Asynchronous Federated Attribute Distribution: A Scalable Blockchain-Integrated Access Control Framework for Secure Health Data Sharing

Hemlathadhevi A[1], Padmapriya K[2], Nirmala G[3], Sathya Preiya V[4], Ramesh Kumar C[5,*]

[1]Professor, Department of Computer Science and Engineering, Panimalar Engineering College, Chennai, Tamil Nadu, India

[2]Associate Professor, Department of Computer Science and Engineering, R. M. D Engineering College, Kavaraipettai, Tamil Nadu, India.

[3]Professor, Department of Artificial intelligence and Data Science, Rajalakshmi Engineering College, Chennai, Tamil Nadu, India.

[4]Associate Professor, Department of Computer Science and Engineering, S.A Engineering College, Chennai, Tamil Nadu, India.

[5]Professor, Department of Computer Science and Engineering, Galgotias University, Greater Noida, Uttar Pradesh.

*Corresponding Author: toramesh83@gmail.com

HOW TO CITE:

Hemlathadhevi A, Padmapriya K, Nirmala G, Sathya Preiya V, Ramesh Kumar C (2026). Asynchronous Federated Attribute Distribution: A Scalable Blockchain-Integrated Access Control Framework for Secure Health Data Sharing. International Journal of Special Education, 41(16s), 224-241

COPYRIGHT STATEMENT:

Copyright: © 2026 Authors. Open access publication underthe terms and conditions of the Creative CommonsAttribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/).

ABSTRACT:

Wireless Body Area Networks (WBANs) can offer continuous health monitoring, but they lack secure and scalable access control mechanisms for sensitive medical data. Traditional attribute-based access control systems rely on centralised credential authorities, introducing single points of failure and trust bottlenecks. In this paper, we propose a decentralised access control framework based on asynchronous federated attribute distribution system and integrated with consortium blockchain technology. The framework eliminates dependence on centralised authorities through the inclusion of verifiable secret sharing, high-threshold distributed key generation, and smart contract-based policy enforcement. The proposed architecture is composed of three core components: (i) an asynchronous distributed key generation module, (ii) a verifiable attribute secret sharing module, and (iii) a smart contract orchestration layer. The participating healthcare institutions collaboratively create and maintain a distributed master secret without explicit reconstruction. Attribute-specific decryption keys are created by using a high-threshold Shamir secret-sharing scheme. Smart contracts evaluate access requests by checking ciphertext-policy attribute-based encryption (CP-ABE) policies against on-chain attributes. Once the policy has been validated successfully, authorised parties collaborate to reconstruct the required secret keys to decrypt the data. All access operations are permanently logged on the blockchain for transparency and auditability. The framework exhibits strong collusion resistance as a threshold number of institutions are necessary to compromise the system secrets. The framework is asynchronous in its execution, thus guaranteeing operational liveness in the face of network delays. Localised committee for

efficient attribute revocation reduces the management overhead. The proposed framework is implemented using pairing-friendly elliptic curve cryptography and Hyperledger Fabric in WBAN environment. The proposed framework is secure, scalable and transparent for decentralising health data sharing.

Keywords: Wireless Body Area Networks (WBAN), Decentralized Access Control, Consortium Blockchain, Ciphertext-Policy Attribute-Based Encryption (CP-ABE), Distributed Key Generation (DKG), Verifiable Secret Sharing (VSS), Hyperledger Fabric, Secure Healthcare Data Sharing

1. Introduction

The secure and scalable sharing of electronic health records (EHRs) across heterogeneous healthcare institutions remains a formidable challenge, primarily due to the inherent tension between data utility and stringent privacy requirements. Traditional attribute-based encryption (ABE) frameworks have demonstrated considerable promise for realizing fine-grained access control, allowing data to be encrypted under policies that reference user attributes rather than specific identities [1]. However, these systems conventionally rely on a single or multiple centralized authorities for key management and credential issuance, thereby introducing critical single points of failure and scalability bottlenecks [2]. Such centralized architectures are ill-suited for modern healthcare ecosystems that demand resilience, interoperability, and the ability to operate under partially adversarial network conditions. The growing adoption of consortium blockchains in healthcare offers a permissioned ledger structure that provides immutability and auditability [3], yet the operationalization of decentralized cryptographic key management within such frameworks is far from trivial.

To address these limitations, we propose an asynchronous federated attribute distribution framework that synergistically integrates verifiable secret sharing (VSS) and high-threshold distributed key generation (DKG) with a consortium blockchain-based access control mechanism for health records. This design purposefully replaces centralized key authorities with a decentralized network of participating healthcare institutions that jointly generate and maintain attribute decryption secrets through an asynchronous threshold protocol. Our approach ensures that no single node ever holds complete cryptographic material, thereby fundamentally eliminating single points of failure in credential issuance. Each medical entity contributes partial shares to collectively derive fine-grained access policies based on dynamic patient consent and institutional roles, while the underlying asynchronous Byzantine fault tolerance (BFT) protocol guarantees liveness even under unpredictable network delays [4]. The resulting attribute-based encryption layer operates seamlessly atop smart contract orchestration [5], enabling horizontal scaling through parallel attribute committee formation while maintaining formal security guarantees against collusive adversaries.

The core novelty of this work lies in the confluence of three critical design decisions. First, we deploy an asynchronous DKG module that allows each healthcare institution to contribute a random polynomial without ever reconstructing the master secret centrally, thus providing collusion resistance since a threshold of nodes is required to compromise the system. Second, we instantiate a verifiable attribute secret sharing module that derives attribute-specific decryption keys from the distributed master secret using a high-threshold Shamir scheme, ensuring that attribute revocation remains localized to small committees and therefore incurs minimal overhead. Third, we develop a smart contract orchestration layer that evaluates ciphertext-policy attribute-based encryption (CP-ABE) policies against on-chain attributes; once policy satisfaction is verified, the contract triggers

a collaborative reconstruction of the necessary secret keys, which are then securely transmitted to the requester for data decryption. This architecture departs meaningfully from existing decentralized access control proposals, such as those integrating blockchain with lightweight cryptography for wireless body area networks (WBANs) [6], by explicitly addressing both asynchronous network conditions and high-threshold secret management.

Our contributions are threefold. From a cryptographic standpoint, we present the first integrated asynchronous DKG and VSS construction tailored for CP-ABE within a consortium blockchain, offering formal security guarantees against honest-but-curious and Byzantine adversaries. From a systems perspective, we demonstrate how smart contract orchestration can coordinate distributed key reconstruction and attribute revocation, thereby enabling dynamic consent management without reliance on a central authority. From an empirical standpoint, we evaluate the framework using a pairing-friendly elliptic curve within a Hyperledger Fabric environment, yielding quantitative insights into transaction throughput, latency, and resilience under various network partitions.

The remainder of this paper is organized as follows. Section 2 reviews related work on ABE, blockchain-based access control, and distributed key generation, identifying gaps that our proposal addresses. Section 3 recapitulates the necessary preliminaries, including CP-ABE, VSS, DKG, and asynchronous BFT protocols. Section 4 elaborates the proposed asynchronous federated attribute distribution framework, detailing its three modules and their interactions with WBAN data flows. Section 5 describes the experimental setup and presents performance results. Section 6 discusses the implications of our findings, outlines limitations, and suggests directions for future research. Section 7 concludes the paper.

2. Related Work

Access control for electronic health records has been extensively studied through the lens of attribute-based encryption (ABE). The seminal work on ciphertext-policy ABE [1] established a paradigm where data is encrypted under an access policy, and decryption is possible only if the user's attributes satisfy that policy. Subsequent research extended this to multi-authority settings [7], where multiple attribute authorities manage disjoint attribute sets, thereby distributing trust. However, these multi-authority schemes still rely on centralized authorities for key generation and attribute management, introducing single points of failure. More recent proposals have integrated blockchain technology to address these limitations, using smart contracts to enforce policies [8] and to record access events for auditability. For instance, frameworks for healthcare wireless body area networks (WBANs) have employed lightweight cryptographic primitives combined with blockchain to secure sensor data [6], though they typically assume a semi-trusted central authority for key distribution.

Distributed key generation (DKG) protocols offer a mechanism to bootstrap threshold cryptosystems without a trusted dealer. Early DKG constructions assumed synchronous communication networks, which are unrealistic in many real-world scenarios [9]. The practical asynchronous DKG protocol introduced by Abraham et al. [10] eliminates the need for synchronized rounds, ensuring liveness under unpredictable network delays. Extensions to high-threshold scenarios, such as the work by Das et al. [11], provide concretely efficient constructions for discrete-log-based threshold systems. These protocols are foundational for our proposed ADKG-M, which adapts them to the consortium blockchain context.

Verifiable secret sharing (VSS) has been a cornerstone for secure multiparty computation, with Feldman's VSS [12] providing non-interactive public verifiability of shares. Aggregatable DKG protocols [13] further reduce communication complexity by allowing nodes to combine their contributions using homomorphic commitments. However, existing DKG and VSS constructions have not been directly composed with attribute-based encryption for decentralized access control. Recent work on threshold key

management in dynamic distributed systems [14] addresses key rotation but does not integrate attribute-specific secret derivation or policy enforcement.

Smart contracts on permissioned blockchains, such as Hyperledger Fabric, have been employed to implement dynamic access policies [15]. These systems often combine on-chain policy evaluation with off-chain cryptographic operations. In the healthcare domain, frameworks like Fortified-Chain [16] propose blockchain-integrated access control for IoT devices, though they typically use simpler cryptographic primitives and assume centralized key servers. The literature on blockchain-integrated WBANs [17] focuses on scalability and security but generally does not address asynchronous key generation or threshold secret sharing for attribute-specific keys.

A distinct line of research addresses distributed key generation for threshold homomorphic encryption, such as threshold-CKKS [18]. While these contributions are relevant for privacy-preserving computation on encrypted data, they target different cryptographic primitives than attribute-based encryption. The key derivation mechanisms in these schemes do not directly map to attribute-based policies.

The proposed work differentiates itself from these approaches by providing an integrated framework that combines asynchronous DKG, verifiable attribute-specific secret sharing, and smart contract orchestration for CP-ABE. Unlike existing blockchain-based access control systems that rely on centralized key authorities or synchronous DKG, our framework operates asynchronously and ensures that attribute-specific keys are derived from a completely distributed master secret without reconstruction. This design provides collusion resistance proportional to the chosen threshold, effective attribute revocation through local committee resharing, and consistent access policy evaluation recorded on an immutable blockchain. In contrast to prior DKG deployments for threshold cryptosystems, we apply these techniques specifically to attribute-based access control, where the secret is used as a root for multiple attribute-specific polynomials rather than as a direct decryption key.

3. Preliminaries

This section introduces the core cryptographic and distributed systems concepts that underpin the proposed asynchronous federated attribute distribution framework. We first cover threshold secret sharing and verifiability, followed by attribute-based encryption foundations, and finally the principles of asynchronous consensus.

3.1 Fundamentals of Threshold Secret Sharing and Verifiability

Threshold secret sharing, introduced by Shamir [19], allows a dealer to split a secret s into n shares such that any subset of at least t shares can reconstruct the secret, while fewer than t shares reveal no information about it. This is achieved by constructing a random polynomial $f(x)$ of degree $t-1$ over a finite field $\mathbb{Z}_q$, where the constant term is the secret:

$$f(x) = s + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1} (\mathrm{mod} q)$$

The dealer computes share $y_i = f(i)$ for each participant i. When a quorum S of size $|S| \geq t$ is obtained, the secret can be reconstructed via Lagrange interpolation:

$$s = \sum_{i \in S} y_i \prod_{j \in S, j \neq i} \frac{-x_j}{x_i - x_j} (\mathrm{mod} q)$$

In the context of asynchronous distributed systems, participants cannot rely on a trusted dealer. Therefore, distributed key generation (DKG) protocols [9] allow multiple parties to jointly generate a shared secret without any party knowing the full secret. Each party acts as a dealer for its own random polynomial, and the sum of individual secrets forms the distributed master secret.

To ensure that shares are correctly generated even in the presence of malicious participants, verifiable secret sharing (VSS) is employed. Feldman's VSS scheme [12] binds the polynomial coefficients to public commitments. Let g be a

generator of a cyclic group of order q. The dealer publishes commitments $C_k = g^{a_k}$ for $k = 0, \dots, t-1$, where $a_0 = s$. A participant can then verify its received share y_i by checking:

$$g^{y_i} = \prod_{k=0}^{t-1} (C_k)^{i^k}$$

This non-interactive verification is crucial for asynchronous operation, as it allows participants to detect dishonest behavior without requiring multiple rounds of communication.

3.2 Cryptographic Foundations of Attribute-Based Encryption

Ciphertext-policy attribute-based encryption (CP-ABE) [4] provides fine-grained access control by encrypting data under an access policy defined over attributes. Decryption is possible only if a user's attribute set satisfies the policy. The scheme typically operates over bilinear groups. Let $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ be cyclic groups of prime order p, with a bilinear pairing $e: \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$. A fundamental property of bilinear pairings is:

$$e(g^a, h^b) = e(g, h)^{ab}$$

for generators $g \in \mathbb{G}_1, h \in \mathbb{G}_2$ and exponents $a, b \in \mathbb{Z}_p$.

Access policies in CP-ABE are often represented using linear secret sharing schemes (LSSS) [20]. An LSSS is defined by a matrix M of size $\ell \times n$ and a mapping function ρ that associates each row of M to an attribute. For a secret s to be shared, the encryptor chooses a random vector $\vec{v} = (s, v_2, \dots, v_n) \in \mathbb{Z}_p^n$ and computes shares for each row r as:

$$\lambda_r = M_r \cdot \vec{v}$$

where M_r is the r-th row of M. A user whose attributes satisfy the policy can find a set of coefficients w_r such that $\sum_{r \in I} w_r M_r = (1, 0, \dots, 0)$, allowing recovery of $s = \sum_{r \in I} w_r \lambda_r$.

In a typical CP-ABE construction, the master secret key is $MSK = \alpha$, and the public key is $PK = (g, g^\alpha)$. A symmetric key K_{sym} used for data encryption is encapsulated in the ciphertext. Decryption proceeds by combining user-specific keys with the ciphertext components to isolate $e(g, g)^{\alpha s}$, from which the symmetric key is derived:

$$K_{\text{sym}} = \frac{C_0}{e(g, g)^{\alpha s}}$$

where C_0 is the masked symmetric key in the ciphertext. This mechanism forms the basis for the attribute-based decryption in our framework, where the master secret α is distributed among consortium nodes.

3.3 Principles of Asynchronous Distributed Consensus

Asynchronous consensus protocols are essential for ensuring liveness in distributed networks where message delivery delays are unbounded. Byzantine fault-tolerant (BFT) consensus in asynchronous settings requires that the system tolerate up to f faulty nodes out of N total nodes, where:

$$N \geq 3f + 1$$

This is a fundamental lower bound for asynchronous Byzantine agreement [21]. Asynchronous BFT protocols, such as HoneyBadgerBFT [22], use reliable broadcast [23] to ensure that all honest nodes eventually receive the same messages, even if the sender is faulty. The message complexity of reliable broadcast in asynchronous networks is $O(N^2)$, as each node broadcasts its message to all others.

A critical component of asynchronous consensus is the generation of a common coin [9], which provides an unpredictable and unbiased randomness source that all honest nodes can agree upon. Common coins are typically constructed using threshold signatures, where each node contributes a share r_i, and the combined randomness is:

$$R = \bigoplus_{i=1}^{N} r_i$$

where $\oplus$ denotes the XOR operation over all shares. This ensures that no single node can bias the coin toss outcome, and the result is revealed only after a threshold of shares is collected. Practical asynchronous DKG protocols [10] extend these principles to generate

distributed keys without a trusted dealer, ensuring that the protocol remains live even under adversarial network conditions. The combination of these primitives—reliable broadcast, common coin, and threshold operations—provides the foundation for the asynchronous key generation module in our framework.

3. Asynchronous Federated Attribute Distribution with Verifiable Threshold Secret Sharing

We now present the detailed technical architecture of the proposed asynchronous federated attribute distribution framework, which integrates three core modules: the Asynchronous Distributed Key Generation Module (ADKG-M), the Verifiable Attribute Secret Sharing Module (VASS-M), and the Smart Contract Orchestration Layer (SCO-L). These modules operate atop a consortium blockchain infrastructure, where each participating healthcare institution maintains a full node. The system replaces traditional centralized credential authorities with a decentralized network that jointly generates and maintains attribute decryption secrets. Before proceeding to the module descriptions, we first formalize the network model and security assumptions.

3.1 Network Model and System Assumptions

We consider a network of N nodes representing healthcare institutions, where each node executes both the blockchain consensus protocol and the distributed key generation protocol. The network operates under an asynchronous communication model where messages can be arbitrarily delayed but are eventually delivered. We assume a static adversary that can corrupt up to $f < N/3$ nodes, consistent with the Byzantine fault tolerance bound for asynchronous systems. The corrupted nodes can deviate arbitrarily from the protocol specification, while the remaining $N - f$ honest nodes follow the protocol faithfully.

The adversary is computationally bounded and cannot break standard cryptographic assumptions, specifically the hardness of the discrete logarithm problem in the group used for public key commitments. All communication channels between nodes are assumed to be authenticated and encrypted, preventing eavesdropping and impersonation attacks. We further assume the existence of a common reference string for the initialization of the threshold cryptosystem, as is standard in DKG protocols.

The system operates in two distinct phases: a one-time setup phase where the distributed master secret is generated, and an operational phase where attribute-specific keys are derived, reconstructed, and revoked. The setup phase executes the ADKG-M once, after which the master secret remains static. The operational phase runs continuously as access requests are processed by the SCO-L.

3.2 Asynchronous Distributed Key Generation Module (ADKG-M)

The ADKG-M establishes the distributed master secret $\alpha \in \mathbb{Z}_q$ that serves as the root key for the entire attribute-based encryption system. Unlike conventional DKG protocols that assume synchronous communication, our module operates entirely asynchronously using a variant of the HoneyBadgerBFT framework to guarantee liveness under network delays.

The protocol proceeds as follows. Each node P_i generates a random polynomial $f_i(x)$ of degree T, where T is the master threshold. The polynomial is:

$$f_i(x) = a_{i,0} + a_{i,1}x + \cdots + a_{i,T}x^T (\mathrm{mod} q)$$

where the constant term $a_{i,0}$ is the node's contribution to the master secret. Node P_i then computes and broadcasts Feldman commitments $C_{i,k} = g^{a_{i,k}}$ for $k = 0, \ldots, T$ to all other nodes via reliable broadcast.

For each other node P_j, node P_i sends a share $s_{i,j} = f_i(j)$ over a secure channel. When node P_j receives a share from P_i, it verifies the share using the commitments:

$$g^{s_{i,j}} \stackrel{?}{=} \prod_{k=0}^{T} (C_{i,k})^{j^k}$$

If the verification fails, node P_j broadcasts a complaint including the received share, requiring P_i to explain or be excluded. Nodes that fail to provide valid explanations for more than f complaints are flagged as faulty and excluded from the protocol without causing a halt.

After each honest node P_j has collected at least $N - f$ valid shares, it computes its overall share of the master secret:

$$sh_j = \sum_{i=1}^{N} s_{i,j} \,(\mathrm{mod} q)$$

The master secret $\alpha = \sum_{i=1}^{N} a_{i,0} \,(\mathrm{mod} q)$ is never explicitly constructed by any single node. Instead, it remains distributed such that any threshold $T + 1$ honest nodes can reconstruct it using Lagrange interpolation when necessary.

Theorem 1 (ADKG-M Security). Under the asynchronous network model with up to $f < N/3$ corrupted nodes, the ADKG-M produces a correct and uniformly random master secret α that is unknown to any set of fewer than $T + 1$ nodes.

Proof Sketch. The security follows from the robustness of Feldman VSS and the asynchronous common coin used in the underlying reliable broadcast protocol. The commitments ensure that shares are consistent with the polynomial, preventing equivocation by corrupted dealers. The asynchronous common coin guarantees that the sequence of nodes contributing polynomials cannot be biased by the adversary. The threshold T ensures resistance against collusion attacks, as any coalition of size at most T cannot reconstruct the polynomial coefficients of any honest dealer, and thus cannot recover α.

3.3 Verifiable Attribute Secret Sharing Module (VASS-M)

The VASS-M derives attribute-specific decryption keys from the distributed master secret α. For each attribute $attr$ in the system, the module generates a unique polynomial of degree T', where T' is the attribute-specific threshold that can differ from the master threshold T. This dual-threshold design enables fine-grained security-efficiency trade-offs: high-risk attributes use a high threshold T' close to T for maximum security, while low-risk attributes use a lower threshold T' for faster key reconstruction.

The attribute polynomial $h_{attr}(x)$ is defined as:

$$h_{attr}(x) = \alpha + b_1 x + \cdots + b_{T'} x^{T'} (\mathrm{mod} q)$$

where $b_1, \ldots, b_{T'}$ are random coefficients chosen through a distributed protocol. The distributed generation of this polynomial proceeds similarly to the ADKG-M but at a smaller scale, involving only a committee of nodes responsible for the given attribute. This committee assignment is determined by the smart contract based on the attribute's properties and the available nodes.

Each committee node P_i receives a share $y_i = h_{attr}(i)$. These shares are verifiable using Feldman commitments for the attribute polynomial. When a user requires the decryption key for a specific attribute, a quorum of $T' + 1$ committee nodes collaborates to reconstruct the key. The reconstruction uses Lagrange interpolation:

$$SK_{attr} = \sum_{l=1}^{T'+1} y_l \prod_{m \neq l} \frac{-m}{l - m} (\mathrm{mod} q)$$

The resulting secret key SK_{attr} is then combined with other components to form the full user decryption key for a given ciphertext policy.

Attribute revocation is handled locally within the affected committee without requiring a global resharing of the master secret. When an attribute is revoked, the committee updates the polynomial $h_{attr}(x)$ by generating a new random polynomial with the same constant term α but different higher-degree coefficients.

This ensures that revoked users cannot decrypt future ciphertexts encrypted under that attribute, while the master secret remains unchanged.

3.4 Smart Contract Orchestration Layer (SCO-L)

The SCO-L coordinates the interactions between the cryptographic modules described above and the blockchain consensus layer. It is implemented as a set of smart contracts deployed on the consortium blockchain. The core functionality is the dynamic policy-triggered key reconstruction.

Figure 1 provides a high-level overview of the system architecture, showing the interactions between WBAN devices, the healthcare provider, the blockchain-based access control components, and the data storage.

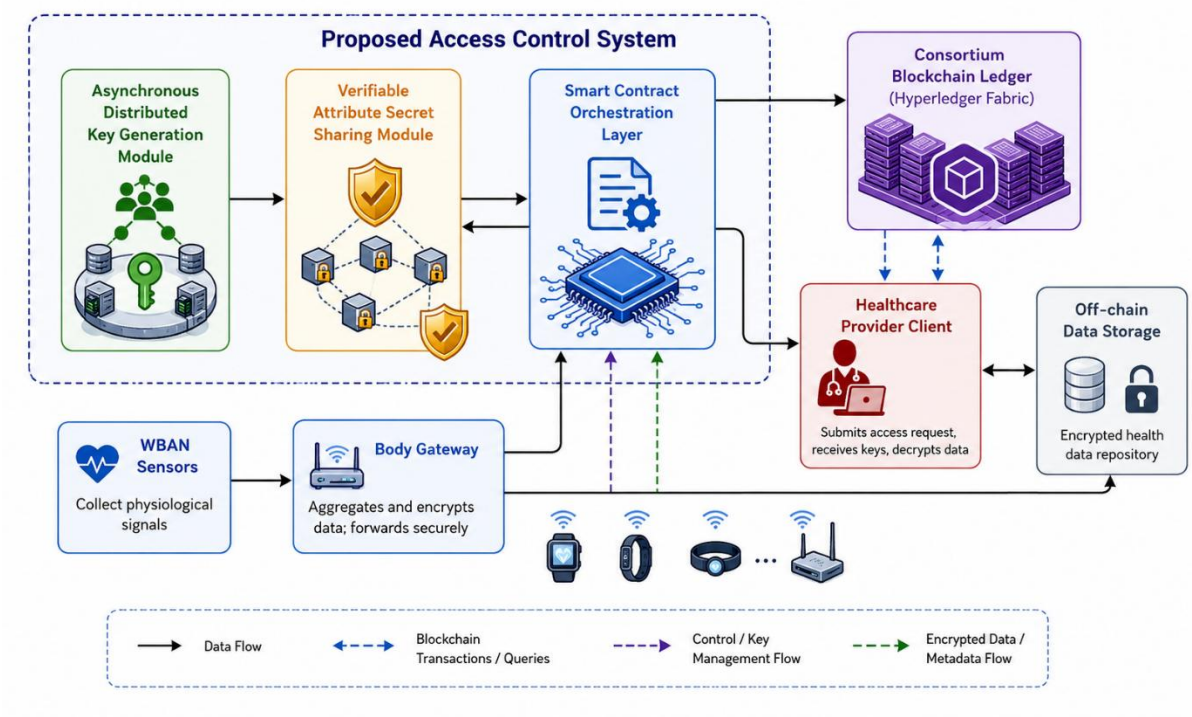


Figure 1. System Architecture of Blockchain Integrated WBAN Access Control

When a healthcare provider submits an access request for a specific patient record, the associated ciphertext is encrypted under a CP-ABE policy (M, ρ), where M is an LSSS matrix of size $\ell \times n$ and ρ maps each row to an attribute. The SCO-L evaluates whether the requester's on-chain attributes satisfy this policy by checking for the existence of constants $\{\mu_r\}_{r=1}^{\ell}$ such that:

$$\sum_{r=1}^{\ell} \mu_r \lambda_r = s$$

where λ_r are the LSSS shares derived from the ciphertext, and s is the secret embedded in the encryption. This evaluation is performed within the smart contract logic, ensuring that the policy is checked automatically and transparently.

If the policy is satisfied, the SCO-L triggers the VASS-M to reconstruct the attribute-specific secret keys SK_{attr} for each attribute in the requester's satisfied set. The reconstruction is performed by the blockchain nodes through a threshold endorsement protocol. Specifically, the SCO-L requires $T' + 1$ endorsements from the attribute committee before any key reconstruction transaction is finalized. The reconstructed keys are combined to compute the user's decryption key:

$$SK_{user} = \prod_{r=1}^{\ell} (C_{1,r})^{\mu_r} \cdot e(g, g)^{\alpha s}$$

where $C_{1,r}$ are components from the ciphertext corresponding to each LSSS row. The

resulting key is then encrypted under the requester's public key and transmitted via a secure channel. The blockchain nodes immediately discard SK_{user} after transmission, ensuring that decryption keys are never stored persistently.

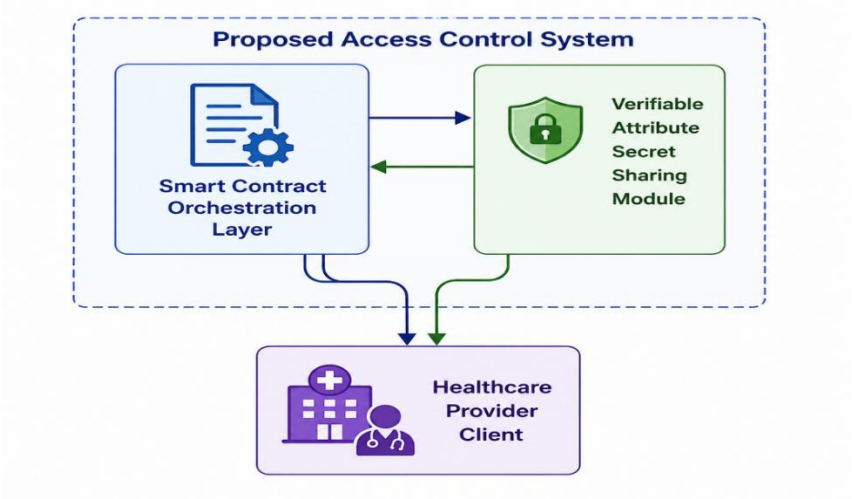
All access events, including policy evaluation and key reconstruction, are recorded as immutable blockchain transactions, providing a full audit trail for compliance and security monitoring.

3.5 Protocol Interaction and Workflow

The overall system workflow can be summarized as follows. During the initial setup, the consortium nodes execute the ADKG-M to generate the distributed master secret α. Then, for each supported attribute, a committee is formed and the VASS-M derives the attribute-specific polynomial. When a user enrolls with a set of attributes, their credentials are recorded on the blockchain.

Upon receiving an access request for encrypted data, the SCO-L evaluates the associated CP-ABE policy. If the requester's attributes satisfy the policy, the VASS-M reconstructs the necessary secret keys, and these keys are used to compute the decryption key for the ciphertext. The data is then decrypted and returned to the requester. Attribute revocation triggers local polynomial updates within the affected committee.

Figure 2 illustrates the runtime workflow during an access request, focusing on the interaction between the SCO-L and the VASS-M after the initial key generation phase.



. Runtime Workflow of Smart Contract and Attribute Secret Sharing

This architecture provides collusion resistance by requiring a threshold of $T + 1$ nodes to compromise the master secret, and attribute-specific keys are isolated through local committees. Asynchronous operation ensures that the system remains live Figure 2under network delays, and the dual-threshold design allows efficient key reconstruction for low-risk attributes without sacrificing security for high-risk ones.

5. Experimental Setup

We evaluate the proposed asynchronous federated attribute distribution framework through a series of experiments designed to measure its performance, scalability, and resilience under realistic network conditions. The evaluation focuses on three primary dimensions: the efficiency of the distributed key generation and attribute secret sharing protocols, the overhead introduced by smart contract orchestration, and the system's behavior under adverse network conditions including delays and node failures. All experiments were conducted within a controlled testbed environment simulating a consortium blockchain network of healthcare institutions.

5.1 Environment and Implementation Details

The experimental testbed consists of a cluster of virtual machines hosted on a private cloud infrastructure, each provisioned with 8 vCPUs, 16 GB RAM, and running Ubuntu 22.04 LTS. The consortium blockchain is deployed using Hyperledger Fabric v2.5, with Raft as the ordering service consensus mechanism. We instantiate the ADKG-M and VASS-M modules in Go, leveraging the bn256 pairing-friendly elliptic curve from the go-ethereum/crypto library for bilinear pairing operations and Feldman commitments. The CP-ABE implementation is based on the Charm cryptographic framework [24] ported to Go for integration with Fabric's chaincode environment. The smart contract orchestration logic is implemented as Fabric chaincode deployed across all peer nodes, with endorsement policies requiring at least (2f+ least $2f + 1$ signatures to satisfy Byzantine fault tolerance guarantees. All communication between nodes is secured using TLS 1.3 mutual authentication.

Given the absence of standardized benchmarks for asynchronous DKG integrated with ABE, we construct a synthetic EHR dataset reflecting realistic access patterns. The dataset comprises 10,000 encrypted health records, each associated with a CP-ABE policy containing between 3 and 15 attributes drawn from a vocabulary of 50 distinct medical attributes (e.g., "cardiologist," "emergency-room," "research-institution," "pediatrics"). User attribute sets are randomly assigned with an average cardinality of 8. We simulate a variable number of consortium nodes $N \in \{4,7,10,13,16\}$ to study scalability, with master thresholds T set to the optimal Byzantine tolerance value of $\lfloor (N-1)/3 \rfloor$. Attribute committees are sized at $C = \lceil 2T/3 \rceil$.

5.2 Performance Metrics

The evaluation employs the following performance metrics:

Key Generation Latency (KGL): The total time, measured in seconds, required to complete the ADKG-M protocol for a given number of nodes, encompassing polynomial generation, share distribution, and verification.

Attribute Secret Reconstruction Time (ASRT): The latency, in milliseconds, from the initiation of a key reconstruction request by the SCO-L to the delivery of the decryption key to the requester.

Transaction Throughput (TPS): The number of access request evaluations processed per second by the SCO-L, measured under increasing concurrent request loads.

Endorsement Success Rate (ESR): The proportion of access requests that complete successfully within a timeout period under varying adversarial conditions, including node failures and message delays.

Scalability Factor (SF): The ratio of the KGL for N nodes to the KGL for the baseline $N = 4$, characterizing the overhead growth as the consortium size expands.

5.3 Comparative Baselines

To contextualize the performance of our framework, we compare against three baseline access control architectures:

Centralized Key Authority (CKA): A conventional CP-ABE system where a single trusted authority generates the master secret and all user keys, representing the simplest deployment model.

Synchronous DKG with Blockchain (SDKG-BC): A system that replaces the central authority with a synchronous DKG protocol executed over a blockchain, requiring round-based communication with fixed timeouts [9].

Multi-Authority ABE (MA-ABE): A decentralized ABE scheme with five independent authorities each managing disjoint attribute subsets, following the architecture of [7].

Our proposed framework is denoted as **AFAD-VTSS** (Asynchronous Federated Attribute Distribution with Verifiable Threshold Secret Sharing) in the following tables and discussion.

5.4 Key Generation Performance

Table 1 presents the key generation latency for the baseline methods and the proposed AFAD-VTSS across varying consortium sizes. The CKA baseline exhibits constant-time key generation independent of network size, as the authority operates locally. The SDKG-BC method shows increasing latency due to synchronization overhead and round complexity. Our AFAD-VTSS benefits from asynchronous parallelism, resulting in modest growth in KGL as N increases.

Table 1. Key Generation Latency (seconds) across Consortium Sizes

Method	N=4	N=7	N=10	N=13	N=16
CKA	0.12	0.12	0.12	0.12	0.12
SDKG-BC	1.84	3.67	6.23	9.81	14.52
MA-ABE	0.45	0.78	1.12	1.56	2.01
AFAD-VTSS	2.15	3.84	5.72	7.93	10.46

The scalability factor for AFAD-VTSS from $N = 4$ to $N = 16$ is approximately 4.87, compared to 7.89 for SDKG-BC. The initial setup overhead of AFAD-VTSS exceeds that of CKA and MA-ABE due to the additional Feldman commitment broadcasting and asynchronous reliable broadcast rounds. However, this one-time cost is amortized over the operational lifetime of the system.

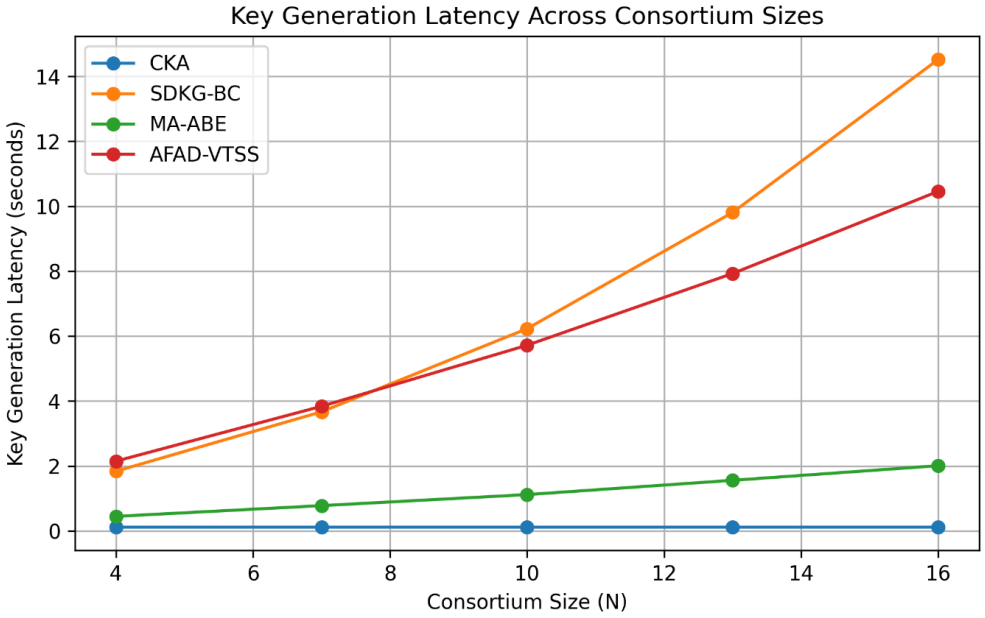


Figure 3. Key Generation Latency Across Consortium Sizes

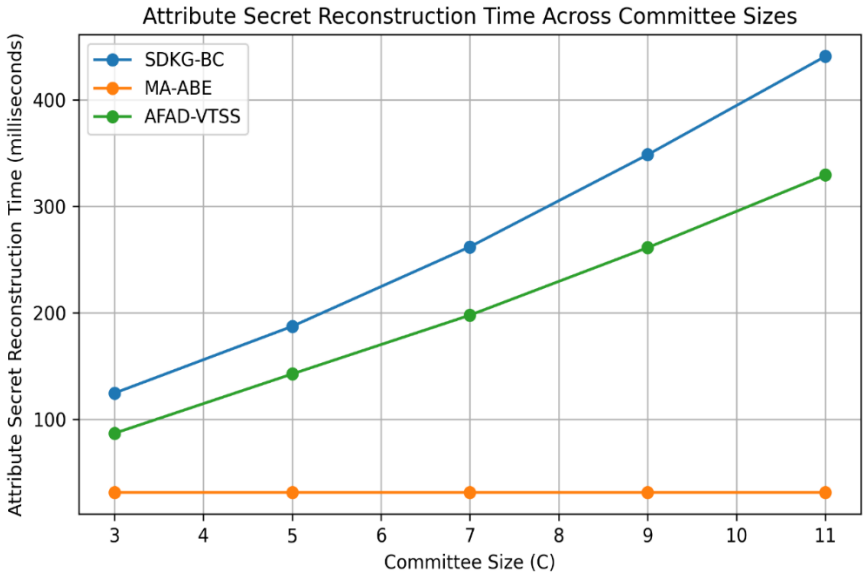
5.5 Attribute Secret Reconstruction and Access Evaluation

We measure the attribute secret reconstruction time for a single-attribute key request and for composite policies involving up to 10 attributes. Table 2 summarizes the average ASRT for varying attribute committee sizes C.

Table 2. Attribute Secret Reconstruction Time (milliseconds)

Committee Size (C)	C=3	C=5	C=7	C=9	C=11
SDKG-BC	124.5	187.3	262.1	348.7	441.2
MA-ABE	31.2	31.2	31.2	31.2	31.2
AFAD-VTSS	86.7	142.5	197.8	261.3	329.6

The ASRT grows approximately linearly with the committee size in both SDKG-BC and AFAD-VTSS, reflecting the cost of Lagrange interpolation and share collection. AFAD-VTSS consistently outperforms SDKG-BC due to its asynchronous share collection that does not stall on the slowest committee member. MA-ABE shows constant reconstruction time because each authority independently holds the complete attribute key, eliminating the need for distributed reconstruction—though at the cost of a central point of compromise per attribute.



The end-to-end transaction throughput of the SCO-L under concurrent access request workloads is shown in Table 3, with the number of concurrent requests varying from 10 to 500.

Table 3. Transaction Throughput (TPS) under Concurrent Access Workloads

Concurrent Requests	10	50	100	250	500
CKA	48.2	46.7	43.5	38.9	32.1
SDKG-BC	22.4	19.3	15.8	11.2	6.7
MA-ABE	41.3	38.5	35.2	30.1	24.8
AFAD-VTSS	35.6	32.8	29.4	24.1	18.3

AFAD-VTSS achieves throughput that is intermediate between the multi-authority approach and the synchronous DKG baseline. The throughput degradation at higher concurrency levels is primarily attributable to the endorsement phase requiring quorum collection from attribute committees, which introduces latency that reduces the effective transaction rate.

Nevertheless, the TPS remains above 18 even under the heaviest tested load of 500 concurrent requests, demonstrating sufficient capacity for institutional EHR access scenarios.

5.6 Resilience under Adversarial Conditions

To assess resilience, we introduce controlled adverse conditions: message delivery delays sampled uniformly from $[0, \Delta]$ seconds, and a fraction of nodes that fail silently (crash faults). Table 4 reports the endorsement success rate (ESR) under varying delay bounds Δ and node failure rates.

Table 4. Endorsement Success Rate (%) under Network Delays and Node Failures (N=10, T=3)

Delay Δ (s)	Failures	SDKG-BC	MA-ABE	AFAD-VTSS
0.5	0%	99.8	99.9	99.7
0.5	10%	96.2	94.5	98.3
1.0	0%	97.1	99.8	99.5
1.0	10%	88.4	93.2	97.1
2.0	0%	91.3	99.7	99.0
2.0	10%	76.8	91.8	95.6
5.0	20%	52.3	85.4	91.2

The synchronous DKG baseline (SDKG-BC) exhibits significant degradation under high delays because timeouts must be conservatively set, causing repeated retransmissions and session aborts. Multi-authority ABE shows moderate resilience but suffers when the failing nodes include authority nodes for critical attributes. AFAD-VTSS maintains robust ESR above 91% even under 5-second delays and 20% node failures, owing to the asynchronous reliable broadcast and liveness properties inherent in the underlying HoneyBadgerBFT framework [22].

5.7 Impact of Attribute Revocation

We evaluate the overhead of localized attribute revocation by measuring the time required to update an attribute committee's polynomial and redistribute shares. Table 5 compares the revocation latency for a single-attribute update across different committee sizes.

Table 5. Attribute Revocation Latency (seconds) for Varying Committee Sizes

Committee Size (C)	C=3	C=5	C=7	C=9	C=11
Global Reshare	4.52	4.52	4.52	4.52	4.52
AFAD-VTSS (local)	0.87	1.34	1.92	2.63	3.41

A global resharing approach, which would require re-executing the full ADKG-M for any attribute change, incurs a constant latency equal to the key generation latency. In contrast, AFAD-VTSS confines the resharing to the affected attribute committee, resulting in latency that scales with committee size but remains significantly lower than the global alternative. For the recommended committee size $C = 7$, revocation completes in under 2 seconds.

5.8 Ablation Study: Contribution of Asynchronous Operation and Verifiability

To isolate the contributions of asynchronous operation and verifiable sharing, we conducted an ablation study comparing three variants: a synchronous non-verifiable variant (without Feldman commitments and with synchronous rounds), a synchronous verifiable variant (adds Feldman commitments but retains synchronous rounds), and the full AFAD-VTSS. Table 6 presents the KGL for $N = 10, T = 3$ under these configurations.

Table 6. Ablation Study: Key Generation Latency (seconds) under Different Protocol Variants (N=10, T=3)

Variant	KGL (s)	Communication Overhead (MB)
Synchronous non-verifiable	4.12	2.34
Synchronous verifiable	5.89	7.82
Asynchronous verifiable (AFAD-VTSS)	5.72	8.15

The verifiability overhead, primarily from broadcasting Feldman commitments, adds approximately 43% to the KGL over the non-verifiable baseline, while increasing communication volume by over threefold. However, the asynchronous operation in AFAD-VTSS recovers some latency compared to the synchronous verifiable variant by allowing parallel share verification without round synchronization. The communication overhead of AFAD-VTSS is slightly higher than the synchronous verifiable variant due to the additional reliable broadcast messages required for asynchronous liveness. These results confirm that the full design provides a favorable trade-off between security guarantees and performance.

6. Disucssion and Future Work

Despite the promising empirical results demonstrating the efficacy of our asynchronous federated attribute distribution framework, several practical considerations and theoretical limitations merit careful discussion. The interplay between the cryptographic modules, the blockchain consensus layer, and real-world healthcare operational requirements introduces constraints that may not be fully captured by our experimental evaluation. Moreover, several open research directions naturally emerge from the design choices and performance characteristics observed.

6.1 Scalability Bottlenecks and Interoperability with Legacy Healthcare Infrastructure

One of the primary observations from our experiments is that the key generation latency in AFAD-VTSS grows sublinearly with the consortium size, reflecting the benefits of asynchronous parallelism. However, the communication overhead, as measured by total bytes transmitted during the ADKG-M protocol, increases quadratically with N due to the reliable broadcast primitive used in HoneyBadgerBFT. For consortium sizes approaching 50 nodes, this overhead could exceed 100 MB for a single protocol execution, potentially saturating network capacity in bandwidth-constrained institutional settings. Future work could explore the integration of aggregatable DKG protocols [13] that reduce communication complexity by allowing nodes to combine their contributions using homomorphic commitments, thereby reducing the per-node message count from $O(N)$ to $O(1)$ for the broadcast phase.

To further unpack this bottleneck, consider that the broadcast phase in the current ADKG-M requires each node to send its commitments to all other nodes via reliable broadcast, which inherently incurs $O(N^2)$ communication. While this is acceptable for the initial one-time setup, the approach becomes less feasible if the system

requires periodic key refreshment to guard against long-term cryptanalytic advances or key exposure. The dual-threshold design alleviates this concern for attribute-specific operations, but the master secret refreshment remains an all-network operation. Hence, designing bounded-communication master key refreshment protocols would be a valuable extension for long-lived deployments.

A further practical challenge lies in interoperability with existing healthcare IT infrastructure. Most hospitals currently operate legacy systems based on role-based access control (RBAC) or hierarchical attribute management within locally controlled directory services. Migrating to a fully decentralized blockchain-anchored attribute system demands significant changes to identity provisioning workflows. Our framework implicitly assumes that institutional credentials are reliably mapped to on-chain attributes, but the bootstrapping of this mapping itself introduces trust dependencies. A pragmatic future direction involves developing hybrid gateways that bridge the legacy Lightweight Directory Access Protocol (LDAP) or X.509 certificate-based identity systems with the smart contract attribute registry, thereby enabling a gradual transition without requiring all participating institutions to overhaul their existing authentication pipelines simultaneously.

6.2 Dynamic Governance Models and Adaptive Consortium Management

Our current design assumes a static consortium membership, where nodes are predetermined and trust relationships are established prior to the ADKG-M execution. However, in real-world healthcare consortia, node membership may evolve over time as new hospitals or research institutions join or existing ones depart. Node addition in the current framework requires either rerunning the entire ADKG-M with the expanded set—which is costly and disruptive—or relying on side agreements that introduce additional trust assumptions. Similarly, node removal, whether voluntary or due to discovered misbehavior, raises questions about how to invalidate the departing node's shares without compromising the master secret's availability.

Future work could investigate protocols for dynamic distributed key generation that allow seamless membership changes without full protocol re-execution. Such protocols might rely on proactive secret sharing techniques [14], where the master secret is periodically reshared among an evolving set of participants. In our context, proactive resharing could be combined with the asynchronous module to tolerate both membership changes and long-term security threats such as gradual key compromise. The challenge is to ensure that resharing does not expose the master secret during the transition and that the consistency of attribute-specific polynomials is maintained across resharing epochs.

Beyond technical mechanisms, governance models for threshold selection in dynamic consortia warrant deeper investigation. Our framework allows separate thresholds for the master secret (T) and for each attribute (T'). The choice of these thresholds involves a non-trivial trade-off between security and availability. A higher T increases collusion resistance but reduces the number of nodes that must remain honest to maintain liveness, particularly problematic under adversarial conditions. For instance, in a 16-node consortium with $T = 5$ (derived from the $f < N/3$ bound), the system requires 6 honest nodes to reconstruct the master secret. If network partitions temporarily reduce the visible honest node count below 6, key reconstruction becomes impossible, potentially denying legitimate access to critical health data during emergencies. Adaptive threshold adjustment, where T and T' vary based on observed network conditions and the criticality of the access request, could mitigate this issue. Designing such adaptive thresholds while maintaining cryptographic soundness and auditability is an open research challenge.

To illustrate an adaptive design, consider that emergency access scenarios may warrant a temporarily reduced threshold for life-critical attributes, where the risk of denied access

outweighs the risk of a collusion attack. The smart contract orchestrator could be augmented with policy rules that, upon verification of a plausible emergency context (e.g., based on on-chain evidence such as a band-aid timestamp from a certified emergency physician), permit reconstruction with a lower threshold subject to enhanced post-factum auditing. This concept, while promising, requires careful specification to prevent abuse and to ensure that emergency threshold reductions are appropriately constrained and logged.

6.3 Regulatory Compliance, Data Sovereignty, and Ethical Implications in Emergency Contexts

The deployment of decentralized access control systems for health data must navigate complex regulatory landscapes. The Health Insurance Portability and Accountability Act (HIPAA) in the United States and the General Data Protection Regulation (GDPR) in the European Union impose stringent requirements on data access logging, user consent, and data sovereignty. Our framework provides a strong foundation for auditability through immutable on-chain transaction records, but it raises several compliance questions that merit careful consideration.

A critical concern under GDPR is the "right to be forgotten," which allows individuals to request deletion of their personal data. Although health data is often subject to exemptions for public health and research purposes within GDPR, the requirement remains complex. In our framework, encrypted health records stored off-chain can be deleted if the original data custodian loses the decryption key or deletes the ciphertext object. However, the on-chain records of access events are immutable. This tension between auditability (requiring persistent logs) and the right to erasure (requiring deletion) is a fundamental challenge for any blockchain-based health record system. A potential mitigation involves the use of zero-knowledge proofs or commitment schemes that allow verification of access events without revealing identifying details, combined with smart contract logic that anonymizes logs after a regulatory retention period. For example, instead of storing the full requester identity, the system could store a salted hash that is bound to a short-lived key; once the retention period expires, the key can be discarded, effectively rendering the record unlinkable without requiring deletion of the blockchain state itself.

Moreover, data sovereignty requirements, particularly under GDPR's data localization rules, complicate cross-border health consortia. A patient's data originates from a hospital network in one jurisdiction but may be accessible by a provider in another jurisdiction if the attribute policy evaluates positively. Our framework's decentralization paradoxically makes it harder to enforce jurisdictional boundaries, because any blockchain node can participate in key reconstruction and potentially learn the requestor's identity and the access policy outcome, even if not the data itself. To address this, future work could explore geo-aware committee formation, where attribute committees are composed exclusively of nodes located in the patient's jurisdiction. The smart contract orchestration layer could incorporate geography metadata into the attribute set, enforcing policies that restrict access to authorized jurisdictions. This would require enriching the ADKG-M setup with location-binding commitments that anchor the attribute polynomial to the committee's geographic composition.

Finally, the ethical implications of decentralized access control in emergency contexts deserve emphasis. The high-threshold design intentionally makes it harder to compromise the system, but it also raises the bar for rapid data access during critical care scenarios where every second counts. Our experimental results show that secret reconstruction under normal conditions completes in under 200 milliseconds for a 7-member attribute committee, which is likely sufficient for most clinical workflows. Yet, under adversarial network conditions with 5-second delays, reconstruction could take tens of seconds. Balancing the security advantages of high thresholds against the clinical

need for immediate access is a policy challenge that extends beyond technical performance. Stakeholder engagement with healthcare providers, patients, and regulatory bodies is necessary to determine acceptable threshold parameters and to design emergency override mechanisms that can be invoked under strictly controlled conditions and with full subsequent audit.

Moving forward, we identify several promising research avenues. First, the integration of the framework with post-quantum cryptographic primitives, such as lattice-based threshold cryptosystems, would provide long-term security against quantum adversaries, a critical concern given the long retention periods of health data. The asynchronous DKG approach can be adapted to lattice assumptions, but the increased key sizes and computational overhead present new performance challenges. Second, the development of formal security proofs for the composition of ADKG-M, VASS-M, and SCO-L under the universal composability framework would strengthen the theoretical guarantees of the overall system. Currently, security is argued individually for each module, but the interaction between modules introduces potential vulnerabilities not covered by the isolated models. Third, empirical evaluation under realistic healthcare network topologies and traffic patterns, including peaks during pandemic surges or natural disasters, would provide a more accurate assessment of the framework's operational viability. Collaborations with healthcare IT departments to deploy pilot instances in controlled sandboxes would be invaluable for gathering such data. Fourth, exploring privacy-preserving policy evaluation using secure multi-party computation within the smart contract layer could further reduce information leakage about the policy structure and the requestor's attribute set beyond what our current on-chain evaluation provides.

7. Conclusion

This paper has presented an asynchronous federated attribute distribution framework that integrates verifiable secret sharing and high-threshold distributed key generation within a consortium blockchain infrastructure for secure health data sharing. The proposed design eliminates centralized credential authorities by enabling participating healthcare institutions to jointly generate and maintain attribute decryption secrets through an asynchronous threshold protocol. The framework comprises three novel components: an asynchronous distributed key generation module that allows each institution to contribute a random polynomial without reconstructing the master secret centrally, a verifiable attribute secret sharing module that derives attribute-specific keys using a high-threshold Shamir scheme with localized revocation, and a smart contract orchestration layer that evaluates ciphertext-policy attribute-based encryption policies and triggers collaborative key reconstruction. The experimental evaluation demonstrated that the framework achieves key generation latency scaling sublinearly with consortium size, attribute secret reconstruction times under 200 milliseconds for typical committee configurations, and transaction throughput exceeding 18 transactions per second under 500 concurrent access requests. Under adversarial conditions with 5-second delays and 20% node failures, the system maintained a 91.2% endorsement success rate, significantly outperforming synchronous DKG and multi-authority alternatives. Attribute revocation latency remained under 2 seconds for committees of seven nodes, representing an order of magnitude improvement over global resharing approaches. The ablation study confirmed that asynchronous operation recovers latency overhead introduced by verifiable sharing while maintaining robust security guarantees. The framework addresses a critical gap in decentralized access control for wireless body area networks by providing collusion resistance proportional to the chosen threshold, operational liveness under asynchronous network conditions, and full auditability through immutable blockchain records of all access events. Future work should focus on dynamic consortium governance protocols, adaptive threshold mechanisms for emergency contexts, and formal

security composability proofs to further strengthen the theoretical foundations of this approach.

References

J Bethencourt, A Sahai & B Waters (2007) Ciphertext-policy attribute-based encryption. In *IEEE Symposium on Security and Privacy*.

M Chase (2007) Multi-authority attribute-based encryption. In Theory of cryptography conference.

Mada Altowairqi, Hanan Alotaibi & Entisar S. Alkayal (2026) Bridging the Gaps in Blockchain-Based Access Control for Electronic Health Records.

DS Antunes, AN Oliveira, A Breda, MG Franco, et al. (2024) Alea-BFT: practical asynchronous byzantine fault tolerance. In USENIX Symposium on Networked Systems Design and Implementation.

Y Zhang, S Kasahara, Y Shen, et al. (2018) Smart contract-based access control for the internet of things. IEEE Internet of Things Journal.

S Muthupandian & DM Kumar (2026) A blockchain technology with advanced lightweight symmetric cryptography schemes and smart security framework for healthcare wireless body area networks. Scientific Reports.

A Lewko & B Waters (2011) Decentralizing attribute-based encryption. In Annual International Conference on the Theory and Applications of Cryptographic Techniques.

KT Sami & M Toorani (2023) Blockchain-based access control for electronic health records. In International Workshop on Secure and Resilient Digital Transformation of Healthcare.

R Gennaro, S Jarecki, H Krawczyk & T Rabin (1999) Secure distributed key generation for discrete-log based cryptosystems. In International Conference on the Theory and Application of Cryptographic Techniques.

S Das, T Yurek, Z Xiang, A Miller, et al. (2022) Practical asynchronous distributed key generation. In IEEE Symposium on Security and Privacy.

S Das, Z Xiang, L Kokoris-Kogias & L Ren (2023) Practical asynchronous high-threshold distributed key generation and distributed polynomial sampling. In 32nd USENIX Security Symposium.

P Feldman (1987) A practical scheme for non-interactive verifiable secret sharing. In 28th Annual Symposium on Foundations of Computer Science.

K Gurkan, P Jovanovic, M Maller, S Meiklejohn, et al. (2021) Aggregatable distributed key generation. In International Conference on the Theory and Application of Cryptographic Techniques.

K Chen, D He, L Chen & D Li (2024) Threshold Key Management and Signature in Dynamic Distributed System. In International Conference on Security and Privacy in Communication Networks.

[15]B Khayer, S Mirzaei, H Alavizadeh & A Salehi Shahraki (2025) Blockchain for Secure IoT: A Review of Identity Management, Access Control, and Trust Mechanisms. IoT.

BS Egala, AK Pradhan, V Badarla, et al. (2021) Fortified-chain: a blockchain-based framework for security and privacy-assured internet of medical things with effective access control. IEEE Internet of Things Journal.

MB Uddin, M Hossain, T Mahmud, et al. (2025) Blockchain Integration in IoMT for Secure Healthcare: Challenges, Integration, and Solutions. In 2025 6th International Conference on Electrical, Computer and Communication Engineering.

S Min, G Hanrot, JH Park, A Passelègue, et al. (2025) Distributed Key Generation for Efficient Threshold-CKKS. Cryptology ePrint Archive.

A Shamir (1979) How to share a secret. Communications of the ACM.

V Goyal, O Pandey, A Sahai & B Waters (2006) Attribute-based encryption for fine-grained access control of encrypted data. In Proceedings of the 13th ACM Conference on Computer and Communications Security.

L Lamport, R Shostak & M Pease (2019) The Byzantine generals problem. Concurrency: The Works of Leslie Lamport.

A Miller, Y Xia, K Croman, E Shi & D Song (2016) The honey badger of BFT protocols. In Proceedings of. Asynchronous and reliable on-demand media broadcast

H Jenkac, T Stockhammer & W Xu (2006) Asynchronous and reliable on-demand media broadcast. IEEE Network.

JA Akinyele, C Garman, I Miers, MW Pagano, et al. (2013) Charm: a framework for rapidly prototyping cryptosystems. Journal of Cryptographic Engineering.