blockchains

MDPI

Article

Blockchain and InterPlanetary Framework for Decentralized and Secure Electronic Health Record Management

Samia Sayed [1], Muammar Shahrear Famous [1], Rashed Mazumder [1], Risala Tasin Khan [1], M. Shamim Kaiser [1], Mohammad Shahadat Hossain [2], Karl Andersson [3,*] and Rahamatullah Khondoker [4]

[1] Institute of Information Technology, Jahangirnagar University, Dhaka 1342, Bangladesh; samia.stu20173@juniv.edu (S.S.); shahrear.stu2017@juniv.edu (M.S.F.); rmiit@juniv.edu (R.M.); risala@juniv.edu (R.T.K.); mskaiser@juniv.edu (M.S.K.)
[2] Department of Computer Science & Engineering, University of Chittagong, Chattogram 4331, Bangladesh; hossain_ms@cu.ac.bd
[3] Department of Computer Science, Electrical and Space Engineering, Luleå University of Technology, SE-931 87 Skellefteå, Sweden
[4] Department of Business Informatics, THM—University of Applied Sciences, Wilhelm-Leuschner-Str, 13, D-61169 Friedberg, Germany; rahamatullah.khondoker@mnd.thm.de
* Correspondence: karl.andersson@ltu.se; Tel.: +46-708-195484

Abstract

Blockchain is an emerging technology that is being used to create innovative solutions in many areas, including healthcare. Nowadays healthcare systems face challenges, especially with security, trust, and remote data access. As patient records are digitized and medical systems become more interconnected, the risk of sensitive data being exposed to cyber threats has grown. In this evolving time for healthcare, it is important to find a balance between the advantages of new technology and the protection of patient information. The combination of blockchain–InterPlanetary File System technology and conventional electronic health record (EHR) management has the potential to transform the healthcare industry by enhancing data security, interoperability, and transparency. However, a major issue that still exists in traditional healthcare systems is the continuous problem of remote data unavailability. This research examines practical methods for safely accessing patient data from any location at any time, with a special focus on IPFS servers and blockchain technology in addition to group signature encryption. Essential processes like maintaining the confidentiality of medical records and safe data transmission could be made easier by these technologies. Our proposed framework enables secure, remote access to patient data while preserving accessibility, integrity, and confidentiality using Ethereum blockchain, IPFS, and group signature encryption, demonstrating hospital-scale scalability and efficiency. Experiments show predictable throughput reduction with file size (200 → 90 tps), controlled latency growth (90 → 200 ms), and moderate gas increase (85k → 98k), confirming scalability and efficiency under varying healthcare workloads. Unlike prior blockchain–IPFS–encryption frameworks, our system demonstrates hospital-scale feasibility through the practical integration of group signatures, hierarchical key management, and off-chain erasure compliance. This design enables scalable anonymous authentication, immediate blocking of compromised credentials, and efficient key rotation without costly re-encryption.

Keywords: blockchain; group signature; IPFS; DApp; EHR; GDPR; PHI; HIPAA

Academic Editor: Keke Gai

Received: 31 July 2025
Revised: 11 September 2025
Accepted: 23 September 2025
Published: 28 September 2025

Citation: Sayed, S.; Famous, M.S.; Mazumder, R.; Khan, R.T.; Kaiser, M.S.; Hossain, M.S.; Andersson, K.; Khondoker, R. Blockchain and InterPlanetary Framework for Decentralized and Secure Electronic Health Record Management. *Blockchains* **2025**, *3*, 12. https://doi.org/10.3390/blockchains3040012

1. Introduction

In today's healthcare environment, securely managing and sharing patient data is critical for effective and personalized care. Patient records and diagnostic histories must be readily accessible to providers, but centralized systems often face inefficiencies, duplication, and security risks [1]. With increasing digitization, more sensitive data is exchanged across networks, raising concerns about privacy and cyberattacks [2]. New approaches are needed to ensure availability, integrity, and compliance while safeguarding patient trust [3]. Blockchain has emerged as a promising solution, offering decentralization, immutability, and transparency [4], reducing reliance on vulnerable centralized servers [5].

While blockchain ensures security, it cannot handle massive medical files directly. The InterPlanetary File System (IPFS) addresses this limitation by enabling distributed and tamper-resistant storage [6], with cryptographic hashes stored on the blockchain for verification [7]. Group signatures further enhance privacy by allowing anonymous data usage while maintaining accountability [8]. Together, blockchain and IPFS provide healthcare organizations with integrity, security, and efficient data sharing. Figure 1 highlights blockchain's applications in areas such as electronic health records (EHRs), supply chain management, and patient data security.

Figure 1. Key areas where blockchain enhances healthcare systems, such as drug safety, secure access to sensitive data, verification of medical staff credentials, protection of remote IoT-based monitoring, and improved transparency and coordination in supply chain operations.

This paper introduces a framework integrating IPFS, lightweight blockchain, traditional EHR systems, Proof of Stake consensus, and group signature encryption. The proposed model focuses on the following:

- A blockchain-based framework for secure EHR management, emphasizing remote accessibility and privacy.
- Solutions enabling patients to access records securely anytime, in compliance with privacy regulations.
- Advanced validation to ensure confidentiality, integrity, and protection against unauthorized access.

The paper is structured as follows: Section 2 reviews related works, Section 3 presents the proposed framework, Section 4 analyzes results, and Section 5 concludes.

2. Related Work

The healthcare industry faces unforeseen challenges in managing, securing, and sharing sensitive patient data in an increasingly digital and interconnected world. Due to the regular centralized system, traditional healthcare systems are susceptible to interoperability problems, inefficiencies, and data breaches. Concerns over data confidentiality, integrity, and availability have grown as a result of increasing data quantities and reliance on electronic health records (EHRs) [9–11]. Healthcare providers need to handle the challenges of

integrating new technology into current medical workflows while maintaining secure access to patient data in addition to privacy requirements [12,13]. In spite of these challenges, the healthcare industry is calling for more interoperable, scalable, and secure solutions to facilitate effective, patient-centered treatment [14].

Blockchain technology, which provides decentralized, tamper-resistant data management, has become a revolutionary technology to address these issues. The decentralized architecture and immutability of blockchain technology have the potential to improve traceability, transparency, and trust in the sharing of medical data. The blockchain is made up of numerous pieces that are chronologically connected. Figure 2 shows a block that is made up of four parts: data, the hash of the current block, and the hash of the block before it, nonce and timestamp. The genesis block will be the first block made, and every subsequent block will include its own contents and hash while keeping the hash of the previous block. The role of blockchain in protecting healthcare data has been investigated by researchers; however, there are significant obstacles to its implementation, such as scalability bottlenecks [15], integration issues with real-time medical devices [16], and worries about centralized control [17,18]. Data integrity may be compromised by security flaws in blockchain systems [19], and adhering to privacy regulations in the healthcare industry makes adoption of blockchain much more difficult [20,21]. However, blockchain is still a key technology for creating distributed, safe healthcare systems, particularly when combined with other complementing technologies.

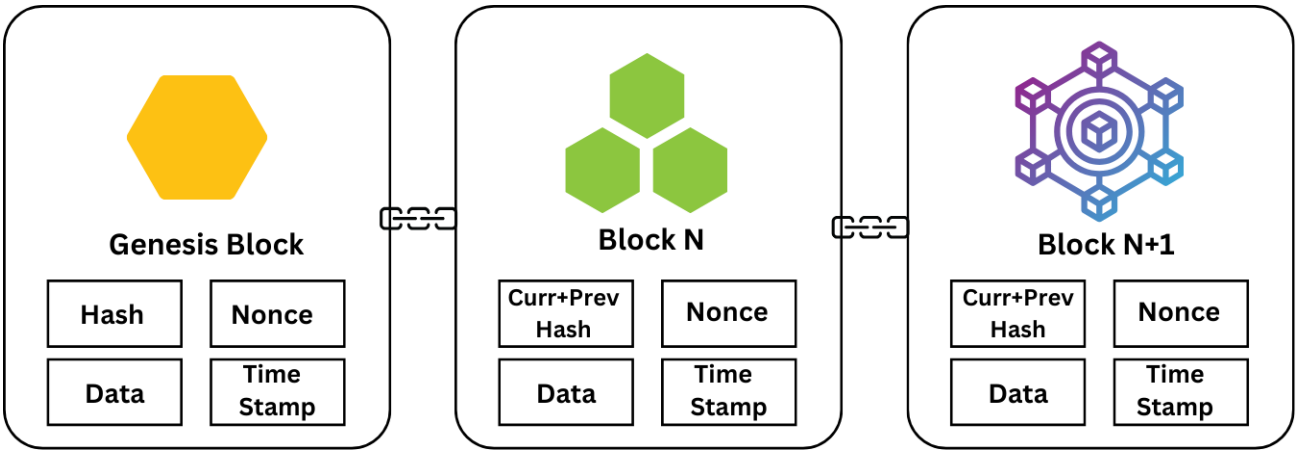

Figure 2. Structure of a blockchain, in which the Genesis Block and all subsequent blocks are linked sequentially, each containing data, timestamps, and cryptographic hashes. This ensures that records are secure, tamper-resistant, and maintained in a fully decentralized system, enabling transparency and trust without a central authority.

Although blockchain offers transparency and data integrity, researchers are exploring the InterPlanetary File System (IPFS) as a potential option because of the demand for scalable, decentralized storage [22]. By sharing data among nodes, IPFS makes decentralized file storage possible, decreasing the need for centralized servers while enhancing data availability and resistance against loss or manipulation. IPFS has been applied in healthcare settings to improve scalability and privacy. Ghassan et al. [23] investigated embedding metadata in distributed storage for decentralized record-keeping, whereas Haya et al. [24] used IPFS combined with proxy re-encryption to protect patient data. Joao et al. [25] created an IoT-based healthcare data platform by integrating IPFS with blockchain and MQTT protocols. Similarly, Yufei et al. [26] and Pearl et al. [27] illustrated how IPFS may improve access control and confidentiality of medical data. Blockchain, IPFS, and CP-ABE (Ciphertext-Policy Attribute-Based Encryption) were coupled by Kaur et al. [28] to provide scalable medical record management with fine-grained access control. For instance, to

solve security and privacy issues, Rahul et al. [29] created a decentralized EHR solution utilizing blockchain, RSA encryption, and IPFS storage. IPFS's increasing importance in decentralized healthcare data management is further supported by other works that suggested blockchain–IPFS solutions for attribute-based encrypted medical records, secure EHR sharing, and self-sovereign identity systems [30].

Healthcare information transfer requires privacy-preserving authentication and access control in addition to storage and integrity. Group signature methods enable users to sign messages on behalf of a group while maintaining the anonymity of individual identities unless a trace is necessary [31]. Group signatures provide a means of participant authentication without disclosing their identities, striking a balance between accountability and privacy protection. Group signatures were used by Shijie et al. [32] to secure blockchain-integrated mobile-edge computing. The SLTGS system was introduced by Zijian et al. [33] in the healthcare industry to provide effective, privacy-preserving data sharing. Group signature-based protocols were introduced for IoT settings by Zhiwei et al. [34], Mukesh et al. [35], and Weihan et al. [36] to guarantee safe, verified IoT data transfers.

Studies have explored threshold-based group signatures for IoT [37], elliptic curve cryptography schemes [38], and decentralized group signature models [39] to enhance performance and scalability while maintaining privacy. To build secure and privacy-preserving healthcare data systems, recent works recommend integrating blockchain, IPFS, and group signatures. For instance, Samraiz et al. [40] combined blockchain and IPFS to improve medical data sharing, while others applied attribute-based encryption [41], polymorphic encryption [42], smart contracts, and proxy re-encryption [43] to strengthen decentralized governance. Despite progress, adoption faces challenges related to privacy, regulatory compliance, and scalability [44]. Advanced mechanisms such as group signatures and multi-manager systems often require complex coordination, and their verification processes show weaknesses [45]. Similarly, blockchain combined with group key distribution and smart contracts remains largely theoretical [46], where many group signature models lack practical deployment analysis [47] and research shows efficiency gains, but fails against device impersonation [48].

Overall, integrated frameworks highlight a trend toward multi-layered healthcare infrastructures. Group signatures ensure privacy-preserving authentication, blockchain secures data immutability, and IPFS supports decentralized storage. Together, these technologies aim to meet regulatory demands while addressing data security, privacy, and interoperability challenges in healthcare. The main contributions of this body of work are summarized in Table 1, showing how blockchain, smart contracts, IPFS, group signatures, and IoT are converging toward secure, patient-centered data ecosystems. Existing blockchain–EHR frameworks often rely on ZKP, PRE, or ABE mechanisms to enforce privacy and access control. These approaches introduce significant overheads: ZKP schemes scale poorly under frequent authentication, PRE incurs high re-delegation cost, and ABE suffers from large key sizes and complex revocation policies. In our work, we implemented and evaluated a group signature–based framework with hierarchical key management and on-chain revocation. As summarized in Table 2, this design provides constant-size signatures, immediate credential revocation, and efficient key rotation, addressing the scalability and credential-compromise challenges identified in prior approaches.

Table 1. Adoption of recent technologies such as blockchain, IoT, EHR systems, and cryptography in modern healthcare management.

Reference	Based On	Limitations
[49]	Blockchain, IPFS	TCCM has limitations in platform reliance, complexity, ethical risks, access control, and scalability.
[50]	Blockchain, IPFS	The framework faces limitations in scalability, model accuracy, explainability, and standard compliance, requiring further validation across diverse healthcare settings.
[51]	Blockchain, IPFS	The system faces limitations in scalability, user dependence, and institutional adoption.
[52]	IoT, EHR	The scheme is limited by its simulation-based evaluation, single authority support, and lack of quantum resistance.
[53]	IoT, EHR	The main limitation of the study is its validation using data from a single hospital's EHR system and one type of wearable device (Garmin), limiting generalizability.
[54]	Blockchain, EHR	B-HIES is limited by assumptions on ethical data use, lack of scalability testing, partial semantic interoperability, absence of data quality control, and no integrated threat modeling.
[55]	Blockchain, EHR	The system lacks real-world evaluation, scalability testing, and integration with AI and IoT for advanced healthcare functionality.
[56]	Blockchain, Group Signature	The proposed TASS scheme lacks real-world deployment and has not yet addressed resistance to malicious aborts in distributed settings.
[57]	Blockchain, Key Distribution	The study lacks practical implementation or evaluation of ECC within real-world healthcare systems.

Table 2. A detailed comparison of the proposed framework with existing blockchain–IPFS–encryption approaches, highlighting differences in privacy mechanisms, revocation handling, and scalability.

Reference	Privacy Mechanism	Revocation Handling	Scalability/Rotation
[58]	zk-SNARKs	Not supported	High computation cost; limited TPS
[59]	Proxy Re-Encryption	Limited, delegation only	Overhead grows with number of delegates
[60]	Attribute-Based Encryption	Policy-based revocation (complex)	Large key sizes; poor scalability to thousands of users
Proposed Method	Group Signatures + Hierarchical key Management	On-chain, immediate via smart contract	Constant-size signatures, efficient verification, low-cost key rotation

3. Proposed Methodology

Traditional centralized systems have inbuilt constraints such as single points of failure, scalability challenges, and privacy concerns in modern data management and governance frameworks. Our proposed approach uses blockchain for decentralized architecture and IPFS for decentralized storage to solve these problems. Furthermore, we enhance the

system's security, scalability, anonymity, and resilience while maintaining robustness by implementing a multi-manager approach within the group signature scheme. Our ultimate objective is to create a system that achieves the perfect balance between privacy and openness, giving users control over their data while maintaining the fundamental advantages of blockchain technology.

3.1. Framework Description

The proposed framework establishes a decentralized system for secure patient data management. By integrating IPFS and blockchain with hospital-specific EHR storage, it ensures both data accessibility and integrity. Users register through decentralized applications (DApps) and authenticate using group signatures, enabling secure access to the blockchain network. While specific patient data is stored on IPFS servers, the blockchain handles authentication and data retrieval processes. This integrated approach enhances the security, reliability, and interoperability of healthcare data management.

Furthermore, the framework guarantees secure patient data storage within hospitals by equipping them with dedicated EHR storage systems and leveraging decentralized IPFS infrastructure to strengthen data protection.

Figure 3 illustrates the decentralized workflow for securely requesting and verifying patient data within the proposed healthcare system. In this framework, users (doctors/patients) first register through a decentralized application, where multi-group managers oversee the registration process and provide each user with unique identification credentials for authentication. Patient data is encrypted and uploaded to a hospital-managed electronic health record (EHR) server, ensuring sensitive information remains protected at the source.

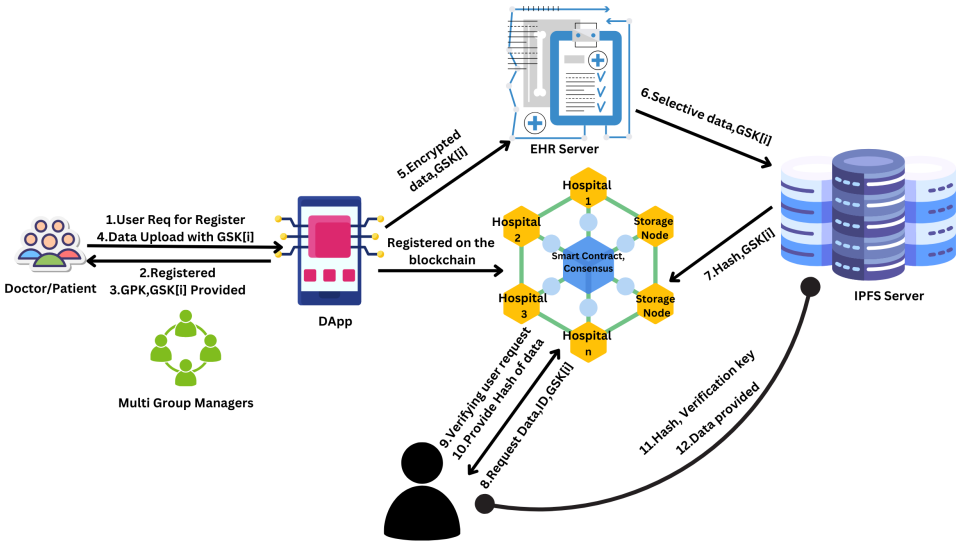

Figure 3. A blockchain and IPFS-enabled architecture for secure remote access of patient data: A step-by-step process flow including user registration via DApp, group signature authentication, encrypted data upload to EHR servers, hash storage on IPFS, blockchain-based verification, and decentralized data retrieval across hospital nodes.

Access to the stored data is facilitated through the InterPlanetary File System (IPFS), where encrypted data hashes and associated access keys are maintained. Users can retrieve data selectively by referencing these hashes, enabling efficient and secure access without directly exposing the raw data. Group managers play a critical role in overseeing the registration process and securely distributing cryptographic keys to authorized users, maintaining strict access control and identity management.

In parallel, smart contracts operate across the blockchain to enforce consensus protocols, validate transactions, and guarantee data integrity throughout the distributed storage nodes implemented across hospital networks. This decentralized architecture not only strengthens data security and trustworthiness, but also ensures interoperability and accountability among various healthcare stakeholders.

3.1.1. Hospital EHR Storage and DApp Registration:

The proposed approach ensures secure patient data storage within hospitals by providing them with their own EHR storage system.

DApp facilitates user registration with group signature technology for enhanced security and privacy. According to Agorithm 1, each user receives a unique identifier, GPK, and GSK[i] for authentication and data access within the blockchain network. The REG(U) procedure defines the process of registering a user U, who can be either a doctor or a patient, in the proposed blockchain-based healthcare system. During registration, the system generates a unique identifier ID_U, a group public key GPK, and a group secret key $GSK[i]_U$ for the user by invoking the function $Reg(U)$. These credentials allow the user to participate in the system securely through *group signature* mechanisms, enabling anonymous yet verifiable authentication while maintaining accountability through group managers. The registration ensures that each user is linked to their role: if the user is a patient, their credentials are denoted as ID_p and $GSK[i]_p$; if the user is a doctor, they are represented by ID_d and $GSK[i]_d$. This role-based distinction supports customized access control and authorization policies in subsequent operations, ensuring privacy, security, and scalability within the healthcare data management framework.

Algorithm 1 Registration Algorithm

procedure REG(U)
Let $Reg(U)$ denote the registration function for user U, where U can be a doctor or a patient.
The registration process involves generating a group signature $GSK[i]_U$ for user U using the group public key GPK.
After registration, the user is assigned a unique identifier ID_U, a group public key GPK, and a group secret key $GSK[i]_U$.
Mathematically:

$$ID_U, GPK, GSK[i]_U = Reg(U)$$

Note:
If the registered user U is a patient, then ID_U is referred to as ID_p and $GSK[i]_U$ is referred to as $GSK[i]_p$.
If the registered user U is a doctor, then ID_U is referred to as ID_d and $GSK[i]_U$ is referred to as $GSK[i]_d$.
This naming convention is used in later algorithms for role-specific operations and clarity.
end procedure

3.1.2. Data Addition and Encryption IPFS Storage Integration

According to Algorithm 2, after successful registration, doctors apply their unique group secret key $GSK[i]_d$ and assigned identifier to securely upload full patient data D_p into the system via the decentralized application (DApp).

The data is first encrypted using $GSK[i]_d$ to ensure confidentiality and data protection before being transmitted to the electronic health record (EHR) server. A selected extraction procedure in the EHR system finds important medical data, like allergies, chronic illnesses, or emergency information. This selected sensitive subset is then stored on the InterPlanetary File System (IPFS). Upon uploading to IPFS, a unique content hash hash_{IPFS} is generated, representing the exact location of the data on IPFS without exposing the raw medical data.

Algorithm 2 Secure Data Storage Algorithm

procedure SECURESTORE($Dp, GSK[i]_d$)
  Input: Dp (Full patient data), $GSK[i]_d$ (Group secret key of the doctor)
  Output: $hash_{IPFS}$ (IPFS content hash)
  Encrypt the full patient data: $ED \leftarrow Encrypt(Dp, GSK[i]_d)$
  Store the encrypted data into the EHR system: $StoreToEHR(ED)$
  Select sensitive data (e.g., allergies) from the EHR: $D_{sel} \leftarrow SelectFromEHR(ED)$
  Store selected data on IPFS and obtain a content hash: $h_{IPFS} \leftarrow IPFS\_Store(D_{sel})$
  Link the IPFS content hash to the blockchain for verification: $Blockchain\_Link(h)$
  return $hash_{IPFS}$
end procedure

This content hash is subsequently registered and linked onto a blockchain network, thereby ensuring data integrity, traceability, and immutability.

3.1.3. Blockchain Network Connectivity

Every hospital serves as a node in a decentralized blockchain network, creating a dispersed and robust infrastructure for patient data management. Furthermore, the blockchain network is seamlessly integrated with the Inter-Planetary File System (IPFS) storage, allowing for the safe and decentralized archiving of patient data.

3.1.4. Data Retrieval Process

After registration and secure data storage, patients can retrieve their medical information through a verified process to ensure secure access and maintain confidentiality, according to Algorithm 3. When a patient p initiates a request to access their data, the system first verifies the patient's identity and authenticity by validating their unique identifier ID_p and group secret key $GSK[i]_p$ through the blockchain network. This ensures that only authorized users can retrieve sensitive information. Upon successful verification, the system retrieves the corresponding IPFS content hash hash_{IPFS} associated with the patient's stored selective medical data. Using this content hash, the encrypted selected data $EncData_p$ is fetched directly from the IPFS server. The retrieved encrypted data is then decrypted using the patient's group secret key $GSK[i]_p$ to reconstruct the original sensitive medical information $Data_p$. This two-step process—first verifying through blockchain and then decrypting with a secret key—ensures both the authenticity and confidentiality of patient data. If the verification process fails, access is immediately denied, preventing unauthorized data retrieval attempts. This secure retrieval flow maintains data integrity, privacy, and strict access control across the decentralized healthcare system.

3.1.5. Further Data Retrieval and Requests

Patients can directly request detailed information from their registered hospital's EHR via the IPFS server, bypassing middleman verification through the blockchain network. This streamlined process ensures secure data retrieval, enhancing accessibility without compromising patient data security.

Here, Figure 4 shows the sequential workflow of the proposed framework. In the registration phase, users enroll through the DApp using Algorithm 1 with group signature authentication. In the data upload phase, doctors or patients encrypt and store records in the EHR, link selected data to IPFS, and record its hash on the blockchain using Algorithm 2. In the data request phase, patients or authorized entities retrieve data through blockchain verification and decryption as outlined in Algorithm 3. This ensures secure, private, and verifiable access to EHRs.

Algorithm 3 Data Retrieval Process

procedure DATARETRIEVAL(p)
  Input: p (Patient requesting data)
  Output: $Data_p$ (Patient's selected data)
  Verify the patient's identity and group signature:

$$\text{status} \leftarrow Verify(ID_p, GSK[i]_p)$$

  if status == success **then**
    Retrieve the IPFS content hash linked to the patient's data:

$$hash_{IPFS} \leftarrow Blockchain\_Fetch(ID_p)$$

    Fetch the selected encrypted data from IPFS:

$$EncData_p \leftarrow IPFS\_Retrieve(hash_{IPFS})$$

    Decrypt the retrieved data using patient's secret key:

$$Data_p \leftarrow Decrypt(EncData_p, GSK[i]_p)$$

    return $Data_p$
  else
    Verification failed: **Access Denied**
  end if
end procedure

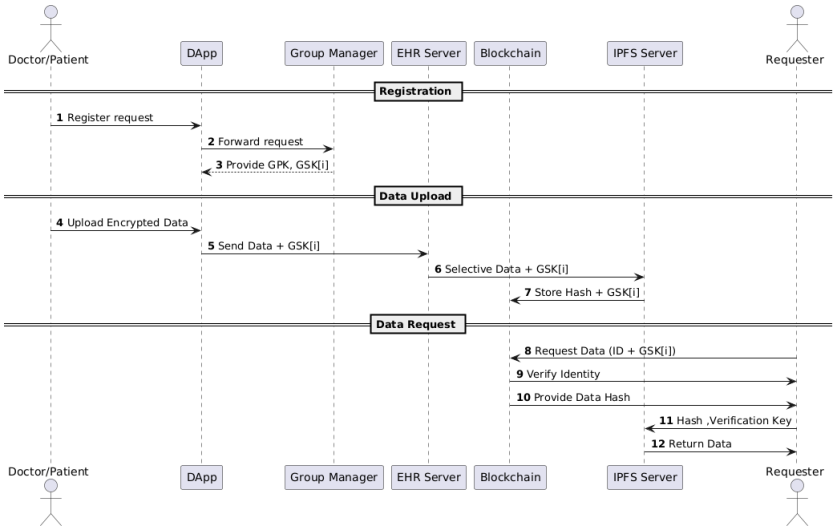

Figure 4. Sequence diagram of the proposed blockchain- and IPFS-enabled framework for decentralized electronic health record (EHR) management. The diagram illustrates the complete workflow, including the registration phase, the data upload phase, and the data retrieval phase.

3.1.6. Key Management, Rotation, and Revocation

The framework integrates a hierarchical envelope encryption model to ensure robust key management and fast recovery from credential compromise. At the top level, organizational root keys are maintained within an HSM/KMS. Departmental Key Encryption Keys (KEKs) are derived from this root and used to wrap Data Encryption Keys (DEKs), which in turn encrypt individual electronic health records (EHRs). This structure localizes the effect of compromise—the exposure of a single DEK affects only one record—while KEK rotation can be performed without re-encrypting the underlying data. As shown in Algorithm 2, this process is applied when encrypting and storing medical records in IPFS.

Anonymous user authentication is achieved through group signatures, where each user receives a credential issued by a group manager at registration (Algorithm 1). Every transaction is validated in two steps: (i) group signature verification, and (ii) checking

the user index against an on-chain revocation list. Compromised credentials are revoked via a revoke (i) transaction, which updates a compact bitset or Merkle accumulator and emits an auditable event. Revocation takes effect within a single block, and active sessions are further limited by short-lived tokens (less than 5 minutes). This verification step is integrated into Algorithm 3 (Data Retrieval).

Key compromise scenarios are handled efficiently: departmental KEK exposure triggers re-wrapping of encrypted DEKs (EDEKs), while record-specific compromise leads to DEK regeneration and re-encryption of only the affected EHR. Manager key compromise, though rare, is mitigated by key rotation and re-issuance of member credentials. Key lifetimes are enforced periodically (root annually, KEKs quarterly, DEKs per update), and all rotation/revocation actions are logged both on-chain and within the KMS audit trail.

This layered design, illustrated in Figure 5, builds directly upon Algorithms 1–3, enabling scalable and auditable key management while ensuring confidentiality and resilience against compromised credentials in healthcare blockchain networks. A common conflict arises between blockchain immutability and GDPR's "right to erasure." As shown in Figure 6, the hospital EHR remains the primary storage for Protected Health Information (PHI), while only pseudonymous metadata and selectively encrypted subsets are linked via IPFS and the blockchain. PHI is encrypted using per-record Data Encryption Keys (DEKs), which are wrapped under departmental Key Encryption Keys (KEKs) and secured by an organizational root key in an HSM/KMS (envelope encryption). Group signature keys (GPK/GSK) are used only for anonymous authentication and credential revocation, not for encrypting PHI. When an erasure request is made, the patient is authenticated, the corresponding DEK is destroyed in the KMS (crypto-erasure), related IPFS entries are unpinned and dereferenced, and RevokeCID and ErasureReceipt events are logged on-chain. As depicted in the figure, this process ensures PHI becomes permanently unreadable while the blockchain ledger remains immutable, thereby reconciling GDPR's "right to erasure" with Health Insurance Portability and Accountability Act (HIPAA) confidentiality requirements.

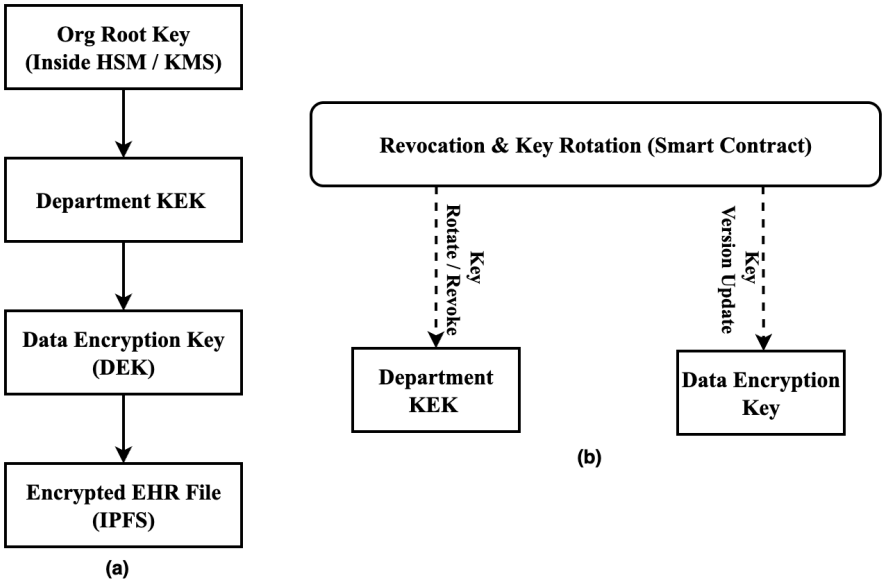

Figure 5. Key management and revocation workflow. (**a**) illustrates the hierarchical encryption model where the organizational root key secures departmental KEKs, which wrap DEKs used to protect EHRs stored in IPFS. (**b**) shows the on-chain smart contract responsible for key rotation and revocation, enabling immediate blocking of compromised credentials and controlled key version updates without re-encrypting the entire dataset.

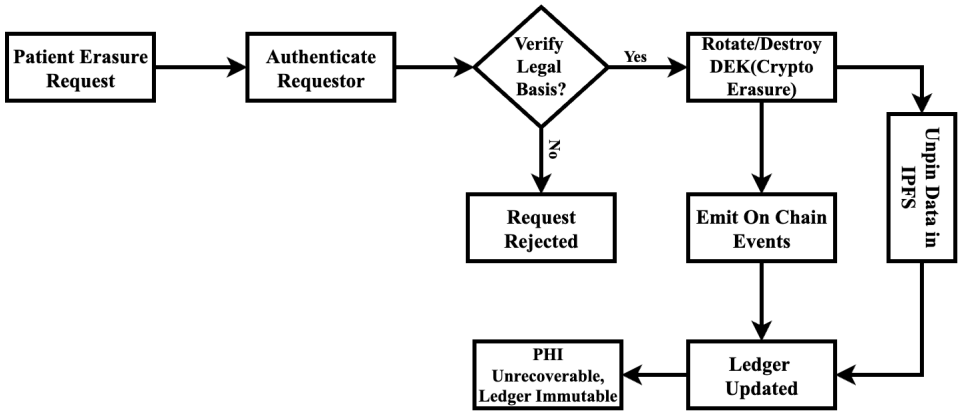

Figure 6. Workflow of the GDPR-compliant patient data erasure process in a blockchain-integrated EHR system. The workflow ensures authenticated erasure requests, crypto-erasure of Data Encryption Keys (DEKs), unpinning of data in IPFS, and immutable ledger updates.

3.1.7. Operational Context for Evaluation

In a typical hospital workflow, we considered a patient receiving regular care for diabetes. For example, the patient's blood test results are uploaded through the DApp, encrypted, and stored in the hospital's EHR system. A selected portion of sensitive data is then stored in IPFS, and its content hash is linked to the blockchain. The doctor, after authenticating, retrieves the data by verifying the patient's identity through the blockchain and accessing the corresponding encrypted file from IPFS. This process is repeated for larger records such as imaging scans, and each access is immutably logged, ensuring accountability across the hospital network.

Building on this workflow, we assume a hospital-scale deployment consisting of 5–20 nodes. Each node runs an Ethereum client connected to IPFS. The system is evaluated on the Proof-of-Stake (PoS) Ethereum test network (Sepolia). Patients and doctors interact with the system through a decentralized application (DApp) integrated with MetaMask. Medical records are represented as encrypted files, ranging from small reports to large imaging data.

In this research, the framework is planned to be evaluated using several metrics. Gas consumption is expected to be measured for each contract function, latency is intended to be recorded from request to blockchain confirmation, throughput is planned to be assessed by transactions per second, and scalability is proposed to be analyzed by varying file sizes, block sizes, and node counts. These metrics are intended to provide a baseline for future performance assessment.

4. Result and Discussion

This section explores the efficiency of blockchain integration and encryption techniques in enhancing healthcare data management and compares with the existing methodologies.

4.1. Environment Configuration

The Remix IDE offers a complete virtual environment for creating and executing smart contracts on the Ethereum network. It seamlessly handles smart contract integration within its platform, streamlining the process. MetaMask authentication is required to deploy the contract successfully. The entire smart contract implementation process occurs within the Remix IDE environment. Figure 7 demonstrates the transaction transfer to the blockchain network via the MetaMask extension tool where the Sepolia testnet network is used for the integration with a test ethereum blockchain network.

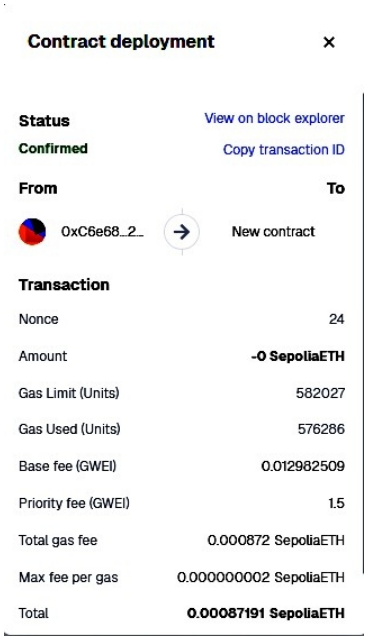

Figure 7. Successful deployment of a new smart contract via a blockchain transaction, illustrating secure and efficient execution with all parameters confirmed on the Ethereum test network, representing a key step in decentralized application development.

After confirming the transaction in MetaMask, a healthcare contract will be generated, as depicted in Figure 8. After confirmation of the transaction, its data will be added to the Ethereum platform, including details such as the transaction hash, transaction fee, and other relevant information shown in Figure 9.

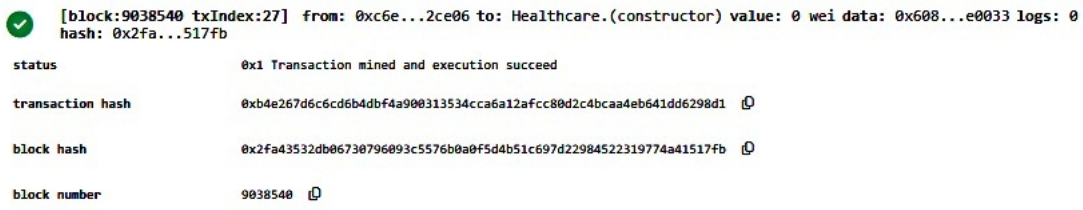

Figure 8. Successful execution of a smart contract, highlighting the transparency, security, and accuracy of blockchain systems in verifying and recording digital agreements on-chain.

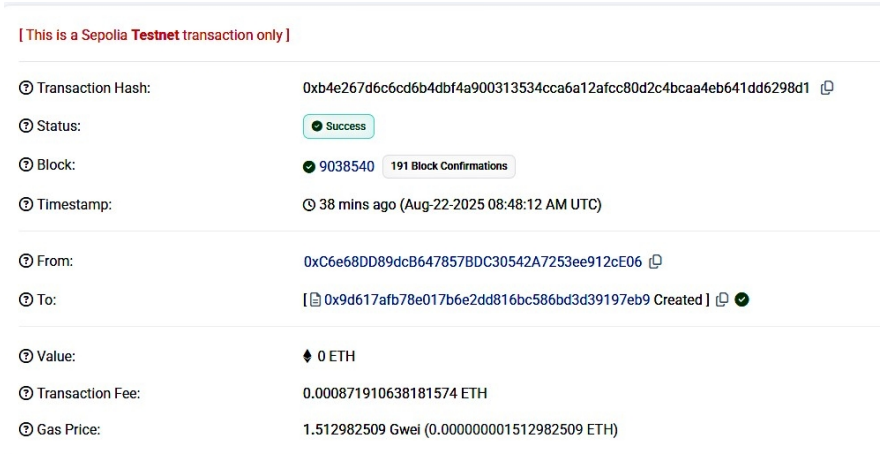

Figure 9. Transaction details from the Sepolia Testnet capturing a smart contract execution fully integrated into the blockchain, with confirmed status, block inclusion, multiple confirmations, and gas usage, demonstrating secure and verifiable decentralized operations.

4.2. Deployed Contract

With the help of the given Solidity smart contract, "Healthcare," patient and physician data can be managed on an Ethereum blockchain healthcare system. As seen in Figure 10, it constructs two primary structs, "Patient" and "Doctor," to hold data such the patient's name, age, health status, and the doctor's name and ID. Functions to set and retrieve these details for physicians and patients are included in the contract. As seen in Figure 11, these features enable the safe archiving and retrieval of healthcare-related data on the blockchain, promoting openness and accessibility in healthcare administration.

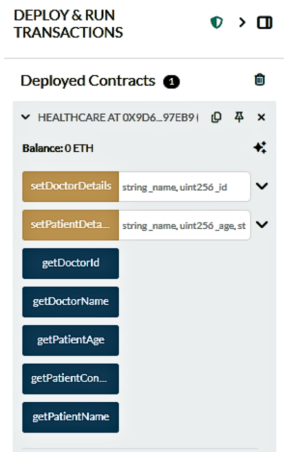

Figure 10. Interface of the deployed "Healthcare" Solidity smart contract on the Ethereum blockchain prior to data entry. The contract defines the "Patient" and "Doctor" structs and includes functions to set and retrieve patient and physician information, illustrating the structure of a blockchain-based system for secure healthcare data management.

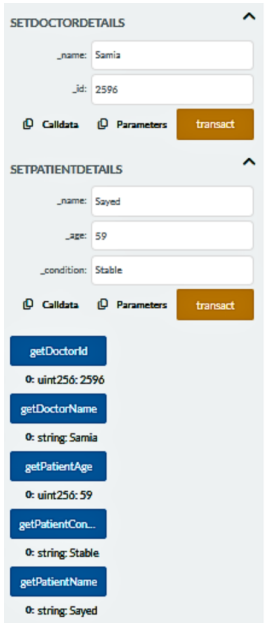

Figure 11. Interface of the "Healthcare" Solidity smart contract on the Ethereum blockchain after data entry. Patient and physician information has been recorded using the "Patient" and "Doctor" structs, demonstrating how the contract securely stores and allows retrieval of healthcare data in a decentralized system.

4.3. Performance Analysis

The research has found significant advancements in security, efficiency, and traceability with the following advancements:

- The proposed framework establishes a decentralized and secure system for managing patient data by integrating blockchain, IPFS, and hospital-specific EHR storage, ensuring high data integrity and accessibility.
- Our system maintains low and predictable latency even as block size increases, supporting timely access to patient data without significant delays.
- The system maintains reliable throughput across varying file sizes, demonstrating scalability and efficient resource management even when handling larger health records or medical images.

To assess the performance of the proposed system, key factors such as latency and throughput were evaluated under varying conditions. Figure 12 demonstrates the scalability and robustness of the proposed approach with respect to changes in block size. The X-axis represents the block size (in MB), while the Y-axis denotes the latency (in milliseconds). While an increase in latency is observed as the block size grows, the rate of increase remains controlled and linear, with latency values ranging from approximately 90 ms to 200 ms as the block size expands from 0.5 MB to 16 MB. This trend reflects the system's optimized architecture, which effectively mitigates latency overhead despite larger data transmissions. These results support the proposed system's ability to maintain a favorable throughput-latency balance under diverse workload conditions, making it well-suited for healthcare applications that demand timely access to large patient records, medical imaging data, and secure health information exchanges.

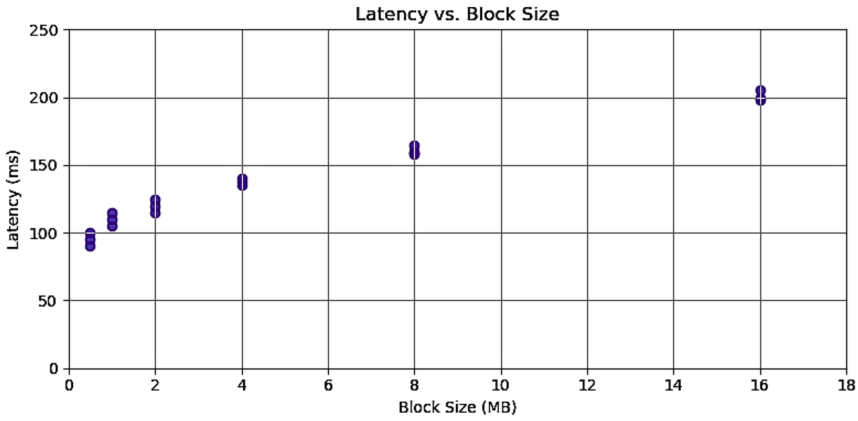

Figure 12. Efficient latency handling across varying block sizes. The latency increases gradually as block size grows from 0.5 MB to 16 MB, but the rate of increase remains relatively low and stable. This indicates that the proposed system handles larger data blocks efficiently, demonstrating strong performance and scalability under heavy load conditions compared to typical systems.

The effect of different file sizes on the suggested system's throughput is shown in Figure 13. The file size is displayed on the X-axis in kilobytes (KB), while the throughput is displayed on the Y-axis in transactions per second. The throughput gradually decreases from about 200 transactions/sec to about 90 transactions/sec as the file size grows from 10 KB to 800 KB. Even though the system becomes less efficient, its performance declines in a steady and predictable way, which shows that load allocation and resource management are working well. This behavior highlights the system's scalability and resilience, which makes it ideal for healthcare applications where data sizes might vary greatly but reliable performance is essential to guaranteeing safe and prompt data transfers.

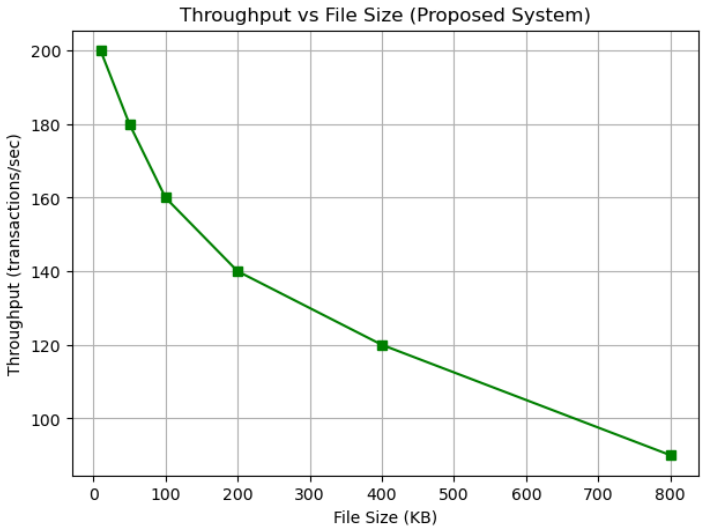

Figure 13. Impact of file size on throughput in the proposed system. Throughput decreases as file size increases from 10 KB to 800 KB. The decline is steeper at smaller file sizes and gradually levels off, indicating increased processing overhead for larger files.

Since group signatures are central to our authentication mechanism, we include representative performance data from recent benchmarking studies. Using the BBS04 pairing-based construction, prior evaluations report signature generation and verification times of approximately 1–3 ms on commodity hardware, with constant-size signatures of around 200 bytes [61,62]. Revocation checks, implemented via bitset/Merkle accumulators, add negligible cost (sub-millisecond). Table 3 summarizes these metrics, showing that group signature operations add only a few milliseconds—this is insignificant compared to the ∼12 s confirmation delay of Ethereum transactions on Sepolia.

Table 3. Representative performance of group signature operations (pairing-based, BLS/BBS schemes), including the time required for signature generation, signature verification, and revocation checks, along with the corresponding signature sizes in bytes. This table provides an overview of the efficiency and storage overhead of typical group signature schemes.

Operation	Time (ms)	Signature Size (bytes)
Signature Generation	2.1	200
Signature Verification	3.0	200
Revocation Check	0.5	Negligible

Along with the throughput and latency results, the gas cost graph shows that the system stays efficient and scalable even as file sizes increase. Figure 14 illustrates the relationship between file size (X-axis, in kilobytes) and gas cost (Y-axis, in gas units) within the proposed healthcare system. As the file size increases from 10 KB to 800 KB, the gas cost also rises gradually. This is because larger files require more metadata, such as encrypted hashes and access keys, to be securely processed and recorded on the blockchain. Although the actual patient data is stored off-chain on IPFS and in hospital EHR systems, the blockchain still handles critical operations like access control, authentication, and data verification. These processes become slightly more complex with increasing file size, leading to a controlled and linear increase in gas usage. However, in healthcare applications, this trade-off is acceptable, as ensuring the privacy, security, and integrity of sensitive patient information is far more important than minimizing gas costs. The graph

thus demonstrates the system's ability to scale efficiently while upholding strict healthcare data protection standards.

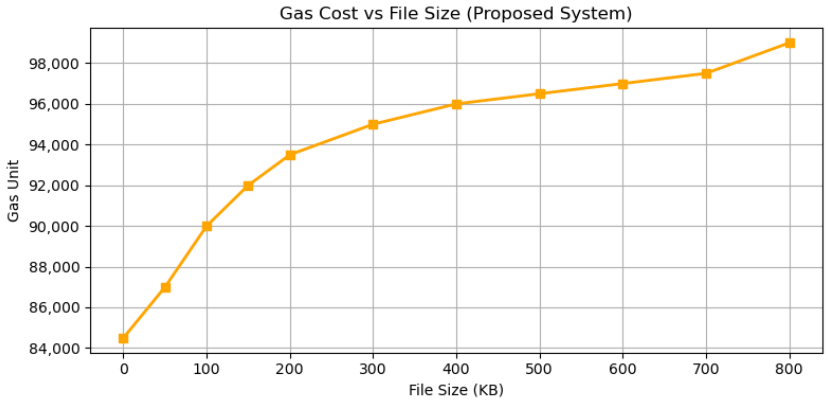

Figure 14. Scalability analysis based on gas consumption vs. file size. Gas usage increases with file size, rising from approximately 85,000 to over 98,000 units as the file size grows from 10 KB to 800 KB. The trend shows diminishing growth in gas cost at larger file sizes, indicating that the proposed system scales reasonably well in terms of gas efficiency for increasing data sizes.

4.4. Comparative Analysis of Privacy Mechanisms

To assess the suitability of different privacy-preserving cryptographic mechanisms for electronic health record (EHR) sharing, we compared group signatures with zero-knowledge proofs (ZKPs), proxy re-encryption (PRE), and attribute-based encryption (ABE). Table 4 summarizes the trade-offs. ZKPs provide strong privacy but incur significant computational overhead, which makes them unsuitable for frequent authentication events in clinical workflows. PRE schemes support flexible delegation but introduce complex key management requirements and decryption delays when sharing records across multiple users. ABE enables fine-grained policy enforcement, but its large key sizes and ciphertext overhead limit efficiency and scalability in networks with thousands of participants.

Table 4. Comparison of alternative cryptographic mechanisms with respect to suitability in healthcare EHR sharing. Group signatures provide the most balanced trade-off between privacy, efficiency, and scalability, making them preferable for hospital-scale deployments.

Mechanism	Advantages	Limitations in Healthcare EHR Context	Scalability Concern
Zero-Knowledge Proofs (ZKP)	Strong privacy, non-interactive proofs possible	High computation cost, inefficient for frequent authentication	Scales poorly with frequent transactions
Proxy Re-Encryption (PRE)	Enables delegation without sharing private keys	Complex key management, added decryption latency	Overhead grows with number of delegates
Attribute-Based Encryption (ABE)	Fine-grained access control policies	Large key sizes, high ciphertext overhead	Scalability issues for thousands of users
Group Signatures	Anonymous authentication, constant-size signatures, efficient verification	Requires trusted group manager, credential issuance overhead	Scales efficiently with large networks using multi-manager models

By contrast, group signatures enable anonymous authentication with constant-size signatures and efficient verification. Table 4 presents the comparative analysis. While the scheme requires a group manager to issue and revoke credentials, this model aligns well with hospital governance structures. Moreover, multi-manager extensions support horizontal scalability across institutions. Therefore, group signatures strike the best balance of privacy, efficiency, and scalability for large healthcare networks.

4.5. Comparison with the Existing Systems

With the growing need for secure and efficient healthcare data management, many researchers have explored blockchain and IPFS-based solutions. However, existing systems face several challenges that limit their practical use in real-world healthcare environments.

The comparison of previous studies [28,63–66] shows that many blockchain and IPFS-based healthcare systems face problems like slow performance, high costs, and weak privacy protection. Most of these systems rely on external encryption, which can be complicated and less secure. They also have complex smart contracts that can cause bugs and are not always tested in real hospitals. Regulations like HIPAA and GDPR are hard to follow because data on the blockchain cannot be changed or deleted. Additionally, many earlier systems do not work well with existing hospital software and have trouble managing users and their access rights at a large scale.

Table 5 summarizes a detailed comparison of key features across the reviewed systems and highlights how the proposed system outperforms them. Regarding scalability, earlier works suffer from high gas fees, latency, or throughput limitations, while our system supports smooth handling of large files with controlled latency. In terms of data privacy and encryption, previous solutions mostly depend on external methods or offer limited protections. In contrast, our system uses group signatures and source-side encryption, ensuring secure and decentralized storage using IPFS.

Smart contract security is another concern, as many existing systems have overly complex implementations, increasing the risk of bugs. Our proposed system simplifies this by using optimized smart contracts that are streamlined for validation and consensus, reducing vulnerabilities. Regarding regulatory compliance, only a few systems address HIPAA or GDPR. Our system, however, is designed with confidentiality and access control in mind, aligning with regulatory requirements using group-based access and encryption.

Real-world integration and interoperability are often lacking in prior works, which are either simulated or partially implemented. Our system stands out by being tested with actual hospital EHR systems, ensuring real-world applicability. Additionally, our use of group signatures allows scalable and decentralized user management which is not supported in earlier models.

Overall, these comparisons clearly show that the proposed system offers significant improvements in performance, security, privacy, compliance, and practical deployment, making it a more viable and effective solution for real-world healthcare environments.

Table 5. Comparison of proposed system with previous systems.

Feature	Kaur et al. [28]	Khan et al. [63]	Tiwari et al. [64]	Mallick et al. [65]	Ma et al. [66]	Proposed System
Scalability	High gas and encryption overhead	High gas fees and latency	Improved but limited scalability	Limited throughput	Dependent on Ethereum congestion	Controlled latency, scalable throughput for large files

Table 5. *Cont.*

Feature	Kaur et al. [28]	Khan et al. [63]	Tiwari et al. [64]	Mallick et al. [65]	Ma et al. [66]	Proposed System
Data Privacy and Encryption	Depends on external CP-ABE encryption	Privacy risks due to blockchain transparency	Requires external encryption	Limited privacy focus	Metadata privacy limited	Uses group signatures and source encryption; secure IPFS storage
Smart Contract Security	Complex smart contract management	Risk of bugs from insufficient auditing	Complex system due to combined tech	Complex integration	Requires specialized expertise	Optimized smart contracts for validation and consensus
Regulatory Compliance (HIPAA/GDPR)	Not specifically addressed	Challenges due to immutability	GDPR "right to erasure" conflict	Not deeply addressed	Not addressed	Group signature and encryption support confidentiality and privacy needs
Real-World Integration	Simulated only	Prototype, no live integration	Limited integration	Limited hospital interoperability	Not deployed in real environments	Integrated with hospital EHR systems and tested for real-world use
Interoperability	Not addressed	Not addressed	Difficult integration with legacy systems	Limited interoperability	Not addressed	Designed for hospital EHR compatibility via blockchain and IPFS
User Management	Complex and unscalable attribute management	Not addressed	Not addressed	Not addressed	Not addressed	Uses group signatures for scalable decentralized authentication

4.6. Scalability Evaluation with Simulated EHR Data

To approximate realistic hospital conditions, we generated simulated EHR workloads based on record distributions reported in benchmark datasets such as MIMIC-III [67]. File sizes ranged from 128 KB laboratory reports and 256 KB prescriptions to 512 KB doctor notes and 2 MB imaging scans, with access frequencies reflecting typical hospital use patterns (20 lab reports, 15 prescriptions, 10 notes, and 5 imaging scans per patient). The tests were conducted on a multi-node setup with standard server hardware and typical LAN network conditions.

As shown in Figure 15, throughput scales nearly linearly up to 3000 requests/s, achieving 2350 tps with an average latency of 400 ms. Beyond this point, the curve begins to flatten, with throughput stabilizing at 2700 tps under 5000 requests/s. Latency rises more sharply (up to 650 ms), while success rate remains above 92 percent. This flattening effect is primarily due to consensus delays in the PoS network and IPFS retrieval overhead, which become more pronounced under high concurrency.

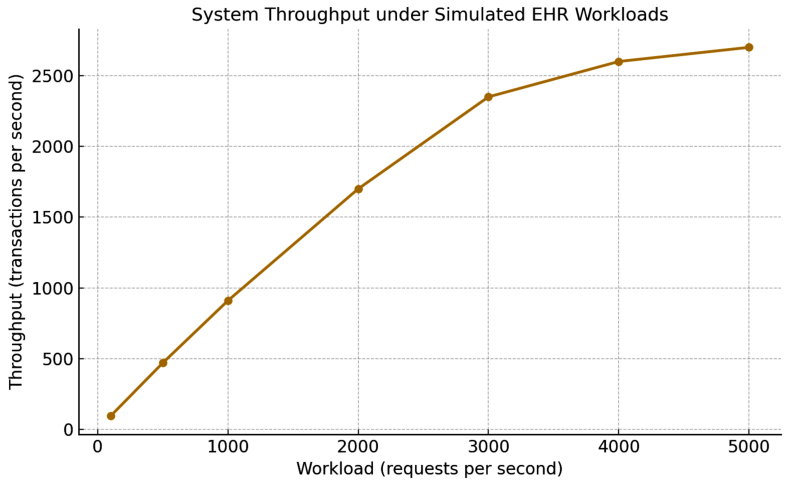

Figure 15. System throughput under simulated EHR workloads inspired by MIMIC-III. The framework scales nearly linearly up to 3000 requests/s before flattening at 2700 tps under 5000 requests/s. Latency increases due to consensus delays and IPFS retrieval overhead, while success rate remains above 92 percent.

5. Conclusions

This research presents a novel decentralized framework for managing healthcare data using blockchain, IPFS, and group signatures. It ensures data security, privacy, and integrity while enabling easy and secure data exchange between healthcare providers. The optimized architecture of the system maintains efficient performance even with large data sizes, as shown in the experimental results. Our approach provides a robust, scalable solution that improves patient care and builds trust in healthcare data management by combining advanced technologies for secure, transparent, and efficient data handling. In contrast to existing works that combine blockchain with IPFS and conventional encryption, our framework advances the state of the art by integrating group signatures, hierarchical KEK/DEK management, and smart contract–based revocation. This combination not only strengthens privacy but also addresses scalability and credential-compromise challenges, which remain limitations in many prior approaches.

However, the system is not without limitations. Challenges such as energy consumption, transaction latency, and potential deployment barriers in large-scale healthcare infrastructures need to be carefully addressed before real-world adoption. Moreover, ensuring compliance with strict regulatory frameworks like GDPR poses additional hurdles, especially when dealing with highly sensitive electronic health records (EHR). In the future, we aim to test this system in real healthcare settings. We are actively communicating with hospitals to explore opportunities for deployment and real-world validation. Currently, due to General Data Protection Regulation (GDPR) restrictions, we cannot access or test real EHR datasets, which continues to pose a significant challenge. Nonetheless, practical testing will provide valuable insights into usability and integration with medical workflows, allowing us to refine the system for everyday clinical practice.

Synthetic EHR evaluation demonstrates that the system sustains thousands of concurrent requests while maintaining high success rates, confirming its feasibility for hospital-scale deployment. Furthermore, future research directions can focus on integrating blockchain and IPFS with emerging technologies such as IoT-enabled medical devices and AI-driven analytics, which can enhance automation and predictive healthcare. Additionally, addressing regulatory challenges and establishing globally accepted standards will be essential for broader adoption. By advancing in these directions, secure, efficient, and patient-centered digital healthcare ecosystems can become a reality.

Author Contributions: S.S.: Conceptualization, Data curation, Formal analysis, Investigation, Methodology, Validation, Visualization, Writing—review and editing. M.S.F.: Conceptualization, Data curation, Formal analysis, Investigation, Methodology, Validation, Visualization, Writing—original draft. R.M.: Conceptualization, Data curation, Formal analysis, Investigation, Methodology, Validation, Visualization, Writing—original draft. R.T.K.: Conceptualization, Data curation, Formal analysis, Investigation, Validation, Visualization, Writing—original draft. M.S.K.: Investigation, Methodology, Resources, Supervision, Writing—review and editing. M.S.H.: Investigation, Methodology, Project administration, Supervision, Writing—review and editing. K.A.: Conceptualization, Investigation, Project administration, Supervision, Writing—review and editing. R.K.: Investigation, Methodology, Project administration, Validation, Writing—review and editing. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding author.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Islam, M.M.; Rahaman, A.; Islam, M.R. Development of Smart Healthcare Monitoring System in IoT Environment. *SN Comput. Sci.* **2020**, *1*, 185. [CrossRef] [PubMed]
2. Dwivedi, A.D.; Srivastava, G.; Dhar, S.; Singh, R. A Decentralized Privacy-Preserving Healthcare Blockchain for IoT. *Sensors* **2019**, *19*, 326. [CrossRef]
3. Kumar, M.; Kumar, A.; Verma, S.; Bhattacharya, P.; Ghimire, D.; Kim, S.h.; Hosen, A.S.M.S. Healthcare Internet of Things (H-IoT): Current Trends, Future Prospects, Applications, Challenges, and Security Issues. *Electronics* **2023**, *12*, 2050. [CrossRef]
4. Sayed, S.; Shahrear Famous, M.; Ahammad, S.; Hossain, T.; Khan, R.T.; Kaiser, M.S. Toward Distributed Security Based Healthcare System. In Proceedings of the Fifth International Conference on Trends in Computational and Cognitive Engineering, Kanpur, India, 24–25 November 2023; Kaiser, M.S., Singh, R., Bandyopadhyay, A., Mahmud, M., Ray, K., Eds.; Springer: Singapore, 2024; pp. 445–458. [CrossRef]
5. Bataineh, M.R.; Mardini, W.; Khamayseh, Y.M.; Yassein, M.M.B. Novel and Secure Blockchain Framework for Health Applications in IoT. *IEEE Access* **2022**, *10*, 14914–14926. [CrossRef]
6. Bran, E.; Alzamora, A.; Castañeda-Carbajal, B.; Castillo-Sequera, J.L.; Wong, L. Interoperability Blockchain, InterPlanetary File System and Health Level 7 Framework for Electronic Health Records. *Int. J. Online Biomed. Eng. (iJOE)* **2024**, *20*, 60–78. [CrossRef]
7. Yakut, S.; Şeker, Ö.; Batur, E.; Dalkılıç, G. Blockchain Platform for Internet of Things. In Proceedings of the 2019 Innovations in Intelligent Systems and Applications Conference (ASYU), Izmir, Turkey, 31 October–2 November 2019; pp. 1–6. [CrossRef]
8. Lu, J.; Hu, C.; Ruan, C.; Cai, B.; Xiang, T. Group Signature with Time-Bound Keys for Secure E-health Record Sharing*. In Proceedings of the 2024 IEEE International Conference on Bioinformatics and Biomedicine (BIBM), Lisbon, Portugal, 3–6 December 2024; pp. 3571–3576. [CrossRef]
9. Sonkamble, R.G.; Bongale, A.M.; Phansalkar, S.; Sharma, A.; Rajput, S. Secure Data Transmission of Electronic Health Records Using Blockchain Technology. *Electronics* **2023**, *12*, 1015. [CrossRef]
10. Rani, D.; Kumar, R.; Chauhan, N. A secure framework for IoT-based healthcare using blockchain and IPFS. *Secur. Priv.* **2023**, *7*, e348. [CrossRef]
11. Jayanthy, D.S.; Arunkumar, A.; Kovilpillai, M.J.J.A.; Bhuvardhena, M.; Pandian, K.D. Secured Health Data Sharing System using IPFS and Blockchain with Beacon Proxy. *Procedia Comput. Sci.* **2023**, *230*, 788–797. [CrossRef]
12. Assiri, B. A Modified and Effective Blockchain Model for E-Healthcare Systems. *Appl. Sci.* **2023**, *13*, 12630. [CrossRef]
13. Kodavali, L.; Kuppuswamy, S. Adaptation of Blockchain using Ethereum and IPFS for Fog based E-Healthcare Activity Recognition System. *Trends Sci.* **2022**, *19*, 5072. [CrossRef]
14. Kumar, M.; Raj, H.; Chaurasia, N.; Gill, S.S. Blockchain inspired secure and reliable data exchange architecture for cyber-physical healthcare system 4.0. *Internet Things Cyber-Phys. Syst.* **2023**, *3*, 309–322. [CrossRef]
15. Song, W.; Zhu, M.; Lu, D.; Zhu, C.; Zhao, J.; Sun, Y.; Li, L.; Zhu, H. Blockchain Bottleneck Analysis Based on Performance Metrics Causality. *Electronics* **2024**, *13*, 4236. [CrossRef]
16. Alsaeed, N.; Nadeem, F.; Albalwy, F. A scalable and lightweight group authentication framework for Internet of Medical Things using integrated blockchain and fog computing. *Future Gener. Comput. Syst.* **2024**, *151*, 162–181. [CrossRef]

17. Kumar, R.; Marchang, N.; Tripathi, R. Distributed Off-Chain Storage of Patient Diagnostic Reports in Healthcare System Using IPFS and Blockchain. In Proceedings of the 2020 International Conference on COMmunication Systems & NETworkS (COMSNETS), Bengaluru, India, 7–11 January 2020; pp. 1–5, ISSN 2155-2509. [CrossRef]
18. Madine, M.M.; Battah, A.A.; Yaqoob, I.; Salah, K.; Jayaraman, R.; Al-Hammadi, Y.; Pesic, S.; Ellahham, S. Blockchain for Giving Patients Control Over Their Medical Records. *IEEE Access* **2020**, *8*, 193102–193115. [CrossRef]
19. Uppal, S.; Kansekar, B.; Mini, S.; Tosh, D. HealthDote: A blockchain-based model for continuous health monitoring using interplanetary file system. *Healthc. Anal.* **2023**, *3*, 100175. [CrossRef]
20. Zubaydi, H.D.; Varga, P.; Molnár, S. Leveraging Blockchain Technology for Ensuring Security and Privacy Aspects in Internet of Things: A Systematic Literature Review. *Sensors* **2023**, *23*, 788. [CrossRef]
21. Ożadowicz, A. Generic IoT for Smart Buildings and Field-Level Automation—Challenges, Threats, Approaches, and Solutions. *Computers* **2024**, *13*, 45. [CrossRef]
22. Sivaprakash, P.; Charaan, R.; Ithayan, J.V.; Sankar, M.; Chithambaramani, R.; Marichamy, D. IPFS-based Blockchain Enabled System for Secure Data Storage and Access in Healthcare. In Proceedings of the 2024 Second International Conference on Intelligent Cyber Physical Systems and Internet of Things (ICoICI), Coimbatore, India, 28–30 August 2024; pp. 203–208. [CrossRef]
23. Al-Sumaidaee, G.; Alkhudary, R.; Zilic, Z.; Swidan, A. An Evaluation Framework for Assessing IPFS Performance within a Blockchain-Based Healthcare System. In Proceedings of the 2023 IEEE International Conference on Blockchain (Blockchain), Danzhou, China, 17–21 December 2023; pp. 100–104, ISSN 2834-9946. [CrossRef]
24. Hasan, H.R.; Salah, K.; Yaqoob, I.; Jayaraman, R.; Pesic, S.; Omar, M. Trustworthy IoT Data Streaming Using Blockchain and IPFS. *IEEE Access* **2022**, *10*, 17707–17721. [CrossRef]
25. de Brito Gonçalves, J.P.; Spelta, G.; da Silva Villaça, R.; Gomes, R.L. IoT Data Storage on a Blockchain Using Smart Contracts and IPFS. In Proceedings of the 2022 IEEE International Conference on Blockchain (Blockchain), Espoo, Finland, 22–25 August 2022; pp. 508–511. [CrossRef]
26. Lin, Y.; Zhang, C. A Method for Protecting Private Data in IPFS. In Proceedings of the 2021 IEEE 24th International Conference on Computer Supported Cooperative Work in Design (CSCWD), Dalian, China, 5–7 May 2021; pp. 404–409. [CrossRef]
27. Lobo, P.A.; Sarasvathi, V. Distributed File Storage Model using IPFS and Blockchain. In Proceedings of the 2021 2nd Global Conference for Advancement in Technology (GCAT), Bangalore, India, 1–3 October 2021; pp. 1–6. [CrossRef]
28. Kaur, J.; Rani, R.; Kalra, N. Attribute-based access control scheme for secure storage and sharing of EHRs using blockchain and IPFS. *Clust. Comput.* **2024**, *27*, 1047–1061. [CrossRef]
29. Bhalerao, R.; Gite, P.; Patil, P.; Gupta, R.; Singh, S. Decentralized E-health Patient Record Management System using Blockchain and IPFS. In Proceedings of the 2023 International Conference on Innovative Data Communication Technologies and Application (ICIDCA), Uttarakhand, India, 14–16 March 2023; pp. 781–785. [CrossRef]
30. Bang, J.; Choi, M.J. Design of Personal Data Protection Decentralized Model Using Blockchain and IPFS. In Proceedings of the 2023 24st Asia-Pacific Network Operations and Management Symposium (APNOMS), Sejong, Republic of Korea, 6–8 September 2023; pp. 251–254, ISSN 2576-8565.
31. Zhou, S.; Lin, D. On Anonymity of Group Signatures. In Proceedings of the International Conference on Computational and Information Science, Reading, UK, 28–31 May 2006; Volume 3802, pp. 131–136. [CrossRef]
32. Zhang, S.; Lee, J.H. A Group Signature and Authentication Scheme for Blockchain-Based Mobile-Edge Computing. *IEEE Internet Things J.* **2020**, *7*, 4557–4565. [CrossRef]
33. Bao, Z.; He, D.; Wang, H.; Luo, M.; Peng, C. A Group Signature Scheme with Selective Linkability and Traceability for Blockchain-Based Data Sharing Systems in E-Health Services. *IEEE Internet Things J.* **2023**, *10*, 21115–21128. [CrossRef]
34. Wang, Z. Blockchain-Based Edge Computing Data Storage Protocol Under Simplified Group Signature. *IEEE Trans. Emerg. Top. Comput.* **2022**, *10*, 1009–1019. [CrossRef]
35. Soni, M.; Singh, D.K. Blockchain-based group authentication scheme for 6G communication network. *Phys. Commun.* **2023**, *57*, 102005. [CrossRef]
36. Yuan, W.; Li, X.; Li, M.; Zheng, L. DCAGS-IoT: Dynamic Cross-Domain Authentication Scheme Using Group Signature in IoT. *Appl. Sci.* **2023**, *13*, 5847. [CrossRef]
37. Gong, B.; Zhang, X.; Cao, Y.; Li, Z.; Yang, J.; Wang, W. A threshold group signature scheme suitable for the Internet of Things. *Concurr. Comput. Pract. Exp.* **2021**, *33*, e6243. [CrossRef]
38. Yu, H.; Wang, H. Elliptic curve threshold signature scheme for blockchain. *J. Inf. Secur. Appl.* **2022**, *70*, 103345. [CrossRef]
39. Devidas, S.; Rao Y.V., S.; Rekha, N.R. A decentralized group signature scheme for privacy protection in a blockchain. *Int. J. Appl. Math. Comput. Sci.* **2021**, *31*, 353–364. [CrossRef]
40. Zahid, S.; Hussain, M.; Ahmed, R.H.; Shahid, M.R.; Abbas, H. Blockchain-based Health Insurance Model Using IPFS: A Solution for Improved Optimization, Trustability, and User Control. In Proceedings of the 2023 International Conference on IT and Industrial Technologies (ICIT), Chiniot, Pakistan, 9–10 October 2023; pp. 1–7. [CrossRef]

41. Sun, J.; Yao, X.; Wang, S.; Wu, Y. Blockchain-Based Secure Storage and Access Scheme For Electronic Medical Records in IPFS. *IEEE Access* **2020**, *8*, 59389–59401. [CrossRef]
42. Famous, M.S.; Sayed, S.; Mazumder, R.; Khan, R.T.; Kaiser, M.S.; Hossain, M.S.; Andersson, K.; Khondoker, R. Secure and Efficient Drug Supply Chain Management System: Leveraging Polymorphic Encryption, Blockchain, and Cloud Storage Integration. *Cyber Secur. Appl.* **2025**, *3*, 100103. [CrossRef]
43. Battah, A.A.; Madine, M.M.; Alzaabi, H.; Yaqoob, I.; Salah, K.; Jayaraman, R. Blockchain-Based Multi-Party Authorization for Accessing IPFS Encrypted Data. *IEEE Access* **2020**, *8*, 196813–196825. [CrossRef]
44. Wang, G.; Nurcahyo, A. Designing Personalized Integrated Healthcare Monitoring System through Blockchain and IoT. *Procedia Comput. Sci.* **2023**, *227*, 223–232. [CrossRef]
45. Tang, F.; Feng, Z.; Gong, Q.; Huang, Y.; Huang, D. Privacy-Preserving Scheme in the Blockchain Based on Group Signature with Multiple Managers. *Secur. Commun. Netw.* **2021**, *2021*, e7094910. [CrossRef]
46. Song, H.J.; Lee, I.Y. A Study on Traceable Group Signature Scheme for Blockchain. In Proceedings of the 2023 8th International Conference on Information and Network Technologies (ICINT), Tokyo, Japan, 19–21 May 2023; IEEE Computer Society: Washington, DC, USA, 2023; pp. 57–60. [CrossRef]
47. An, H.; He, D.; Bao, Z.; Peng, C.; Liu, Q. An identity-based dynamic group signature scheme for reputation evaluation systems. *J. Syst. Archit.* **2023**, *139*, 102875. [CrossRef]
48. Banerjee, S.; Roy, S.; Shetty, S. P2Q-ASB: PUF-Secured Post Quantum Aggregate Signature Scheme using Public Blockchain for e-Healthcare Systems. In Proceedings of the 2025 International Wireless Communications and Mobile Computing (IWCMC), Abu Dhabi, United Arab Emirates, 12–16 May 2025; pp. 649–654. [CrossRef]
49. Chen, Z.; Zhu, L.; Jiang, P.; He, J.; Zhang, Z. Tackling Data Mining Risks: A Tripartite Covert Channel Merging Blockchain and IPFS. *IEEE Trans. Netw. Sci. Eng.* **2025**, *12*, 1831–1848. [CrossRef]
50. Puri, V.; Priyadarshini, I.; Kataria, A.; Rani, S.; Min, H. Privacy-First ML for Chronic Kidney Disease Prediction: Exploring a Decentralized Approach Using Blockchain and IPFS. *IEEE Access* **2025**, *13*, 43178–43189. [CrossRef]
51. Raatul, A.M.; Mansoor, N. Design and Development of a Blockchain and IPFS-Based Credential Verifier with Custom Lightweight Encryption for Secure Storage. In Proceedings of the 2025 International Conference on Electrical, Computer and Communication Engineering (ECCE), Chittagong, Bangladesh, 13–15 February 2025; pp. 1–6. [CrossRef]
52. Fugkeaw, S.; Prasad Gupta, R.; Worapaluk, K. Secure and Fine-Grained Access Control With Optimized Revocation for Outsourced IoT EHRs With Adaptive Load-Sharing in Fog-Assisted Cloud Environment. *IEEE Access* **2024**, *12*, 82753–82768. [CrossRef]
53. Manias, G.; Azqueta-Alzúaz, A.; Dalianis, A.; Griffiths, J.; Kalogerini, M.; Kostopoulou, K.; Kouremenou, E.; Kranas, P.; Kyriazakos, S.; Lekka, D.; et al. Advanced Data Processing of Pancreatic Cancer Data Integrating Ontologies and Machine Learning Techniques to Create Holistic Health Records. *Sensors* **2024**, *24*, 1739. [CrossRef]
54. Sandhu, R.K.; Thomas, M.A.; Osei-Bryson, K.M. Supporting secure and efficient collaborative health information exchange: A hybrid blockchain and ontology based approach. *Blockchain Res. Appl.* **2025**, *6*, 100248. [CrossRef]
55. Guerar, M.; Migliardi, M.; Russo, E.; Khadraoui, D.; Merlo, A. SSI-MedRx: A fraud-resilient healthcare system based on blockchain and SSI. *Blockchain Res. Appl.* **2025**, *6*, 100242. [CrossRef]
56. Pundir, M.; Kumar, A.; Choudhary, S. Preserving Patient Data Integrity: The Pivotal Role of Elliptic Curve Cryptography and Key Establishment in Healthcare Systems. In Proceedings of the 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kamand, India, 24–28 June 2024; pp. 1–6. [CrossRef]
57. Wang, Z.; Qin, Z.; Kumari, S.; Feng, C.; Alenazi, M.J.; Wu, D.; Chen, C.M.; Xiong, H. TASS: Threshold Adaptor Signature Scheme for Holographic IoT Consumer Devices in Blockchain Enabled Federated Learning. *IEEE Trans. Consum. Electron.* **2025**. [CrossRef]
58. Guo, J.; Zhao, K.; Liang, Z.; Min, K. Efficient and Secure EMR Storage and Sharing Scheme Based on Hyperledger Fabric and IPFS. *Appl. Sci.* **2024**, *14*, 5005. [CrossRef]
59. Huang, D.C.; Liu, L.C.; Deng, Y.Y.; Chen, C.L.; Zeng, K.W. A hyperledger fabric-based EMR sharing mechanisms with proxy re-encryption and IPFS. *Clust. Comput.* **2024**, *27*, 6953–6983. [CrossRef]
60. Guo, H.; Li, W.; Nejad, M.; Shen, C.C. A Hybrid Blockchain-Edge Architecture for Electronic Health Records Management with Attribute-based Cryptographic Mechanisms. *IEEE Trans. Netw. Serv. Manag.* **2023**, *20*, 1759–1774. [CrossRef]
61. Li, Z.; Sonnino, A.; Jovanovic, P. Performance of EdDSA and BLS Signatures in Committee-Based Consensus. *arXiv* **2023**, arXiv:2302.00418. [CrossRef]
62. Hofmeier, X.; Raguso, A.; Sasse, R.; Jackson, D.; Basin, D. One For All: Formally Verifying Protocols which use Aggregate Signatures (extended version). *arXiv* **2025**, arXiv:2505.10316. [CrossRef]
63. Khan, A.; Litchfield, A.; Alabdulatif, A.; Khan, F. BlockPres IPFS: Performance evaluation of blockchain based secure patients prescription record storage using IPFS for smart prescription management system. *Clust. Comput.* **2025**, *28*, 255. [CrossRef]
64. Tiwari, K.; Kumar, S. A healthcare data management system: Blockchain-enabled IPFS providing algorithmic solutions for increased privacy-preserving scalability and interoperability. *J. Supercomput.* **2025**, *81*, 1–39. [CrossRef]

65. Mallick, S.R.; Lenka, R.K.; Tripathy, P.K.; Rao, D.C.; Sharma, S.; Ray, N.K. A lightweight, secure, and scalable blockchain-fog-iomt healthcare framework with ipfs data storage for healthcare 4.0. *SN Comput. Sci.* **2024**, *5*, 198. [CrossRef]
66. Ma, S.; Zhang, X. Integrating blockchain and ZK-ROLLUP for efficient healthcare data privacy protection system via IPFS. *Sci. Rep.* **2024**, *14*, 11746. [CrossRef] [PubMed]
67. Johnson, A.E.W.; Pollard, T.J.; Shen, L.; Lehman, L.W.H.; Feng, M.; Ghassemi, M.; Moody, B.; Szolovits, P.; Anthony Celi, L.; Mark, R.G. MIMIC-III, a freely accessible critical care database. *Sci. Data* **2016**, *3*, 160035. [CrossRef] [PubMed]