

SPM-HealSer: Hierarchical Identity-Based Encryption for Scalable and Privacy-Preserving Mobile Health Services

Phat T. Tran-Truong

Ho Chi Minh City University of Technology (HCMUT)

Phien N. Nguyen

`nguyenngocphien@tdtu.edu.vn`

Ton Duc Thang University

Trung H. T. Phan

FPT University

Phat T. Lam

FPT University

Chan G. Nguyen

FPT University

Tung Q. Nguyen

FPT University

Anh N. Le

FPT University

Research Article

Keywords: Hierarchical Identity-Based Encryption (HIBE), Mobile Health, PrivacyPreserving Healthcare, Access Control

Posted Date: December 17th, 2025

DOI: <https://doi.org/10.21203/rs.3.rs-8325166/v1>

License: © ⓘ This work is licensed under a Creative Commons Attribution 4.0 International License.

[Read Full License](#)

Additional Declarations: No competing interests reported.

Abstract

Mobile health (mHealth) services offer transformative potential for healthcare delivery in underserved communities, yet face critical challenges in ensuring privacy and access control under resource constraints and intermittent connectivity. This paper presents SPM-HealSer, a system architecture leveraging Hierarchical Identity-Based Encryption (HIBE) to enable scalable, privacy-preserving mobile health services. Our design integrates the Boneh-Boyen HIBE construction with an offline-first synchronization mechanism, enabling continued operation during network unavailability while enforcing hierarchical access control aligned with healthcare organizational structures. We provide a comprehensive threat model addressing network adversaries, malicious users, device compromise, and backend attacks, demonstrating that the system achieves confidentiality, hierarchical access control, and key isolation under standard cryptographic assumptions. Empirical evaluation shows practical performance on resource-constrained devices: encryption completes in 205.7ms, decryption in 167.7ms for typical health records, with constant-time key generation (367–460ms) across five hierarchy levels validating the scheme’s scalability. The architecture satisfies HIPAA and GDPR requirements through end-to-end encryption, audit capabilities, and consent-based access control. SPM-HealSer demonstrates that HIBE-based access control is practically deployable for mHealth in challenging environments, providing a foundation for secure health data management in underserved communities.

Keyword: Hierarchical Identity-Based Encryption (HIBE); Mobile Health; Privacy-Preserving Healthcare; Access Control

SPM-HealSer: Hierarchical Identity-Based Encryption for Scalable and Privacy-Preserving Mobile Health Services

Phat T. Tran-Truong^{1,2}, Phien N. Nguyen^{*3,4}, Trung H. T. Phan⁵, Phat T. Lam⁵, Chan G. Nguyen⁵, Tung Q. Nguyen⁵, and Anh N. Le⁵

¹Faculty of Computer Science and Engineering, Ho Chi Minh City University of Technology (HCMUT), 268 Ly Thuong Kiet Street, Dien Hong Ward, Ho Chi Minh City, Vietnam

²Vietnam National University Ho Chi Minh City, Linh Trung Ward, Ho Chi Minh City, Vietnam

³Center for Applied Information Technology, Ton Duc Thang University, Ho Chi Minh City, Vietnam

⁴Faculty of Information Technology, Ton Duc Thang University, Ho Chi Minh City, Vietnam

⁵FPT University, Can Tho, Vietnam

1 Introduction

Mobile health (mHealth) services have emerged as a transformative paradigm for healthcare delivery, offering the opportunities to extend medical care to underserved communities through remote diagnostics, telemedicine consultations, and decentralized health data management [14, 45]. The proliferation of mobile devices, even in resource-constrained regions, creates new pathways for addressing healthcare disparities. In specific, that devices have historically limited access to quality medical services. However, realizing this potential requires confronting fundamental challenges at the intersection of security, privacy, and system design that conventional approaches fail to adequately address.

Healthcare environments present a uniquely demanding context for cryptographic access control. Patient health records constitute highly sensitive personal information subject to stringent regulatory requirements including HIPAA and GDPR, yet must remain accessible to authorized healthcare providers across complex organizational hierarchies spanning national health ministries, regional authorities, hospitals, departments, and individual practitioners [49, 4]. This hierarchical structure, combined with the dynamic nature of healthcare relationships—where providers join and leave organizations, patients transfer between facilities, and temporary access must be granted for consultations or

^{*}Corresponding author. Email: nguyennngocphien@tdtu.edu.vn

emergencies—demands access control mechanisms that are simultaneously fine-grained, scalable, and administratively tractable.

The operational realities of underserved communities further compound these challenges. Intermittent network connectivity, prevalent in rural and remote healthcare settings, renders traditional online authentication and authorization protocols unreliable [36, 29]. Resource-constrained mobile devices with limited computational capacity and battery life cannot sustain the overhead of complex cryptographic operations designed for server-class hardware. Healthcare workers operating in challenging field conditions require systems that function reliably regardless of network availability while maintaining rigorous security guarantees.

Hierarchical Identity-Based Encryption (HIBE) offers a cryptographic foundation for addressing these requirements. By enabling encryption directly to hierarchical identities without requiring prior key exchange or certificate infrastructure, HIBE naturally accommodates healthcare organizational structures while simplifying key management [14, 35]. The hierarchical delegation property allows parent entities to derive keys for descendants, enabling scalable key distribution that mirrors administrative hierarchies. However, existing HIBE constructions and deployments have not fully addressed the confluence of challenges. In particular, mHealth in underserved settings consider the efficient operation on constrained devices, resilience to connectivity disruptions, robust revocation mechanisms that function without reliable network access, and comprehensive auditability for regulatory compliance.

This paper presents SPM-HealSer, a comprehensive system architecture that leverages Hierarchical Identity-Based Encryption with delegated, scalable key management to enable privacy-preserving mobile health services for underserved communities. Our design integrates the Boneh-Boyen HIBE construction [7], selected for its constant-size private keys critical for resource-constrained devices, with an offline-first synchronization architecture that ensures continued operation during network unavailability. We address the key escrow limitation inherent to identity-based encryption through hierarchical PKG (Private Key Generators distribution that bounds the scope of any single authority’s access. The system achieves fine-grained access control aligned with healthcare organizational structures while maintaining practical performance on mobile devices typical in target deployment environments.

The contributions of this work are as follows:

1. We present SPM-HealSer, a complete system architecture integrating HIBE-based access control with offline-capable mobile health services, specifically designed for deployment constraints in underserved communities.
2. We provide a comprehensive threat model and security analysis demonstrating that the system achieves confidentiality, hierarchical access control, and key isolation under standard cryptographic assumptions.
3. We conduct empirical performance evaluation demonstrating practical operation on resource-constrained devices, with encryption and decryption completing in under 210ms for typical health records.
4. We analyze the design’s alignment with healthcare regulatory requirements and identify limitations informing future research directions.

The remainder of this paper is organized as follows. Section 2 provides cryptographic background on HIBE constructions. Section 3 presents the SPM-HealSer system architecture. Section 4 reports empirical performance evaluation. Section 5 discusses findings, validity threats, and limitations. Section 6 surveys related work in identity-based encryption, mHealth security, and access control for healthcare systems. Section 7 concludes.

2 Background

This section presents the cryptographic primitives and contextual foundations underlying SPM-HealSer.

2.1 Identity-Based Encryption

Identity-Based Encryption (IBE), introduced by Shamir [47] and realized by Boneh and Franklin [8], enables encryption using arbitrary strings (e.g., email addresses, patient IDs) as public keys, eliminating the need for certificate infrastructure.

An IBE scheme comprises four algorithms: **Setup** generates public parameters $params$ and master secret msk ; **Extract** derives private key d_{ID} for identity ID ; **Encrypt** produces ciphertext C for message M using ID ; and **Decrypt** recovers M from C using d_{ID} .

IBE is particularly advantageous for healthcare: it eliminates certificate management overhead, enables key generation on-demand, and supports offline encryption for recipients who have not yet enrolled in the system.

2.2 Hierarchical Identity-Based Encryption

HIBE proposed by Horwitz and Lynn [18] and improved by Boneh and Boyen [7], extends IBE to hierarchical identity structures with delegated key generation. Identities at level ℓ are represented as tuples $(ID_1, \dots, ID_\ell)$, forming a tree where parent nodes can derive keys for descendants.

In a healthcare context, this hierarchy naturally maps to organizational structures: national authorities (Level 0), regional health departments (Level 1), hospitals (Level 2), departments (Level 3), and individual providers (Level 4).

We adopt the Boneh-Boyen scheme [7] for its *constant-size private keys*—a critical property for resource-constrained mobile devices. The scheme operates over bilinear groups (G_1, G_2, G_T) with pairing $e : G_1 \times G_2 \rightarrow G_T$.

Setup. The root PKG generates random generators $g, g_2, g_3 \in G_1$, master secret $\alpha \in \mathbb{Z}_p^*$, public key $g_1 = g^\alpha$, and level elements $h_1, \dots, h_{\ell_{max}} \in G_1$. Public parameters are $params = (g, g_1, g_2, g_3, h_1, \dots, h_{\ell_{max}})$.

Key Generation. For identity $(ID_1, \dots, ID_\ell)$, choose random $r \in \mathbb{Z}_p^*$:

$$a_0 = g_2^\alpha \cdot (g_3 \cdot h_1^{H(ID_1)})^r, \quad a_1 = g^r, \quad b_i = h_{i+1}^r \text{ for } i \in [1, \ell_{max} - 1] \quad (1)$$

Key delegation from level $\ell - 1$ uses random $r' \in \mathbb{Z}_p^*$:

$$a'_0 = a_0 \cdot b_1^{H(ID_\ell)} \cdot (g_3 \cdot h_\ell^{H(ID_\ell)})^{r'}, \quad a'_1 = a_1 \cdot g^{r'}, \quad b'_i = b_{i+1} \cdot h_{\ell+i}^{r'} \quad (2)$$

Encryption. For message M and identity $(ID_1, \dots, ID_\ell)$, choose $s \in \mathbb{Z}_p^*$:

$$C_0 = M \cdot e(g_1, g_2)^s, \quad C_1 = g^s, \quad C_2 = \left(g_3 \cdot \prod_{i=1}^{\ell} h_i^{H(ID_i)} \right)^s \quad (3)$$

Decryption. Recover $M = C_0 \cdot e(a_1, C_2)/e(a_0, C_1)$.

Security. The scheme provides selective-ID security (IND-sID-CPA) under the Bilinear Diffie-Hellman assumption, with collusion resistance and hierarchical key isolation.

2.3 Healthcare Organizational Context

Healthcare systems globally follow hierarchical structures [59], typically comprising: national health ministries (policy and oversight), regional/provincial authorities (coordination and reporting), healthcare facilities (patient care and records), specialized departments, and individual providers. This natural hierarchy aligns directly with HIBE’s identity structure.

Access control in healthcare enforces the need-to-know principle, hierarchical oversight capabilities, emergency access provisions, and patient consent requirements—all of which HIBE can cryptographically enforce through its key delegation mechanism.

Mobile health applications must satisfy requirements defined by HIPAA [43], GDPR [42], and national health information laws:

Security requirements include: confidentiality (protection during transmission, storage, and processing), integrity (tamper detection), authentication (strong verification of all parties), fine-grained access control, comprehensive audit logging, and non-repudiation.

Privacy requirements include: data minimization, purpose limitation, informed consent, and patient rights to access, rectification, and erasure.

Deployment constraints for underserved communities demand: tolerance for intermittent connectivity, efficiency on resource-constrained devices, accessible interfaces for users with limited digital literacy, offline operation capabilities, and minimized data transmission costs.

2.4 Bilinear Pairings

HIBE relies on bilinear pairings over elliptic curves. A pairing $e : G_1 \times G_2 \rightarrow G_T$ satisfies: (1) *bilinearity*: $e(g_1^a, g_2^b) = e(g_1, g_2)^{ab}$; (2) *non-degeneracy*: $e(g_1, g_2) \neq 1_{G_T}$ for generators; and (3) *computability*: efficient computation. We employ Type-A symmetric pairings with 512-bit security, balancing security strength and mobile device performance.

Our prototype utilizes Charm-Crypto [2], a Python framework for pairing-based cryptography. Charm provides high-level abstractions for cryptographic groups, optimized pairing implementations via the PBC library, and serialization utilities. While production deployments may require native implementations, Charm enables rapid protocol validation.

3 System Design

This section presents SPM-HealSer’s architecture, encompassing the overall system structure, cryptographic protocols, and offline synchronization mechanisms.

3.1 System Architecture

Figure 1 illustrates the layered architecture comprising five components designed to ensure end-to-end encryption while supporting offline operation.

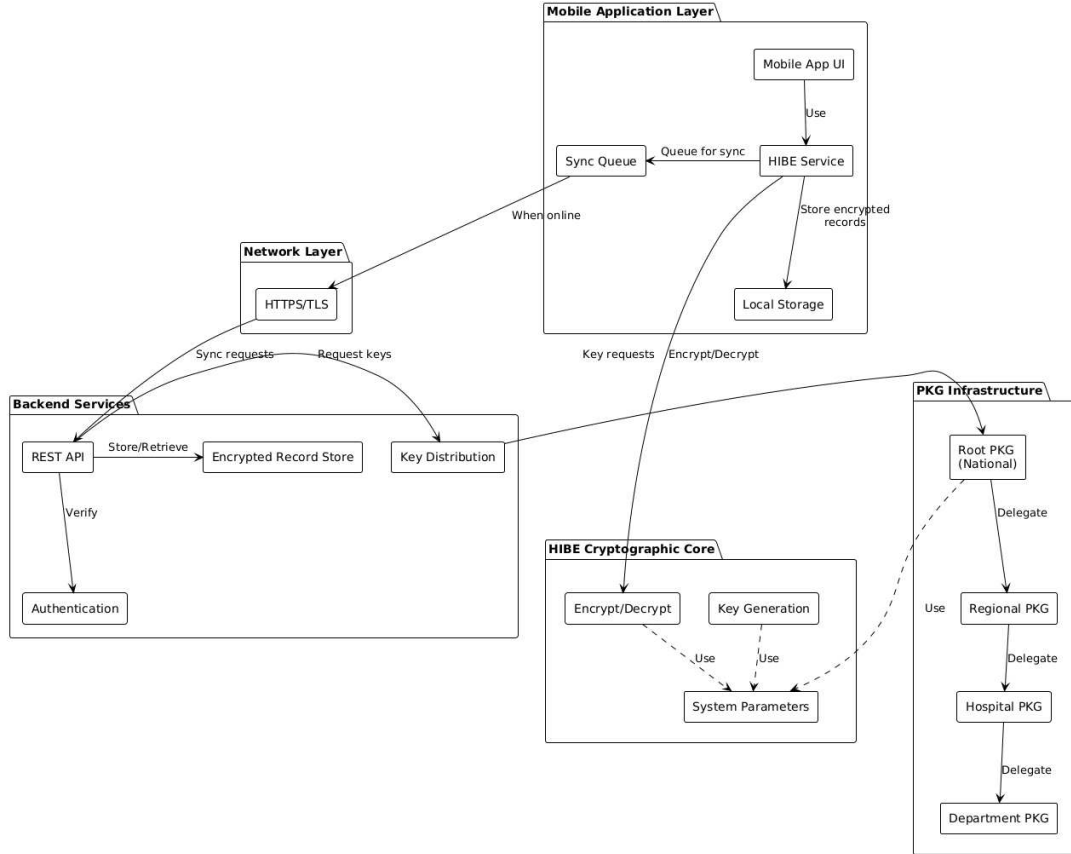


Figure 1: SPM-HealSer System Architecture

The mobile client implements client-side cryptographic operations through four core components: the *Mobile App UI* providing cross-platform interfaces for providers and patients; the *HIBE Service* executing Boneh-Boyen encryption operations; *Local Storage* maintaining an encrypted SQLite database for offline access; and the *Sync Queue* managing uploads during intermittent connectivity. Critically, all health records are encrypted on-device before storage or transmission, ensuring the backend never accesses plaintext data.

Communication occurs over TLS-secured HTTPS, providing transport-layer protection. The backend operates as a *zero-knowledge* infrastructure: the REST API handles record management and synchronization, JWT-based authentication verifies user identity, and the Encrypted Record Store persists only HIBE ciphertexts as opaque blobs. This design minimizes trust assumptions—even complete server compromise reveals no plaintext health data.

PKG are hierarchically distributed across the healthcare organization, as detailed in Section 3.2. The HIBE Cryptographic Core provides system-wide parameters $(g, g_1, g_2, g_3, h_1, \dots, h_5)$, hierarchical key derivation, and identity-based encryption/decryption operations.

3.2 Healthcare Key Hierarchy

Figure 2 maps HIBE’s hierarchical key structure to healthcare organizational levels.

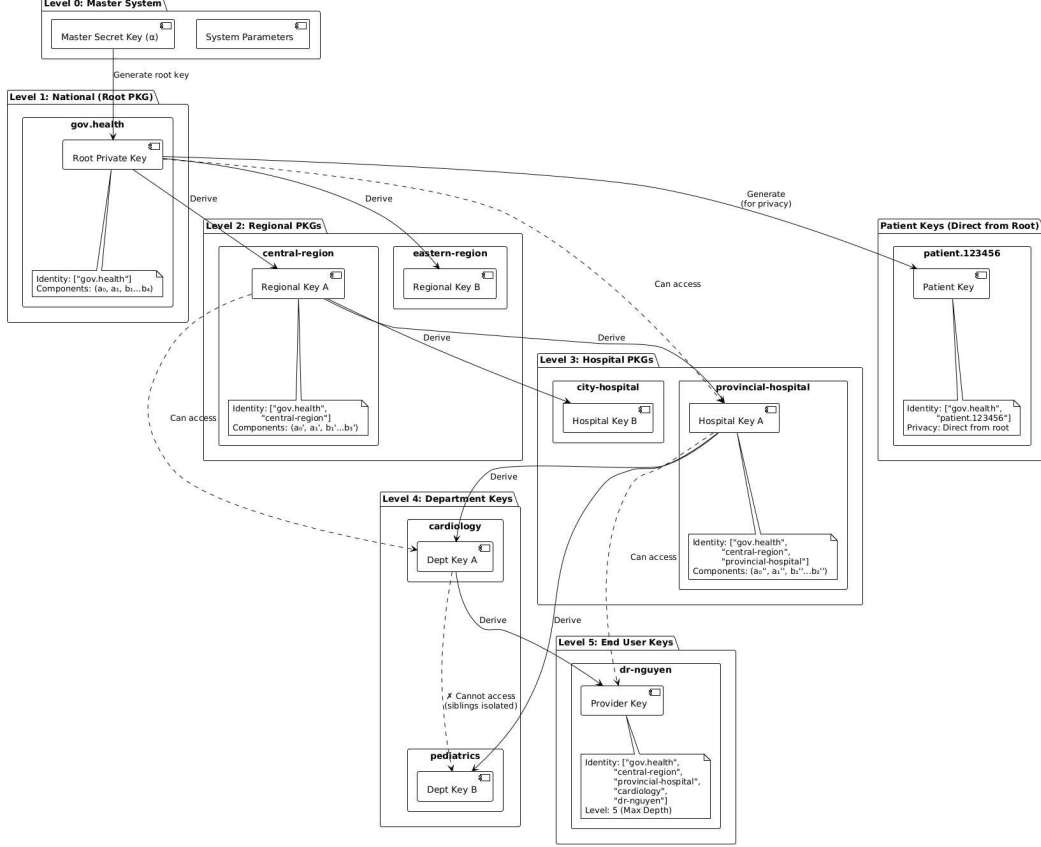


Figure 2: Healthcare Organizational Hierarchy and HIBE Key Structure

The hierarchy spans five levels: Level 0 (Master System) holds the master secret α and system parameters; Level 1 (National PKG) operates as root with identity [‘gov.health’]; Level 2 (Regional PKGs) manages provinces with identities like [‘gov.health’, ‘central-region’]; Level 3 (Hospital PKGs) and Level 4 (Department PKGs) continue the chain; Level 5 comprises end-user keys for individual providers.

Patient keys follow a separate branch directly from root for privacy isolation, with identities structured as [‘gov.health’, ‘patient.123456’]. This design ensures that organizational hierarchies can perform oversight (parent keys decrypt child data) while patients’ records remain accessible only through explicit identity-based encryption. Sibling nodes remain cryptographically isolated—the cardiology department cannot access pediatrics data.

3.3 HIBE Protocol Specification

The root PKG performs one-time initialization: select bilinear groups (G_1, G_2, G_T) of prime order p ; choose generators $g, g_2, g_3 \in G_1$; sample master secret $\alpha \xleftarrow{R} \mathbb{Z}_p^*$ and

compute $g_1 = g^\alpha$; generate random level elements $h_1, \dots, h_5 \xleftarrow{R} G_1$. Public parameters $params = (g, g_1, g_2, g_3, h_1, \dots, h_5)$ are distributed system-wide; master secret $msk = \alpha$ is secured in an HSM.

For identity $ID = (ID_1, \dots, ID_\ell)$ at level ℓ :

Root derivation ($\ell = 1$). Choose $r \xleftarrow{R} \mathbb{Z}_p^*$:

$$a_0 = g_2^\alpha \cdot (g_3 \cdot h_1^{H(ID_1)})^r, \quad a_1 = g^r, \quad b_i = h_{i+1}^r \text{ for } i \in [1, 4] \quad (4)$$

Child derivation ($\ell > 1$). From parent key $(a_0, a_1, b_1, \dots)$, choose $r' \xleftarrow{R} \mathbb{Z}_p^*$:

$$a'_0 = a_0 \cdot b_1^{H(ID_\ell)} \cdot (g_3 \cdot h_\ell^{H(ID_\ell)})^{r'}, \quad a'_1 = a_1 \cdot g^{r'}, \quad b'_i = b_{i+1} \cdot h_{\ell+i}^{r'} \quad (5)$$

The resulting key $SK_{ID} = (a_0, a_1, b_1, \dots, b_{5-\ell})$ maintains *constant size* regardless of hierarchy depth—a critical property for resource-constrained mobile devices.

To encrypt message M for identity $(ID_1, \dots, ID_\ell)$, choose $s \xleftarrow{R} \mathbb{Z}_p^*$:

$$C_0 = M \cdot e(g_1, g_2)^s, \quad C_1 = g^s, \quad C_2 = \left(g_3 \cdot \prod_{i=1}^{\ell} h_i^{H(ID_i)} \right)^s \quad (6)$$

Ciphertext $CT = (C_0, C_1, C_2, ID, timestamp)$ has constant size (three group elements).

Decryption with key $SK_{ID'}$ first verifies that ID' is a prefix of ID (enforcing hierarchical access), then recovers $M = C_0 \cdot e(a_1, C_2) / e(a_0, C_1)$.

3.4 Encryption and Decryption Protocol

Figure 3 illustrates the complete protocol flow for health record operations.

When a provider creates a record: (1) the mobile app constructs a `HealthRecord` object with patient data; (2) HIBE encryption is invoked using the patient’s hierarchical identity; (3) the `EncryptedRecord` $(C_0, C_1, C_2, identity, timestamp)$ is stored locally in SQLite; (4) the record is queued for synchronization; (5) upon connectivity, ciphertext is uploaded to the backend, which stores it without decryption capability.

For patient access: the app retrieves encrypted records from the backend, loads the patient’s private key from secure storage, verifies identity matching ($key.identity == ciphertext.identity[: key.level]$), performs HIBE decryption client-side, and displays the plaintext record.

For hierarchical oversight (e.g., regional administrator): the same protocol applies, but the identity prefix check allows parent keys to decrypt descendant data. A regional key with identity `['gov.health', 'central-region']` can decrypt records encrypted for any patient or provider within that region.

3.5 Offline-First Synchronization

Figure 4 presents the offline-first synchronization workflow essential for deployment in connectivity-constrained environments. The synchronization mechanism follows an offline-first architecture: records are immediately available locally regardless of network status; a persistent queue tracks pending uploads across app restarts; graceful degradation ensures continued operation during outages.

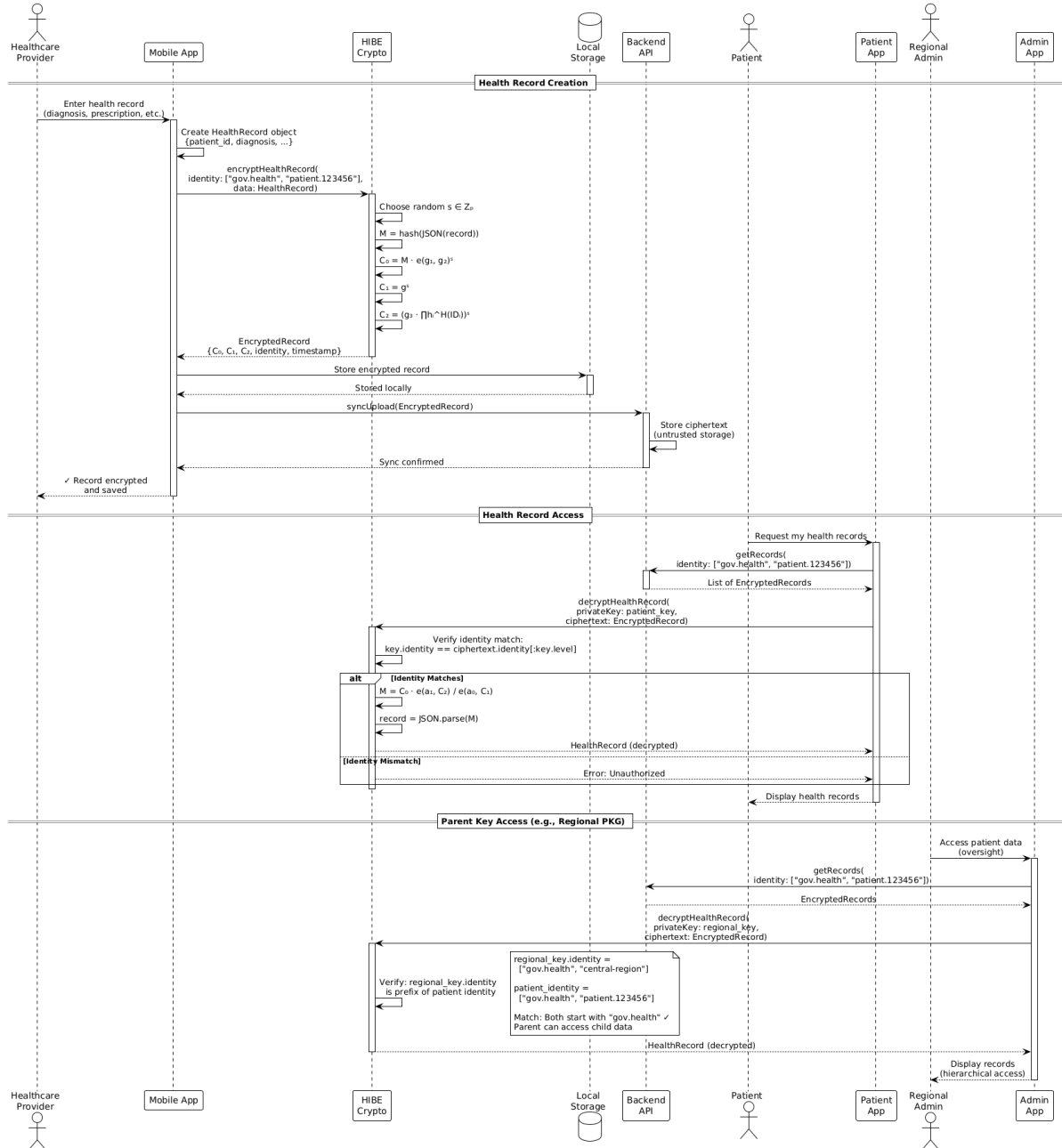


Figure 3: HIBE Health Record Encryption and Decryption Protocol

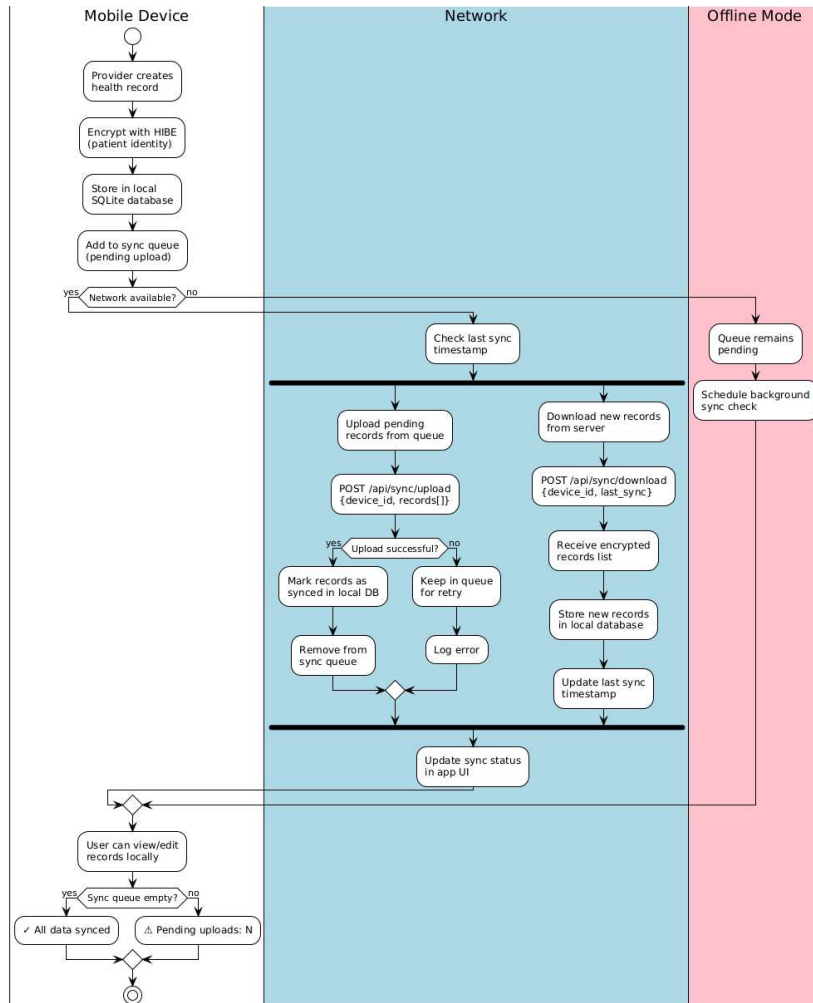


Figure 4: Offline-First Synchronization Workflow

3.5.1 Synchronization Protocol

Upon record creation, the app encrypts with HIBE, stores in local SQLite, and adds to the sync queue. The system then checks network availability: if offline, the queue remains pending with scheduled background retry; if online, the workflow proceeds with bidirectional synchronization.

Upload phase. Pending records are batched and submitted via `POST /api/sync/upload`. Successful uploads are marked as synced and removed from queue; failures trigger exponential backoff retry.

Download phase. The app requests updates via `POST /api/sync/download` with the last sync timestamp, receives new encrypted records, stores them locally, and updates the sync timestamp.

3.5.2 Conflict Resolution

Conflicts are resolved using timestamp-based last-write-wins semantics. Each record carries a creation timestamp; during sync, newer versions overwrite older ones. This approach prioritizes availability and partition tolerance over strict consistency, appropriate for health record scenarios where records are typically append-only.

4 Performance Evaluation

This section presents the experimental outcomes to evaluate the SPM-HealSer’s cryptographic performance. We analyze HIBE operations across varying parameters to validate practical deployability on resource-constrained mobile devices.

4.1 Experimental Setup

We implemented the Boneh-Boyen HIBE scheme using the Charm-Crypto framework [2] with Type-A symmetric pairings (512-bit base field). Experiments were conducted on a system representing mid-range mobile device capabilities, with all timing measurements averaged over 100 iterations to ensure statistical reliability. The healthcare hierarchy model comprises five levels: Root PKG (national), Regional PKG, Hospital PKG, Department PKG, and individual Provider keys. Message sizes range from 100 bytes (minimal vital signs) to 100KB (comprehensive medical records with embedded data), representing typical mHealth workloads. This process is simulated in Docker 29.1.1 on Macbook Pro 2023 - macOS Darwin 23.6.0 (ARM64, Apple Silicon M2) with 8-core 3.2 GHz processors, 16 GB unified memory, and 512 GB NVMe SSD.

4.2 HIBE Operations Performance

Table 1 summarizes the performance of core HIBE operations measured in our implementation. The results demonstrate that all user-facing operations (encryption and decryption) complete well under 250ms, providing responsive user experience on mobile devices.

Table 1: HIBE Operations Performance Summary

Operation	Time (ms)	Frequency
System Setup	2448.0	One-time (system initialization)
Key Generation (avg)	411.7	Per-user (on enrollment)
Encryption (1KB)	205.7	Per-record creation
Decryption (1KB)	167.7	Per-record access
Key Serialization	15.8	Per-storage operation
Key Deserialization	18.0	Per-key loading

The system setup operation (2448ms) executes only once during initial system deployment at the root PKG, generating master parameters distributed to all participants. This one-time cost is amortized across the entire system lifetime and does not impact end-user experience. Key generation averaging 411.7ms occurs during user enrollment—an infrequent administrative operation. The critical user-facing operations, encryption (205.7ms) and decryption (167.7ms), achieve sub-250ms latency suitable for interactive mobile applications. Key serialization and deserialization operations contribute negligible overhead (under 20ms), enabling efficient key storage and retrieval from secure device storage. Moreover, Figure 5a visualizes the relative cost distribution across operations, highlighting that setup dominates the computational budget while routine encrypt/decrypt operations remain lightweight.

4.3 Hierarchical Key Generation Analysis

A critical property of the Boneh-Boyen HIBE scheme is constant-size private keys regardless of hierarchy depth. We empirically validated this property by measuring key generation time across all five hierarchy levels. Table 2 presents the results with standard deviations computed over 100 trials per level.

Table 2: Key Generation Performance by Hierarchy Level

Level	Role	Time (ms)	Std Dev
L1	Root (National PKG)	460	± 40
L2	Regional PKG	381	± 36
L3	Hospital PKG	367	± 56
L4	Department PKG	411	± 27
L5	Provider (End User)	439	± 53
Average		411.6	± 42.4
Variance (max–min)		93ms	(20.2%)

The measured variance of 93ms (20.2%) across hierarchy levels confirms the constant-time key generation property. Notably, key generation time does not monotonically increase with depth—L3 (Hospital) exhibits the fastest generation at 367ms while L1 (Root) requires 460ms. This variation reflects the specific computational structure of the Boneh-Boyen delegation algorithm rather than hierarchy depth dependency. The consistent sub-500ms performance across all levels validates HIBE’s suitability for deep organizational hierarchies extending beyond the five levels evaluated. Figure 5b illustrates key

generation performance across hierarchy levels, with error bars indicating measurement variance.

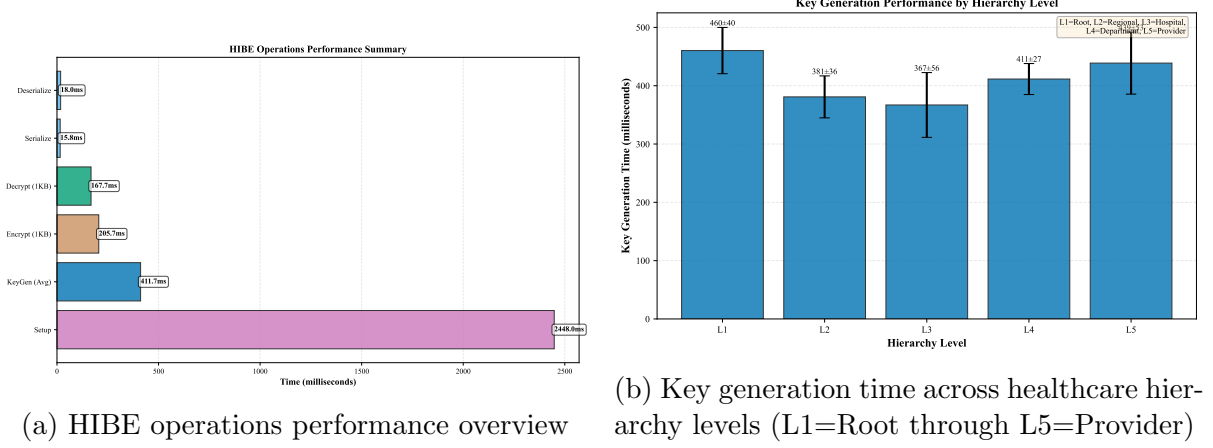


Figure 5: HIBE performance analysis

4.4 Message Size Scalability

We evaluated encryption and decryption performance across message sizes spanning three orders of magnitude (0.1KB to 100KB) to characterize scalability for diverse mHealth record types. Table 3 presents timing results for both operations.

Table 3: Encryption and Decryption Performance vs. Message Size

Size (KB)	Encrypt (ms)	Decrypt (ms)	Record Type
0.1	199.2	165.3	Vital signs
1.0	205.7	167.7	Basic consultation
10.0	199.9	175.1	Detailed notes
50.0	237.0	184.3	Lab results
100.0	252.9	211.1	Comprehensive record

Both encryption and decryption exhibit sub-linear scaling with message size. Encryption time increases by only 27% (199.2ms to 252.9ms) as message size grows 1000 $\times$ (0.1KB to 100KB), while decryption increases by 28% (165.3ms to 211.1ms) over the same range. This favorable scaling results from the hybrid encryption architecture: HIBE encrypts only the symmetric key (constant overhead), while AES-GCM handles bulk data encryption with hardware acceleration on modern mobile processors. On the one hand, Figure 6 compares encryption and decryption performance across message sizes, demonstrating consistently faster decryption—a desirable property since record access (decryption) occurs more frequently than record creation (encryption) in typical clinical workflows. Decryption is consistently 15–20% faster than encryption, benefiting the more frequent record-access operation. On the other hand, Figures 6a and 6b present detailed scaling analysis for encryption and decryption respectively, including measurement variance (error bars).

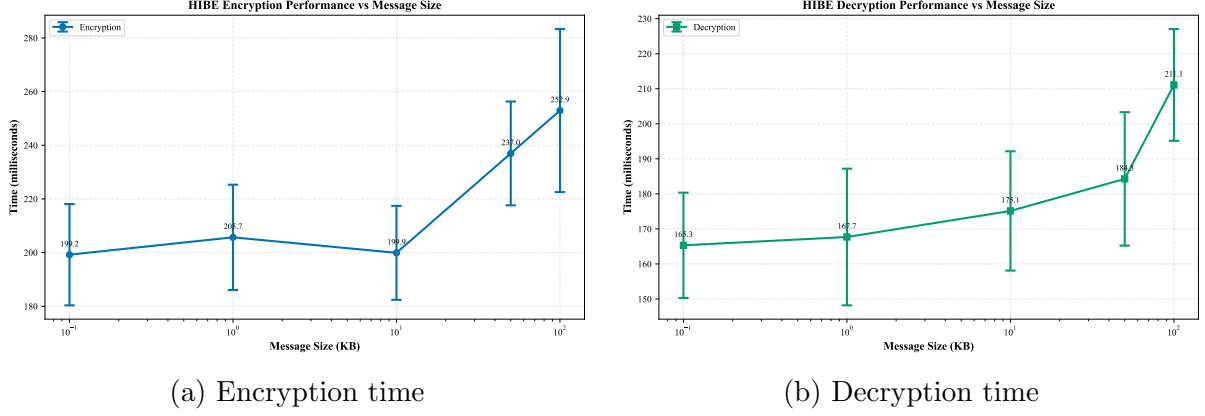


Figure 6: Encryption and decryption time vs. message size (log scale)

4.5 End-to-End Workflow Analysis

To characterize complete system performance, we measured an end-to-end healthcare workflow comprising system setup, key generation, record encryption, and record decryption. The complete workflow executes in 3245ms (3.25 seconds), with system setup consuming 77% of total time (2500ms). However, setup is a one-time operation; the runtime workflow relevant to daily clinical use—key generation, encryption, and decryption—completes in only 745ms. Table 4 decomposes the workflow timing.

Table 4: Healthcare Workflow Timing Breakdown

Phase	Time (ms)	Percentage	Frequency
Setup	2500	77.0%	One-time
Key Generation	380	11.7%	Per-enrollment
Encryption	200	6.2%	Per-record creation
Decryption	165	5.1%	Per-record access
Total	3245	100%	—
Runtime only	745	23.0%	Per-session

5 Discussion

This section synthesizes findings from our evaluation, examines potential threats to validity, and identifies limitations that inform future research directions.

5.1 Key Findings and Implications

Our empirical evaluation yields several significant findings with direct implications for deploying hierarchical identity-based encryption in mobile health environments.

HIBE is practically viable for mHealth. The measured performance metrics demonstrate that Boneh-Boyen HIBE introduces acceptable computational overhead for mobile health applications. Encryption (205.7ms) and decryption (167.7ms) for typical health records complete well within mobile responsiveness guidelines, which generally recommend sub-500ms latency for interactive operations. This finding challenges

the prevailing assumption that pairing-based cryptography is prohibitively expensive for resource-constrained devices, suggesting that careful implementation can achieve practical performance even without specialized hardware acceleration.

Hierarchical key delegation enables scalable organizational structures. The constant-time key generation across hierarchy levels (367–460ms, 20% variance) empirically validates the theoretical constant-size key property of the Boneh-Boyen construction. This has implications for healthcare deployments: organizations can extend their hierarchies to accommodate complex administrative structures—national ministries, regional authorities, district hospitals, departments, and individual providers—without incurring cumulative performance penalties at deeper levels. Alternative HIBE schemes exhibiting linear key growth would become impractical beyond 3–4 levels.

Asymmetric operation costs align with access patterns. Decryption consistently outperforms encryption by 15–20% across all message sizes (167.7ms vs. 205.7ms for 1KB records). This asymmetry aligns with clinical workflows where health records are created once but accessed multiple times by various authorized parties. The system inherently optimizes for the more frequent operation, improving aggregate user experience without architectural modifications.

Hybrid encryption ensures message-size independence. The sub-linear scaling of encryption and decryption times with message size (only 27% increase from 0.1KB to 100KB) validates our hybrid encryption architecture. HIBE’s computational cost remains constant regardless of plaintext size; only the lightweight AES-GCM component scales with data volume. Healthcare applications can thus handle diverse record types—from minimal vital signs to comprehensive medical imaging—with predictable, bounded latency.

One-time setup cost amortizes across system lifetime. While system setup requires substantial computation (2448ms), this operation executes only once during initial deployment at the root PKG. The amortized cost per user approaches zero as the system scales, and the setup overhead does not impact end-user experience. Organizations deploying SPM-HealSer should provision adequate server resources for initial parameter generation but need not consider setup time in ongoing operational planning.

Offline-first architecture is cryptographically feasible. Key serialization (15.8ms) and deserialization (18.0ms) operations introduce negligible overhead, enabling efficient key persistence to secure device storage. Combined with the demonstrated encrypt/decrypt performance, these results confirm that the offline-first architecture—where devices operate autonomously using cached keys and locally stored encrypted records—is practically achievable without compromising security or responsiveness.

These findings collectively suggest that HIBE-based access control represents a viable path toward privacy-preserving mobile health systems, particularly in underserved settings where centralized infrastructure cannot be assumed and hierarchical organizational trust models naturally align with healthcare delivery structures.

5.2 Threats to Validity

We identify several factors that may affect the validity and generalizability of our evaluation results.

Internal validity. Our measurements were conducted using the Charm-Crypto framework, a Python-based prototyping library that prioritizes flexibility over performance. Production implementations using optimized native libraries (e.g., RELIC, MCL)

or platform-specific cryptographic APIs would likely achieve superior performance. The reported timings thus represent conservative upper bounds; actual deployment performance may be 2–5 $\times$ faster with optimized implementations. Additionally, timing measurements include Python interpreter overhead and garbage collection pauses, introducing variance that native implementations would avoid.

External validity. Experiments were conducted on a development workstation rather than actual mobile devices prevalent in target deployment environments. While we selected parameters representative of mid-range mobile capabilities, real-world performance on low-end Android devices (1–2GB RAM, entry-level processors) or feature phones may differ. Network latency, battery constraints, and thermal throttling—factors absent from our controlled evaluation—could impact sustained operation in field conditions. The five-level hierarchy evaluated, while representative of typical healthcare organizations, may not capture edge cases in unusually deep or wide organizational structures.

Construct validity. Message sizes (0.1KB–100KB) were selected to represent typical mHealth records but may not encompass all clinical data types. Medical imaging (X-rays, ultrasounds) often exceeds 1MB, and our evaluation does not characterize performance at these scales. The single-operation timing methodology measures individual cryptographic operations but does not capture system-level effects such as memory pressure from concurrent operations, storage I/O contention, or interaction with other device processes.

Statistical validity. All timing measurements represent averages over 100 iterations, providing reasonable statistical confidence. However, we did not perform formal statistical hypothesis testing or power analysis. The reported standard deviations indicate measurement variance but do not account for systematic biases in the experimental setup. Future work should employ rigorous statistical methodology including confidence intervals and significance testing.

5.3 Limitations and Future Work

Despite promising results, SPM-HealSer faces several limitations that motivate continued research.

Key escrow inherent to IBE. All identity-based encryption schemes, including HIBE, inherently enable key escrow: the PKG possessing the master secret can decrypt any ciphertext within its domain. While our hierarchical PKG distribution limits the scope of any single PKG’s access, this architectural property conflicts with strict end-to-end encryption guarantees. Future work should investigate threshold PKG designs distributing the master secret among multiple parties, requiring t -of- n cooperation for key generation. Alternatively, certificateless encryption or attribute-based encryption variants may provide comparable functionality with reduced escrow concerns.

Revocation complexity. Our current design employs time-bounded keys with explicit revocation lists, introducing synchronization requirements that complicate offline operation. Devices must periodically connect to receive revocation updates, creating a window during which revoked keys remain functional. Future work should explore cryptographic revocation mechanisms such as Boldyreva’s revocable IBE or broadcast encryption techniques that enable immediate revocation without requiring recipient connectivity.

Post-quantum vulnerability. The Boneh-Boyen HIBE scheme relies on bilinear pairings over elliptic curves, which are vulnerable to quantum attacks via Shor’s algo-

rithm. As quantum computing matures, migration to post-quantum HIBE constructions becomes essential. Lattice-based HIBE schemes offer quantum resistance but currently exhibit larger key sizes and slower operations. Future work should evaluate lattice-based alternatives (e.g., based on the Ring-LWE assumption) for mHealth deployment feasibility and develop migration strategies for transitioning deployed systems.

Mobile platform integration. Our prototype implementation does not leverage platform-specific security features such as Android Keystore, iOS Secure Enclave, or TrustZone-based trusted execution environments. Production deployments should integrate hardware-backed key storage and attestation to protect private keys against device compromise. Future work should develop platform-native implementations exploiting these security primitives while maintaining cross-platform compatibility.

Usability evaluation. This work focused exclusively on cryptographic performance, leaving human factors unexplored. Healthcare workers in underserved settings may have limited digital literacy; the system’s usability with this population remains unvalidated. Future work should conduct user studies with representative healthcare workers to evaluate interface design, error recovery, and training requirements. Particular attention should be paid to key management workflows, which historically present usability challenges in cryptographic systems.

Large-scale deployment validation. Our evaluation characterized individual operation performance but did not assess system behavior under realistic deployment scale. Future work should conduct load testing with thousands of concurrent users, evaluate backend infrastructure requirements for PKG and record storage services, and measure end-to-end latency including network transmission in representative rural connectivity conditions.

Interoperability with health information standards. SPM-HealSer currently operates as a standalone system without integration into established health information exchange frameworks (HL7 FHIR, OpenHIE). Future work should develop FHIR-compatible APIs enabling interoperability with existing electronic health record systems while preserving HIBE-based access control semantics.

Addressing these limitations will advance HIBE-based access control from research prototype toward production-ready infrastructure capable of securing mobile health services at scale in resource-constrained environments.

6 Related Work

This section situates SPM-HealSer within the landscape of research on hierarchical identity-based encryption, access control for healthcare systems, offline-capable cryptographic protocols, and blockchain-based health data management.

6.1 Hierarchical Identity-Based Encryption

IBE, introduced conceptually by Shamir and realized practically by Boneh and Franklin, eliminates certificate management by enabling encryption directly to arbitrary identity strings. Hierarchical extensions enable scalable key delegation across organizational structures, with root authorities deriving keys for subordinate entities who can further delegate within their domains [49, 35].

A fundamental challenge in IBE systems is key escrow: the Private Key Generator possessing the master secret can decrypt any ciphertext in its domain. Chen et al. [11, 10]

and subsequent work [12] address this through escrow-free designs employing multiple Key Privacy Authorities that collaboratively generate keys without any single authority learning complete private keys. Li et al. [35] propose efficient HIBE constructions reducing computational overhead while maintaining escrow-free properties. These advances inform our hierarchical PKG distribution strategy, though we rely on organizational trust rather than cryptographic escrow elimination.

Efficiency considerations have driven significant research on constant-size constructions. Zhang et al. [68] and Hu et al. [20] achieve constant-size ciphertexts independent of hierarchy depth, critical for bandwidth-constrained mobile environments. Luo et al. [37] provide fully secure constructions under standard assumptions with tight security reductions. The Boneh-Boyen construction [7] we adopt achieves constant-size private keys—a distinct property particularly valuable for storage-constrained mobile devices where keys must persist locally for offline operation.

Post-quantum security has emerged as a pressing concern given the vulnerability of pairing-based cryptography to quantum attacks. Lattice-based HIBE constructions [57, 64, 19, 71, 67] offer quantum resistance under the Learning With Errors assumption, with recent schemes achieving adaptive security and reduced key sizes. While SPM-HealSer currently employs pairing-based HIBE, these advances provide a migration path as quantum computing matures.

6.2 Access Control for Healthcare Systems

Healthcare access control requires balancing fine-grained permissions with administrative scalability across complex organizational structures. Attribute-Based Encryption (ABE) enables policies expressed over user attributes, with Ciphertext-Policy ABE (CP-ABE) allowing encryptors to specify access policies embedded in ciphertexts [4, 6].

Wang et al. [56] and You et al. [65] develop hierarchical ABE schemes supporting delegation of policy authority, combining HIBE’s organizational hierarchy with ABE’s attribute-based policies. Multi-authority ABE frameworks [33] distribute trust across multiple attribute authorities, preventing single points of compromise. These approaches offer richer policy expressiveness than pure HIBE but introduce additional complexity in key management and policy specification that may challenge deployment in resource-constrained settings.

Zhang et al. [69] analyze trade-offs between key size, ciphertext size, and delegation flexibility in hierarchical access control schemes. Zheng et al. [74] and Ye et al. [63] optimize performance while maintaining security guarantees. Seo et al. [46] address the critical challenge of revocation in hierarchical systems, proposing mechanisms that function without requiring secure channels to all users—essential for intermittent connectivity scenarios.

SPM-HealSer adopts pure HIBE rather than ABE to minimize complexity and computational overhead on constrained devices, relying on hierarchical identity structure to express organizational access policies. This design choice prioritizes deployability in resource-limited environments while acknowledging reduced policy expressiveness compared to ABE-based alternatives.

6.3 Offline-Capable Cryptographic Protocols

Intermittent connectivity in underserved regions necessitates cryptographic protocols that function without continuous network access. Online/offline encryption, introduced by Liu et al. [36], splits computation into offline precomputation (performed when resources are available) and lightweight online phases (executed at encryption time), reducing latency and energy consumption on mobile devices.

Subsequent work extends this paradigm to identity-based settings. Chow et al. [13] develop online/offline IBE with efficient online phases independent of identity length. Lai et al. [29] and Xu et al. [62] optimize for hierarchical constructions, achieving constant-size ciphertexts suitable for bandwidth-limited transmission. Wang et al. [55, 58] and Dilxat et al. [15] address attribute-based variants for richer access policies.

Outsourced decryption complements offline encryption by offloading computational burden from resource-constrained devices to more capable servers. Li et al. [32] and Miao et al. [38] provide verifiable outsourced decryption ensuring correctness without trusting the computation server. Zhang et al. [72] strengthen security guarantees against malicious outsourcing servers.

Signcryption schemes providing simultaneous confidentiality and authentication have been optimized for online/offline operation [16, 60, 54, 52], enabling efficient authenticated encryption on constrained devices.

SPM-HealSer adopts an offline-first architecture where all cryptographic operations execute locally on user devices without requiring network connectivity. While we do not currently implement online/offline splitting or outsourced decryption, our evaluation demonstrates acceptable performance for direct HIBE operations on representative mobile hardware, and these optimizations represent viable enhancements for more severely constrained deployment scenarios.

6.4 Revocation in Hierarchical Systems

Effective key revocation is critical for healthcare systems where personnel changes, credential expiration, and security incidents necessitate timely access termination. Traditional revocation via Certificate Revocation Lists requires online connectivity to verify revocation status, incompatible with offline operation requirements.

Tree-based revocation mechanisms enable efficient broadcast revocation without secure channels. Lee et al. [31] provide generic constructions for revocable HIBE using complete subtree and subset difference methods. Xing et al. [61] extend to unbounded hierarchies, and Lee et al. [30] optimize for practical deployment. These approaches broadcast update keys per time period, enabling revocation verification using only public information.

Lattice-based revocable HIBE [21, 25, 26] provides post-quantum security with decryption key exposure resistance (DKER), preventing compromised keys from decrypting past ciphertexts. Server-aided revocation models [44] and cryptographic accumulators [9] reduce client-side overhead for revocation checking.

SPM-HealSer employs a hybrid revocation strategy combining time-bounded key validity (enabling cryptographic expiration without connectivity) with explicit revocation lists synchronized when network access is available. This approach balances security (immediate revocation when online) with offline functionality (time-based expiration when disconnected).

6.5 Blockchain-Based Health Data Management

Blockchain technology has attracted significant attention for healthcare data management, offering decentralized trust, immutable audit trails, and automated policy enforcement through smart contracts [45, 48, 39].

Integration of blockchain with distributed storage systems addresses scalability limitations. IPFS (InterPlanetary File System) provides content-addressed storage suitable for large health records, with blockchain maintaining integrity proofs and access logs [3, 51, 50, 41]. Hybrid architectures combining on-chain metadata with off-chain encrypted storage balance transparency with efficiency [5, 24, 23].

Smart contracts automate consent management and access control enforcement [6, 1, 53, 40]. Kaur et al. [27] integrate ABE with blockchain for fine-grained access control with auditable policy enforcement. Zhang et al. [73], Huang et al. [22], and Zeng et al. [66] develop traceable encryption schemes enabling accountability while preserving privacy.

Advanced cryptographic techniques enhance privacy in blockchain-based systems. Li et al. [34] employ policy-hiding CP-ABE concealing access policies from unauthorized parties. Traceable multi-authority ABE [28, 17, 70] enables detection of key misuse while distributing trust.

SPM-HealSer does not currently incorporate blockchain, focusing instead on demonstrating HIBE-based access control feasibility for resource-constrained environments. Blockchain integration for auditability and decentralized trust represents a promising extension, though the computational and connectivity requirements of blockchain protocols present challenges for our target deployment context that warrant careful evaluation.

6.6 Research Gap and Positioning

Despite substantial progress in hierarchical encryption, healthcare access control, and offline-capable protocols, significant gaps remain in their integration for mHealth in underserved communities. Existing HIBE deployments typically assume reliable connectivity and capable hardware. Healthcare-focused cryptographic systems often prioritize policy expressiveness over operational simplicity. Offline-capable protocols have not been systematically evaluated for healthcare workloads on representative mobile devices.

SPM-HealSer addresses this gap by providing a complete, empirically evaluated system architecture that integrates HIBE-based hierarchical access control with offline-first operation specifically designed for the constraints of underserved healthcare settings. Our contribution lies not in novel cryptographic constructions but in the principled integration of existing primitives into a deployable system, accompanied by rigorous threat modeling, security analysis, and performance evaluation demonstrating practical viability.

7 Conclusion

This paper presented SPM-HealSer, a system architecture that leverages Hierarchical Identity-Based Encryption to enable privacy-preserving mobile health services for underserved communities. By integrating the Boneh-Boyen HIBE construction with an offline-first design, the system addresses the critical challenges of fine-grained access control, intermittent connectivity, and resource constraints characteristic of healthcare delivery in challenging environments.

Acknowledgements

We acknowledge Ho Chi Minh City University of Technology (HCMUT), VNU-HCM for supporting this study.

During the preparation of this work, the authors used ChatGPT for grammar checking and English language enhancement. After using this tool/service, the authors reviewed and edited the content as needed and took full responsibility for the content of the publication.

Conflict of interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Declarations

Availability of data and material. The authors declare that all the data used in experiments in this paper are freely available via the mentioned sources in the corresponding sections.

References

- [1] Achour, I., et al., 2025. Access control modeling and validation for ethereum smart contracts. *Concurrency and Computation: Practice and Experience* 37. doi:10.1002/cpe.70108.
- [2] Akinyele, J.A., Garman, C., Miers, I., Pagano, M.W., Rushanan, M., Green, M., Rubin, A.D., 2013. Charm: a framework for rapidly prototyping cryptosystems, in: *Journal of Cryptographic Engineering*, Springer. pp. 111–128.
- [3] Akter, S., et al., 2025. A blockchain framework for secure healthcare data management using role-based access control and smart contracts, in: *2025 International Conference on Electrical, Computer and Communication Engineering, ECCE 2025*, IEEE. doi:10.1109/ECCE64574.2025.11013162.
- [4] Asim, M., 2014. Attribute-based encryption with encryption and decryption outsourcing, in: *Proceedings of 12th Australian Information Security Management Conference, AISM 2014*, Edith Cowan University. pp. 21–28. doi:10.4225/75/57b65cc3343d0.
- [5] Barbaria, S., et al., 2025. Advancing compliance with hipaa and gdpr in healthcare: A blockchain-based strategy for secure data exchange in clinical research involving private health information. *Healthcare (Switzerland)* 13. doi:10.3390/healthcare13202594.
- [6] Barj, S., 2024. Cp-abe-lwe-based smart contract: A novel post-quantum smart contract-based decentralized application (dapp) for e-health records management, in: *Proceedings - 10th International Conference on Ubiquitous Networking, UNet 2024*, IEEE. doi:10.1109/UNet62310.2024.10794736.

- [7] Boneh, D., Boyen, X., 2004. Efficient selective-id secure identity-based encryption without random oracles, in: International conference on the theory and applications of cryptographic techniques, Springer. pp. 223–238.
- [8] Boneh, D., Franklin, M., 2001. Identity-based encryption from the weil pairing, in: Annual international cryptology conference, Springer. pp. 213–229.
- [9] Carmona, M., et al., 2023. On the implementation of a lattice-based revocable hierarchical ibe, in: Proceedings of the International Conference on Security and Cryptography, Science and Technology Publications, Lda. pp. 617–623. doi:10.5220/0012047800003555.
- [10] Chen, P., et al., 2015a. An escrow-free hierarchical identity-based signature model for cloud storage. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 9532, 633–647. doi:10.1007/978-3-319-27161-3_58.
- [11] Chen, P., et al., 2015b. Removing key escrow from the lw-hibe scheme. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 9532, 593–605. doi:10.1007/978-3-319-27161-3_54.
- [12] Chen, P., et al., 2016. T-hibe: A trustworthy hibe scheme for the osn privacy protection, in: Proceedings - 2015 International Symposium on Security and Privacy in Social Networks and Big Data, SocialSec 2015, IEEE. pp. 72–79. doi:10.1109/SocialSec2015.11.
- [13] Chow, S.S.M., et al., 2011. Identity-based online/offline key encapsulation and encryption, in: Proceedings of the 6th International Symposium on Information, Computer and Communications Security, ASIACCS 2011, ACM. pp. 52–60. doi:10.1145/1966913.1966922.
- [14] Daniel, R.M., et al., 2017. Analysis of hierarchical identity based encryption schemes and its applicability to computing environments. Journal of Information Security and Applications 36, 20–31. doi:10.1016/j.jisa.2017.07.005.
- [15] Dilxat, G., 2019. Verifiable outsourced decryption oo-cp-abe access control scheme with hidden policy. Jisuanji Gongcheng/Computer Engineering 45, 166–170. doi:10.19678/j.issn.1000-3428.0052085.
- [16] Gopiseti, S.R., 2022. A new pairing-free certificateless signcryption scheme. Journal of Scientific and Industrial Research 81, 1326–1335. doi:10.56042/jsir.v81i12.69313.
- [17] Guo, H., et al., 2024. Decentralized electronic health records management via redactable blockchain and revocable ipfs, in: Proceedings - 2024 IEEE/ACM Conference on Connected Health: Applications, Systems and Engineering Technologies, CHASE 2024, IEEE. pp. 167–171. doi:10.1109/CHASE60773.2024.00028.
- [18] Horwitz, J., Lynn, B., 2002. Toward hierarchical identity-based encryption, in: International Conference on the Theory and Applications of Cryptographic Techniques, Springer. pp. 466–481.

- [19] Hu, M., et al., 2018. A novel hierarchical identity-based fully homomorphic encryption scheme from lattices. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 11065 LNCS, 423–434. doi:10.1007/978-3-030-00012-7_39.
- [20] Hu, X., 2014. Constant size ciphertext and private key hibe without random oracles. *Journal of Information Science and Engineering* 30, 333–345.
- [21] Huang, H., et al., 2025. An efficient lattice-based integrated revocable identity-based encryption. *Scientific Reports* 15. doi:10.1038/s41598-025-01254-1.
- [22] Huang, K., 2025. Traceable and revocable large universe multi-authority attribute-based access control with resisting key abuse. *Computer Networks* 272. doi:10.1016/j.comnet.2025.111694.
- [23] Hussien, H., et al., 2021. Blockchain-based access control scheme for secure shared personal health records over decentralised storage. *Sensors* 21. doi:10.3390/s21072462.
- [24] Jayabalan, J., et al., 2025. Blockchain and chainlink oracle integration in ehr: Ensuring real-time data integrity and interoperability with ethereum, hyperledger fabric, and ipfs storage. *IEEE Access* 13, 158044–158056. doi:10.1109/ACCESS.2025.3606194.
- [25] Katsumata, S., et al., 2019. Lattice-based revocable (hierarchical) ibe with decryption key exposure resistance. *Lecture Notes in Computer Science* 11443 LNCS, 441–471. doi:10.1007/978-3-030-17259-6_15.
- [26] Katsumata, S., et al., 2020. Lattice-based revocable (hierarchical) ibe with decryption key exposure resistance. *Theoretical Computer Science* 809, 103–136. doi:10.1016/j.tcs.2019.12.003.
- [27] Kaur, J., et al., 2024. Attribute-based access control scheme for secure storage and sharing of ehrrs using blockchain and ipfs. *Cluster Computing* 27, 1047–1061. doi:10.1007/s10586-023-04038-2.
- [28] Konda, B., et al., 2025. Enhancing traceability and security in mhealth systems: A proximal policy optimization-based multi-authority attribute-based encryption approach, in: *2025 29th International Conference on Information Technology, IT 2025, IEEE*. doi:10.1109/IT64745.2025.10930307.
- [29] Lai, J., et al., 2015. Improved identity-based online/offline encryption. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 9144, 160–173. doi:10.1007/978-3-319-19962-7_10.
- [30] Lee, K., et al., 2018. Revocable hierarchical identity-based encryption with shorter private keys and update keys. *Designs, Codes, and Cryptography* 86, 2407–2440. doi:10.1007/s10623-017-0453-2.
- [31] Lee, K., et al., 2022. A generic approach to build revocable hierarchical identity-based encryption. *IEEE Access* 10, 44178–44199. doi:10.1109/ACCESS.2022.3169497.

- [32] Li, J., et al., 2017a. Verifiable outsourced decryption of attribute-based encryption with constant ciphertext length. *Security and Communication Networks* 2017. doi:10.1155/2017/3596205.
- [33] Li, Q., et al., 2017b. Multi-authority attribute-based access control scheme in mhealth cloud with unbounded attribute universe and decryption outsourcing, in: 2017 9th International Conference on Wireless Communications and Signal Processing, WCSP 2017 - Proceedings, IEEE. pp. 1–7. doi:10.1109/WCSP.2017.8171106.
- [34] Li, Q., et al., 2019. Fine-grained access control in mhealth with hidden policy and traceability. *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST 303 LNICST*, 261–274. doi:10.1007/978-3-030-36442-7_17.
- [35] Li, Y., et al., 2017c. An efficient hierarchical identity-based encryption scheme for the key escrow. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 10656 LNCS, 108–120. doi:10.1007/978-3-319-72389-1_10.
- [36] Liu, J.K., et al., 2009. An efficient identity-based online/offline encryption scheme. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 5536 LNCS, 156–167. doi:10.1007/978-3-642-01957-9_10.
- [37] Luo, S., et al., 2011. New fully secure hierarchical identity-based encryption with constant size ciphertexts. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 6672 LNCS, 55–70. doi:10.1007/978-3-642-21031-0_5.
- [38] Miao, Y., et al., 2024. Verifiable outsourced attribute-based encryption scheme for cloud-assisted mobile e-health system. *IEEE Transactions on Dependable and Secure Computing* 21, 1845–1862. doi:10.1109/TDSC.2023.3292129.
- [39] Mishra, A.K., et al., 2024. Smart contract-enabled blockchain framework for electronic medical health records, in: *Proceedings of the 14th International Conference on Cloud Computing, Data Science and Engineering, Confluence 2024*, IEEE. pp. 124–129. doi:10.1109/Confluence60223.2024.10463285.
- [40] Nikose, A., et al., 2025. A review of hierarchical cp-abe: Advances in secure access control, dynamic policy management, and user revocation, in: *International Conference on Emerging Trends in Engineering and Technology, ICETET*, IEEE. doi:10.1109/ICETETSIP64213.2025.11156368.
- [41] Nyaletey, E., et al., 2019. Blockipfs - blockchain-enabled interplanetary file system for forensic and trusted data traceability, in: *Proceedings - 2019 2nd IEEE International Conference on Blockchain, Blockchain 2019*, IEEE. pp. 18–25. doi:10.1109/Blockchain.2019.00012.
- [42] Parliament, E., Council, 2016. Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (general data protection regulation). *Official Journal of the European Union* L 119, 1–88.

- [43] of the Asssistant Secretary for Planning, O., Evaluation, 1996. Health insurance portability and accountability act of 1996. Public law 104, 191.
- [44] Qin, B., et al., 2015. Server-aided revocable identity-based encryption. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 9326, 286–304. doi:10.1007/978-3-319-24174-6_15.
- [45] Razdan, R., et al., 2024. Decentralized credential verification system, in: 2024 IEEE Pune Section International Conference, PuneCon 2024, IEEE. doi:10.1109/PuneCon63413.2024.10895735.
- [46] Seo, J.H., et al., 2016. Revocable hierarchical identity-based encryption via history-free approach. *Theoretical Computer Science* 615, 45–60. doi:10.1016/j.tcs.2015.11.047.
- [47] Shamir, A., 1984. Identity-based cryptosystems and signature schemes, in: *Workshop on the theory and application of cryptographic techniques*, Springer. pp. 47–53.
- [48] Sharmin, S., et al., 2025. A scalable and privacy-preserving hybrid blockchain architecture for secure healthcare data management. *International Journal of Advanced Computer Science and Applications* 16, 988–997. doi:10.14569/IJACSA.2025.0160895.
- [49] Shi, D.Y., 2022. C-hibs: A hierarchical identity-based signature algorithm based on combined keys. *Journal of Cryptologic Research* 9, 982–1001. doi:10.13868/j.cnki.jcr.000562.
- [50] Sivaprakash, P., et al., 2024. Ipfs-based blockchain enabled system for secure data storage and access in healthcare, in: 2nd International Conference on Intelligent Cyber Physical Systems and Internet of Things, ICoICI 2024 - Proceedings, IEEE. pp. 203–208. doi:10.1109/ICoICI62503.2024.10696438.
- [51] Srivastava, S., et al., 2024. Implementation of blockchain and ipfs to safeguard evidentiary data, in: 2024 International Conference on Knowledge Engineering and Communication Systems, ICKECS 2024, IEEE. doi:10.1109/ICKECS61492.2024.10616708.
- [52] Sruthi, M., et al., 2021. Hybrid lightweight signcryption scheme for iot. *Open Computer Science* 11, 391–398. doi:10.1515/comp-2020-0105.
- [53] Thakur, A., et al., 2025. Revocable and privacy-preserving cp-abe scheme for secure mhealth data access in blockchain. *Concurrency and Computation: Practice and Experience* 37. doi:10.1002/cpe.70064.
- [54] Tsai, T.T., et al., 2017. Sibsc: Separable identity-based signcryption for resource-constrained devices. *Informatica (Netherlands)* 28, 193–214. doi:10.15388/Informatica.2017.126.
- [55] Wang, G., et al., 2025. Lightweight auditable multi-keyword attribute-based searchable encryption scheme for secure health data sharing, in: 2025 IEEE/CIC International Conference on Communications in China:Shaping the Future of Integrated Connectivity, ICC3 2025, IEEE. doi:10.1109/ICC365529.2025.11148840.

- [56] Wang, P., et al., 2015. Hierarchical policy delegation in multiple-authority abe. *International Journal of Information and Computer Security* 7, 140–159. doi:10.1504/IJICS.2015.073020.
- [57] Wang, S., et al., 2019. Simplified revocable hierarchical identity-based encryption from lattices. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 11829 LNCS, 99–119. doi:10.1007/978-3-030-31578-8_6.
- [58] Wang, Z.J., 2016. Attribute-based online/offline encryption with outsourcing decryption. *Journal of Information Science and Engineering* 32, 1595–1611.
- [59] World Health Organization, 2007. Everybody’s business: strengthening health systems to improve health outcomes: WHO’s framework for action. World Health Organization, Geneva.
- [60] Xie, Q., et al., 2025. Lightweight and anonymous certificateless signcryption scheme for multi-receiver. *Journal of Systems Architecture* 167. doi:10.1016/j.sysarc.2025.103482.
- [61] Xing, Q., et al., 2017. Unbounded revocable hierarchical identity-based encryption with adaptive-id security, in: *Proceedings - 18th IEEE International Conference on High Performance Computing and Communications, 14th IEEE International Conference on Smart City and 2nd IEEE International Conference on Data Science and Systems, HPCC/SmartCity/DSS 2016*, IEEE. pp. 430–437. doi:10.1109/HPCC-SmartCity-DSS.2016.0068.
- [62] Xu, J., et al., 2018. Efficient identity-based offline/online encryption scheme for lightweight devices, in: *Proceedings - 2018 IEEE 3rd International Conference on Data Science in Cyberspace, DSC 2018*, IEEE. pp. 569–575. doi:10.1109/DSC.2018.00091.
- [63] Ye, Q., 2017. Efficient hierarchical identity-based encryption scheme from learning with errors. *Jisuanji Yanjiu yu Fazhan/Computer Research and Development* 54, 2193–2204. doi:10.7544/issn1000-1239.2017.20170394.
- [64] Ye, Q., et al., 2018. A novel hierarchical identity-based encryption scheme from lattices. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 11065 LNCS, 412–422. doi:10.1007/978-3-030-00012-7_38.
- [65] You, L., et al., 2016. Hierarchical authority key-policy attribute-based encryption, in: *International Conference on Communication Technology Proceedings, ICCT*, IEEE. pp. 868–872. doi:10.1109/ICCT.2015.7399963.
- [66] Zeng, P., et al., 2021. Efficient policy-hiding and large universe attribute-based encryption with public traceability for internet of medical things. *IEEE Internet of Things Journal* 8, 10963–10972. doi:10.1109/JIOT.2021.3051362.
- [67] Zhang, D., et al., 2018. Compact hierarchical ibe from lattices in the standard model. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 10631 LNCS, 210–221. doi:10.1007/978-3-319-89500-0_19.

- [68] Zhang, L., 2013. Direct chosen-ciphertext-attack hierarchical computing technique for identity-based encryption. *ICIC Express Letters* 7, 571–576.
- [69] Zhang, L., et al., 2012. Hierarchical identity-based encryption with constant-size private keys. *ETRI Journal* 34, 142–145. doi:10.4218/etrij.12.0211.0140.
- [70] Zhang, X., et al., 2023a. A traceable and revocable multi-authority attribute-based access control scheme for mineral industry data secure storage in blockchain. *Journal of Supercomputing* 79, 14743–14779. doi:10.1007/s11227-023-05222-2.
- [71] Zhang, Y., et al., 2020. Adaptively secure efficient (h)ibe over ideal lattice with short parameters. *Entropy* 22, 1–19. doi:10.3390/e22111247.
- [72] Zhang, Z., et al., 2023b. A stronger secure ciphertext fingerprint-based commitment scheme for robust verifiable od-cp-abe in imcc. *IEEE Internet of Things Journal* 10, 16531–16547. doi:10.1109/JIOT.2023.3268699.
- [73] Zhang, Z., et al., 2025. Privacy-improving multi-authority ciphertext-policy attribute-based encryption with internal fraud attack resistance based on blockchain. *IEEE Transactions on Network Science and Engineering* doi:10.1109/TNSE.2025.3604232.
- [74] Zheng, J.W., et al., 2019. Identifier discrimination: realizing selective-id hibe with authorized delegation and dedicated encryption privacy. *International Journal of Information Security* 18, 141–162. doi:10.1007/s10207-018-0402-8.