pending transactions
12:     Attach proof  $\{W, H, \sigma\}$  to block
13:     Broadcast block to network
14: end if
15: Upon receiving a block:
16: if Verify signature  $\sigma$  using public key  $pk$  then
17:     if  $1 \leq W \leq T_{\max}$  and verify integrity of  $H$  then
18:         if Verify consistency of  $(W, H, \sigma)$  then
19:             Validate transaction syntax and permissions
20:             Verify SHA-512 hash of each transaction
21:             Validate block structure
22:             Append block to blockchain
23:         end if
24:     end if
25: end if

```

26: Repeat process for next consensus round

The dominant computational operations in Algorithm 1 are SHA-512 hashing ($O(n)$ where n is input length) and ECDSA signing and verification ($O(1)$ per node), making PPoET computationally lightweight and suitable for real-time healthcare environments.

4.5 SECURITY CONSIDERATIONS

The proposed privacy-aware enhancement of the Proof of Elapsed Time (PPoET) algorithm improves the security of the conventional PoET mechanism by incorporating multiple layers of cryptographic protection and verifiable validation. A secure random value is generated and processed using SHA-512 hashing to ensure data integrity and resistance to tampering during the consensus process. The Elliptic Curve Digital Signature Algorithm (ECDSA) is extended to the consensus layer by digitally signing the wait time along with its hash, creating a verifiable certificate that can be validated by other nodes. This prevents manipulation of wait times and ensures fairness in node selection. The inclusion of the signed certificate and hash within the block structure enhances transparency and traceability while reducing dependence on implicit trust in Trusted Execution Environments (TEEs). Also a multi-layer verification process checks the consistency of the wait time, hash, and signature to protect against attacks such as data tampering and unauthorized block creation. Replay attacks are mitigated by binding the signature σ to both W and H simultaneously, ensuring that previously broadcast wait certificates cannot be reused in subsequent consensus rounds. The use of asynchronous wait time execution also improves system efficiency by reducing delays and supporting better performance under high transaction loads. The entire proposed PPoET mechanism provides a secure, efficient, and reliable solution for healthcare blockchain applications.

4.6 THREAT MODEL FOR PPOET

The proposed PPoET framework operates within a permissioned blockchain environment where participating nodes are authenticated but may exhibit semi-honest or malicious behavior. The threat model considers three types of adversaries: (i) honest-but-curious nodes that follow the protocol while attempting to infer sensitive information, (ii) malicious validators that attempt to manipulate consensus parameters such as wait times or block generation, and (iii) external attackers aiming to tamper with transaction data or disrupt network communication. The execution environment is treated as partially trusted, meaning that internal operations cannot be fully relied upon without external validation. Therefore, the framework incorporates cryptographic verification to ensure correctness. The primary security objective is to guarantee the integrity and authenticity of consensus-related parameters, including wait time values and block generation decisions. The use of ECDSA signatures and SHA-512 hashing prevents unauthorized modification, forgery, and replay of consensus messages. The proposed model does not target full anonymity or zero-knowledge privacy; instead, it focuses on achieving verifiable and tamper-resistant consensus suitable for healthcare blockchain applications. While full patient data privacy is managed at the application layer through access control mechanisms, PPoET ensures consensus-layer privacy by protecting the integrity and confidentiality of decision parameters.

In this work, privacy refers to the protection of consensus-related parameters, particularly wait-time values and their generation process, from unauthorized manipulation and inference. The proposed approach ensures that consensus decisions are verifiable without exposing internal randomness or allowing adversarial modification. EHR payload encryption at the application layer complements the consensus-layer security provided by PPoET, ensuring end-to-end protection of sensitive patient data from submission to blockchain storage.

5. PROMINENCE OF ECDSA INTEGRATION WITH PROPOSED PPOET

The proposed framework introduces a novel integration of the Privacy-Aware Proof of Elapsed Time (PPoET) consensus mechanism with SHA-512-based hashing and an extended application of the Elliptic Curve Digital Signature Algorithm (ECDSA). Traditional approaches restrict ECDSA to transaction authentication, whereas the proposed model extends its role to the consensus layer, enabling validation of node participation and ensuring integrity during block generation. SHA-512 is used to provide a secure and verifiable representation of generated values, contributing to the secure derivation of wait times within the PPoET mechanism. This approach improves unpredictability and fairness in validator selection while reducing susceptibility to manipulation. The use of asynchronous wait time execution further enhances system efficiency by allowing concurrent processing and reducing idle delays. The framework operates within a software-based secure execution environment, eliminating the need for specialized hardware, thereby improving resistance to key exposure and unauthorized modification. Together, these enhancements form a unified architecture that improves security, transparency, and scalability for healthcare blockchain applications. Fig.2 illustrates the technological architecture of the proposed framework, showing the interaction between transaction processing, cryptographic validation, and PPoET-based consensus.

5.1 TRANSACTION PROPOSAL

The process begins with EHR data being encrypted at the application layer to ensure patient data confidentiality. The encrypted payload is then hashed using SHA-512 to ensure integrity, and the resulting hash is digitally signed using ECDSA with the sender's private key, producing a verifiable digital signature. Formally, the signed transaction is represented as $ST = (T, \text{SHA-512}(T), \text{ECDSA}.\text{Sign}(\text{sk}, \text{SHA-512}(T)))$, where T denotes the encrypted transaction data and sk is the sender's private key. The signed transaction is then broadcast to the blockchain network for further validation.

5.2 TRANSACTION AND BLOCK VALIDATION

Validator nodes verify each transaction by checking the ECDSA signature using the sender's public key and validating the integrity of the associated hash. Only transactions that pass these checks are considered valid and forwarded for block inclusion.

Transactions that fail signature verification or hash validation are discarded and flagged for logging, ensuring only authenticated data enters the block formation process. In parallel, nodes participate in the PPoET consensus process by generating and signing wait times for leader selection.

5.3 BLOCK GENERATION AND TRANSACTION GROUPING

The node with the shortest valid wait time is selected as the leader under the PPoET mechanism. This node aggregates validated transactions into a block based on predefined constraints. A Merkle root hash is computed to represent the transaction set efficiently. The block is then appended with the wait certificate (W, H, σ) and broadcast to the network, where other nodes verify the certificate before accepting the block and updating the blockchain. The block header includes the PPoET Leader ID to enable traceability and auditability of the consensus decision. In the event of block rejection, the node with the next shortest valid wait time assumes the leader role and proposes a new block, ensuring continuous consensus operation without network disruption.

6. EXPERIMENTS AND RESULTS

The proposed framework was implemented and evaluated to assess its computational performance and security characteristics in managing Electronic Healthcare Records (EHRs). The prototype was developed using Hyperledger Sawtooth deployed in a Windows-based environment, providing a controlled permissioned blockchain platform for analyzing the behavior of the Privacy-Aware Proof of Elapsed Time (PPoET) mechanism integrated with SHA-512 and ECDSA cryptography. The framework operates within a software-based execution environment, eliminating the need for hardware-based TEEs while maintaining cryptographic security through ECDSA and SHA-512. While conventional PoET implementations rely on Trusted Execution Environments (TEEs) for secure wait-time generation, the proposed PPoET reduces dependence on implicit trust by enabling external cryptographic verification of consensus parameters. This design improves flexibility and allows deployment in environments where dedicated hardware support may be limited. The evaluation was conducted under varying transactional workloads to examine key performance metrics, including transaction processing time, block generation latency, and cryptographic overhead. The results primarily capture the efficiency of hashing operations, digital signature generation and verification, and secure wait-time computation within the proposed framework. It is important to note that the current implementation represents a prototype-level evaluation performed in a single-node environment. While it does not emulate a fully distributed blockchain network, it enables controlled analysis of the computational impact and feasibility of the proposed enhancements. Future work will extend the evaluation to multi-node distributed settings to validate scalability, consensus robustness, and network-level performance.

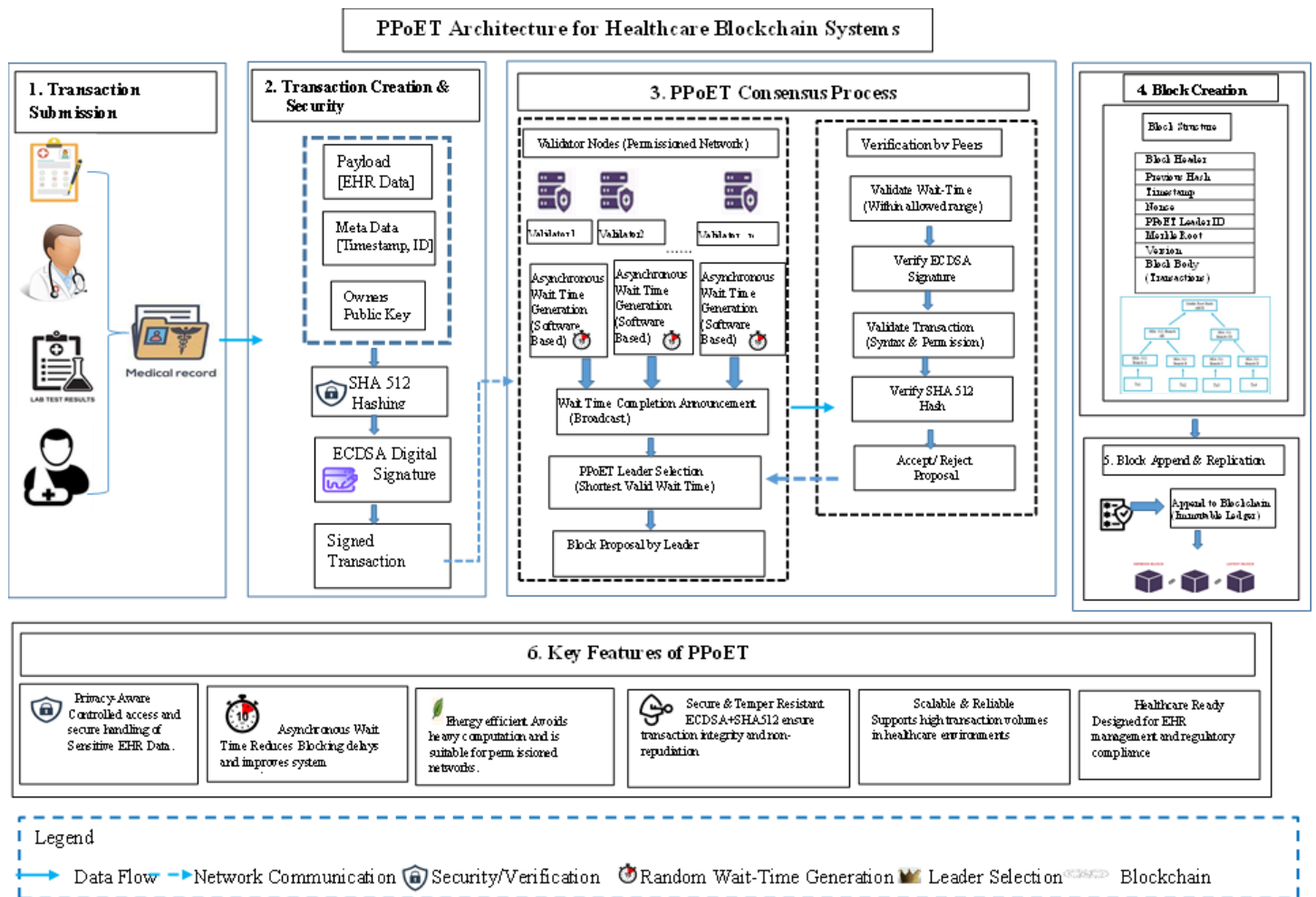


Fig.2. Technological Architecture

6.1 ROUND TRIP EXECUTION TIME

Round trip execution time represents the total delay from transaction submission to final block confirmation. Fig.3 compares the round trip execution time of PoET and the proposed PPoET under different workloads.

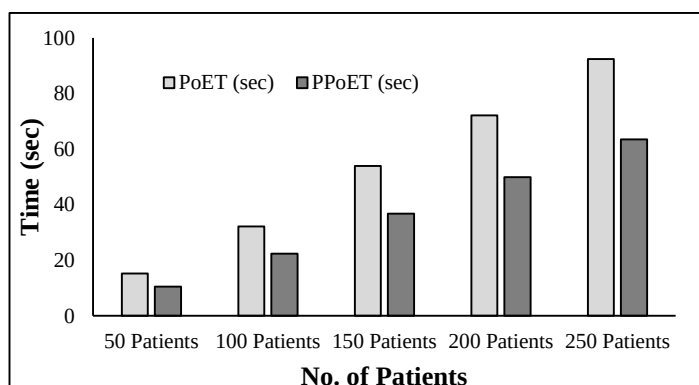


Fig.3. Round Trip Execution Time

As the number of transactions increases, execution time increases for both methods. PPoET consistently achieves lower latency than PoET. For example, the execution time is reduced from about 15 seconds to 10 seconds at lower load and from about

90 seconds to 63 seconds at higher load, showing an improvement of approximately 25–30%. This improvement is due to efficient wait-time generation and reduced validation overhead. The results also indicate that the proposed method maintains stable performance as workload increases, demonstrating better scalability and reduced congestion compared to conventional approaches.

6.2 COMPUTATIONAL PERFORMANCE OF POET AND PPOET

6.2.1 Transaction Throughput (TP):

Transaction throughput measures the number of transactions processed per unit time and reflects the overall efficiency of the blockchain system. It is calculated as:

$$TP = \text{Total number of transactions} / \text{Total execution time}$$

The Fig.4 shows the transaction throughput of PoET and the proposed PPoET under varying transaction loads. As the number of transactions increases, the throughput of both methods improves due to better resource utilization. PoET achieves slightly higher throughput than PPoET across all workloads, with a difference of approximately 5–10%. This difference is due to the additional cryptographic operations in the proposed PPoET, including secure randomness generation and ECDSA-based validation, which introduce moderate computational overhead.

Despite this, PPOET maintains competitive throughput while providing enhanced security, data integrity, and privacy, making it suitable for healthcare applications where security is prioritized over raw throughput.

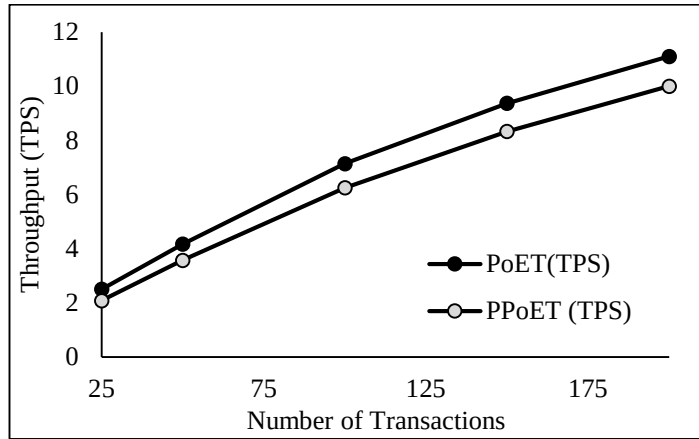


Fig.4. Transaction Throughput

6.2.2 Resource Utilization (RU):

Resource utilization evaluates the efficiency of system resource usage, including CPU, memory, disk space, and network bandwidth, during blockchain operations. It is computed as

$$RU = \left(\frac{\text{Actual resource utilization}}{\text{Maximum resource Capacity}} \right) \times 100\%$$

The Table.2 presents the resource utilization metrics observed during the implementation of the Proposed PPOET framework.

Table.2. Resource Utilization Metrics

Resource	CPU Usage (%)	Memory Usage (GB)	Disk Space (GB)	Network Bandwidth (Mbps)
1 org-1 peer	30	2.5	150	100
2 org-1 peer	35	2.8	155	90
2 org-2 peer	40	3.2	160	85
Average Consumption	35	2.83	155	91.67

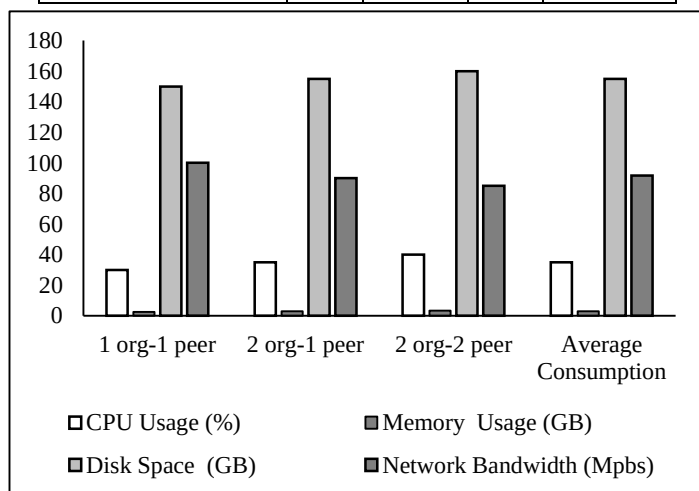


Fig.5. Resource Utilization Metrics

The results indicate that resource consumption increases moderately with the number of participating nodes. CPU usage rises from 30% to 40%, while memory usage increases from 2.5 GB to 3.2 GB. Similarly, disk usage and network bandwidth show gradual variation due to increased transaction processing and communication overhead. Despite the additional cryptographic operations introduced by the proposed PPOET mechanism, the total resource utilization remains within acceptable limits. This demonstrates that the framework achieves a balance between security and system efficiency, making it suitable for practical healthcare blockchain deployment. Fig.5 illustrates resource utilization metrics.

6.2.3 Block Creation Time (BCT):

Block Creation Time (BCT) measures the average time required to generate a block in the blockchain network. It is calculated as:

$$BCT = \frac{\text{Total time for block creation}}{\text{Number of blocks created}}$$

The Fig.6 illustrates the block creation behavior of the proposed system. The results show that the total block creation time increases linearly with the number of blocks, while the average block creation time remains relatively stable.

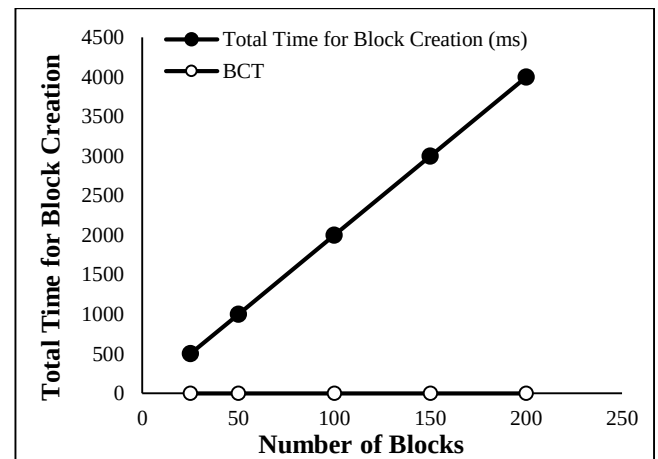


Fig.6. Block Creation Time

For example, the average BCT remained stable at approximately 20 milliseconds across all workloads, demonstrating consistent block generation performance under increasing transaction loads. This indicates that the system maintains a consistent block generation rate regardless of increasing workload. The stable BCT values demonstrate the efficiency of the proposed PPOET consensus mechanism and its ability to scale without significant performance degradation.

6.2.4 Cryptographic Overhead (CO):

The performance of the ECDSA model is analyzed by measuring the execution time of its key operations, including key generation, signing, and verification, under varying transaction loads. Key generation incurs a one-time cost per node initialization, while signing and verification contribute to per-transaction processing time.

Among these operations, signature generation and verification dominate the cryptographic overhead, particularly as the number of transactions increases. Fig.7 presents the execution time for different cryptographic stages under varying patient scenarios. Three patient scenarios are considered: Scenario 1 - single patient with 10 EHR records, Scenario 2 - 10 patients with 100 EHR records, and Scenario 3 - 100 patients with 1000 EHR records. The results indicate that signing and verification contribute the majority of the cryptographic overhead, while key generation incurs a one-time cost. Although the proposed PPoET framework introduces additional cryptographic processing, the observed overhead remains within acceptable limits, demonstrating that the system achieves a balance between security and performance. The cryptographic overhead is calculated as:

The integration of strong cryptographic mechanisms enhances data integrity, authenticity, and resistance to tampering, which are essential for healthcare applications.

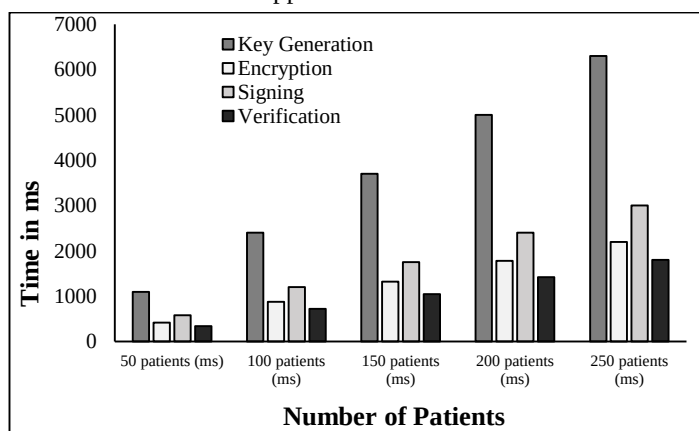


Fig.7. Cryptographic overhead across different stages and patient scenarios

The evaluation of the proposed Privacy-Aware Proof of Elapsed Time (PPoET) demonstrates its effectiveness in supporting secure healthcare blockchain applications. The results show reduced transaction latency and stable resource utilization, while maintaining acceptable throughput and scalability. Although additional cryptographic operations introduce moderate overhead, they significantly enhance data integrity and security. The proposed framework integrates efficiency, security, and compliance considerations, making it suitable for reliable and privacy-aware healthcare data management.

7. DISCUSSION

The evaluation of the proposed Privacy-Aware Proof of Elapsed Time (PPoET) demonstrates its potential to enhance healthcare blockchain adoption. The results indicate reduced transaction latency and stable resource utilization, while maintaining acceptable throughput and scalability. Although the integration of cryptographic mechanisms introduces moderate computational overhead, it remains within acceptable limits and is justified by the improved data integrity and security. The incorporation of compliance-aware mechanisms within the consensus layer supports alignment with healthcare requirements and facilitates interoperability across diverse Electronic Health Record (EHR) systems. Enhanced cryptographic safeguards

strengthen transaction authenticity and reduce the risk of tampering and unauthorized access. The proposed PPoET framework achieves a balanced trade-off between performance, security, and regulatory compliance, providing a practical solution for secure and privacy-aware healthcare data management.

8. CONCLUSION

Experimental results confirm that the proposed approach achieves reduced transaction latency, stable resource utilization, and acceptable throughput, while introducing moderate cryptographic overhead. This balance highlights the effectiveness of PPoET in addressing key challenges such as data integrity, scalability, and secure transaction processing in healthcare environments. The current evaluation is limited to a prototype-level single-node environment and does not capture network congestion or multi-node consensus behavior. Future work will extend the evaluation using distributed testbeds and benchmarking tools to analyze performance under high-load and adversarial conditions, as well as compare PPoET with other privacy-oriented consensus mechanisms.

REFERENCES

- [1] Rui Zhang, Rui Xue and Ling Liu, "Security and Privacy on Blockchain", *ACM Computing Surveys*, Vol. 52, No. 3, pp. 1-33, 2019.
- [2] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", Available at: <https://bitcoin.org/bitcoin.pdf>, Accessed in 2018.
- [3] Bela Shrimali and B. Hiren Patel, "Blockchain State-of-the-Art: Architecture, Use Cases, Consensus, Challenges and Opportunities", *Journal of King Saud University-Computer and Information Sciences*, Vol. 34, No. 9, pp. 6793-6807, 2011.
- [4] Sivleen Kaur, Sheeta Chaturvedi, Aabha Sharma and Jayaprakash Kar, "A Research Survey on Applications of Consensus Protocols in Blockchain", *Security and Communication Networks*, Vol. 2021, pp. 1-11, 2021.
- [5] Ahmed Afif Monrat, Olov Schelen and Karl Andersson, "A Survey of Blockchain from the Perspectives of Applications, Challenges and Opportunities", *IEEE Access*, Vol. 7, pp. 117134-117151, 2019.
- [6] Asad Ali Siyal, Aisha Zahid Junejo, Muhammad Zawish, Kainat Ahmed, Aiman Khalil and Georgia Soursou, "Applications of Blockchain Technology in Medicine and Healthcare: Challenges and Future Perspectives", *Cryptography*, Vol. 3, No. 1, pp. 1-10, 2021.
- [7] Erikson Julio De Aguiar and S. Bruno Faical, "A Survey of Blockchain-based Strategies for Healthcare", *ACM Computing Surveys*, Vol. 53, No. 2, pp. 1-13, 2020.
- [8] Merlinda Andoni, Valentin Robu, David Flynn, Simone Abram, Dale Geach, David Jenkins, Peter McCallum and Andrew Peacock, "Blockchain Technology in the Energy Sector: A Systematic Review of Challenges and Opportunities", *Renewable and Sustainable Energy Reviews*, Vol. 100, pp. 143-174, 2019.

- [9] Mic Bowman, Debajyoti Das, Avradip Manda and Hart Montgomery, "On Elapsed Time Consensus Protocols", *Progress in Cryptology*, Vol. 2, pp. 559-583, 2021.
- [10] Benjamin Ampel, Mark Patton and Hsinchun Chen, "Performance Modeling of Hyperledger Sawtooth Blockchain", *Proceedings of International Conference on Intelligence and Security Informatics*, Vol. 8, pp. 1-11, 2019.
- [11] Y. Mohammad and Alshahrani, "Implementation of a Blockchain System using Improved Elliptic Curve Cryptography Algorithm for the Performance Assessment of the Students in the E-Learning Platform", *Applied Sciences*, Vol. 12, No. 74, pp. 1-13, 2022.
- [12] Yanjun Jiang and Siye Ding, "A High Performance Consensus Algorithm for Consortium Blockchain", *Proceedings of International Conference on Computer and Communications*, Vol. 5, pp. 1-15, 2018.
- [13] Adrian Antipa, Daniel Brown, Robert Gallant, Rob Lambert, Rene Struik and Scott Vanstone, "Accelerated Verification of ECDSA Signatures", *International Workshop on Selected Areas in Cryptography*, Vol. 3897, pp. 307-318, 2006.
- [14] Diba Chowdhury, Laila Tamanna Anni, Mahmudul Hasan, Nayeem Al-Tamzid Bhuiyan, Nafiul Islam and Rahat Pervez, "Cryptographic Ledger of Blockchain Technology in Healthcare", *GSC Biological and Pharmaceutical Sciences*, Vol. 7, No. 3, pp. 28-37, 2021.
- [15] S. Kanagasankari and V. Vallinayagi, "A Comparative Analysis of Consensus Algorithms in the Health Care Sector using Block Chain Technology", *International Journal of Health Sciences*, Vol. 6, No. 1, pp. 11702-11716, 2019.
- [16] Shunrong Jiang, Haiqin Wu and Liangmin Wang, "Patients-Controlled Secure and Privacy-Preserving EHRs Sharing Scheme based on Consortium Blockchain", *Proceedings of International Conference on Global Communications*, Vol. 8, pp. 1-11, 2019.
- [17] Weiquan Ni, Xumin Huang, Junxing Zhang and Rong Yu, "HealChain: A Decentralized Data Management System for Mobile Healthcare using Consortium Blockchain", *Proceedings of International Conference on Global Communications*, Vol. 9, pp. 6333-6338, 2019.
- [18] Randhir Kumar and Rakesh Tripathi, "A Secure and Distributed Framework for Sharing COVID-19 Patient Reports using Consortium Blockchain and IPFS", *Proceedings of International Conference on Parallel, Distributed and Grid Computing*, Vol. 8, pp. 1-11, 2020.
- [19] Yanjun Jiang and Siye Ding, "A High Performance Consensus Algorithm for Consortium Blockchain", *Proceedings of International Conference on Computer and Communications*, Vol. 12, pp. 1-17, 2018.
- [20] Ashok Kumar Yadav, "Significance of Elliptic Curve Cryptography in Blockchain IoT with Comparative Analysis of RSA Algorithm", *Proceedings of International Conference on Computing, Communication and Intelligent Systems*, Vol. 8, pp. 256-261, 2021.
- [21] Elif Hilal Umucu, "Elliptic Curve Cryptography in Blockchain Technology", *Proceedings of International Conference on Computing, Communication, and Intelligent Systems*, Vol. 8, pp. 1-9, 2019.
- [22] Yen-Liang Lee, Hsiu-An Lee, Chien-Yeh Hsu and Hsin-Hua Kung, "SEMRES-A Triple Security Protected Blockchain based Medical Record Exchange Structure", *Computer Methods and Programs in Biomedicine*, Vol. 215, pp. 1-18, 2021.
- [23] Kundan Munjal and Rekha Bhatia, "A Systematic Review of Homomorphic Encryption and its Contributions in Healthcare Industry", *Complex and Intelligent Systems*, Vol. 8, pp. 1-9, 2021.
- [24] W. Joppe Bos, J. Alex Halderman, Nadia Heninger, Jonathan Moore, Michael Naehrig and Eric Wustrow, "Elliptic Curve Cryptography in Practice", *Proceedings of International Conference on Financial Cryptography and Data Security*, Vol. 8437, pp. 157-175, 2021.
- [25] Anubis Graciela de Moraes Rossetto, Christofer Sega and Valderi Reis Quietinho Leithardt, "An Architecture for Managing Data Privacy in Healthcare with Blockchain", *Sensors*, Vol. 22, No. 21, pp. 1-15, 2022.
- [26] Aniruddha Bhattacharjya, Kamil Kozdroj, Grzegorz Bazydło and Remigiusz Wisniewski, "Trusted and Secure Blockchain-based Architecture for Internet-of-Medical-Things", *Electronics*, Vol. 11, No. 16, pp. 1-17, 2018.
- [27] Giang-Truong Nguyen and Kyungbaek Kim, "A Survey about Consensus Algorithms Used in Blockchain", *Journal of Information Processing Systems*, Vol. 14, No. 1, pp. 101-128, 2019.
- [28] Sudeep Tanwar, Karan Parekh and Richard Evans, "Blockchain-based Electronic Healthcare Record System for Healthcare 4.0 Applications", *Journal of Information Security and Applications*, Vol. 50, pp. 1-13, 2019.
- [29] Wanbing Zhan, Chin-Ling Chen, Wei Weng, Woei-Jiunn Tsaor, Zi-Yi Lim and Yong-Yuan Deng, "Incentive EMR Sharing System based on Consortium Blockchain and IPFS", *Healthcare*, Vol. 10, No. 10, pp. 1-7, 2019.
- [30] Muhammad Rashid, Harish Kumar, Sikandar Zulqarnain Khan, Ismail Bahkali, Ahmed Alhomoud and Zahid Mehmood, "Throughput/Area Optimized Architecture for Elliptic-Curve Diffie-Hellman Protocol", *Applied Sciences*, Vol. 12, No. 8, pp. 1-13, 2018.
- [31] Alexandru Bratu and Florin Haralimbe, "Blockchain Bridges for Verifiable Credentials in Healthcare-A Cross-Chain Interoperability Approach", *IEEE*, Vol. 12, pp. 1-17, 2025.
- [32] Arjun Rajasekharan and Rani Koshy, "EMRChain: Electronic Medical Records Management System using Blockchain", *IEEE*, Vol. 7, pp. 1-10, 2024.
- [33] S. Nekkhalapudi, R.K. Mishra and M. Pandey, "Blockchain-based Healthcare Outcome Improvement: A Decentralized Method of Patient Care", *Proceedings of International Conference on Data, Computation and Communication*, Vol. 23, pp. 546-550, 2024.
- [34] F. Bratu, P. Haralambie, A. Raluca-Ioana, A. Aloman and N. Goga, "Blockchain Bridges for Verifiable Credentials in Healthcare - A Cross-Chain Interoperability Approach", *Proceedings of International Conference on Blockchain, Smart Healthcare and Emerging Technologies*, Vol. 12, pp. 1-6, 2025.
- [35] S Kanagasankari and V. Vallinayagi, "An Efficient Byzantine Consensus Mechanism based on Healthcare Sector in Blockchain", *Multimedia Tools and Applications*, Vol. 23, pp. 51129-51158, 2025.
- [36] Soubhagya Ranjan Mallick, Suraj Sharma and Niranjana Kumar Ray, "Fog-Assisted Blockchain-IoMT Healthcare

- Framework with Role-based Access Control for Critically ill Patients”, *SN Computer Science*, Vol. 5, pp. 1-19, 2024.
- [37] Soubhagya Ranjan Mallick, Srichandan, Sobhanayak and Rakesh Kumar Lenka, “Blockchain-Enhanced IoT Ecosystem for Healthcare: Transformative Potentials, Applications, Challenges, Solutions and Future Perspectives”, *Computers and Industrial Engineering*, Vol. 197, pp. 1-9, 2024.
- [38] Soubhagya Ranjan Mallick, Rakesh Kumar Lenka and Srichandan Sobhanayak, “Secure and Scalable Dual Blockchain and IPFS Driven IoT Ecosystem for Next Gen Healthcare Systems”, *Scientific Reports*, Vol. 15, No. 4, pp. 1-7, 2024.