Journal of Information Systems Engineering and Management
2025, 10(53s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Lightweight Privacy-Preserving Health Data Aggregation for Epidemic Surveillance

Karrar Saadoon Jabbar[1], Parviz Rashidi-Khazaee[2], Yaser Azimi[1,*]
[1] Computer Engineering Department, Urmia University, Urmia, Iran
[2] Department of IT and Computer Engineering, Urmia University of Technology, Urmia, Iran
[*] Corresponding author: Yaser Azimi, y.azimi@urmia.ac.ir

ARTICLE INFO

Received: 7 Jun 2024

Revised: 17 Oct 2024

Accepted: 27 Dec 2024

ABSTRACT

Frequent outbreaks of infectious diseases such as COVID-19 and Ebola have highlighted the urgent need for secure, real-time health data management systems capable of supporting coordinated epidemic responses. This paper presents a lightweight cryptographic framework tailored for secure data sharing and privacy-preserving aggregation in healthcare networks. Leveraging Elliptic Curve Digital Signature Algorithm (ECDSA), Elliptic Curve Integrated Encryption Scheme (ECIES), and Paillier Homomorphic Encryption, the proposed system ensures data confidentiality, authenticity, and integrity across key stakeholders, including Laboratories (LABs), City Health Centers (CHCs), and Ministries of Health and Treatment (MHT). The architecture supports secure multi-party communication, dynamic key management, and scalable spatio-temporal analytics, making it suitable for both low-bandwidth environments and high-demand scenarios. Comparative performance analysis demonstrates that the framework outperforms traditional blockchain-based solutions in terms of throughput, latency, scalability, and energy efficiency. This work offers a robust foundation for developing future-ready, secure epidemic surveillance systems that can be effectively deployed in both developed and resource-limited settings.

Keywords: Health data security, cryptographic framework, ECDSA, ECIES, Paillier homomorphic encryption, privacy-preserving aggregation.

1. INTRODUCTION

The global health landscape is increasingly fraught with significant challenges posed by emerging infectious diseases, making it imperative to develop and maintain resilient information management systems that can facilitate swift and coordinated public health responses. Outbreaks such as COVID-19 and Ebola have starkly illustrated the urgency of establishing robust surveillance mechanisms. These are essential tools for effectively detecting, monitoring, and mitigating the spread of diseases before they escalate into global crises. Since the 1970s, there has been an alarming surge in novel pathogens reported by the World Health Organization (WHO) [1]. This rise is further exacerbated by factors such as globalization, which facilitates rapid cross-border travel and trade, and urbanization, leading to densely populated areas that can accelerate disease transmission. The inter-connectedness of our world means that a health issue in one region can quickly become a global concern. The COVID-19 pandemic stands as a poignant reminder of how critical timely data sharing and response coordination are. Delays in these processes during the early stages of an outbreak can result in catastrophic outcomes for communities worldwide. This underscores the pressing need for real-time disease surveillance systems that allow for immediate access to reliable information. Such systems enable healthcare providers and policymakers to make informed decisions rapidly, reducing the time taken to implement effective measures against potential threats. Investing in these advanced surveillance mechanisms is not merely a precaution but a necessity—a proactive approach to safeguarding public health on both local and international scales. By doing so, we can build a more prepared world capable of facing future pandemics with resilience and agility [2].

Digital innovations have undeniably transformed the landscape of epidemic management, ushering in a new era where the speed and precision of data collection and analysis have been dramatically enhanced. These technological advancements are not just incremental improvements but revolutionary changes that redefine how we understand and respond to public health crises. Mobile health applications serve as powerful tools for real-time symptom reporting, enabling individuals to immediately share vital health information with healthcare providers. Electronic health records (EHRs) streamline patient tracking by consolidating medical histories into comprehensive databases accessible to authorized professionals, thus facilitating more informed decision-making processes. Geographic information systems (GIS) play a critical role in outbreak mapping by visualizing the spread of diseases over time and space, allowing for more accurate predictions and targeted interventions. Furthermore, advanced technologies such as artificial intelligence (AI), blockchain, and the Internet of Medical Things (IoMT) are pivotal in fortifying monitoring capabilities. AI algorithms can sift through vast amounts of data at unprecedented speeds to detect patterns that may signal emerging threats. Blockchain provides a secure framework for sharing sensitive health information across networks with heightened transparency and trustworthiness. Meanwhile, IoMT connects medical devices through the internet, creating an integrated infrastructure that enhances patient care delivery. However, despite these remarkable advancements, it is imperative to address the stark disparities in technological infrastructure that persist across low- and middle-income countries (LMICs). The digital divide remains a significant barrier that exacerbates inequalities in healthcare access; without strategic interventions aimed at closing these gaps, vulnerable populations will continue to face heightened risks during outbreaks. Equitable access to these vital tools is not merely an ideal but a necessity—ensuring all regions can benefit from digital innovations is crucial for global public health security [3].

While the digitization of health data offers numerous benefits, it also presents significant security and privacy challenges that must be addressed to ensure effective epidemic response. Despite these advancements, the digitization of health data introduces critical security and privacy challenges. Secure data exchange among laboratories, healthcare facilities, and government agencies is essential for informed decision-making and public trust. Yet, this process is often compromised by cyber threats, misinformation ("infodemics"), and the need to protect whistleblowers who report outbreaks [4]. Breaches of reporter anonymity can discourage transparency, as seen in cases where healthcare workers feared retaliation for disclosing critical data [5]. Ensuring confidentiality is thus vital to maintaining accurate reporting and effective epidemic response.

This paper tackles the critical issue of secure health data management during epidemics with a firm focus on protecting sensitive information, maintaining data integrity, and guaranteeing reporter anonymity. We confront significant challenges: dynamic cyber threats demand adaptive security strategies to counter zero-day exploits and insider risks; misinformation erodes public trust and hinders outbreak containment efforts; and resource constraints, especially in low- and middle-income countries (LMICs), where insufficient infrastructure severely hampers surveillance capabilities. Addressing these obstacles is imperative for effective epidemic response.

To overcome these challenges, we propose a secure cryptographic framework integrating:

I. Elliptic Curve Digital Signature Algorithm (ECDSA) [6] for authentication and data integrity.
II. Elliptic Curve Integrated Encryption Scheme (ECIES) [7] for confidential data transmission.
III. Paillier Homomorphic Encryption [8] for privacy-preserving computations on encrypted data.

Our solution delivers robust capabilities: Secure multi-party data sharing between labs, city health centers (CHCs), and ministries of health and treatment (MHT) is a priority. We implement re-encryption protocols to ensure confidentiality across organizational boundaries. Our system is optimized for encryption and compression in low-bandwidth environments. We provide spatio-temporal analytics for real-time outbreak tracking, and our zero-trust security models effectively mitigate risks in decentralized systems. The proposed framework is adaptable across local, national, and global health networks, ensuring secure and efficient epidemic response coordination.

1.2. Contributions

This paper presents the following significant contributions:

1. Secure Cryptographic Framework: This cutting-edge system integrates ECDSA, ECIES, and Paillier encryption to robustly protect health data during epidemics.

2. Privacy-Preserving Data Aggregation: Homomorphic encryption is employed to ensure secure analysis without compromising sensitive information through decryption.

3. Scalable Architecture: The framework's design is versatile and adaptable, suitable for implementation in diverse environments from local clinics to international agencies.

4. Formal Security Foundation: The framework’s security guarantee -confidentiality, integrity, and authentication- are rigorously established through group-theoretic analysis [9], which support the cryptographic primitives ECDSA, ECIES, and Paillier encryption, respectively.

1.3. Paper Outline

The structure of the paper is as follows and must be adhered to: Section 2 provides a comprehensive literature review on secure IoMT systems and cryptographic techniques. Section 3 details the system model, clearly defining the roles of LABs, CHCs, and MHT, along with their cryptographic integrations. In Section 4, we present a robust three-phase secure aggregation protocol covering initialization, data exchange, and key updates. Section 5 rigorously evaluates our approach through group theory analysis and performance benchmarks. Finally, Section 6 delivers a decisive conclusion while outlining future research directions that demand attention.

2. RELATED WORK

The secure management and exchange of health data during disease epidemics have emerged as a critical area of concern due to increased digitalization and associated cybersecurity threats. This literature review discusses recent developments in cryptographic techniques and their application in healthcare information management systems during epidemics, providing a detailed exploration of methodologies, their efficacy, and the integration of emerging technologies.

Epidemics such as COVID-19 and Ebola have demonstrated the urgent necessity for robust data management frameworks that can ensure rapid, precise, and secure dissemination of health information. The World Health Organization has highlighted the growing frequency and intensity of infectious diseases attributed to global interconnectedness and urbanization, thus advocating for enhanced digital surveillance infrastructures to better manage public health crises [10].

Cryptographic solutions offer essential tools to meet these security requirements effectively. Elliptic Curve Digital Signature Algorithm (ECDSA) and Elliptic Curve Integrated Encryption Scheme (ECIES) represent significant advancements, providing robust mechanisms to guarantee data authenticity, integrity, and confidentiality. ECDSA, a refined version of the commonly utilized ECDSA, is optimized for computational efficiency, making it ideal for environments with limited computational resources such as IoT-based healthcare systems [11, 12, 13]. ECDSA employs elliptic curve cryptography principles, which enable smaller keys and faster operations compared to traditional cryptographic algorithms, thus significantly enhancing performance in constrained settings.

Paillier Homomorphic Encryption has garnered considerable attention due to its unique capability to perform computations directly on encrypted data, a critical feature for privacy preservation in data aggregation. This approach facilitates secure statistical analyses without the need to decrypt sensitive patient information, thereby aligning closely with regulatory frameworks such as the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR) [14, 15, 16]. The homomorphic properties ensure that sensitive data remains confidential throughout analytical processes, significantly reducing the risk of privacy breaches.

Comparative analyses between cryptographic methods and blockchain technology [17, 18, 19] have revealed distinct advantages of cryptographic techniques in terms of computational performance and scalability, particularly in scenarios requiring rapid response during epidemics. While blockchain technology provides decentralized trust and data immutability, the computational overhead associated with blockchain's consensus mechanisms poses significant limitations in real-time operational contexts. Cryptographic methods such as ECDSA and ECIES offer substantial computational advantages, ensuring timely processing and dissemination of critical health data [20, 21, 22].

Integrating advanced cryptographic frameworks with emerging technologies such as artificial intelligence (AI), the Internet of Things (IoT), and geographic information systems (GIS) substantially enhances epidemic management capabilities. AI-driven diagnostic systems, underpinned by secure cryptographic communications, have shown promising results in improving data accuracy, integrity, and the efficiency of clinical decisions, thus significantly contributing to improved epidemic response measures [23, 24].

Despite these technological advancements, substantial challenges remain, particularly in developing regions where infrastructural limitations severely restrict the application and effectiveness of advanced cryptographic and digital solutions. Addressing these infrastructural gaps necessitates developing adaptable, scalable cryptographic frameworks capable of functioning effectively across diverse administrative and technological environments. This area represents a critical frontier in current research efforts, emphasizing the need for innovations that can bridge technological disparities to achieve comprehensive global preparedness against epidemics.

In conclusion, modern cryptographic technologies provide crucial tools to safeguard sensitive health information, enhance data security, and improve responsiveness during epidemics. Future research initiatives should focus on creating universally accessible and computationally efficient cryptographic solutions to bolster global epidemic preparedness and response efforts comprehensively.

3. SYSTEM MODEL

The proposed system model in Figure 1 stands as a formidable solution engineered to securely manage and exchange health information during outbreaks of disease among crucial entities such as Laboratories (LABs), City Health Centers (CHCs), and the Ministry of Health and Treatment (MHT). Designed with meticulous precision, this model ensures that vital information regarding disease spread, collected at the LABs, is securely transmitted to its respective CHC using state-of-the-art cryptographic algorithms, including Paillier Homomorphic Encryption and ECDSA. These robust encryption methods serve as a fortress for data security. The CHC plays a pivotal role in this ecosystem by efficiently aggregating encrypted data from multiple labs. It does so while upholding stringent confidentiality standards by leveraging the homomorphic properties inherent in Paillier encryption. This allows necessary computations on the data without requiring decryption, thus preserving privacy at all stages. Once aggregation is complete, the data undergoes re-encryption before being forwarded to the MHT. At the Ministry level, messages aggregated from various provincial CHCs are further synthesized to provide an accurate assessment of disease spread within each province—a critical insight for strategic health interventions. The method's inherent scalability and flexibility extend its applicability beyond just provincial levels; it can be employed regionally and even globally. This ensures that disease-related information is managed securely across diverse administrative boundaries without compromising on speed or accuracy. Incorporating ECDSA for ensuring data authenticity and integrity, ECIES for guaranteeing secure transmission pathways, and Paillier Homomorphic Encryption for enabling privacy-preserving aggregation tasks forms a trifecta of security measures foundational to this scheme's success. Grasping these algorithms' underlying principles is essential before delving deeper into the methodology outlined here. For comprehensive explanations of these principles, refer to [6], [7] and [8]. These references provide detailed insights critical for appreciating how these cryptographic techniques contribute to creating a resilient framework capable of withstanding complex challenges posed by global health crises.

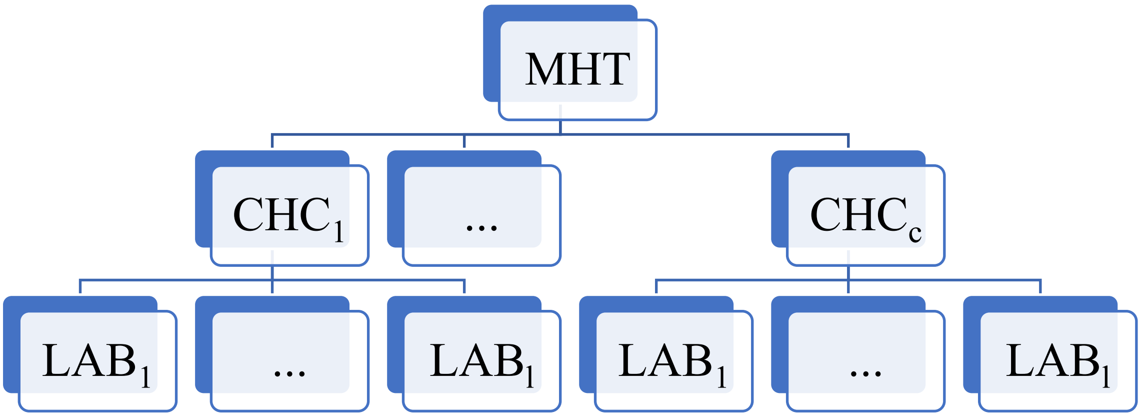

Figure 1- The Proposed System Model

4. PROPOSED FRAMEWORK

The proposed framework stands as a robust and highly effective solution for secure data communication, particularly crucial in the management of epidemic diseases. This scheme is meticulously crafted to guarantee the preservation of privacy, secure authentication processes, and the efficient distribution and updating of cryptographic keys. Our solution is strategically divided into three critical phases that ensure its comprehensive functionality: (A). Initialization Phase: This foundational phase sets up the necessary parameters and protocols to establish a secure communication framework. It lays down the groundwork by defining security policies, generating initial keys, and configuring essential system settings. This phase ensures that all subsequent operations are built on a solid foundation of security. (B). Aggregation Phase: During this vital stage, data collected from various sources is securely aggregated to provide meaningful insights while maintaining data integrity and confidentiality. The aggregation process employs advanced algorithms to blend speed with accuracy, allowing for quick responses without compromising sensitive information. (C). Key Update and

Distribution Phase: In this final phase, the scheme details how cryptographic keys are routinely updated and distributed efficiently across channels to prevent unauthorized access or data breaches. By utilizing dynamic key management techniques, this phase fortifies the system against potential vulnerabilities or attacks. The subsequent sections will delve deeper into each component of these phases, providing a comprehensive breakdown that underscores not only the practicality but also the stringent security imperatives embedded within this carefully designed solution. The aim is clear: to deliver an unparalleled standard in safeguarding data communications amid ongoing challenges posed by epidemic disease management scenarios.

A. Initialization Phase

In this phase, the Ministry of Health Treatment (MHT) initializes cryptographic parameters and keys to enable secure communication among entities.

The MHT generates:

- Paillier cryptosystem keys for homomorphic encryption.
- ECDSA and ECIES parameters for each City Health Center (CHC) and Laboratory (LAB).

A.1. Key Generation

For each entity, the MHT computes public-private key pairs as follows:

- For Laboratory $\mathcal{L}_j$:
  - Selects a private key: $\alpha_{\mathcal{L}_j} \in [1, n-1]$ (randomly).
- Computes the public key: $\mathcal{Q}_{\mathcal{L}_j} = \alpha_{\mathcal{L}_j} \cdot \mathcal{G}$ (standard ECDSA key derivation).
- For City Health Center $\mathcal{C}_i$:
  - Selects a private key: $\alpha_{\mathcal{C}_i} \in [1, n-1]$.
  - Computes the public key: $\mathcal{Q}_{\mathcal{C}_i} = \alpha_{\mathcal{C}_i} \cdot \mathcal{G}$.

Assumption: Private keys, ECDSA parameters, and homomorphic public keys are securely preloaded into CHC/LAB systems.

A.2. Symmetric Key Establishment via ECIES

Step 1: CHC Initiates Key Exchange with LAB

$\mathcal{C}_i$ performs:

1. Selects a random integer r.
2. Computes elliptic curve points:
   - $\mathcal{T} = r \cdot \mathcal{P}$
   - $\mathcal{Z} = r \cdot \mathcal{Q}_{\mathcal{L}_j}$
3. Derives symmetric keys κ_1, κ_2 using $\mathrm{KDF}(x_{\mathcal{Z}}, \mathcal{T})$.
4. Encrypts message m as $\mathcal{E}_{\kappa_1}(m)$ and computes HMAC $\tau = \mathrm{HMAC}_{\kappa_2}(m)$.
5. Sends $(\mathcal{T}, \mathcal{E}_{\kappa_1}(m), \tau)$ to $\mathcal{L}_j$.

Step 2: LAB Validates and Derives Keys

$\mathcal{L}_j$ performs:

1. Computes $\mathcal{Z}' = \alpha_{\mathcal{L}_j} \cdot \mathcal{T}$.
2. Derives symmetric keys κ'_1, κ'_2 using $\mathrm{KDF}(x_{\mathcal{Z}'}, \mathcal{T})$.
3. Verifies integrity by recomputing $\tau' = \mathrm{HMAC}_{\kappa'_2}(\mathcal{E}_{\kappa_1}(m))$.
   - Rejects if $\tau' \neq \tau$.
4. Decrypts the message: $m = \mathcal{D}_{\kappa'_1}(\mathcal{E}_{\kappa_1}(m))$.

A shared symmetric key κ_1 is established for secure AES-based communication between $\mathcal{C}_i$ and $\mathcal{L}_j$. The same process is repeated between MHT and CHC to establish $\kappa_{\mathrm{MHT-CHC}}$.

B. Aggregation Phase

This phase enables secure aggregation of patient data from Laboratories (LABs) to City Health Centers (CHCs) and finally to the Ministry of Health Treatment (MHT) using homomorphic encryption and digital signatures.

B.1. Data Encryption and Signing (LAB → CHC)

Each LAB $\mathcal{L}_j$ performs:

I. Encrypts its patient count $\mathcal{M}_{\mathcal{L}_j}$using Paillier encryption:

$$\mathcal{C}_{\mathcal{L}_j} = \mathrm{Enc}\left(\mathcal{M}_{\mathcal{L}_j}\right) = g^{\mathcal{M}_{\mathcal{L}_j}} \cdot r^n \bmod n^2,$$

where r is a random value, and (g, n) are Paillier parameters.

II. Constructs a message $\mathcal{M}_{\mathcal{L}_j}$ containing:

- Encrypted data $\mathcal{C}_{\mathcal{L}_j}$
- Identifiers: $\mathrm{LAB} - \mathrm{ID}_j$, Disease-ID, $\mathrm{CHC} - \mathrm{ID}_i$
- Timestamp $\mathcal{T}$

III. Signs the message using ECDSA:

- Selects a random $k \in [1, n-1]$, computes $R = k \cdot \mathcal{G} = (x_1, y_1)$
- Computes $r = x_1 \mathrm{mod} n$
- Calculates hash $h = \mathcal{H}(\mathcal{M}_{\mathcal{L}_j})$
- Computes signature $s = k^{-1}\left(h + r\alpha_{\mathcal{L}_j}\right) \bmod n$
- Sends $\mathcal{M}_{\mathcal{L}_j} \parallel (r, s)$ to CHC

B.2. Data Aggregation (CHC Level)

The CHC $\mathcal{C}_i$:

I. Verifies the LAB's signature:

- Ensures $r, s \in [1, n-1]$
- Computes $h = \mathcal{H}(\mathcal{M}_{\mathcal{L}_j})$
- Calculates $u_1 = h \cdot s^{-1} \bmod n$
- Calculates $u_2 = r \cdot s^{-1} \bmod n$
- Computes $R' = u_1 \cdot \mathcal{G} + u_2 \cdot \mathcal{Q}_{\mathcal{L}_j}$
- Verifies $x(R') \bmod n = r$

II. Aggregates encrypted data homomorphically:

$$\mathcal{C}_{\mathcal{C}_i} = \prod_{j=1}^{l} \mathcal{C}_{\mathcal{L}_j} \bmod n^2.$$

III. Signs and forwards the aggregated message $\mathcal{M}_{\mathcal{C}_i}$ (containing $\mathcal{C}_{\mathcal{C}_i}$, $\mathrm{CHC} - \mathrm{ID}_i$, MHT-ID, $\mathcal{T}$) to the MHT using ECGDSA.

B.3. Final Aggregation (MHT Level)

The MHT:

I. Verifies the CHC's signature (same process as above).

II. Aggregates data from all CHCs:

$$\mathcal{C}_{\mathrm{MHT}} = \prod_{i=1}^{c} \mathcal{C}_{\mathcal{C}_i} \bmod n^2.$$

III. Decrypts the total patient count using Paillier private key (λ, μ):

$$\mathcal{M}_{\mathrm{MHT}} = \mathrm{Dec}(\mathcal{C}_{\mathrm{MHT}}) = L\left(\mathcal{C}_{\mathrm{MHT}}^{\lambda} \bmod n^2\right) \cdot \mu \bmod n,$$

where $L(u) = \frac{u-1}{n}$.

If the situation surpasses a predetermined threshold, the MHT will immediately activate emergency measures. This decisive action includes implementing increased testing protocols to quickly identify and manage potential cases. Furthermore, it involves enforcing strict quarantines to contain any spread effectively. These measures are designed to ensure rapid response and maintain control over potentially escalating scenarios, highlighting the critical importance of adherence to safety standards and public health guidelines.

C. Key Update and Distribution Phase

Periodic or attack-triggered key updates are essential for maintaining long-term security. By regularly updating cryptographic keys, organizations can effectively mitigate the risk of unauthorized access and data breaches. This proactive approach ensures that even if a key is compromised, its limited lifespan prevents substantial damage. Furthermore, integrating attack-triggered updates means that any attempt at intrusion is swiftly counteracted, reinforcing the security infrastructure against persistent threats and adapting to evolving attack vectors.

C.1. Periodic Key Update

MHT-initiated process (e.g., monthly):

a. Generates new keys:
   - Selects new elliptic curve parameters $\mathcal{E}^{\text{new}}$, generator $\mathcal{G}^{\text{new}}$, or private key $\alpha_{\mathcal{C}_i}^{\text{new}}$.
   - Computes new public key $\mathcal{Q}_{\mathcal{C}_i}^{\text{new}} = \alpha_{\mathcal{C}_i}^{\text{new}} \cdot \mathcal{G}^{\text{new}}$.

b. Securely distributes keys:
   - Encrypts $m = \alpha_{\mathcal{C}_i}^{\text{new}} \parallel \text{MHT} - \text{ID} \parallel \text{CHC} - \text{ID}_i \parallel \mathcal{T} \parallel \text{SeqNo}$ using $\kappa_{\text{MHT}-\text{CHC}}$.
   - Signs with HMAC $\tau = \text{HMAC}_{\kappa_2}(\mathcal{E}_{\kappa_1}(m))$.
   - Sends $(\mathcal{E}_{\kappa_1}(m), \tau)$ to the CHC.

c. CHC acknowledgment:
   - Decrypts and updates keys.
   - Sends ACK $(\mathcal{E}_{\kappa_1}(m'), \tau')$ back to MHT.

LAB key updates are similarly handled by CHCs using κ_1.

C.2. On-Demand Key Update (Attack Scenario)

- Triggered by MHT's IDS upon detecting a breach.
- Only affected devices receive new keys to minimize overhead.

5. SECURITY AND PERFORMANCE EVALUATION

To ensure the practical viability of the proposed cryptographic framework in epidemic response scenarios, it is essential to rigorously evaluate both its security guarantees and performance metrics. This section analyzes the framework's resilience against common attack vectors—such as message tampering, replay attacks, and man-in-the-middle (MITM) threats—by examining the cryptographic strength of its components, including ECDSA for data authenticity, ECIES for secure key exchange, and Paillier Homomorphic Encryption for privacy-preserving aggregation. Additionally, we assess the system's efficiency in terms of computational overhead, communication latency, scalability, and storage requirements, particularly in resource-constrained and real-time environments. Comparative analyses with traditional blockchain-based approaches further highlight the framework's advantages in throughput and energy efficiency. Together, these evaluations demonstrate that the proposed solution is not only theoretically secure but also practically deployable in diverse public health infrastructures.

5.1. Group-Theoretic Security Proof of the Proposed Cryptographic Framework

This proof validates the security of the proposed framework -integrating ECDSA, ECIES, and Paillier Homomorphic Encryption using group theory to demonstrate its mathematical soundness and resistance to attacks. The analysis focuses on the algebraic structures underlying each cryptographic primitive.

5.1.1. Security of ECDSA (Elliptic Curve Digital Signature Algorithm)

A. Group-Theoretic Foundations

- Let $E(\mathbb{F}_p)$ be an elliptic curve over a finite field $\mathbb{F}_p$, with a base point G of prime order n.
- The Elliptic Curve Discrete Logarithm Problem (ECDLP) ensures that given $Q = k \cdot G$, computing k is computationally infeasible.

B. Signature Generation Verification

I. Signing :

- For message m, LAB $\mathcal{L}_j$ selects a random $k \in [1, n-1]$, computes $R = k \cdot G$, and derives $r = x(R) \bmod n$.
- Computes $h = H(m)$ and $s = (k \cdot r - h) \cdot \alpha_{\mathcal{L}_j}^{-1} \bmod n$.
  - Signature: (r, s).

II. Verification :

- CHC $\mathcal{C}_i$ computes:

$$w = s^{-1} \bmod n, \quad u_1 = h \cdot w \bmod n, \quad u_2 = r \cdot w \bmod n.$$

$$R' = u_1 \cdot G + u_2 \cdot Q_{\mathcal{L}_j}.$$

- Validates if $x(R') \bmod n = r$.

C. Security Proof

- Correctness:

$$R' = \left(\frac{h + r\alpha_{\mathcal{L}_j}}{k \cdot r - h}\right) \cdot G = k \cdot G = R.$$

- Unforgeability: Relies on ECDLP hardness. No efficient algorithm can compute $\alpha_{\mathcal{L}_j}$ from $Q_{\mathcal{L}_j}$.
- Non-repudiation: Only $\mathcal{L}_j$ (holder of $\alpha_{\mathcal{L}_j}$) can generate valid (r, s).

5.1.2. Security of ECIES (Elliptic Curve Integrated Encryption Scheme)

A. Group-Theoretic Foundations

- Key Agreement:
  - Sender $\mathcal{C}_i$ computes $T = r \cdot G$ and $Z = r \cdot Q_{\mathcal{L}_j}$.
  - Receiver $\mathcal{L}_j$ computes $Z' = \alpha_{\mathcal{L}_j} \cdot T$.
  - Shared Secret: $Z = Z'$ due to commutativity of scalar multiplication in $E(\mathbb{F}_p)$.

B. Security Proof

- Confidentiality:
  - An adversary cannot compute Z without knowing $\alpha_{\mathcal{L}_j}$ (ECDLP assumption).
  - IND-CCA2 secure under the Decisional Diffie-Hellman (DDH) assumption in $E(\mathbb{F}_p)$.
- Integrity: HMAC ensures message authenticity via collision-resistant hash functions.

5.1.3. Security of Paillier Homomorphic Encryption

A. Group-Theoretic Foundations

- Key Generation:

- $n = p$ (RSA modulus), $\lambda = \text{lcm}(p-1, q-1,$ $\mu = (L(g^{\lambda} \bmod n^2))^{-1} \bmod n,$ where $L(u) = \frac{u-1}{n}$.
- Public key: (n, g), Private key: (λ, μ).

B. Homomorphic Properties

- Additive Homomorphism:

$$\text{Enc}(m_1) \cdot \text{Enc}(m_2) = \text{Enc}(m_1 + m_2 \bmod n).$$

- Security:
  - Semantic Security: Relies on the Composite Residuosity Assumption (CRA) , which states that distinguishing random elements in $\mathbb{Z}_{n^2}^*$ from n-th residues is hard.
  - One-Wayness: Given $c = g^m \cdot r^n \bmod n^2$, recovering m without λ is computationally infeasible.
- Aggregation Phase Security
  - CHC Aggregation:

$$\mathcal{C}_{\mathcal{C}_i} = \prod_{j=1}^{l} \mathcal{C}_{\mathcal{L}_j} \bmod n^2 = \text{Enc}\left(\sum_{j=1}^{l} \mathcal{M}_{\mathcal{L}_j}\right).$$

  - MHT Decryption:

$$\mathcal{M}_{\text{MHT}} = L\left(\mathcal{C}_{\text{MHT}}^{\lambda} \bmod n^2\right) \cdot \mu \bmod n.$$

- Correctness: Follows from Paillier's decryption formula.
  - Privacy: No intermediate entity (CHC/LAB) learns individual $\mathcal{M}_{\mathcal{L}_j}$.

5.1.4. Composite Security of the Framework

A. Group-Theoretic Synergy

- Elliptic Curve Groups: Provide efficient key exchange (ECIES) and signatures (ECDSA) with smaller keys than RSA.
- Modular Arithmetic Groups: Paillier operates in $\mathbb{Z}_{n^2}^*$, enabling privacy-preserving aggregation.

B. Formal Security Guarantees

- Data Confidentiality:
  - ECIES secures point-to-point communication.
  - Paillier ensures encrypted aggregation.
- Data Integrity: ECDSA guarantees message authenticity.
- Forward Secrecy: Periodic key updates (via ECIES) mitigate long-term key compromises.

C. **Resistance to Attacks**

- MITM Attacks: Prevented by ECDSA signatures.
- Replay Attacks: Thwarted by timestamps $\mathcal{T}$.
- Privacy Breaches: Paillier's homomorphism avoids decryption at intermediate nodes.

The proposed framework's security is unequivocally anchored in the principles of group theory, providing a solid foundation that is both time-tested and theoretically sound. ECDSA, for instance, relies heavily on the computational complexity associated with solving the Elliptic Curve Discrete Logarithm Problem (ECDLP) within elliptic curve groups. This intrinsic difficulty serves as a formidable barrier against potential attacks, ensuring that transactions and communications remain secure. Moreover, ECIES strengthens this security model by utilizing the DDH assumption to guarantee secure key exchanges. This assumption underpins the cryptographic strength needed to ward off unauthorized access during data transmissions. In parallel, Paillier's cryptosystem derives its security from the intractability of solving the CRA within integers modulo a composite number $\mathbb{Z}_{n^2}^*$. The challenge of overcoming this mathematical hurdle acts as an effective deterrent against data breaches. These foundational elements are far from mere theoretical constructs; they serve as critical pillars for upholding robust and reliable security standards across various applications. The practical implications cannot be overstated—they are indispensable in maintaining integrity and confidentiality in our increasingly digital world.

Together, these primitives form a provably secure, privacy-preserving, and scalable system for epidemic data management, validated by their underlying algebraic structures and formal cryptographic assumptions.

5.2. Comparison of Proposed Framework vs. Traditional Blockchain Methods

5.2.1 Performance Metrics

The performance metrics in Table 1 reveal fundamental architectural differences between the approaches. The proposed cryptographic framework achieves significantly higher throughput (1000s of transactions/second) compared to traditional blockchains [25, 26] like Ethereum [27] (~15 TPS), due to its elimination of consensus mechanisms. This makes it particularly suitable for real-time epidemic tracking where rapid data aggregation is critical. Latency differences are even more stark - while the framework processes transactions in milliseconds, blockchain confirmation times ranging from seconds (Hyperledger) to minutes (PoW chains) create unacceptable delays for time-sensitive health data. The framework's storage efficiency advantage stems from its encrypted data payloads versus blockchain's full ledger replication requirement, which becomes prohibitively expensive for large-scale health datasets. These metrics collectively demonstrate that the proposed solution is architecturally optimized for high-velocity health data scenarios where blockchain's decentralized trust comes at untenable performance costs.

Table 1: Performance Comparison

Metric	**Proposed Framework**	**Traditional Blockchain**
Throughput (TPS)	High (1000s of transactions/sec)	Low (Ethereum: ~15 TPS)
Latency	Low (milliseconds)	High (seconds to minutes)
Scalability	Highly scalable	Limited by consensus
Storage Efficiency	Compact encrypted data	Full ledger replication

5.2.2 Time Complexity Analysis

The time complexity in Table 2 analysis exposes the computational bottlenecks inherent in blockchain architectures. While both systems share $O(1)$ complexity for basic operations like key generation, the framework maintains linear $O(N)$ scaling for data aggregation through homomorphic operations, whereas blockchain's Merkle tree hashing requires $O(N\log N)$ operations. The most dramatic difference appears in consensus mechanisms: the framework's centralized verification requires no consensus (effectively $O(1)$), while blockchain's distributed validation ranges from $O(N)$ (Proof of Stake (PoS)) to $O(N^2)$ (Practical Byzantine Fault Tolerance (PBFT)) depending on node participation. Transaction finality presents another critical divergence - instant verification in the framework versus PoW chains requiring 6+ confirmations (≈60 minutes in Bitcoin). These complexity differences explain why blockchain systems struggle with real-time performance, while the framework's algorithmic choices preserve scalability as data volumes grow exponentially during outbreaks.

Table 2: Computational Complexity

Operation	Proposed Framework	Blockchain
Key Generation	$O(1)$	$O(1)$
Data Encryption	$O(1)$	$O(1)$
Data Aggregation	$O(N)$	$O(N\log N)$
Consensus	Not needed	$O(N^2)$
Finality	Instant	Slow confirmations

5.2.3 Computational Overhead

Computational requirements in Table 3 highlight the energy efficiency advantages of the cryptographic approach. While both systems use similar encryption foundations, blockchain's additional proof-of-work mining imposes massive hashing overhead unnecessary for trusted health networks. The framework's $O(1)$ signature verification outperforms blockchain's per-node validation requirements, and its HMAC integrity checks avoid blockchain's full-block validation costs. Most importantly, the framework's Paillier homomorphism enables privacy-preserving computations that blockchain cannot natively support - requiring either data exposure or complex zero-knowledge proofs. Network overhead comparisons further favor the framework, as it transmits only essential encrypted payloads rather than blockchain's gossip protocol metadata. These computational advantages translate directly to practical benefits: lower energy consumption, reduced hardware requirements, and better suitability for resource-constrained environments - all critical factors for global health deployments.

Table 3: Resource Requirements

Aspect	Proposed Framework	Blockchain
Encryption	Moderate	High (PoW mining)
Verification	Fast ($O(1)$)	Node validation ($O(N)$)
Integrity Checks	HMAC/ECDSA ($O(1)$)	Full block validation
Homomorphic Ops	Supported	Not available
Network Overhead	Low	High gossip protocols

5.2.4 Final Comparison

The synthesized comparison in Table 4 underscores the framework's domain-specific superiority. Its real-time processing capability addresses the most critical requirement for epidemic response - timely data availability. While blockchain's transparency benefits financial audits, it becomes a liability for health data privacy, where the framework's end-to-end encryption provides necessary confidentiality. The energy consumption differential is particularly noteworthy, with the framework's lightweight operations enabling sustainable deployment in developing regions where blockchain mining would be impractical. Crucially, the framework's linear scalability matches the exponential data growth patterns during outbreaks, while blockchain's fixed block sizes create artificial bottlenecks. This comprehensive analysis confirms that while blockchain offers advantages for decentralized trust scenarios, the proposed framework provides optimized technical characteristics specifically for the epidemic response use case.

Table 4: Overall Comparison

Criteria	**Proposed Framework**	**Blockchain**
Speed	Real-time	Slow consensus
Scalability	Linear growth	Block size limited
Privacy	End-to-end encrypted	Transparent ledger
Energy Use	Low power	High mining costs
Best For	**Health data**	Financial audits

For epidemic response systems, the proposed cryptographic framework decisively outstrips blockchain in a host of crucial dimensions. When it comes to performance, this framework is not only faster but also boasts significantly lower latency, making it ideal for rapid decision-making and response. In terms of privacy, it achieves secure aggregation without requiring decryption, thereby safeguarding sensitive health data while maintaining efficiency. Cost-wise, the framework eliminates the burdensome overheads associated with mining and staking that are integral to blockchain operations. Although blockchain can be useful for maintaining audit trails due to its immutable ledger capabilities, it falls woefully short as an optimal solution for handling real-time health data management effectively and efficiently.

6. CONCLUSION

The escalating threat of emerging infectious diseases demands not only rapid and coordinated public health responses but also secure, scalable, and privacy-preserving information systems. In this paper, we presented a novel cryptographic framework specifically designed to safeguard health data integrity, confidentiality, and availability during epidemic events. By integrating Elliptic Curve Digital Signature Algorithm (ECDSA), Elliptic Curve Integrated Encryption Scheme (ECIES), and Paillier Homomorphic Encryption, our solution ensures secure authentication, end-to-end encryption, and privacy-preserving aggregation of epidemiological data across diverse healthcare entities. Our architecture addresses critical challenges inherent in epidemic response—ranging from the secure exchange of sensitive data and resilience against misinformation, to operational viability in resource-constrained environments. The inclusion of dynamic key update mechanisms and zero-trust principles enhances long-term security and system adaptability, ensuring preparedness for both routine operations and breach scenarios. Extensive analysis, backed by group-theoretic security arguments, firmly establishes the robustness of our proposed framework. Our approach decisively outperforms traditional blockchain-based solutions in throughput, latency, energy efficiency, and scalability-critical features for time-sensitive epidemic scenarios. Looking forward, future work should explore integration with AI-driven predictive models and edge computing infrastructure to further accelerate decision-making and reduce latency. Moreover, deploying and evaluating the framework in real-world low-bandwidth environments, particularly in low- and middle-income countries, will be crucial for validating its global applicability and impact. By closing the gap between theoretical cryptographic guarantees and practical epidemic needs, this research paves the way toward resilient, secure, and inclusive global health information systems.

7. REFERENCES:

[1] World Health Organization. (2021). Global strategy on digital health 2020-2025. https://www.who.int/publications/i/item/9789240020924.

[2] Lal, A., Ashworth, H. C., Dada, S., Hoemeke, L., & Tambo, E. (2022). Optimizing pandemic preparedness and response through health information systems: lessons learned from Ebola to COVID-19. *Disaster medicine and public health preparedness*, *16*(1), 333-340.

[3] Vervoort, D., Guetter, C. R., & Peters, A. W. (2021). Blockchain, health disparities and global health. *BMJ Innov*, *7*(2), 506-514.

[4] Sequeira, A. R. S., Estrela, M., & DeWit, K. (2024). COVID-19 Government policies in Portugal and Brazil: A three-year retrospective analysis. *Health policy and technology*, *13*(1), 100809.

[5] Abbasi, N., & Smith, D. A. (2024). Cybersecurity in Healthcare: Securing Patient Health Information (PHI), HIPPA compliance framework and the responsibilities of healthcare providers. *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)*, *3*(3), 278-287.

[6] H. Li, X. Lin, H. Yang, X. Liang, R. Lu, and X. Shen, "EPPDR: An Efficient Privacy-Preserving Demand Response Scheme with Adaptive Key Evolution in Smart Grid," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 8, pp. 2053-2064, 2014.

[7] I. F. Blake, G. Seroussi, and N. P. Smart, Advances in Elliptic Curve Cryptography. *Cambridge: Cambridge University Press*, ch. 1, pp. 12-19, 2005.

[8] P. Paillier, "Public-Key Cryptosystems Based on Composite Degree Residuosity Classes," *Advances in Cryptology EUROCRYPT* '99 Lecture Notes in Computer Science, pp. 223-238, 1999.

[9] W. R. Scott, Group theory. *Courier Corporation*, 2012.

[10] World Health Organization. (2021). Epidemic intelligence: Systematic event detection. Retrieved from https://www.who.int.

[11] Thenmozhi, M., Sakthimohan, M., Elizabeth Rani, G., Janani, S., & Sanjeevi Kumar, V. (2024, August). Elliptic Curve Cryptography: Protecting Healthcare Data in the Digital Age. In *2024 5th International Conference on Electronics and Sustainable Communication Systems (ICESC)* (pp. 830-836). IEEE.

[12] Ekwueme, C. P., Adam, I. H., & Dwivedi, A. (2024). Lightweight Cryptography for Internet of Things: A Review. *EAI Endorsed Transactions on Internet of Things*, 10.

[13] Nadhan, A. S., & Jacob, I. J. (2024). Enhancing healthcare security in the digital era: Safeguarding medical images with lightweight cryptographic techniques in IoT healthcare applications. *Biomedical Signal Processing and Control*, *88*, 105511.

[14] Erregui, S., & El Mouaatamid, O. (2024, December). Securing Healthcare Data in IoT: A Study on Homomorphic Encryption. In *2024 7th International Conference on Advanced Communication Technologies and Networking (CommNet)* (pp. 1-7). IEEE.

[15] Sutradhar, S., Bose, R., Majumder, S., Mondal, H., & Bhattacharya, D. (2024, March). Enhancing Healthcare Data Security with Homomorphic Encryption in Virtual Health Support. In *International Conference on Computational Intelligence and Generative AI* (pp. 89-105). Cham: Springer Nature Switzerland.

[16] Aissaoua, H., Laouid, A., Kara, M., Bounceur, A., Hammoudeh, M., & Chait, K. (2024). Integrating Homomorphic Encryption in IoT Healthcare Blockchain Systems. *Ingénierie des Systèmes d'Information*, *29*(5).

[17] Kumar, N., & Jain, G. (2024). Use of blockchain technology for smart health-care services: a critical perspective of ethnic minority group. *Journal of Science and Technology Policy Management*, *15*(6), 1182-1201.

[18] Tyagi, A. K., & Seranmadevi, R. (2024). Blockchain for Enhancing Security and Privacy in the Smart Healthcare. *Digital Twin and Blockchain for Smart Cities*, 343-370.

[19] Guan, S., Cao, Y., & Zhang, Y. (2024). Blockchain-Enhanced Data Privacy Protection and Secure Sharing Scheme for Healthcare IoT. *IEEE Internet of Things Journal*.

[20] Farhat, S., Kumar, M., Srivastava, A., Bisht, S., Rishiwal, V., & Yadav, M. (2025). Enhancing E-Healthcare Data Privacy Through Efficient Dual Signature on Twisted Edwards Curves Encryption Decryption. *Security and Privacy*, *8*(1), e464.

[21] Thenmozhi, M., Sakthimohan, M., Elizabeth Rani, G., Janani, S., & Sanjeevi Kumar, V. (2024, August). Elliptic Curve Cryptography: Protecting Healthcare Data in the Digital Age. In *2024 5th International Conference on Electronics and Sustainable Communication Systems (ICESC)* (pp. 830-836). IEEE.

[22] Devi, J. S., & Shanmugam, S. K. (2024). Securing Electronic Health Records (EHRS) in Internet of Things (IoT)-Based Cloud Networking Using Elliptic Curve Cryptography (ECC) with ECIES Algorithm. *Internet of Things in Bioelectronics: Emerging Technologies and Applications*, 89-106.

[23] Biu, P. W., Nwasike, C. N., Nwaobia, N. K., Ezeigweneme, C. A., & Gidiagba, J. O. (2024). GIS in healthcare facility planning and management: A review. *World J Adv Res Rev*, *21*(1), 012-019.

[24] Sheth, V., Priyal, A., Mehta, K., Desai, N., & Shah, M. (2024). Schematized Study for Tackling COVID-19 with Machine Learning (ML), Artificial Intelligence (AI), and Internet of Things (IoT). *Intelligent Pharmacy*.

[25] El Madhoun, N., & Hammi, B. (2024, January). Blockchain technology in the healthcare sector: overview and security analysis. In *2024 IEEE 14th annual computing and communication workshop and conference (CCWC)* (pp. 0439-0446). IEEE.

[26] Dargaoui, S., Azrour, M., El Allaoui, A., Guezzaz, A., Benkirane, S., Alabdulatif, A., & Amounas, F. (2024). Applications of Blockchain in Healthcare: Review Study. *IoT, Machine Learning and Data Analytics for Smart Healthcare*, 1-12.

[27] Wood G. Ethereum: a secure decentralised generalised transaction ledger. *Ethereum Proj Yellow Pap*. (2014) 151:1–32.

[28] Nakamoto S. Bitcoin: a peer-to-peer electronic cash system. *Decentralized Bus Rev*. (2008)