Protecting Multi-Source Cardiovascular Disease Data Through an Innovative Token-Based Pure Proof of Stake Blockchain

D. Chandrakantham[1], D. Gayathri Devi[2]

[1]Research Scholar, Department of Computer Science, Sri Ramakrishna College of Arts and Science for Women,
Coimbatore -641044, Tamil Nadu, India
Corresponding Author Email: *chandra.it3phd[at]gmail.com*

[2]Associate Professor, Department of Computer Science, Sri Ramakrishna College of Arts and Science for Women,
Coimbatore -641044, Tamil Nadu, India

Abstract: ***The rapid growth of Cardiovascular Disease (CVD) data from heterogeneous sources, including diagnostic imaging systems, electrocardiography devices, wearable sensors, and public research repositories, has created major challenges in ensuring data confidentiality, integrity, controlled access, and scalable management. Conventional centralized data storage architectures are prone to security breaches, and limited audit transparency. To address these limitations, this paper proposes a secure and scalable Token-Based PPos Heart chain (TPPoSHChain) framework for the management of multi-source CVD datasets by integrating blockchain technology, decentralized identity, authenticated encryption, and token-based access governance. The framework employs a hybrid on-chain/off-chain architecture, where the Algorand blockchain with a Pure Proof of Stake (PPoS) consensus mechanism provides immutable audit logging and access control enforcement, while encrypted datasets are stored off-chain in the InterPlanetary File System (IPFS) to enhance scalability. ChaCha20-Poly1305 authenticated encryption is used to protect datasets prior to storage and transmission, ensuring both confidentiality and integrity. Decentralized Identifiers (DIDs) establish a self-sovereign identity layer for data contributors, and actors, eliminating reliance on centralized identity providers. A blockchain-supported token-based access control mechanism enables fine-grained authorization, usage traceability, and secure cross-institutional data sharing. Experimental evaluation demonstrates that the proposed TPPoSHChain framework significantly improves transaction throughput, reduces latency, lowers storage overhead, and achieves efficient encryption performance than other existing models, making it well suited for secure and scalable CVD datasets.***

Keywords: Cardiovascular Disease dataset, Algorand Blockchain, Decentralized Identifiers, ChaCha20-Poly1305, InterPlanetary File System.

1. Introduction

Cardiovascular disease (CVD) remains the leading cause of mortality worldwide and represents a major focus of modern biomedical research [1]. The rapid advancement of diagnostic technologies, medical imaging systems, electrocardiography devices, wearable health monitors, and large-scale clinical studies has led to the generation of vast volumes of heterogeneous cardiovascular data [2]. These data play a crucial role in predictive modelling, disease classification, early risk detection, and the development of Artificial Intelligence (AI)–based healthcare solutions. However, the distributed and sensitive nature of such data introduces serious challenges related to data confidentiality, integrity, controlled sharing, and system scalability [3, 4]. Traditional centralized data management approaches are not well suited for handling multi-source medical datasets. Central repositories suffer from single points of failure, vulnerability to cyberattacks, limited transparency, and difficulties in maintaining data provenance and auditability [5, 6]. Unauthorized data access, tampering, and misuse can lead to ethical, legal, and financial consequences, particularly when dealing with health-related information. As research increasingly involves multiple institutions and data contributors, there is a growing need for a decentralized, trust-driven framework capable of securely managing CVD datasets while preserving performance efficiency.

Blockchain technology has emerged as a promising solution for addressing these challenges due to its decentralized architecture, immutability, and cryptographic security [7]. By maintaining a distributed ledger of transactions validated through consensus mechanisms, blockchain enables transparent auditing and tamper-resistant record management [8]. However, conventional blockchain platforms such as Ethereum face scalability limitations, high computational overhead, and increased transaction latency when handling large volumes of data [9]. Storing large medical datasets directly on-chain is impractical due to storage costs and performance degradation.

To address these limitations, hybrid blockchain architectures that combine on-chain verification with off-chain storage have gained attention. Meanwhile, secure identity management and efficient encryption mechanisms are essential to ensure end-to-end protection. Identifiers provide self-identity management without reliance on centralized authorities, enabling secure authentication and role verification. Also, authenticated encryption algorithms offer strong confidentiality, and integrity guarantees with lower computational overhead compared to traditional block ciphers, making them suitable for heterogeneous healthcare environments.

Motivated by these needs, this paper proposes a secure and scalable Token-Based PPos Heart chain (TPPoSHChain) framework for managing multi-source CVD datasets by

Paper ID: SR26226150952 DOI: https://dx.doi.org/10.21275/SR26226150952

integrating Algorand's Pure Proof of Stake (PPoS) consensus mechanism, decentralized identity through Decentralized Identifiers (DIDs), authenticated encryption using ChaCha20-Poly1305, and token-based access control within a hybrid on-chain/off-chain architecture. Encrypted datasets are stored in the InterPlanetary File System (IPFS), while only content hashes and access metadata are recorded on the blockchain, ensuring scalability and immutability. The proposed TPPoSHChain framework aims to provide trustworthy data governance, efficient resource utilization, and robust protection against unauthorized access and data tampering. The effectiveness of the system is validated using real cardiovascular datasets, where performance is evaluated in terms of transaction throughput, latency, storage overhead, and encryption efficiency.

The remainder of the article is: Section 2 highlights some of the relevant literatures. Section 3 presents the proposed TPPoSHChain framework in detail and section 4 evaluates it and provides result. Finally, section 5 summarizes the article and suggests future directions.

2. Literature Survey

2.1 Related to different consensus mechanisms

Aluko & Kolonin [10] developed a Proof-of-Reputation (PoR) consensus mechanism in which blockchain consensus was achieved by dynamically selecting a group of nodes with the highest reputation values to validate and append new blocks. The method computed node reputation using a liquid reputation model that combined normalized interaction ratings with the historical reputation of the rating nodes, thereby weighting feedback based on the trustworthiness of the rater. A temporal decay factor was incorporated to reduce the influence of older interactions, enabling the system to adapt to behavioral changes over time. However, the approach incurred additional computational and storage overhead due to continuous reputation evaluation and side-chain maintenance, which potentially limited its scalability.

Xu et al. [11] devised a Proof-of-Engagement (PoE) consensus mechanism for blockchain-based smart contract systems that incorporated contract quality and node activity into the block production process. The method modelled consensus as a proof-class mechanism in which leader election probability was determined by a combined metric of smart contract quality and node engagement. It further introduced work-area–specific engagement to support differentiated application domains and employed incentive compatibility analysis to encourage nodes to remain active and improve contract quality. However, the model increased computational overhead and system complexity, potentially limiting its scalability.

Baageel & Rahman [12] suggested a hybrid Proof of Stake and Work (PoSW) which combined Proof of Stake (PoS) for miner-to-shard assignment with Proof of Work (PoW) for block validation within shards, where miners were allocated to shard levels based on their stake and computational capacity. Transaction workloads were distributed proportionally across shards, and shard-specific PoW difficulty levels were applied to balance efficiency and fairness, with higher-capability shards handling higher-fee transactions. Periodic reshuffling of miners within shards was employed to mitigate long-range and Sybil attacks. But heterogeneous PoW difficulty management increased system complexity and introduced additional coordination overhead. Narayan et al. [13] suggested a Delegated PoS with Exponential Back-off (DPoSEB) consensus algorithm to reduce delays in blockchain networks. The method selected delegate nodes based on stake and coinage, granting them exclusive rights to propose and mine blocks, while introducing a random sleep-time mechanism to determine the leader for each consensus round. To mitigate collisions arising from identical wake-up times among delegates, an exponential back-off strategy was applied, allowing collided nodes to reattempt block proposal after progressively increasing wait intervals. However, the randomized waiting affects scalability in densely populated blockchain networks.

Siraj et al. [14] suggested a Proof-of-Green (PoG) consensus mechanism to achieve scalability and security. The method employed a weighted voting–based leader election process that incorporated a credibility scoring system and operated through three sequential stages: Red Announcements, Yellow Transactions, and Green Blocks to validate transactions and produce blocks. Credibility scores were used to determine voting influence and to enhance resilience against malicious behavior, while an on-chain provenance mechanism supported accountability and attack resistance. However, the algorithm required careful calibration of trust parameters, that may introduce overhead in highly dynamic or large-scale decentralized networks.

Fu et al. [15] developed a Zero-Knowledge Proof of Training (ZKPoT) consensus mechanism to enhance privacy, security, and efficiency in federated learning based blockchain systems. A customized blockchain architecture was designed that incorporated ZKPoT-specific block and transaction structures along with IPFS integration to reduce communication and storage overhead during federated learning. The approach enabled secure validation of local model updates while maintaining robustness against Byzantine and privacy attacks across diverse blockchain settings. However, the model introduced significant cryptographic complexity and computational overhead.

Lei et al. [16] devised a Quadratic Voting–based Delegated Proof of Stake (Q-DPoS) consensus mechanism to mitigate stake centralization. The method integrated quadratic voting into delegate selection, vote counting, and reward settlement processes to redistribute voting power more equitably and incentivize participation from low-stake users. To enhance robustness, admission rules and vote similarity detection techniques were incorporated to prevent Sybil attacks and avoid regression to linear reward structures. However, it increased computational overhead and system complexity, potentially affecting its scalability.

2.2 Related to blockchain security

Azbeg et al. [17] suggested a blockchain-based framework for securing remote patient monitoring, particularly for chronic disease management. To enhance data integrity, transparency, and access control, the framework integrated an Ethereum blockchain using a Proof of Authority (PoA) consensus mechanism, which provided faster transaction processing and reduced latency. To address blockchain storage limitations and improve scalability, medical data were stored off-chain in the InterPlanetary File System (IPFS), while only hash references and access policies were maintained on-chain. However, Ethereum PoA may limit scalability under large data volumes potentially affecting system performance in large-scale deployments.

Sasikumar & Karthikeyan [18] developed an Attribute-Based Access Control (ABAC) mechanism for secure sharing of medical data such as heart disease with enhanced privacy and access control. Also, the framework integrated a Gaussian Naïve Bayes algorithm to predict cardiovascular disease risk, enabling physicians to identify high-risk patients and assess severity levels through feature-weighted analysis. A dynamic emergency access mechanism was also introduced, granting temporary privileges to emergency personnel, which were automatically revoked after the emergency based on severity scores. However, the model introduced additional computational overhead.

Hegde & Maddikunta [19] devised a secure and lightweight blockchain framework for healthcare applications including CVD based on a modified Practical Byzantine Fault Tolerance (PBFT) consensus algorithm. To enhance the PBFT mechanism, the system incorporated the Eigen Trust model to evaluate node reputation and restrict consensus participation to highly trusted nodes. Additionally, a Verifiable Random Function (VRF) was employed to randomly select the primary node from the trusted node set, improving fairness and reducing the risk of targeted attacks. But the model imposed additional coordination overhead, which may limit its scalability.

Saxena et al. [20] developed a framework incorporating Hyperledger Fabric for scalability, privacy, and customizable access control. The model integrated AI and blockchain to enable tamper-proof storage and secure data sharing among stakeholders. However, the blockchain component remains at a conceptual stage without full system deployment.

3. Proposed Methodology

This section proposes a secure and scalable TPPoSHChain framework for managing CVD–related EHRs using a combination of Algorand consensus, decentralized identifiers, cryptographic encryption, and token-based access control. This methodology is designed to address key challenges in healthcare data management, including data confidentiality, integrity, access control, scalability, and real-time availability. Fig. 1 shows the block diagram of the research.

3.1 System Architecture

The proposed TPPoSHChain system adopts a hybrid on-chain/off-chain architecture. The Algorand blockchain, which includes PPoS, serves as the on-chain layer responsible for transaction validation, access control enforcement, and immutable audit logging. In contrast, CVD medical data is stored off-chain using the Inter Planetary File System (IPFS) to overcome blockchain storage limitations and enhance scalability. Additionally, ChaCha20-Poly1305 encryption is used to further enhance the data security. The following subsections will break down these mechanisms for improving the security of CVD dataset.

1) Algorand Consensus Mechanism

The Algorand blockchain is a decentralized distributed ledger system to securely record and validate transactions across a network of participating nodes. Similar to other blockchain platforms, Algorand maintains an append-only structure in which data are organized into sequential blocks that are cryptographically linked. A distinguishing characteristic of Algorand lies in its consensus mechanism, which is specifically engineered to address the scalability, latency, and energy inefficiencies observed in earlier blockchain systems such as Bitcoin and Ethereum Algorand employs a PPoS consensus protocol which significantly reduces energy consumption while enabling rapid transaction finality and high throughput.

In the PPoS model, block proposers and validators are selected randomly and privately from the set of users holding Algo cryptocurrency. The probability of selection is proportional to the user's stake, ensuring that participants with higher token holdings have a correspondingly greater influence in proposing and validating blocks. This mechanism discourages malicious behavior, as adversarial actions would directly undermine the value of the attacker's own stake. Moreover, the private and randomized nature of participant selection enhances security by limiting targeted attacks on known validators. The PPoS consensus process in Algorand follows a structured multi-phase protocol that ensures agreement among network participants without requiring excessive computational effort [base]. The process consists of four principal stages including block proposal, soft voting, certify voting, and block finalization.

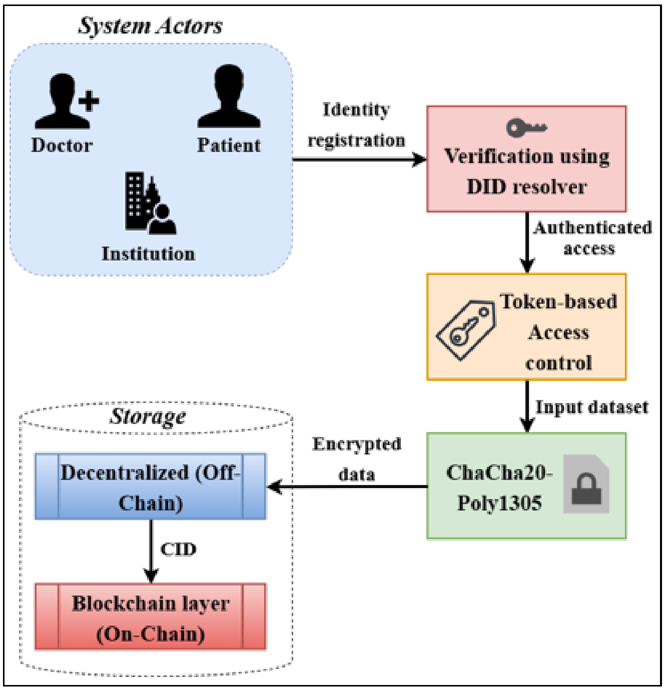

Figure 1: Block diagram of the proposed model

Paper ID: SR26226150952 DOI: https://dx.doi.org/10.21275/SR26226150952

Through this mechanism, Algorand achieves fast confirmation times, strong security guarantees, and high scalability, while avoiding the excessive energy and computational costs associated with traditional blockchains.

2) Decentralized Identifiers (DIDs)

Conventional digital identity management relies predominantly on centralized identifiers such as usernames, email addresses, and passwords, which have long served as the primary means of accessing online services and applications. However, centralized identity repositories are vulnerable to cyberattacks, expose sensitive personal information to service providers, and suffer from single points of failure that can lead to large-scale service disruptions. In distributed research environments that manage sensitive cardiovascular data, these limitations pose serious risks to privacy, data governance, and operational continuity. To address these shortcomings, this research adopts Decentralized Identifiers (DIDs) as a core component of the proposed TPPoSHChain framework. DIDs are globally unique identifiers that are registered and managed within a decentralized infrastructure, typically supported by blockchain technology. They are cryptographically verifiable and are not tied to centralized identity providers. Each DID is associated with a DID document containing essential metadata such as public cryptographic keys, authentication methods, service endpoints, and verification parameters. Within the proposed system, DIDs serve multiple roles beyond simple authentication. They provide a trusted mechanism for binding system participants including data providers, doctors acting as clinical validators, dataset contributors, and researchers to cryptographic credentials that support secure and controlled access to CVD datasets. The DID lifecycle follows a structured process:

- DID Creation and Registration: A DID is generated and registered on the blockchain ledger, establishing a tamper-resistant identity record within the decentralized network.
- DID Document Association: Each DID is linked to a DID document that stores cryptographic keys, digital signatures, and service references required for identity verification and authorization.
- Identity Resolution and Verification: When identity validation is required, a DID resolver interacts with the blockchain to retrieve the corresponding DID document and verify its authenticity. Fig. 2 shows the block diagram of DID.

Cryptographic operations form the foundation of DID security. Key generation is performed using established public-key cryptographic principles to produce secure public–private key pairs. These keys are used to digitally sign identity-related data, ensuring non-repudiation and authenticity. During the signing process, a cryptographic hash of the data is generated and encrypted using the private key to produce a digital signature. Verification is achieved by applying the corresponding public key to validate the signature, confirming both the integrity of the identity data and the legitimacy of the participant.

3) Encryption Algorithm

After identity management, the selection of an appropriate encryption algorithm is a critical design decision for systems handling sensitive CVD datasets. Several factors must be considered when choosing an encryption scheme, including security strength, computational efficiency, scalability, and compatibility with heterogeneous hardware environments. The Advanced Encryption Standard (AES) is widely recognized for its strong security guarantees and high performance, particularly on platforms that support AES-New Instructions (AES-NI). However, modern CVD data ecosystems involve diverse devices such as mobile platforms, wearable sensors, edge devices, and legacy systems, many of which lack AES-NI support. In such environments, the performance advantages of AES may diminish, potentially affecting real-time data acquisition, distributed storage, and cross-institutional dataset sharing.

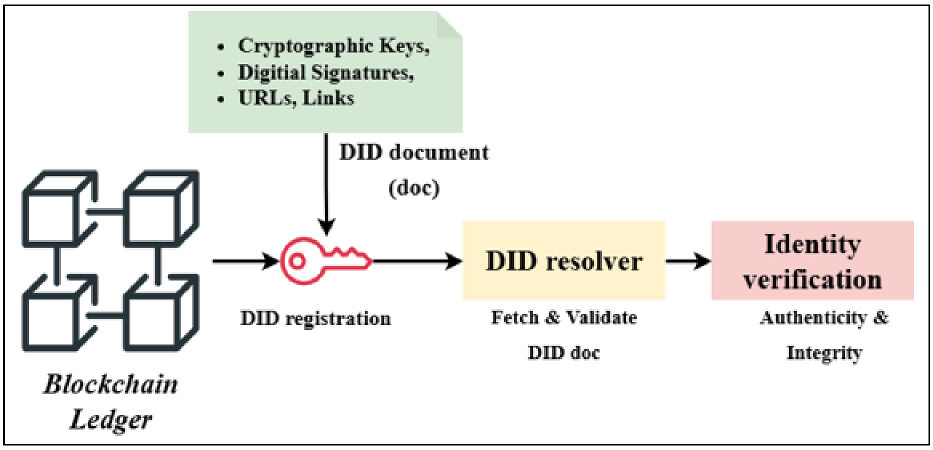

Figure 2: Decentralized identifier management workflow

In contrast, ChaCha20-Poly1305 emerges as a highly versatile and robust alternative. It provides a level of security comparable to AES while maintaining consistently high performance across a wide range of hardware platforms, including those without specialized cryptographic acceleration. Based on these considerations, ChaCha20-Poly1305 is adopted in this research due to its flexibility, strong security properties, and efficient performance across diverse platforms. Its ability to deliver reliable encryption without dependence on specific hardware features makes it well aligned with the distributed and heterogeneous nature of multi-source CVD dataset environments, ensuring that sensitive cardiovascular data remains protected regardless of the underlying infrastructure.

In this algorithm, multi-source CVD datasets such as ECG recordings and echocardiography images are encrypted prior to storage or transmission. A unique encryption key is derived for each operation by combining a secret key with a nonce and a counter, ensuring that identical plaintext data never produce the same ciphertext. The plaintext dataset is combined with a keystream generated by the ChaCha20 cipher using an XOR operation, after which the Poly1305 algorithm generates an authentication tag to verify data integrity and authenticity. The resulting encrypted output consists of the ciphertext accompanied by a verification tag, providing strong protection against unauthorized modification.

- Key and Nonce Generation: A 256-bit secret key is generated for the encryption process and securely maintained. Additionally, a 96-bit nonce is created for each encryption operation to ensure uniqueness and prevent ciphertext repetition.
- ChaCha20 Encryption: ChaCha20 operates as a stream cipher that produces a pseudorandom keystream based on the secret key and nonce. The CVD dataset is encrypted by applying a bitwise XOR operation between the plaintext and the generated keystream, producing the ciphertext.
- Poly1305 Authentication: Poly1305 computes a Message Authentication Code (MAC) over the ciphertext and any associated authenticated data. A one-time authentication key is derived from the ChaCha20 key and nonce, ensuring that each authentication tag is unique and resistant to forgery.
- Output Generation and Verification: The final encrypted output consists of the ciphertext concatenated with the Poly1305 authentication tag. During decryption, the receiver regenerates the keystream using the same key and nonce, decrypts the ciphertext, and verifies the authentication tag. Any mismatch in verification indicates potential data tampering, and the dataset is rejected.

Through this authenticated encryption approach, ChaCha20-Poly1305 ensures both confidentiality and integrity of multi-source CVD datasets, making it a reliable cryptographic foundation for secure, distributed cardiovascular data management systems.

4) Access control with Tokens

Token-based access control is a security mechanism designed to regulate user access to system resources using digitally generated tokens rather than static credentials. It issues encrypted tokens by encapsulating user identity, roles, permissions, and session validity. These tokens act as temporary, verifiable credentials that enable secure and controlled access to protected resources. In this research, the integration of blockchain-supported tokens enables fine-grained authorization, traceability of access events, and improved transparency in dataset usage. Within the proposed TPPoSHChain framework, actors like doctors, patients and institutions can control which entities are permitted to access specific CVD datasets derived from their physiological or diagnostic data. Doctors and clinical experts are granted permissions primarily for data validation and annotation roles, while patients obtain access strictly according to approved research objectives and role-based policies. This ensures that sensitive cardiovascular datasets are shared only with authorized parties under well-defined usage conditions.

In addition, tokens support dataset access auditing, service authorization, and accountability by recording access transactions on the blockchain ledger. This mechanism not only strengthens security but also enhances trust among participating institutions by providing transparent and immutable logs of dataset usage. Token-based governance therefore forms a critical component of secure, collaborative CVD datasets.

3.2 Workflow of the model

This section offers a structured, multi-stage workflow of the proposed TPPoSHChain model to ensure secure registration, controlled access, encrypted data handling, and immutable management for CVD datasets. It consists of various steps, which is illustrated in Fig. 3.

Algorithm 1: Secure Management of CVD datasets using TPPoSHChain

Input: Institution wallet W_I, Doctor wallet W_D, Patient wallet W_P, Raw CVD dataset D

Output: Secure storage, controlled access, and immutable verification of encrypted CVD datasets

```
### System Initialization and Role Definition
Institution connects wallet $W_I$ to the platform
Verify identity on blockchain
Define system roles $R = \{Administrator, Doctor, Patient\}$
Assign role-based permissions
Record role definitions on blockchain

### User Registration and Authentication
Doctor and Patient connect wallets $W_D, W_P$
Users submit credentials
If credentials are valid:
    Authenticate user
Else:
    Reject access

### Token Issuance and Opt-In
Institution receives dataset participation request
Verify authenticated user identity
Generate role-based access token $T$
Encrypt and digitally sign token
Assign token expiration
Record token issuance on blockchain

### Verification and Patient–Doctor Assignment
Validate doctor token $T_D$
Validate patient token $T_P$
If both tokens are valid:
    Authorize doctor to validate/annotate patient dataset
    Update association mapping on blockchain
Else:
    Deny assignment
```

```
### DID Generation and Data Encryption
25) Generate Decentralized Identifier (DID) for participant
26) Generate encryption key $K$ and nonce $N$
27) Encrypt dataset using ChaCha20
28)         $C = D \oplus KS(K, N)$
29) Generate authentication tag using Poly1305
30) Bind encrypted dataset with DID

### Decentralized Storage via IPFS
31) Upload encrypted data $C \mid\mid Tag$ to IPFS
32) Generate Content Identifier (CID)
33) Map CID to corresponding DID

### Blockchain Recording and Verification
34) Create blockchain transaction containing {CID, DID,
    access metadata}
35) Validate transaction using PPoS consensus
36) Append transaction to Algorand ledger
37) Confirm transaction finality

### Secure Data Access and Retrieval
38) User submits access request with token $T$
39) Validate token authenticity and expiration
40) Verify access permissions
41) Retrieve CID from blockchain
42) Fetch encrypted data from IPFS
43) Verify Poly1305 authentication tag
44) Decrypt data using ChaCha20
45) Grant access if verification succeeds
46) Else deny access
47) End Algorithm
```

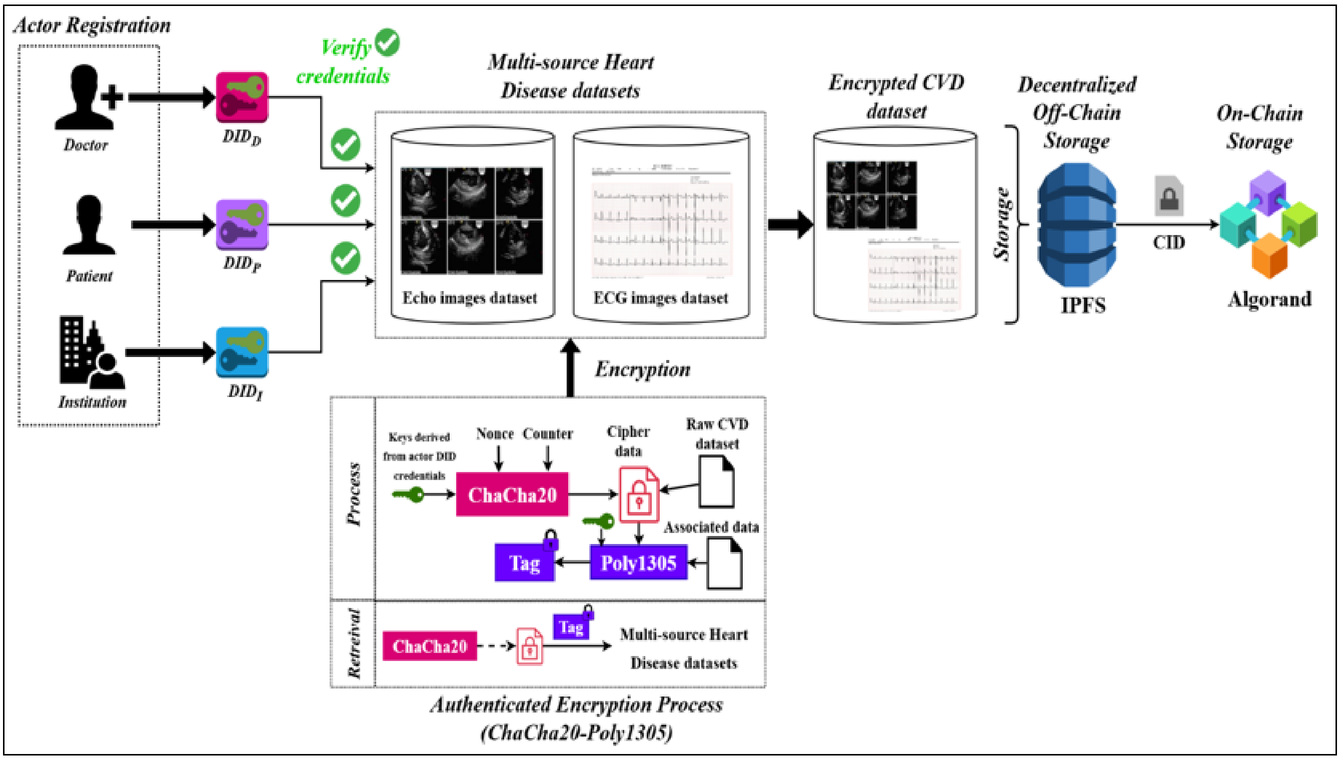

Figure 3: Overall system architecture of TPPoSHChain

4. Results and Discussion

This section evaluates the proposed TPPoSHChain framework.

4.1 Dataset Description

- HMC-QU Dataset [21]: This dataset has partition of left ventricular walls. It contains over 10,000 echocardiography samples from 2018 and 2019, containing over 800 instances of acute ST-elevation A subset of 109 A4C view echocardiography recordings have ground-truth differentiation masks at each pixel during a heartbeat covering the whole left ventricle. To conduct the experiment, 2346 frames were considered.
- ECG Images Dataset of Cardiac Patients [22]: It contains clinically validated electrocardiogram images collected at the Ch. Pervaiz Elahi Institute of Cardiology, Multan, Pakistan. The dataset supports research in cardiac disease detection, signal interpretation, and image-based deep learning methods. It includes four major categories representing diverse patient conditions. Myocardial infarction cases include ECG images from patients with confirmed MI. Abnormal heartbeat cases contain ECG images exhibiting irregular rhythm patterns. History of myocardial infarction cases include patients previously diagnosed with MI but not currently experiencing an acute episode. Normal cases represent ECG images from individuals with no cardiac abnormalities reported.

4.2 Evaluation Metrics

The metrics used for assessing the model's performance against existing models is listed in this section. They are:

- Transaction Throughput (TPS): It denotes the number of blockchain transactions successfully processed per second.

$$TPS = \frac{Total\ Confirmed\ Transactions}{Execution\ time} \quad (1)$$

- Transaction Latency: It refers to the time required for a transaction to be confirmed and finalized on the blockchain.

$$Latency = T_{confirmed} - T_{submitted} \quad (2)$$

- Storage Overhead (SOH): It is the amount of on-chain storage required per data.

$$SOH = \frac{Blockchain\ data\ size}{Number\ of\ Stored\ data} \quad (3)$$

- Encryption and Decryption Time: It refers to the time required to encrypt and decrypt the data.

4.3 Performance Analysis

The proposed TPPoSHChain model is evaluated against different existing blockchain based security models such as Ethereum-based POA [17], Attribute Based Access Control [18], modified PBFT model [19], and Hyperledger Fabric [20] to prove its efficiency.

Fig. 4 shows the percentage improvement in transaction throughput of the proposed TPPoSHChain framework over existing blockchain-based models for the HMC-QU and ECG image datasets. For the HMC-QU dataset, the proposed TPPoSHChain system achieves approximately 710%, 105%, 49%, and 35% higher throughput compared to Ethereum based PoA, ABAC, modified PBFT, and Hyperledger Fabric. For the ECG dataset, the proposed TPPoSHChain framework improves throughput by about 573% over Ethereum based PoA, 73% over ABAC, 56% over modified PBFT, and 13% over Hyperledger Fabric.

Fig. 5 compares transaction latency of different blockchain-based frameworks using the HMC-QU and ECG image datasets. For the HMC-QU dataset, the proposed TPPoSHChain framework reduces latency by approximately 70% compared to Ethereum based PoA, 57% compared to ABAC, 50% compared to modified PBFT, and 25% compared to Hyperledger Fabric. For the ECG dataset, latency is reduced by about 69% relative to Ethereum based PoA, 56% compared to ABAC, 43% compared to modified PBFT, and 50% compared to Hyperledger Fabric.

Fig. 6 illustrates storage overhead performance, expressed as the percentage reduction achieved by the proposed TPPoSHChain framework relative to existing blockchain-based models for the HMC-QU and ECG image datasets. For the HMC-QU dataset, the proposed TPPoSHChain model reduces storage overhead by approximately 67% compared to Ethereum based PoA, 65% compared to ABAC, 45% compared to modified PBFT, and 38% compared to Hyperledger Fabric. For the ECG dataset, the proposed TPPoSHChain system achieves about 74% reduction relative to Ethereum based PoA, 63% compared to ABAC, 51% compared to modified PBFT, and 29% compared to Hyperledger Fabric.

4.4 Comparison of Encryption and Decryption time

Fig. 7 compares the computational time of AES, DES, and ChaCha20-Poly1305 across increasing data lengths for encryption and decryption operations. Across all data sizes, ChaCha20-Poly1305 consistently requires less processing time. For a data length of 100 units, it reduces processing time by approximately 59% compared to AES and 34% compared to DES. At 200 units, the reduction is about 59% over AES and 37% over DES. Fig. 8 illustrates the computational performance of AES, DES, and ChaCha20-Poly1305 for varying data lengths, expressed as the percentage time reduction achieved by ChaCha20-Poly1305 over traditional algorithms. DES.

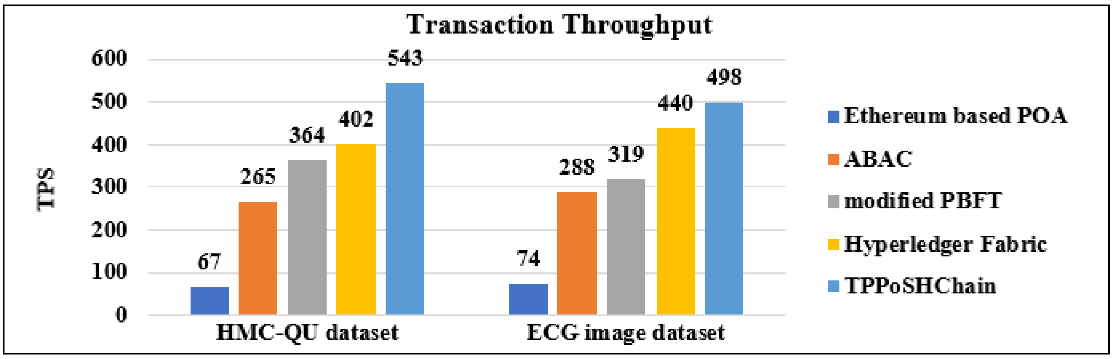

Figure 4: Transaction throughput comparison of various models

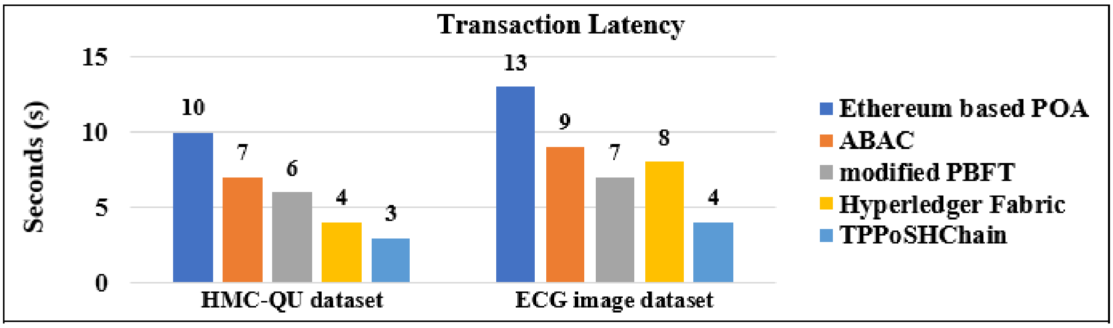

Figure 5: Transaction latency comparison of various models

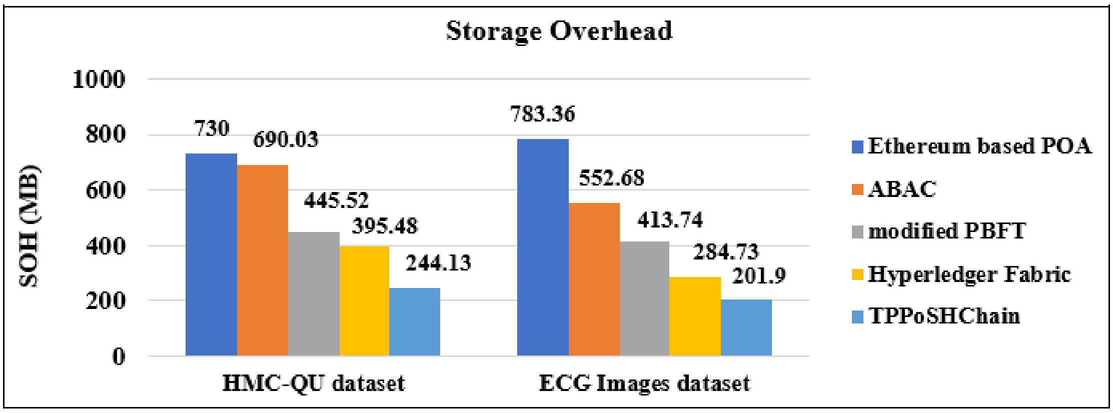

Figure 6: SOH comparison of various models

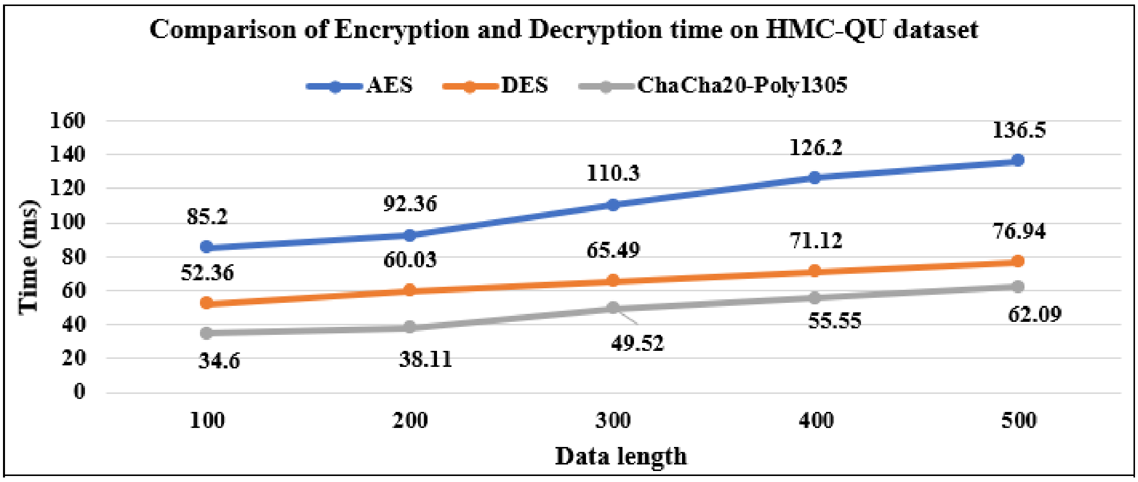

Figure 7: Comparison of Encryption and decryption time for the ChaCha20-Poly1305 and existing encryption models in HMC-QU dataset

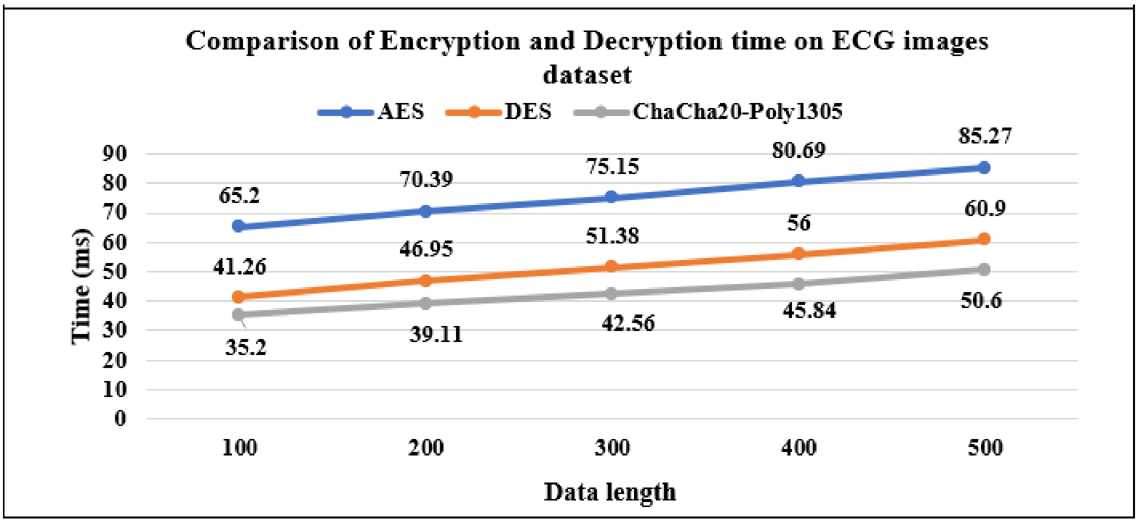

Figure 8: Comparison of encryption and decryption time for the ChaCha20-Poly1305 and existing encryption models in ECG images dataset

5. Conclusion

CVD remains a leading global health challenge, generating vast amounts of heterogeneous data. However, the sensitive nature of CVD data introduces critical concerns related to security, confidentiality, integrity, controlled access, and trustworthy data sharing. Traditional centralized data management solutions are inadequate for such environments due to single points of failure, vulnerability to cyberattacks, limited transparency, and poor scalability. Existing blockchain-based security approaches attempt to address these issues but often suffer from high computational overhead, storage inefficiency, increased latency, complex consensus mechanisms, or excessive on-chain data storage, which restrict their practical deployment for large-scale medical datasets. To overcome these limitations, this paper proposed a secure and scalable TPPoSHChain framework for managing multi-source CVD datasets by integrating Algorand PPoS consensus, DIDs, ChaCha20-Poly1305 encryption, and token-based access control within a hybrid on-chain/off-chain architecture. Experimental results using the HMC-QU and ECG image datasets demonstrate that the proposed TPPoSHChain framework significantly outperforms existing models. It achieves markedly higher transaction throughput, reductions in transaction latency, and storage overhead. Additionally, ChaCha20-Poly1305 shows consistently lower encryption and decryption times compared to AES and DES, validating its efficiency for large-scale CVD dataset protection.

References

[1] World Health Organization, “Cardiovascular diseases (CVDs),” WHO Fact Sheets, 2025.

[2] P. Sharma, P. Sharma, K. Sharma, V. Varma, V. Patel, J. Sarvaiya, and K. Shah, “Revolutionizing utility of big data analytics in personalized cardiovascular healthcare,” Bioengineering, vol. 12, no. 5, p. 463, 2025.

[3] A. Silverio, P. Cavallo, R. De Rosa, and G. Galasso, “Big health data and cardiovascular diseases: A challenge for research, an opportunity for clinical care,” Frontiers in Medicine, vol. 6, p. 36, 2019.

[4] T. Liu, A. J. Krentz, Z. Huo, and V. Ćurčin, “Opportunities and challenges of cardiovascular disease risk prediction for primary prevention using machine learning and electronic health records: A systematic review,” Reviews in Cardiovascular Medicine, vol. 26, no. 4, p. 37443, 2025.

[5] Y. Liu, X. Li, D. Yu, and Y. Xu, “Medical information management system based on multi-source heterogeneous big data,” Computer Methods in Biomechanics and Biomedical Engineering: Imaging & Visualization, vol. 12, no. 1, p. 2389816, 2024.

[6] U. Nweje, “Blockchain technology for secure data integrity and transparent audit trails in cybersecurity,” International Journal of Research Publication and Reviews, vol. 5, no. 12, pp. 4902–4916, 2024.

[7] Z. Wenhua, F. Qamar, T. A. N. Abdali, R. Hassan, S. T. A. Jafri, and Q. N. Nguyen, “Blockchain technology: Security issues, healthcare applications, challenges and future trends,” Electronics, vol. 12, no. 3, p. 546, 2023.

[8] M. N. M. Bhutta, A. A. Khwaja, A. Nadeem, H. F. Ahmad, M. K. Khan, M. A. Hanif, and Y. Cao, “A survey on blockchain technology: Evolution, architecture and security,” IEEE Access, vol. 9, pp. 61048–61073, 2021.

[9] I. S. Rao, M. M. Kiah, M. M. Hameed, and Z. A. Memon, “Scalability of blockchain: A comprehensive review and future research direction,” Cluster Computing, vol. 27, no. 5, pp. 5547–5570, 2024.

[10] O. Aluko and A. Kolonin, “Proof-of-reputation: An alternative consensus mechanism for blockchain systems,” International Journal of Network Security and Its Applications, vol. 13, no. 4, 2021.

[11] Y. Xu, X. Yang, J. Zhang, J. Zhu, M. Sun, and B. Chen, “Proof of engagement: A flexible blockchain consensus mechanism,” Wireless Communications and Mobile Computing, vol. 2021, no. 1, p. 6185910, 2021.

[12] H. Baageel and M. M. Rahman, “Leveraging sharding-based hybrid consensus for blockchain,” Computers, Materials & Continua, vol. 81, no. 1, 2024.

[13] D. G. Narayan, A. Naveen, and R. Tejas, “DPoSEB: Delegated proof of stake with exponential backoff consensus algorithm for Ethereum blockchain,” Computer Science Journal of Moldova, vol. 95, no. 2, pp. 262–288, 2024.

[14] M. Siraj, M. I. H. Ninggal, N. I. Udzir, A. Asmawi, M. Daniel, H. Abdullah, and P. Malaysia, “Proof-of-Green (PoG): A new permissionless blockchain structure and consensus mechanism,” vol. 70, no. 1, 2025.

[15] T. Fu, J. Hu, G. Min, and Z. Wang, “Zero-knowledge proof-based consensus for blockchain-secured federated learning,” arXiv preprint arXiv:2503.13255, 2025.

[16] T. Lei, Q. Zhang, W. Qiu, H. Zheng, S. Miao, W. Jie, and Z. Zheng, “An enhanced DPoS consensus mechanism using quadratic voting in Web 3.0 ecosystem,” Blockchain, vol. 3, no. 1, pp. 1–2, 2025.

[17] K. Azbeg, O. Ouchetto, and S. J. Andaloussi, “Access control and privacy-preserving blockchain-based system for diseases management,” IEEE Transactions on Computational Social Systems, vol. 10, no. 4, pp. 1515–1527, 2022.

[18] R. Sasikumar and P. Karthikeyan, “Heart disease severity level identification system on Hyperledger consortium network,” PeerJ Computer Science, vol. 9, p. e1626, 2023.

[19] P. Hegde and P. K. R. Maddikunta, “Secure PBFT consensus-based lightweight blockchain for healthcare application,” Applied Sciences, vol. 13, no. 6, p. 3757, 2023.

[20] S. Saxena, S. Saxena, N. Tahilramani, and P. Charanarur, “Blockchain enhanced smart healthcare management for chronic diseases,” Discover Computing, vol. 28, no. 1, p. 112, 2025.

[21] “HMCQU Dataset,” Kaggle. Available: https://www.kaggle.com/datasets/aysendegerli/hmcqu-dataset

[22] “ECG Analysis Dataset,” Kaggle. Available: https://www.kaggle.com/datasets/evilspirit05/ecg-analysis.