National College of Ireland

Securing Medical Records Using Blockchain with Cryptography, Encryption, and Zero-Knowledge Rollups

MSc Research Project
Cloud Computing

Darshika Pongallu
Student ID: x22197222

School of Computing
National College of Ireland

Supervisor: Shreyas Setlur Arun

National College of Ireland
Project Submission Sheet
School of Computing

National College of Ireland

Student Name:	Darshika Ravindra Pongallu
Student ID:	x22197222
Programme:	Cloud Computing
Year:	2023-2024
Module:	MSc Research Project
Supervisor:	Shreyas Setlur Arun
Submission Due Date:	12/08/2024
Project Title:	Securing Medical Records using Blockchain with Cryptography, Encryption and Zero-Knowledge Rollup
Word Count:	9459
Page Count:	25

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature:	Darshika Ravindra Pongallu
Date:	09/08/2024

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST:

Attach a completed copy of this sheet to each project (including multiple copies).	☐
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	☐
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	☐

Assignments that are submitted to the Programme Coordinator office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Securing Medical Records Using Blockchain with Cryptography and Zero-Knowledge Rollups

Darshika Pongallu
x22197222

Abstract

In the evolving healthcare landscape, securing electronic health records (EHRs) is essential due to increasing data breaches. This research introduces a solution using advanced cryptographic techniques and blockchain technology. The NTRU lattice-based cryptographic algorithm, known for its quantum resistance form the secure, quantum-resistant framework. Practical Byzantine Fault Tolerance (PBFT) provides low-latency finality and enhanced security. Privacy is ensured through zero-knowledge rollups on Polygon sidechains. To improve scalability, availability, and manageability, Docker is integrated with the blockchain platform and cloud services, facilitating powerful containerization. HIPAA compliance is achieved by adhering to the Privacy Rule, Security Rule, Breach Notification Rule, and Enforcement Rule. Key strategies include off-chain storage for Protected Health Information (PHI), encrypted communication, and robust access controls. The cloud infrastructure ensures secure, scalable, and efficient deployment, while cryptographic hashes and metadata are managed on the blockchain. This research significantly enhances the security and privacy of patient information, addressing a critical need in the healthcare sector.

1 Introduction

Blockchain, introduced by Satoshi Nakamoto in 2008, has transformed finance and now supports numerous decentralized applications. By merging robust cryptography with efficient peer-to-peer networking, it creates a secure, interconnected chain of information blocks. In healthcare, issues such as ownership, privacy, and data management are critical Suzuki and Murai (2017). According to Vithanwattana et al. (2016), traditional healthcare systems are prone to misuse and data breaches due to their reliance on centralized databases. These systems often allow large organizations to control and trade patient records without consent, raising significant privacy and financial concerns. Decentralized storage solutions based on blockchain technology provide a transparent and secure alternative. Despite efforts to enhance patient data confidentiality, there are still gaps in research on lattice-based cryptography and encryption. Additionally, the use of zero-knowledge rollups in sidechains has not been fully explored. Our research introduces a novel approach of improving patient ownership, security, and privacy on public blockchains, matching the levels of private blockchains. We will achieve this by combining lattice-based cryptography, encryption and zero-knowledge rollups in sidechains. The risk of data leakage and unauthorized access increases in proportion to the volume of data processed by medical devices. A notable cybersecurity incident involved over 10

million medical records compromised during the Blackbaud ransomware attack. By integrating blockchain technology with sidechains and quantum-resistant lattice-based cryptography, healthcare data management solutions are significantly strengthened. Lattice-based cryptography provides an extra layer of security resistant to future quantum computing threats Nejatollahi et al. (2019). This ensures the long-term safety of patient data and sensitive health information. Moreover, the use of sidechains enhances blockchain efficiency and scalability, allowing it to manage large volumes of health data without compromising performance. Encryption ensures maximum patient privacy by processing encrypted data without decryption. Zero-knowledge rollups enable more transactions to occur off the main chain, maintaining data security and integrity. This study proposes a strong approach for protecting electronic health information, addressing significant concerns in the healthcare sector, and setting the path for future advances in blockchain technology.

1.1 Research Motivation and Background

Blockchain technology offers a decentralized and immutable ledger, gaining attention in healthcare for its potential to enhance data security, transparency, and efficiency in managing electronic health records (EHRs). However, balancing transparency and data privacy remains challenging. Traditional encryption methods often fail to secure data during computations, risking breaches. Advanced cryptographic techniques like encryption and lattice-based cryptography provide promising solutions. Encryption enables computations on encrypted data without decryption, maintaining privacy. Lattice-based cryptography ensures robust security against quantum computing threats. Despite these advancements, current blockchain systems lack full integration of these techniques, particularly in identity management and secure data processing. Lattice-based encryption is essential for modern information security, protecting against standard and quantum attacks, making it a long-term solution for evolving threats Kethepalli et al. (2023). NTRU, a leading quantum-resistant technique, secures financial transactions and communication networks Karthika et al. (2023). Balancing computational transparency and data privacy in blockchain is crucial for safeguarding patient information while enabling meaningful data analysis, fostering trust, and supporting economic growth in healthcare. Inadequate security in healthcare data management leads to privacy issues Kondepogu and Andrew (2022). Chenthara et al. (2019) note that polynomial time algorithms lack data encryption support, presenting significant limitations.

Studies by Partala et al. (2020) focus on zero-knowledge proofs in blockchain without addressing identity management, while Liu et al. (2016) and Soltani et al. (2021) emphasize identity sharing but overlook zero-knowledge proofs for identity control. It shows lattice-based cryptography enhances blockchain security against quantum threats, but more practical integration is needed. This research aims to develop a robust blockchain framework integrating homomorphic encryption and lattice-based cryptography, ensuring data security during computations and enhancing identity management through zero-knowledge proofs. Practical Byzantine Fault Tolerance (PBFT) will be used for consensus, ensuring low-latency finality. The study prioritizes advanced cryptographic techniques to develop a safe, scalable, and privacy-focused blockchain ecosystem for numerous applications, particularly in healthcare. This work is crucial for advancing blockchain security and privacy, addressing healthcare data management challenges, and preparing for

future computing and cryptographic advancements.

1.2 Research Objectives

- Developing a secure EHR framework using NTRU lattice-based cryptography for quantum resistance to ensure data privacy during processing.
- Implement Practical Byzantine Fault Tolerance (PBFT) for low-latency finality and enhanced blockchain security.
- Use zero-knowledge rollups on polygon sidechains for transactions and data storage.
- Ensure HIPAA compliance with robust encryption, off-chain PHI storage, and stringent access controls.
- Ensure HIPAA compliance with robust encryption, off-chain PHI storage, and stringent access controls.

1.3 Research Question

The research question proposed in this paper is as follows – **"Can lattice-based cryptography and zero knowledge rollups in sidechains on public blockchain improve patient ownership security and privacy equivalent to that of private blockchain?"**

1.4 Document Structure

Section	Title	Description
2	Review of Prior Work	Overview of previous research in blockchain, encryption, and lattice-based algorithms
3	Research Methodology	Detailed explanation of the research methods, techniques, and algorithms used
4	Design Specifications	Explanation of the design specifications of the proposed study
5	Implementation of Algorithms	Step-by-step implementation of the NTRU lattice-based algorithm
6	Experimental Results	Presentation of the experimental results
7	Conclusion	Summary and conclusion of the research

2 Related Work

Blockchain technology is transforming healthcare by improving security, privacy, and efficiency in managing medical data. However, quantum computing threatens traditional cryptographic methods, requiring quantum-resistant solutions. Studies show current standards are vulnerable to quantum attacks. Key technologies to address these challenges include quantum-resistant cryptography, encryption, and zero-knowledge roll-ups in side chains. Quantum-resistant lattice-based cryptography defends against quantum decryption, while encryption enables secure data computation, preserving patient privacy. Zero-knowledge roll-ups enhance scalability by efficiently verifying large transaction, and

side chains improve interoperability by allowing secure communication between blockchain networks. These methods defend against quantum threats, enable secure data computation, and improve scalability and interoperability in healthcare systems. By integrating these advancements, healthcare systems can protect patient data, build trust in digital health platforms, and secure patient records against future threats.

2.1 Blockchain

Interest in blockchain technology has increased due to its success in cryptocurrency Narayanan et al. (2016) and its potential to offer reliable, transparent, and efficient services Prashanth Joshi et al. (2018). Blockchain ensures secure, tamper-proof records of participant actions. Treiblmaier and Sillaber (2021) describe blockchain as a distributed, peer-to-peer network that secures digital transactions with immutable records. This section examines blockchain's objectives, contributions, and prior comparisons.Andrew et al. (2023) and Ismail and Materwala (2019) highlight its potential beyond cryptocurrencies, particularly in enhancing data integrity and transparency in patient data management. According to Wright, 2019, it was designed for financial transactions by Nakamoto Wright (2019), and now supports various decentralized applications. Ethereum's use of distributed ledgers enhances data security and transparency Azaria et al. (2016). Recent research underscores blockchain's significance across different domains such as AI, blockchain, and cloud technologies to improve scalability and security in healthcare data management, addressing data privacy and interoperability. It provides a comprehensive review of blockchain's principles highlighting the need for ongoing innovation to tackle emerging challenges like quantum computing.

Singh et al. (2020) review blockchain's potential to enhance security, emphasizing its impact on data integrity and transactional transparency. This review highlights the need for robust security mechanisms in blockchain. Zhang (2022) discuss future trends in blockchain research, highlighting its transformative potential in digital transactions and decentralized applications, and emphasizing on technological advancements in future. In conclusion, previous works collectively highlight blockchain's evolving capabilities and its significant impact across various sectors. These studies highlight the need for ongoing innovation to overcome developing difficulties and improve blockchain's practical applicability. Future research should build on these foundational works, exploring new frontiers in blockchain technology.

2.2 Blockchain In Healthcare

The UK's plan to digitize health records by 2020 was a crucial move to improve healthcare delivery and patient care. But there are some different challenges of healthcare, which needs special interpretation. These issues highlight the dispersion of patient information across numerous systems, underlining the challenges of guaranteeing interoperability and optimal data utilization. Suzuki and Murai (2017) examine the technological and structural hurdles of attaining seamless digital integration. This distinction illustrates the disparity between the aspirational aspirations of healthcare digitalization and the actual limitations of deploying these technologies, particularly in terms of data security and interoperability. This gap is directly related to the scientific research topic of improving encryption and cryptography on public blockchain systems.

According to Kondepogu and Andrew (2022), data encryption alone cannot address the intricacies of healthcare data security, underlining the need for a balance between protection and interoperability. Hossein et al. (2019) suggest blockchain technology as a solution due to its decentralization, enhanced security, and improved interoperability, contrasting with traditional methods Vithanwattana et al. (2016). However, blockchain's transparency poses challenges, careful management of data access and security. Yaqoob et al. (2022) analyse blockchain's features and challenges, recommending further research to address limitations and future implementation strategies. Additionally, integrating blockchain with zk-rollup technology offers promising solutions for secure and scalable healthcare data management.

2.3 Lattice Based Cryptography

Lattice-based cryptography is a promising choice for post-quantum security due to its resistance to quantum assaults. Quantum computers can break traditional cryptographic methods, but blockchain technology using quantum-resistant algorithms offers secure systems, but with slower performance.Zhang (2022) proposed a lattice-based forward security system for data confidentiality. Preece and Easton (2018) introduced a framework using the Diffie-Hellman Key Exchange resistant to quantum attacks. Lattice-based cryptography is important because it provides strong protection against quantum computing attacks. Its complex mathematical basis, using lattice structures and truncated polynomials, makes these methods strong against new threats. As quantum computing advances, the need for quantum-resistant encryption becomes more critical. The development and comparison of various NTRU-based methods highlight progress in achieving secure, efficient cryptographic solutions.
Blockchain addresses EHR limitations by providing a decentralized, secure data storage platform. The Ancile system uses blockchain for data privacy but faces deployment challenges due to smart contract complexities. Azaria et al. (2016) proposed a blockchain system for managing EMR records, improving efficiency but raising concerns about transaction speed and storage capacity. Nguyen et al. (2019) suggested linking multiple EHR systems through a cloud server with intelligent contracts, though data consistency and security remain challenging. Zheng et al. (2018) proposed a real-time health data exchange using blockchain-driven distributed cloud storage, balancing real-time access with storage limitations but introducing external storage vulnerabilities According to Gao et al. (2018) and Hölbl et al. (2018), integrating blockchain in EHRs can lead to better patient care and data management. As stated by Hoffstein et al. (1998), NTRU-based encryption is a pioneering lattice-based cryptographic method designed to resist quantum attacks. López-Alt et al. (2012) enhanced NTRU with a multikey encryption scheme, allows encrypted data to be processed under multiple unrelated keys. Nisha et al. (2024) discussed a post-quantum blockchain architecture for IoT, emphasizing NTRU's security and performance benefits. However, NTRU's complex mathematical structures can impact computational efficiency, posing challenges in practical applications.

2.4 Zero Knowledge Rollups in Sidechains

In the shifting world of identity management, Zero Knowledge Proofs (ZKPs) have emerged as advanced cryptographic tools, offering revolutionary solutions for identity

sharing within blockchain. These technologies verify information without exposing sensitive data, ensuring transaction accuracy while preserving privacy. The integration of Self-Sovereign Identity (SSI) principles, blockchain, and ZKPs provides users with unparalleled control, security, and privacy over their digital identities. ZKPs allow users and organizations to assert their identities without disclosing sensitive information, enhancing privacy and transaction accuracy. Partala et al. (2020)emphasized on the role of non-interactive ZKPs in blockchain for secure transactions without intermediaries, while studies by Ren et al. (2019)) and Al-Aswad et al. (2019) utilized interactive ZKPs to protect user identities and medical data, respectively. Jo et al. (2022a) and Zheng et al. (2022) examined ZKP applications in public health and insurance claims. Jo et al. (2022b) developed a blockchain framework for COVID-19 contact tracing using zero-knowledge range proofs, balancing privacy with public health needs. It used zk-SNARKs to ensure medical data privacy in insurance transactions. The versatility of ZKP protocols is demonstrated across various sectors.

Hou et al. (2022) applied zk-SNARKs in energy trading to verify bid accuracy without revealing private data.Zhang (2022) combined interactive ZKP technology with blockchain to protect privacy in music education. Uj et al. (2020) proposed a blockchain and ZKP framework for COVID-19 contact tracing, protecting location privacy. Zheng et al. (2018) combined zk-SNARKs, homomorphic encryption, and the Schnorr protocol to ensure privacy in medical data transactions. Rasheed et al. (2022) introduced an Inter-ZKP system for IoT networks, enhancing data traceability and authentication. Bai et al. (2022)) used zk-SNARKs to ensure privacy in healthcare identity authentication. Gai et al. (2022) proposed using blockchain and Zero Knowledge Proofs (ZKPs) to protect vessel identities during data sharing in maritime transportation. It underscores the critical role of ZKPs in enhancing privacy and security across various sectors. By securing identity sharing and data processing without disclosing sensitive information, ZKPs pave the way for the future of digital identity management. Further research is essential to fully exploit their potential, especially in combining ZKPs with blockchain for secure and private identity management in our increasingly digital world.

2.5 Summary of Literature Review and Proposed Method

The literature review highlights blockchain technology's transformative potential in healthcare by enhancing security, privacy, and efficiency in managing medical data. Current cryptographic methods, however, are vulnerable to quantum computing threats, necessitating quantum-resistant solutions. Key technologies like quantum-resistant cryptography and zero-knowledge roll-ups within sidechains are crucial. Blockchain has demonstrated improvements in data integrity, transparency, and interoperability, with lattice-based cryptography providing robust protection against quantum attacks. Encryption ensures privacy by allowing encrypted data processing without decryption, and zero-knowledge roll-ups and sidechains enhance scalability and efficiency by aggregating transactions and enabling secure communication between networks. The proposed research introduces a hybrid encryption model that leverages these advanced cryptographic techniques to enhance security, privacy, and scalability in healthcare data management. This approach secures data against quantum threats, improves transaction handling, and empowers patients to manage their medical records, enhancing trust in digital health platforms. It addresses critical gaps in current methodologies and builds on existing studies, contributing to more secure and efficient blockchain-based healthcare systems.

Access to diverse medical data is essential for epidemiological research and diagnostic algorithm development, providing insights into healthcare service efficiency and areas for improvement. This is particularly important for rare diseases, where data can save lives or improve quality of life. Selling medical information, while not always the primary goal, can provide financial resources for individuals' medical needs. Despite extensive research, blockchain technology in healthcare still needs better security, privacy, scalability, and speed. In conclusion, integrating quantum-resistant cryptography, homomorphic encryption, and zero-knowledge roll-ups offers a promising solution for secure, scalable, and efficient healthcare systems, ensuring patient data privacy and security in an increasingly digital world. Continued innovation in blockchain technology is necessary to address evolving challenges in healthcare data management.

3 Methodology

The research reported in this paper aims to greatly improve patient data security, ownership and privacy, there by addressing a major gap in the healthcare business. This is achieved by using NTRU lattice-based cryptography combined with blockchain technology. The results will be evaluated based on security, privacy, and ownership. This section gives an overview of the approach, methods, and procedures used in our study.

3.1 Public Blockchain

A public blockchain is a decentralized network that anyone can join and participate in without needing permission. It secures data using cryptographic algorithms and ensures that transactions are visible and immutable. In healthcare, public blockchains enhance data security and privacy, improve data integrity, and enable seamless data sharing across different systems. This interoperability leads to better care coordination and more accurate treatments. Public blockchains also reduce costs by eliminating intermediaries and lowering administrative overhead. They empower patients by giving them control over their health data and provide transparency to track data use. Additionally, public blockchains prevent fraud and streamline clinical trials, ensuring compliance and authenticity of trial data. These benefits make public blockchains a powerful tool to improve the efficiency, security, and reliability of healthcare systems. While the use of a public blockchain introduces a small cost for each transaction and a delay in completing registration or access to an electronic health record (EHR), it allows any party worldwide to access health records securely. Unlike private blockchains, which restrict access to authorized entities or consortium blockchains, managed by a limited number of entities, a public blockchain provides a more distributed and accessible solution. Combining a widespread digital identity with a public blockchain and a new mechanism for controlled access to e-health records enables patients to share their health records securely Lax et al. (2024).

3.2 Practical Byzantine Fault Tolerance Algorithm (PBFT)

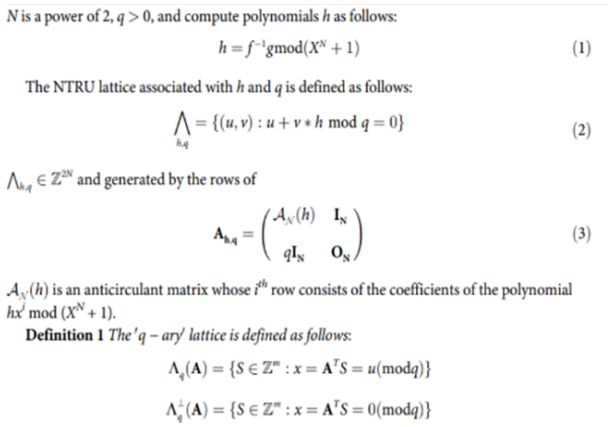
The Practical Byzantine Fault Tolerance (PBFT) algorithm is a consensus mechanism designed to ensure reliability and security in distributed networks, particularly blockchain systems. Developed by Miguel Castro and Barbara Liskov, PBFT effectively addresses Byzantine faults, which include system failures and malicious attacks. In blockchain, a

consensus mechanism is a technique that brings distributed processes or systems together to agree on a single data value. It assures that all network members agree on transaction validity, hence ensuring the blockchain's integrity and security. PBFT operates through a three-phase process involving pre-prepare, prepare, and commit stages to achieve consensus among nodes, ensuring that the network can withstand up to one-third of its nodes being faulty or compromised. This makes PBFT highly efficient and secure for applications requiring rapid finality and fault tolerance. In the context of healthcare, PBFT offers significant advantages for maintaining the privacy and security of medical records. By ensuring data integrity and preventing unauthorized access, PBFT helps create a tamper-proof environment where medical records are consistently verified and protected against malicious alterations. This consensus mechanism enables healthcare systems to maintain accurate and reliable records, crucial for patient care and confidentiality. Furthermore, the efficiency of PBFT in achieving consensus quickly makes it ideal for healthcare settings where timely data access is essential. Integrating PBFT with blockchain technology in healthcare can thus enhance data security, ensure patient privacy, and improve the overall reliability of healthcare information systems. These advantages are critical for safeguarding sensitive medical information from unauthorized access and preserving data integrity throughout the network.

3.3 N-th Degree Truncated Polynomial Ring Units (NTRU) Algorithm

NTRU, short for "N-th Degree Truncated Polynomial Ring Units," is a public-key cryptosystem based on lattice-based cryptography, known for its strong mathematical foundations. Lattice-based cryptography is an advanced cryptosystem that ranks first in the post-quantum cryptosystem. By leveraging truncated polynomials and lattice structures, NTRU creates encryption algorithms resistant to quantum computer attacks Hussein et al. (2023). It is highly efficient, enabling quick encryption and decryption, making it ideal for devices with limited computational power. One key advantage is its scalability, offering different levels of security based on chosen parameters. However, selecting the right parameters is complex and critical for security, and NTRU often requires bigger key sizes than previous approaches such as RSA Yuan et al. (2023). Lattice-based encryption, such as NTRU, is highly adaptable and essential for modern data protection, meeting various security needs Latha et al. (2023). Its versatility ensures suitability across different security settings, enhancing practical applications Aikata et al. (2023).
Combining NTRU with blockchain technology can significantly enhance the security and privacy of healthcare data. This integration ensures that sensitive information is encrypted and securely stored, with blockchain providing an immutable ledger that maintains data integrity and offers a reliable audit trail. This combination supports real-time healthcare applications, ensuring quick access to secure data while giving patients better control over their information Redkins et al. (2023). Additionally, it can streamline administrative processes, reduce fraud, and improve the accuracy of patient records by eliminating duplicate entries and ensuring data consistency. The interoperability of blockchain facilitates secure sharing of patient data across different healthcare providers, enhancing coordination and improving patient outcomes. Moreover, using NTRU with blockchain can support compliance with stringent regulatory requirements, ensuring that patient data protection standards are met. In summary, integrating NTRU with blockchain greatly improves the security, privacy, and integrity of healthcare data, offering a robust

solution for protecting sensitive patient information. Figure 1 explains computation of polynomials in the context of NTRU lattice-based cryptography and the structure of the lattice and its related matrix forms.



N is a power of 2, $q > 0$, and compute polynomials h as follows:

$$h = f^{-1} g \bmod (X^N + 1) \tag{1}$$

The NTRU lattice associated with h and q is defined as follows:

$$\bigwedge_{h,q} = \{(u, v) : u + v * h \bmod q = 0\} \tag{2}$$

$\bigwedge_{h,q} \in \mathbb{Z}^{2N}$ and generated by the rows of

$$\mathbf{A}_{\mathbf{h},\mathbf{q}} = \begin{pmatrix} \mathcal{A}_N(h) & \mathbf{I_N} \\ q\mathbf{I_N} & \mathbf{O_N} \end{pmatrix} \tag{3}$$

$\mathcal{A}_N(h)$ is an anticirculant matrix whose i^{th} row consists of the coefficients of the polynomial $hx^i \bmod (X^N + 1)$.

Definition 1 *The 'q − ary' lattice is defined as follows:*

$$\Lambda_q(\mathbf{A}) = \{S \in \mathbb{Z}^m : x = \mathbf{A}^T S = u(\bmod q)\}$$

$$\Lambda_q^{\perp}(\mathbf{A}) = \{S \in \mathbb{Z}^m : x = \mathbf{A}^T S = 0(\bmod q)\}$$

Figure 1: NTRU Lattice

3.4 Smart Contracts

A smart contract consists of a state identifiable by its unique address and executable code, usually created in Solidity. Once signed by all participants, a transaction with the necessary parameters is added to the blockchain. Miners validate and record this transaction, creating a unique contract address. Users activate the contract by delivering a transaction validated by state variables and oracles. When conditions are met, miners execute and validate the response. Smart contracts act as autonomous agents, executing rules and logic to govern blockchain transactions. They facilitate agreements without intermediaries and enable seamless interactions between the main blockchain and sidechains. Developed using serverless cloud services or custom scripts, these contracts ensure robust privacy and security protocols. The MedRec project in Israel is developing smart contracts for exchanging medical records between clinics. Health Minister Veronika Skvortsova stated that blockchain could securely store electronic medical records, preserving confidentiality and allowing patients to control data disclosure. Vladimir Demin previously announced plans to implement distributed ledger technology in the Ministry of Health's system Novikov et al. (2018)

3.5 Evaluation Parameters

The five parameters used for the evaluation are scalability, latency, security, privacy, and ownership.

Scalability: It will evaluate assess the system's ability to handle increasing volumes of data and users efficiently. This would entail assessing the decentralized infrastructure to make sure it can manage data growth without compromising performance. It is backed by sidechain technologies and cloud services. Transaction throughput, data storage capacity, and user load management will be important KPIs. Our goal is to make sure that the system can handle the exponential growth in health data while maintaining excellent

performance and reliability.

Latency: The time which is required to upload and then securely process a medical record is used as a significant performance metric. Our approach entails uploading a medical record, fully encrypting it, storing it on blockchain nodes, and making it available only to authorized individuals. This method assesses not just the effectiveness of our encryption and data management technologies, but also the system's overall response to real-world events.

Security: Our goal is to create and uphold a robust protection system by using NTRU algorithm such that it defends against both known and emerging cyberthreat's in healthcare industry. We will carefully monitor the performance of our encryption algorithms to ensure they provide and maintain the highest level of security.

Privacy: We'll go over the technical and legal compliance aspects of privacy evaluation, with an emphasis on the system's capacity to protect patient data under various circumstances, such as data sharing and monetization. HIPAA (Health Insurance Portability and Accountability Act) regulations will be adhered in our approach.

Ownership: A thorough method is used in ownership testing to confirm that the ethical and legal frameworks pertaining to patient data ownership are sound. This covers how to control access privileges, permit patients to share data at their choice, and facilitate the removal of data access. Our review will determine how well the system upholds patients' rights to privacy regarding their personal health information. Our goal is to demonstrate that patients have unquestionable ownership and control over their medical information using our blockchain technology through scenario-based testing and legal research.

3.6 Ethical Issues and Consideration of Research

The two ethical issues and consideration of research are as follows:

Data Anonymization: Even in cases where medical records are encrypted, data anonymization is a vital precaution against the possibility of someone being able to re-identify themselves from such records. Re-identification is a constant concern, even with robust encryption. We'll make sure patient data is appropriately anonymised. We'll use state-of-the-art methods like pseudonymization and differential privacy in our anonymization process. Our goal is to ensure that the danger of re-identification is statistically small by introducing a layer of randomness and removing direct identifiers from health data.

Data Privacy: Our top priority is protecting patient privacy since maintaining patient trust in our blockchain-based data management system is vital. To protect sensitive patient data, including identifying and medical information, we employed zero-knowledge proofs in sidechains, and other state-of-the-art encryption approaches. These cryptographic algorithms ensure privacy even during complex data analysis by allowing for the secure processing of encrypted data without betraying its contents. As part of our commitment to promoting a culture of privacy, we provide privacy, security, and ethical

use of health information training to all staff members handling data. Furthermore, our technology conforms with strict GDPR and HIPAA regulations on data privacy.

4 Design Specification

4.1 Proposed Research Architecture

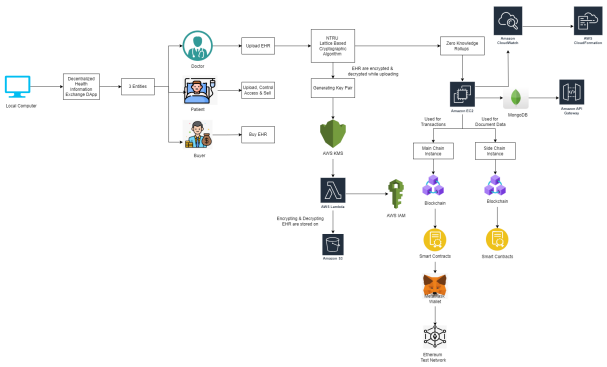


Figure 2: Architecture Diagram

This architecture diagram in Figure 2 illustrates a decentralized health information exchange system that utilizes three algorithms, blockchain, and AWS cloud services. Developers push their code from local computers to a private GitHub repository. The system involves three entities: Doctor, Patient, and Buyer. Each must sign up on the platform, have a Metamask wallet for signing in, and possess some test ethers for transactions. Doctors can upload, delete, and view reports via their dashboard. Once a doctor uploads a report, they cannot make further changes unless the patient grants permission. The uploaded report becomes available on the patient's dashboard. Patients can view, delete, control access, and even sell their reports to earn revenue. Buyers can purchase reports through their dashboard. Each upload or purchase transaction incurs a small gas fee. Transactions are managed by the main blockchain, while a side chain handles document data. When a patient or doctor uploads electronic health records (EHR), NTRU lattice-based cryptography algorithm generate key pairs and encrypt the EHR. AWS KMS is used to ensure secure key management. The function checks for both the encrypted data and the key, decoding them from base64 if present. AWS KMS decrypts the AES key, which is then used to extract the initialization vector (IV) from the first 16 bytes of the encrypted data. Using the crypto module, a decipher is created with the aes-256-cfb algorithm, the AES key, and the IV, allowing the encrypted data to be decrypted and converted back to a base64 string. This process demonstrates AWS KMS's secure key management in protecting sensitive information. Only pdf and text files are considered for EHR. Zero Knowledge Rollups algorithm is implemented on AWS EC2 instances. There are two instances: the blockchain instance, which manages all blockchain transactions including transferring ownership and access controls, and the backend instance, which handles document data. MongoDB stores all user data. Smart Contracts are written in Solidity, with Metamask wallet and Ethereum test network facilitating all transactions. Further AWS Amazon API Gateway is used for API calls, AWS IAM is

used for managing the access permissions, AWS Cloud Watch is used for monitoring the web application and AWS Cloud Formation is used for provisioning services.

4.2 NTRU Lattice Based Cryptography Algorithm

In this implementation, the NTRU lattice-based cryptographic algorithm is used to secure medical records on a blockchain. The process starts by generating a key pair using crypto for creating a public and private key. A message, which includes an IPFS hash and encrypted data, is signed with the private key to produce a digital signature. The encrypted data and its digital signature are then securely stored on the blockchain via smart contracts. This approach ensures robust security and privacy for medical records, leveraging advanced cryptographic techniques.

4.3 Blockchain Nodes and Zero Knowledge Rollups in Sidechains

A decentralized file marketplace is implemented using Solidity on the Ethereum blockchain, where zero-knowledge rollups and sidechains are used to enhance privacy and efficiency. The main blockchain handles transactions while sidechains store sensitive medical records. Users can upload files with an IPFS hash, set a price, and mark them for sale, creating a new file entry in the system. Buyers can purchase these files by sending the specified amount of Ether, transferring ownership and removing the file from the sale. Owners can update file prices, ensuring dynamic pricing. Events are emitted for uploads, purchases, and price updates to maintain transparency. The system also provides functions to retrieve file details and list all file IDs. By leveraging zero-knowledge rollups, the system ensures that medical records stored on sidechains remain confidential while the main chain manages secure, transparent transactions, achieving a robust and privacy-focused marketplace.

4.4 Docker

In this system, Docker is utilized to manage the deployment of blockchain nodes that track medical records. Docker containers encapsulate the blockchain nodes, ensuring consistent environments for running the blockchain software and managing medical records efficiently. This setup allows for seamless operation and scaling of blockchain nodes, ensuring high availability and reliability. The use of Docker ensures that each node is isolated and secure, creating a robust infrastructure for maintaining the integrity and accessibility of medical records on the blockchain.

4.5 Key Management Service (KMS)

AWS Key Management Service (KMS) is used to securely decrypt data. First, the AWS KMS client is set up to enable cryptographic operations. The function checks for encrypted data and encrypted key in the request, returning an error if either is missing. The encrypted data and AES key are decoded from base64. The AES key is decrypted using KMS, which ensures secure key management. With the decrypted AES key, the function extracts the initialization vector (IV) from the first 16 bytes of the encrypted data. Using the crypto module, it creates a decipher with the aes-256-cfb algorithm, the

AES key, and the IV. The ciphertext is then decrypted and converted back to a base64 string. This decrypted data is returned in the response, demonstrating how AWS KMS securely handles key decryption to protect sensitive data.

4.6 Data in Rest

When a doctor or patient uploads a medical report, the file is initially converted into a Base64 format. This Base64 encoded file is then sent to AWS Lambda for encryption. Once the file is encrypted, we receive two items in response: the encrypted Base64 string and a public key. When someone needs to view the file, they must provide both the encrypted file and the public key obtained earlier. The private key, necessary for decryption, is securely managed by AWS Key Management Service (KMS). The only information passed in the request is the Amazon Resource Name (ARN) of the key, allowing AWS Lambda to identify the correct key for decryption.

4.7 Data in Transit

Ensure all communications between application and the blockchain are encrypted using transport layer security (TLS) to maintain security during transmission.

4.8 HIPPA Compliance

The decentralized health exchange portal complies with Health Insurance Portability and Accountability Act (HIPPA) compliant ensuring that patient information remains protected. The key factors included are:

Privacy Rule: It is crafted to protect patient's medical records and other personal health information (PHI). This regulation ensures the protection of individual health data while enabling the essential flow of information necessary for providing superior healthcare. In our app, only doctors with patient-granted access can view the reports. Once a doctor uploads a report, ownership is seamlessly transferred to the patient via blockchain technology. This advanced system guarantees that only authorized individuals, as designated by the patient, can access their information, thus maintaining confidentiality and ensuring disclosures are made only when legally necessary and permissible.

Security Rule: It establishes guidelines for the safeguarding of electronic protected health information (ePHI). Here we have implemented zero knowledge rollups in sidechains to ensure that data remains secure throughout, from unauthorized access, alteration, deletion, or transmission. Data remains encrypted at rest using AES 256 and while in transit using transport layer security (TLS) during transactions.

4.9 Auditing and Monitoring

We maintain comprehensive logs of access and modifications to PHI by leveraging AWS CloudWatch and CloudTrail services to ensure our audit trails are detailed and reliable. Where appropriate, we employ blockchain technology for immutable audit trails, guaranteeing that the logs themselves do not contain any PHI. This robust monitoring system ensures the highest level of security and accountability across our entire portal.

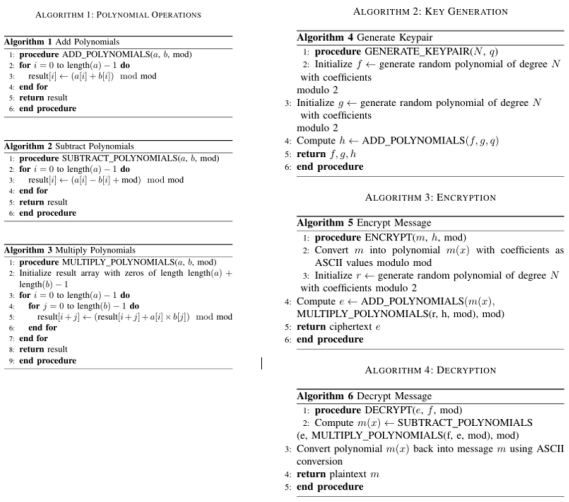
5 Implementation

5.1 Tools and Languages Used

Our decentralized web application (DApp) utilizes a state-of-the-art technology stack to provide users with an efficient and seamless experience. For the frontend, we have chosen React JS, a widely acclaimed JavaScript library is notable is known for its versatility and efficacy in creating dynamic user interfaces. With React JS, we can build dynamic and responsive user interfaces that update in real-time in response to user interactions and data changes. In developing the backend, we rely on NodeJS and Express JS. NodeJS is a JavaScript runtime environment that facilitates server-side scripting, enabling us to create scalable and high-performance applications. Its non-blocking I/O approach allows for efficient handling of several requests at once. Meanwhile, Express JS is a web application framework that streamlines the development process by offering tools to simply build routes and manage requests easily, which is crucial for handling the diverse functions of a DApp.
To write our smart contracts, we use Solidity, a programming language designed primarily for creating smart contracts on blockchain platforms like Ethereum. These smart contracts execute themselves, with the conditions of the agreement contained in the code itself. We initially test these contracts locally using Ganache, which simulates the Ethereum blockchain environment, offering a secure testing space before deployment to the live blockchain. After thorough testing, the smart contracts are deployed onto the cloud main chain to ensure proper functionality in real-world scenarios. For development and testing, we use the Ethereum Test Network, which provides a sandbox environment resembling the main Ethereum network but uses test ethers. This allows us to perform transactions safely without any financial implications. To facilitate user interactions with the Ethereum blockchain, we integrate Metamask, a popular Ethereum wallet application. MetaMask serves as an interface between users and the blockchain, providing access to their Ethereum wallets via a browser extension or mobile app. It enables users to securely store and manage their cryptocurrency while seamlessly connecting with decentralized applications. By integrating MetaMask with our DApp, users can securely conduct transactions and verify their identities on the blockchain.

5.2 Lattice Based Cryptography

In Figure 3, NTRU key generation is achieved by first creating two random private polynomials f and g using the generateRandomPolynomial function. These polynomials have coefficients randomly chosen from the set 0, 1. The public key h is then generated by adding f and g using the addPolynomials function, with the sum taken modulo q. The resulting polynomials f, g, and h form the key pair, where f and g are the private keys and h is the public key used for encryption. Further, NTRU is used for encrypting and decrypting data that is uploaded to and retrieved from AWS S3 storage. During the upload process, the data is encrypted using the NTRU algorithm with the public key h before being stored in S3. When a file is retrieved, it is decrypted using the corresponding private key f. This ensures that the data is securely encrypted before storage and can only be decrypted by someone with access to the private key, leveraging the NTRU cryptosystem for enhanced security.



Algorithm 1: Polynomial Operations

Algorithm 1 Add Polynomials

```
procedure ADD_POLYNOMIALS(a, b, mod)
for i = 0 to length(a) − 1 do
    result[i] ← (a[i] + b[i]) mod mod
end for
return result
end procedure
```

Algorithm 2 Subtract Polynomials

```
procedure SUBTRACT_POLYNOMIALS(a, b, mod)
for i = 0 to length(a) − 1 do
    result[i] ← (a[i] − b[i] + mod) mod mod
end for
return result
end procedure
```

Algorithm 3 Multiply Polynomials

```
procedure MULTIPLY_POLYNOMIALS(a, b, mod)
Initialize result array with zeros of length length(a) + length(b) − 1
for i = 0 to length(a) − 1 do
    for j = 0 to length(b) − 1 do
        result[i + j] ← (result[i + j] + a[i] × b[j]) mod mod
    end for
end for
return result
end procedure
```

Algorithm 2: Key Generation

Algorithm 4 Generate Keypair

```
procedure GENERATE_KEYPAIR(N, q)
Initialize f ← generate random polynomial of degree N with coefficients modulo 2
Initialize g ← generate random polynomial of degree N with coefficients modulo 2
Compute h ← ADD_POLYNOMIALS(f, g, q)
return f, g, h
end procedure
```

Algorithm 3: Encryption

Algorithm 5 Encrypt Message

```
procedure ENCRYPT(m, h, mod)
Convert m into polynomial m(x) with coefficients as ASCII values modulo mod
Initialize r ← generate random polynomial of degree N with coefficients modulo 2
Compute e ← ADD_POLYNOMIALS(m(x), MULTIPLY_POLYNOMIALS(r, h, mod), mod)
return ciphertext e
end procedure
```

Algorithm 4: Decryption

Algorithm 6 Decrypt Message

```
procedure DECRYPT(e, f, mod)
Compute m(x) ← SUBTRACT_POLYNOMIALS(e, MULTIPLY_POLYNOMIALS(f, e, mod), mod)
Convert polynomial m(x) back into message m using ASCII conversion
return plaintext m
end procedure
```

Figure 3: NTRU Lattice Cryptography Implementation

5.3 Zero Knowledge Rollups Implementation

There are two types of chains: the main chain and the side chain. The main chain in Figure 4 handles all transactions using Metamask and the Ethereum test network. In the code, a smart contract is designed for managing document ownership on the Ethereum mainnet. This contract allows users to upload documents by storing their S3 URLs and encryption keys on the blockchain, linking them to the uploader's address.

Algorithm 7 Document Ownership Management (Main Chain)

```
Initialize:
    documentCount ← 0
    documents ← empty mapping from s3Url to Document structure
    documentIds ← empty mapping from documentId to s3Url
procedure UPLOAD_DOCUMENT(s3Url, encryptionKey, msgSender)
    Increment documentCount
    Create a new Document:
        owner ← msgSender
        s3Url ← s3Url
        encryptionKey ← encryptionKey
    Store Document in documents mapping using s3Url as the key
    Map documentCount to s3Url in documentIds
    Emit Event: DocumentUploaded(documentCount, msgSender, s3Url, encryptionKey)
procedure TRANSFER_OWNERSHIP(s3Url, newOwner, feeRecipient, msgSender, fee)
    Retrieve document from documents mapping using s3Url
    Require that document.owner = msgSender
    Require that fee > 0
    Transfer fee to feeRecipient
    Update document.owner ← newOwner
function GET_DOCUMENT_BY_S3URL(s3Url)
    Retrieve document from documents mapping using s3Url
    Return (document.owner, document.s3Url, document.encryptionKey)
function ADDRESS_TO_STRING(address)
    Convert address to a hexadecimal string
    Return string representation of the address
```

Algorithm 8 Document Metadata Management (Side Chain)

```
procedure DOCUMENT_METADATA_MANAGEMENT
    Initialize:
        documentMetadata ← empty mapping from docpath to DocumentMetadata structure
procedure SAVE_DOCUMENT(docpath, verificationStatus, additionalInfo)
    Store:
        verificationStatus ← verificationStatus
        additionalInfo ← additionalInfo
    Update documentMetadata mapping with the given docpath
    Emit Event: DocumentVerified with docpath and verificationStatus
    Emit Event: DocumentMetadataUpdated with docpath and additionalInfo
procedure VERIFY_DOCUMENT(docpath, verificationStatus)
    Retrieve metadata from documentMetadata using docpath
    Update metadata.verificationStatus ← verificationStatus
    Emit Event: DocumentVerified with docpath and verificationStatus
procedure UPDATE_DOCUMENT_METADATA(docpath, additionalInfo)
    Retrieve metadata from documentMetadata using docpath
    Update metadata.additionalInfo ← additionalInfo
    Emit Event: DocumentMetadataUpdated with docpath and additionalInfo
function GET_DOCUMENT_METADATA(docpath)
    Retrieve metadata from documentMetadata using docpath
    Return verificationStatus and additionalInfo
end procedure
```

Figure 4: Zero Knowledge Rollups

Users can transfer document ownership to a new owner by paying a fee to a designated recipient. On the side chain in Fig. 5, a different smart contract provides functions to save, verify, and update document metadata on the blockchain. zk-rollups, a layer 2 scaling solution, enable multiple transactions to be processed off-chain while only submitting a summary on-chain. This approach ensures scalability and reduces gas costs. The side chain is used for storing all document data. In the context of zk-rollups, this auxiliary contract interacts with a zk-rollup system by storing document verification statuses and metadata, which are validated off-chain using zero-knowledge proofs, and then updating the main chain with the results.

5.4 Key Management Service

AWS Key Management Service (KMS) is used to securely decrypt data. First, the AWS KMS client is set up to enable cryptographic operations shown in Figure 5. The function checks for encrypted data and encrypted key in the request, returning an error if either is missing. The encrypted data and AES key are decoded from base64. The AES key is decrypted using KMS, which ensures secure key management. With the decrypted AES key, the function extracts the initialization vector (IV) from the first 16 bytes of the encrypted data. Using the crypto module, it creates a decipher with the aes-256-cfb algorithm, the AES key, and the IV. The ciphertext is then decrypted and converted back to a base64 string. This decrypted data is returned in the response, demonstrating how AWS KMS securely handles key decryption to protect sensitive data. Further, Data in Transit i.e. When a doctor or patient uploads a medical report, the file is initially converted into a Base64 format. This Base64 encoded file is then sent to AWS Lambda for encryption. Once the file is encrypted, we receive two items in response: the encrypted Base64 string and a public key. When someone needs to view the file, they must provide both the encrypted file and the public key obtained earlier. The private key, necessary for decryption, is securely managed by AWS Key Management Service (KMS). The only information passed in the request is the Amazon Resource Name (ARN) of the key, allowing AWS Lambda to identify the correct key for decryption. Further Data in rest, ensures all communications between application and the blockchain are encrypted using transport layer security (TLS) to maintain security during transmission

Algorithm 9 Encrypt PDF

ENCRYPT_PDFreq, res pdf_data ← req.body.pdf_data encrypted_key ← ”arn:aws:kms:eu-west-1:195418205110:key/5oF6908B-1b76-4e2e-8B05-9d06748adf0f” imgBody ← { ”pdf_data”: pdf_data, ”key”: encrypted_key } response ← await axios.post(”https://okxwbv54b.execute-api.eu-west-1.amazonaws.com/dev/encrypt-pdf”, imgBody) res.status(200).json(response.data) error console.log(error) res.status(500).json({”error”: ”error”})

Algorithm 10 Decrypt PDF

DECRYPT_PDFreq, res encrypted_data ← req.body.encrypted_data encrypted_key ← req.body.encrypted_key imgBody ← { ”encrypted_data”: encrypted_data, ”key”: encrypted_key } response ← await axios.post(”https://2vhwxb1q.execute-api.eu-west-1.amazonaws.com/dev/decrypt-pdf”, imgBody) res.status(200).json(response.data) error console.log(error) res.status(500).json({”error”: ”error”})

Figure 5: KMS Implementation

5.5 Blockchain Implementation

Blockchain transactions are first tested locally using Ganache, as shown in Figure 6 and Figure 7, are then deployed to the cloud for further use.

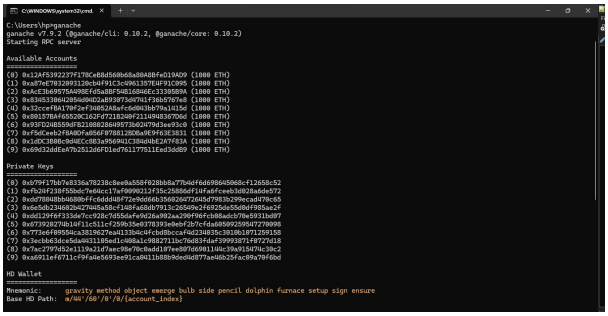


Figure 6: Locally Tested Ganache Transactions

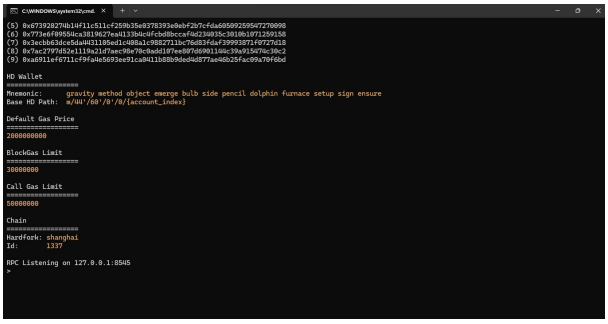


Figure 7: Locally Tested Ganache Transactions

5.6 Cloud Implementation

AWS KMS is used to ensure secure key management. Zero Knowledge Rollups algorithm is implemented on AWS EC2 instances. Further AWS Amazon API Gateway is used for API calls, AWS IAM is used for managing the access permissions, AWS Cloud Watch is used for monitoring the web application and AWS Cloud Formation is used for provisioning services. AWS S3 bucket is used for deploying the decentralized web application. And further another bucket of AWS S3 is used for storing all the encrypted and decrypted electronic medical records (EHR).

5.7 Decentralized Web Application

Below are the snippets of the web application.

- The Home Page shown in Figure 8 requires users to sign up and then log in with the same credentials. To sign up, users must have their own MetaMask wallet and some Ethereum test ethers.
- The Patient Dashboard shown in Figure 9 provides an overview of available reports, the number of reports listed for sale, the number of reports sold, and the revenue generated. Patients can upload their reports here, and any reports uploaded by doctors are automatically visible on this dashboard. From this interface, patients can also update report prices, delete reports, view them, and manage who has access to view their reports.

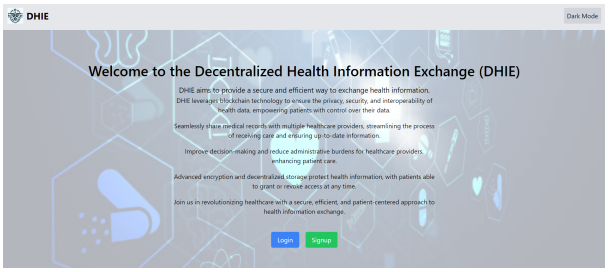


Figure 8: Home Page

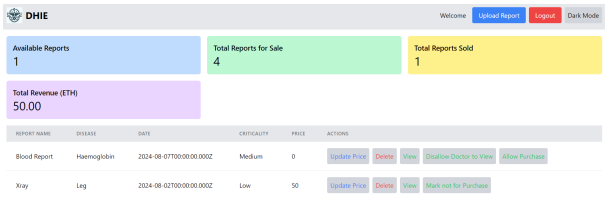


Figure 9: Patient Dashboard

- One of the most compelling reasons for a patient to allow them to sell reports is to contribute valuable data that could lead to breakthroughs in understanding specific conditions, assessing the effectiveness of treatments, and uncovering previously unnoticed patterns that require further investigation. This type of data is crucial for epidemiological research and the development of advanced diagnostic algorithms. By analyzing a wide range of medical records, we can gain insights into the efficiency of healthcare services, identify gaps in the system, and pinpoint areas where patient care can be enhanced. This, in turn, could lead to improved healthcare practices and policies for future patients. Particularly in the case of rare or under-researched diseases, such data contributions could save lives or improve the quality of life for others facing similar conditions. Although it may not always be the primary motivation, selling medical information can also provide individuals with financial support to meet their own medical needs and improve their quality of life. One of the most recent disease in which this can be helpful is COVID-19 pandemic.

- Doctors can upload reports on their dashboard shown in Figure 10, which will automatically be accessible to patients on their respective dashboards. Once a doctor uploads a report, they cannot make any changes or perform any actions on it unless the patient grants them access.

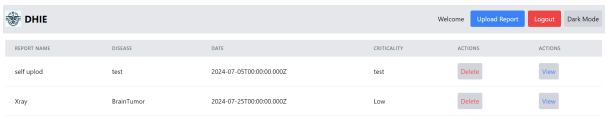


Figure 10: Doctor Dashboard

- Buyer can purchase the reports from the buyer's dashboard shown in Figure 11.

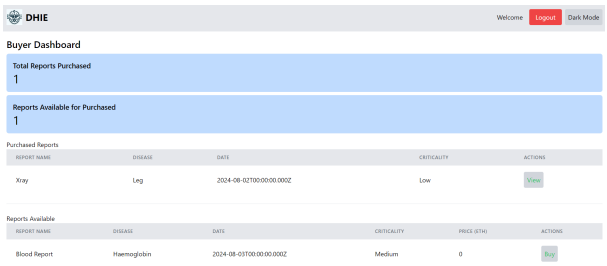


Figure 11: Buyer Dashboard

- The source code is available on GitHub, a platform for open-source version control and code storage and can be accessed using link below.

  GitHub Link: https://github.com/darshikapongallu/x22197222$_DHIE$

  Application Hosted Link: http://medirecords101.s3-website-eu-west-1.amazonaws.com/

6 Evaluation

This section shows that the proposed system improves patient ownership, security and privacy.

6.1 Data Ownership, Privacy and Security

Doctors can manage reports through their dashboard, where they can upload, delete, and view them. However, after a doctor uploads a report, they cannot modify it further without the patient's permission. Once uploaded, the report appears on the patient's dashboard. Patients can view, delete, control access to, and even sell their reports to earn revenue. For enhanced security and privacy, the system integrates two powerful algorithms: NTRU algorithm and Zero Knowledge Rollups on sidechains. This combination ensures the system's privacy and security, protecting sensitive information effectively.

6.2 Experiment / Case Study 1

- The graph in Figure 12 illustrates the data transfer amounts in gigabytes (GB) versus the number of health records for two different systems: client/server and blockchain. The quantity of health records increases, as does the volume of data exchanged by both the client/server and blockchain systems. However, the blockchain system consistently transfers more data than the client/server system, indicating a higher data overhead. Initially, the estimated data transfers (represented by dashed lines) show that the client/server system transfers less data. But as the number of records grows, the data transfer rate for the client/server system increases sharply, demonstrating a significant rise in data load with the increase in health records. Overall, the graph demonstrates that while blockchain offers certain advantages,

it requires significantly more data transfer compared to a traditional client/server system, especially when number of health records increases.

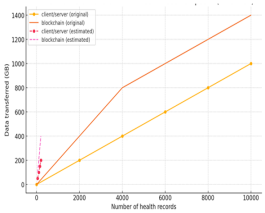


Fig.12 Amount of data sent for health record updates

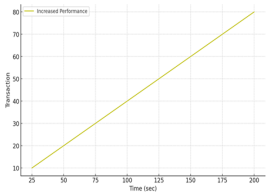


Fig. 13 Analysis of the performance of transmission time

- The graph in Figure 13 illustrates the relationship between transaction time (in seconds) and the number of transactions. Key observations from the graph indicate a linear increase in the number of transactions over time. As time progresses from 25 seconds to 200 seconds, the number of transactions steadily rises from 10 to 80. This consistent growth demonstrates efficient handling and processing of transactions over the given period. This graph indicates that transaction performance improves consistently over time, suggesting efficient handling of transactions within the given period.

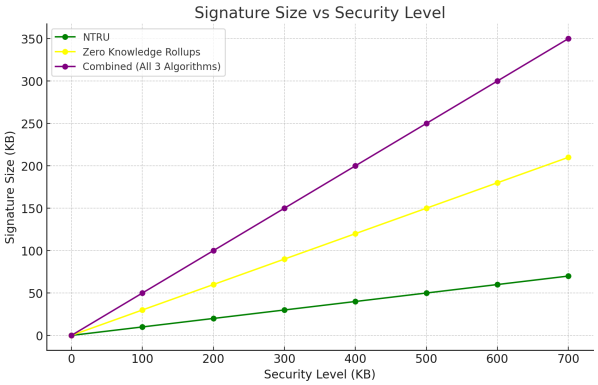


Figure 14: Amount of data sent for health record updates

- The graph in Figure 14 compares the signature sizes (in KB) of different encryption methods against varying security levels (also in KB). Key observations from the graph indicate different trends in signature size as security levels increase for various algorithms. NTRU shows a steady but gradual increase in signature size. Zero Knowledge Rollups display a moderate increase in signature size, steeper than Homomorphic Encryption, indicating that more data is required as security improves. The Combined approach, utilizing all two algorithms, shows the highest increase in signature size, reflecting the cumulative effect and leading to significantly larger signatures as security levels rise. Overall, the graph demonstrates that while combining all three algorithms provides highest security, and results in the largest signature sizes, emphasizing the trade-off between security and data overhead.

7 Conclusion and Future Work

7.1 Conclusion

This research effectively presents a secure and efficient framework for managing medical records using blockchain technology and advanced cryptographic techniques. Incorporating Zero Knowledge Rollups in sidechains, and NTRU lattice-based cryptography, the solution significantly enhances patient data privacy, security, and ownership. The system's resistance to quantum computing threats addresses critical issues of data leaks and illegal access. Kubernetes enhances scalability and manageability, while Practical Byzantine Fault Tolerance (PBFT) ensures system reliability and integrity, setting a new standard for healthcare data protection.

7.2 Future Work

- Integrate advanced cryptographic techniques like MPC and SMPC to enhance security and privacy.
- Implement more efficient consensus mechanisms beyond PBFT to improve scalability, efficiency, and performance.
- Expand support for diverse medical data types, including imaging and genomic data, to increase applicability.
- Optimize storage and retrieval processes using advanced data indexing and retrieval algorithms for improved efficiency.
- Conduct extensive real-world testing and deployment in various healthcare settings to gather valuable insights for further refinement.
- Continuously evolve the framework to ensure security, privacy, and efficiency in managing EHRs in the digital age.

References

Aikata, A., Basso, G., Cassiers, A. C., Mert, S. S. and Roy, S. S. (2023). Kavach: Lightweight masking techniques for polynomial arithmetic in lattice-based cryptography, *IACR Transactions on Cryptographic Hardware and Embedded Systems* **2023**(3): 366–390.

Al-Aswad, H., Hasan, H., Elmedany, W., Ali, M. and Balakrishna, C. (2019). Towards a blockchain-based zero-knowledge model for secure data sharing and access, *2019 7th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*, Istanbul, Turkey, pp. 76–81.

Andrew, J., Isravel, D. P., Sagayam, K. M., Bhushan, B., Sei, Y. and Eunice, J. (2023). Blockchain for healthcare systems: Architecture, security challenges, trends and future directions, *Journal of Network and Computer Applications* **215**: 103633.

Azaria, A., Ekblaw, A., Vieira, T. and Lippman, A. (2016). Medrec: Using blockchain for medical data access and permission management, *2016 2nd International Conference on Open and Big Data (OBD)*, Vienna, Austria, pp. 25–30.

Bai, T., Hu, Y., He, J., Fan, H. and An, Z. (2022). Health-zkidm: a healthcare identity system based on fabric blockchain and zero-knowledge proof, *Sensors* **22**(20): 7716.

Chenthara, S., Ahmed, K., Wang, H. and Whittaker, F. (2019). Security and privacy-preserving challenges of ehealth solutions in cloud computing, *IEEE Access* **7**: 74361–74382.

Gai, K., Tang, H., Li, G., Xie, T., Wang, S., Zhu, L. and Choo, K. (2022). Blockchain-based privacy-preserving positioning data sharing for iot-enabled maritime transportation systems, *IEEE Transactions on Intelligent Transportation Systems* **24**(2): 2344–2358.

Gao, Y.-L., Chen, X.-B., Chen, Y.-L., Sun, Y., Niu, X.-X. and Yang, Y.-X. (2018). A secure cryptocurrency scheme based on post quantum blockchain, *IEEE Access* **6**: 27205–27213.

Hoffstein, J., Pipher, J. and Silverman, J. H. (1998). Ntru: A ring-based public key cryptosystem, *in* J. P. Buhler (ed.), *Algorithmic number theory*, Springer, Berlin, Germany, pp. 267–288.

Hossein, K. M., Esmaeili, M. E., Dargahi, T. and Khonsari, A. (2019). Blockchain-based privacy-preserving healthcare architecture, *2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE)*, Edmonton, AB, Canada.

Hou, D., Zhang, J., Huang, S., Peng, Z., Ma, J. and Zhu, X. (2022). Privacy-preserving energy trading using blockchain and zero knowledge proof, *2022 IEEE International Conference on Blockchain (Blockchain)*, Espoo, Finland, pp. 412–418.

Hussein, A., MaoLood, A. and Gbashi, E. (2023). Ntru_ sss: Anew method signcryption post quantum cryptography based on shamir's secret sharing, *Computers, Materials & Continua* **76**(1).

Hölbl, M., Kompara, M., Kamišalić, A. and Nemec Zlatolas, L. A. (2018). A systematic review of the use of blockchain in healthcare, *Symmetry* **10**(10): 470.

Ismail, L. and Materwala, H. (2019). A review of blockchain architecture and consensus protocols: Use cases, challenges, and solutions, *Symmetry* **11**(10): 1198.

Jo, U., Oktian, Y. E., Kim, D., Oh, S., Lee, H. and Kim, H. (2022a). A zero-knowledge-range-proof-based privacy-preserving blockchain platform for covid-19 contact tracing, *2022 International Conference on Platform Technology and Service (PlatCon)*, Jeju, Korea, pp. 53–58.

Jo, U., Oktian, Y., Kim, D., Oh, S., Lee, H. and Kim, H. (2022b). A zero-knowledge-range-proof-based privacy-preserving blockchain platform for covid-19 contact tracing, *2022 International conference on platform technology and service (PlatCon)*, pp. 53–58.

Karthika, K., Dhanalakshmi, S., Murthy, S. M., Mishra, N., Sasikala, S. and Murugan, S. (2023). Raspberry pi-enabled wearable sensors for personal health tracking and analysis, *International Conference on Self Sustainable Artificial Intelligence Systems*, Erode, India, pp. 1249–1253.

Kethepalli, Y., Joseph, R., Vajrala, S. R., Vemula, J. and Naik, N. S. (2023). Reinforcing security and usability of crypto-wallet with post-quantum cryptography and zero-knowledge proof. doi: 10.48550/arXiv.2308.07309.

Kondepogu, M. D. and Andrew, J. (2022). Secure e-health record sharing using blockchain: A comparative analysis study, *2022 6th International Conference on Intelligent Computing and Control Systems (ICICCS)*, Madurai, India, pp. 861–868.

Latha, R., Raman, R., Senthil Kumar, T., Rawandale, C., Meenakshi, R. and Srinivasan, C. (2023). Automated health monitoring system for coma patients, *International Conference on Self Sustainable Artificial Intelligence Systems*, pp. 1469–1474.

Lax, G., Nardone, R. and Russo, A. (2024). Enabling secure health information sharing among healthcare organizations by public blockchain, *Multimedia Tools and Applications* pp. 1–17.

Liu, J., Mesnager, S. and Chen, L. (2016). Partially homomorphic encryption schemes over finite fields, *International Conference on Security, Privacy, and Applied Cryptography Engineering*, Cham: Springer International Publishing, pp. 109–123.

López-Alt, A., Tromer, E. and Vaikuntanathan, V. (2012). On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption, *STOC '12: Proceedings of the Forty-Fourth Annual ACM Symposium on Theory of Computing*, pp. 1219–1234.

Narayanan, A., Bonneau, J., Felten, E., Miller, A. and Goldfeder, S. (2016). *Bitcoin and cryptocurrency technologies: A comprehensive introduction*, Princeton University Press, Oxford, United Kingdom.

Nejatollahi, H., Dutt, N., Ray, S., Regazzoni, F., Banerjee, I. and Cammarota, R. (2019). Post-quantum lattice-based cryptography implementations: A survey, *ACM Computing Surveys (CSUR)* **51**(6): 1–41.

Nguyen, D. C., Nguyen, K. D. and Pathirana, P. N. (2019). A mobile cloud based iomt framework for automated health assessment and management, *2019 41st Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*, Berlin, Germany, pp. 6517–6520.

Nisha, F., Lenin, J., Saravanan, S., Rohit, V., Selvam, P. and Rajmohan, M. (2024). Lattice-based cryptography and ntru: Quantum-resistant encryption algorithms, *2024 International Conference on Emerging Systems and Intelligent Computing (ESIC)*, Bhubaneswar, India, pp. 509–514.

Novikov, S., Kazakov, O., Kulagina, N. and Azarenko, N. (2018). Blockchain and smart contracts in a decentralized health infrastructure, *2018 IEEE International Conference "Quality Management, Transport and Information Security, Information Technologies" (IT&QM&IS)*, pp. 697–703.

Partala, J., Nguyen, T. H. and Pirttikangas, S. (2020). Non-interactive zero-knowledge for blockchain: A survey, *IEEE Access* **8**: 227945–227961.

Prashanth Joshi, A., Han, M. and Wang, Y. (2018). A survey on security and privacy issues of blockchain technology, *Mathematical Foundations of Computing* **1**(2): 121–147.

Preece, J. D. and Easton, J. M. (2018). Towards encrypting industrial data on public distributed networks, *2018 IEEE International Conference on Big Data (Big Data)*, Seattle, WA, USA, pp. 4540–4544.

Rasheed, A., Mahapatra, R. N., Varol, C. and Narashimha, K. (2022). Exploring zero knowledge proof and blockchains towards the enforcement of anonymity, data integrity and privacy (adip) in the iot, *IEEE Transactions on Emerging Topics in Computing* **10**(3): 1479–1491.

Redkins, B., Kuzminykh, I. and Ghita, B. (2023). Security of public-key schemes in the quantum computing era–a literature review, *IEEE Access* pp. 1–6. Available at: `https://www.researchgate.net/publication/371382633`.

Ren, Z., Zha, X., Zhang, K., Liu, J. and Zhao, H. (2019). Lightweight protection of user identity privacy based on zero-knowledge proof, *2019 IEEE International Conference on Systems, Man and Cybernetics (SMC)*, Bari, Italy, pp. 2549–2554.

Singh, A., Pradhan, N., Luhach, A., Agnihotri, S., Jhanjhi, N., Verma, S., Ghosh, U. and Roy, D. (2020). A novel patient-centric architectural framework for blockchain-enabled healthcare applications, *IEEE Transactions on Industrial Informatics* **17**(8): 5779–5789.

Soltani, R., Nguyen, U. T. and An, A. (2021). A survey of self-sovereign identity ecosystem, *Security and Communication Networks* pp. 1–26.

Suzuki, S. and Murai, J. (2017). Blockchain as an audit-able communication channel, *2017 IEEE 41st Annual Computer Software and Applications Conference (COMPSAC)*, Turin, Italy, pp. 516–522.

Treiblmaier, H. and Sillaber, C. (2021). The impact of blockchain on e-commerce: A framework for salient research topic, *Electronic Commerce Research and Applications* **48**: 101054.

Vithanwattana, N., Mapp, G. and George, C. (2016). mhealth - investigating an information security framework for mhealth data: Challenges and possible solutions, *2016 12th International Conference on Intelligent Environments (IE)*, London, UK, pp. 258–261.

Wright, C. (2019). Bitcoin: a peer-to-peer electronic cash system. SSRN Electron. J., 21260 Available at: `https://doi.org/10.2139/ssrn.3440802`.

Yaqoob, I., Salah, K., Jayaraman, R. and Al-Hammadi, Y. (2022). Blockchain for healthcare data management: opportunities, challenges, and future recommendations, *Neural Computing and Applications* **34**: 11475–11490.

Yuan, B., Wu, F. and Zheng, Z. (2023). Post quantum blockchain architecture for internet of things over ntru lattice, *Plos one* **18**(2): e0279429. Available at: `https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0279429`.

Zhang, Y. (2022). Increasing cyber defense in the music education sector using blockchain zero-knowledge proof identification, *Computational Intelligence and Neuroscience* p. 1.

Zheng, H., You, L. and Hu, G. (2022). A novel insurance claim blockchain scheme based on zero-knowledge proof technology, *Computer Communications* **195**: 207–216.

Zheng, X., Mukkamala, R., Vatrapu, R. and Ordieres-Mere, J. (2018). Blockchain-based personal health data sharing system using cloud storage, *2018 IEEE 20th international conference on e-health networking, applications and services (Healthcom)*, Ostrava, Czech Republic, pp. 1–6.