Available online at www.ijournalse.org

Emerging Science Journal

(ISSN: 2610-9182)

Vol. 9, No. 1, February, 2025

Pioneering the Security of EHRs Using an Immersive Blockchain Conceptual Framework

Rihab Benaich [1*], Youssef Gahi [1], Saida El Mendili [1]

[1] *Engineering Sciences Laboratory, National School of Applied Sciences, Ibn Tofail University, Kenitra, Morocco.*

Abstract

This study develops a conceptual framework to enhance the security and functionality of Electronic Health Records (EHRs) in response to advancing healthcare needs. Objectives include strengthening data protection against both traditional and quantum cyber threats, increasing system resilience, and improving user experience and operational efficiency. Methods/Analysis involve a novel combination of Advanced Encryption Standard (AES) and quantum cryptographic algorithms CRYSTALS-Dilithium and CRYSTALS-Kyber within a hybrid blockchain architecture to secure EHRs. Decentralized Autonomous Organizations (DAOs) are incorporated to decentralize control and reinforce security, while artificial intelligence and metaverse integration facilitate user engagement and streamline operations. Findings indicate that this hybrid blockchain model, enhanced with quantum-resistant cryptography and decentralized governance, significantly improves EHR security. AI and the metaverse contribute to user interaction and operational flow. Novelty/Improvement lies in integrating hybrid blockchain, quantum cryptography, AI, and the metaverse into a unified framework, effectively addressing current and future healthcare data management challenges. This multi-layered approach represents a significant advancement over existing systems by bolstering EHR security, user engagement, and operational capabilities.

Keywords:

AI Assistance;

Blockchain; Metaverse;

EHRs;

Security;

Post-Quantum Computing.

Article History:

Received:	31	August	2024
Revised:	23	November	2024
Accepted:	09	December	2024
Published:	01	February	2025

1- Introduction

In today's technology-driven world, healthcare relies heavily on data to deliver high-quality care and make informed decisions. The advent of electronic health records (EHRs) and big data analytics has provided healthcare institutions with unprecedented patient data access. However, this wealth of information also brings with it significant security concerns. Protecting the privacy and security of healthcare data is of utmost importance due to the potential consequences of unauthorized access or breaches. Healthcare data includes sensitive details such as patients' and caregivers' identities and comprehensive medical histories. Therefore, implementing robust security measures to safeguard this information from cyber threats and breaches is critical and urgent. Historically, healthcare information systems have been vulnerable, leading to security breaches that present significant challenges (Figure 1). The increasing number of data breaches in the healthcare sector underscores the urgent need for stringent security protocols. Recent statistics reveal that the healthcare industry is a prime target for cyberattacks, with hospitals accounting for 30% of data breaches. In 2021, 50 million Americans experienced breaches in their protected health information, a threefold increase within three years; furthermore, the average healthcare data breach in 2023 exposed over 215,000 records [1]. Moreover, the security measures in healthcare systems are often hindered in providing a secure environment for patients and professionals vulnerable to cyber threats. These conventional systems typically use classical encryption methods and store data that exposes EHRs to the risk of breaches, unauthorized access, and tampering. The emergence of quantum computing worsens these weaknesses since quantum computers can break classical encryption methods currently considered secure.

[*] **CONTACT**: rihab.benaich@uit.ac.ma

DOI: http://dx.doi.org/10.28991/ESJ-2025-09-01-010

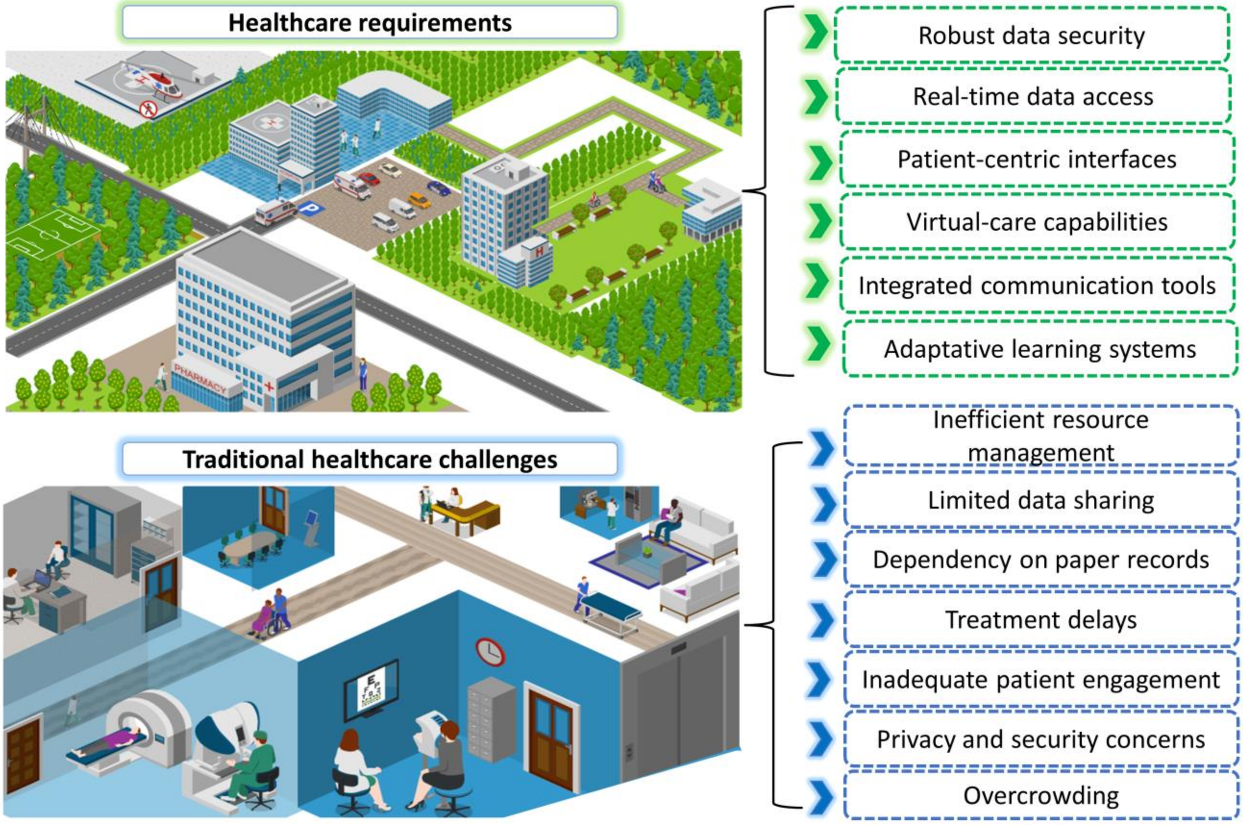

Healthcare requirements
Robust data security
Real-time data access
Patient-centric interfaces
Virtual-care capabilities
Integrated communication tools
Adaptative learning systems
Traditional healthcare challenges
Inefficient resource management
Limited data sharing
Dependency on paper records
Treatment delays
Inadequate patient engagement
Privacy and security concerns
Overcrowding

Figure 1. Current Healthcare Requirements Amidst Traditional Healthcare Challenges

Considering the sensitive nature of healthcare information, including medical data, it is crucial to implement advanced security protocols. Safeguarding the confidentiality, integrity, and accessibility of EHRs is essential for upholding confidence and protecting health [2]. This requires adopting advanced encryption techniques resistant to quantum attacks and utilizing data storage solutions like blockchain technology to ensure robust security against present and future threats [3]. Another primary concern with traditional healthcare information systems is their restricted focus on patient engagement. Patients usually have a neglectable or passive role in their healthcare data and need more control of their medical information. These traditional systems overlook the chance to involve patients in their treatment, which could enhance outcomes and patient satisfaction [4]. Additionally, conventional health records systems often restrict patients' access to their data, making it easier for them to view their records or share them with specialists without permission from their primary caregivers. This lack of transparency can make it challenging for patients to make decisions about their healthcare or seek opinions. Moreover, these systems rarely facilitate real-time communication between patients and healthcare providers. Activities like scheduling appointments, asking follow-up questions post-consultation or receiving health updates generally require communication channels, causing delays and inefficiencies. Furthermore, traditional healthcare information systems typically follow a one-size-fits-all approach that does not consider patient needs, such as personalized treatment plans or targeted health maintenance reminders.

This pattern highlights the importance of strengthening security measures in traditional healthcare data systems. As a response, numerous studies have incorporated cutting-edge technologies like blockchain, metaverse and artificial intelligence (AI) [5-7] to support the security and engagement of healthcare data systems. For instance, blockchain has been applied to establish tamper-proof records, which can significantly reduce access and data manipulation. An example of this is using blockchain to manage consent logs and treatment records securely, ensuring their integrity and transparency [8]. Similarly, AI has been utilized to identify abnormal patterns and potential breaches by analyzing real-time data access logs and network traffic and offering warnings before significant harm occurs.

Despite these advancements, significant research gaps still need to be addressed [9]. Current literature on Electronic Health Records security largely focuses on traditional encryption methods and centralized database systems [10, 11], which are increasingly vulnerable to cyber threats and lack scalability for the anticipated impact of quantum computing. While some studies have explored blockchain and artificial intelligence for EHRs, they often address only single-layer security solutions and do not integrate quantum-resistant cryptography or decentralized governance models effectively. Furthermore, few studies have examined user engagement and interoperability with legacy healthcare systems in areas with limited technological infrastructure.

This research addresses these gaps by developing a multi-layered approach that combines quantum-resistant cryptography, a hybrid blockchain structure, and Decentralized Autonomous Organizations (DAOs) to safeguard EHRs. By integrating CRYSTALS-Kyber and CRYSTALS-Dilithium, our approach strengthens resilience against quantum attacks, an area not fully explored in healthcare data management. Additionally, the inclusion of DAOs and metaverse elements enhances user autonomy and interaction, creating a secure, user-centred experience that addresses both current and future healthcare challenges. Our proposed framework, therefore, fills an essential gap in EHR security by offering a comprehensive solution that addresses scalability, interoperability, and quantum resistance advancing EHR security beyond existing models.

Additionally, implementing integrated solutions in healthcare environments presents a considerable challenge in terms of scalability. Moreover, regulatory frameworks that can adapt to rapid technological progress are necessary to safeguard data privacy and security effectively. Lastly, the implications of using technologies, including patient consent and data ownership issues, must be explored meticulously, as it is crucial to align technological progress with ethical healthcare practices.

To address these challenges, this study aims to explore the following research questions:

- How does a hybrid blockchain handle sensitive and less sensitive health data?
- How do combined contemporary technologies such as blockchain, AI and metaverse enhance patient health service delivery?
- How does combining classical and post-quantum cryptography enhance security and resist new-age cyber threats?

Keeping this in mind, in this paper, we propose a novel theoretical architecture intending to create and assess a healthcare environment that improves the security and effectiveness of managing healthcare data. This is achieved by using a design incorporating elements of the metaverse and employing advanced cryptographic techniques. The proposed architecture aims to tackle issues related to data privacy, security and accessibility in healthcare through the following contributions:

1) ***Integration of a Hybrid Blockchain Structure:*** The core element of this proposition involves creating and evaluating a framework that efficiently separates sensitive and nonsensitive health data. The framework integrates a permissionless blockchain for critical information to ensure transparency and traceability while implementing a private blockchain for susceptible data to prevent unauthorized access.

2) ***Integration of Metaverse in Healthcare:*** This initiative examines the metaverse's possibilities for delivering healthcare services, such as consultations and treatments, within a decentralized autonomous organization (DAO) setup. It explores using avatars for healthcare professionals and patients to introduce interaction models alongside integrating AI-driven diagnostics and treatment planning in a virtual environment.

3) ***Strengthening Data Security with Post Quantum Cryptography and Advanced Encryption Standard:*** Employing post-quantum cryptographic methods and AES to protect EHRs and imaging data like MRI and X-rays from potential future quantum cryptographic threats involves assessing the effectiveness of these techniques in real-world healthcare scenarios.

4) ***Assessment of User Interface Accessibility:*** This involves evaluating how easy it is for users to interact with devices like smartphones, computers, VR headsets, and tablets when accessing healthcare services. It also involves looking at how engaged users (patients) are and how practical the interface is in a healthcare environment.

5) ***Patient Engagement and Reward Systems:*** Investigating how reward systems in virtual reality environments can influence patient engagement and commitment to following treatment plans. This includes examining how incentives can be designed to encourage patients to take a role in managing their healthcare.

The rest of the paper is organized as follows: Section 2 overviews classical healthcare systems' challenges. Section 3 highlights relevant studies on blockchain-based security in healthcare, EHRs, and the AI metaverse and discusses their limitations. Section 4 presents the background of our proposed solution, incorporating blockchain, AI, DAO, and the metaverse. Section 5 details our approach to each layer, explaining the different elements involved. Section 6 outlines the workflow of our proposed system, including specific steps and a use-case scenario. Section 7 presents the benefits of our system, while Section 8 discusses its various aspects and implications. Section 9 compares our proposed solution to traditional and existing studies. Finally, Section 10 provides challenges and addresses some implemented solutions, and Section 11 outlines the main directions for future research.

2- Shortcomings of Classical Healthcare Information Systems

2-1- Paper-Based Records Challenges

For centuries, healthcare professionals have relied on paper-based records to document patient information, such as medical histories, treatment plans, diagnoses, and follow-up care. These records are typically stored in files or folders within healthcare facilities. One of the benefits of using paper records is their simplicity and accessibility. They do not require technology or digital skills, making them suitable for areas with limited access to electricity or modern IT systems. Some healthcare professionals appreciate the hands-on approach of reviewing a patient's history through physical records, providing a tangible way to manage sensitive information. However, paper-based systems have various drawbacks. One significant drawback of paper records is their susceptibility to damage during disasters such as floods or fires. Over time, the information may deteriorate, making it challenging to ensure accuracy, which requires handling and storage. The large volume of paper records also presents an obstacle to healthcare facilities operating; the number of records accumulates, leading to the need for storage space and high overhead costs. Managing these records becomes more labour-intensive over time, necessitating staff and resources to maintain a filing system.

Moreover, transferring paper records between departments or facilities is slow and ineffective. It involves duplicating or transferring documents, which consumes time and raises the risk of loss or misplacement. These delays could be critical in emergencies where swift access to data is crucial for effective treatment. Retrieving information from paper systems often involves sorting through files, causing delays in data access and potentially disrupting diagnoses and treatment plans. The manual search process also heightens the chances of misfiling or losing records. Moreover, inputting information into paper records increases the likelihood of errors. Illegible handwriting can lead to misunderstandings regarding medication dosages, allergies, or medical histories. Furthermore, the absence of forms and reliance on notes can result in incomplete or inconsistent record-keeping, potentially leaving out crucial details, heightening mistakes like these and putting patients at risk. This may result in treatments causing legal troubles for healthcare providers.

2-2- Electronic Health Records Challenges

Electronic Health Records, or EHRs, mark immense progress in handling medical information. Converting paper records into format EHRs makes storing, accessing, and updating patient data easier, ultimately enhancing healthcare services' efficiency. Despite their advantages, EHR systems encounter obstacles that impact their implementation and functionality. An electronic health record is a rendition of a patient's paper chart. These real-time records are patient-focused and grant authorized users secure access to information. While an EHR includes patients' medical histories and treatments, it goes beyond data typically recorded in healthcare facilities to offer a more comprehensive view of patient care. EHRs are designed to extend beyond the organization that compiles the data by sharing information with healthcare providers like laboratories and specialists involved in a patient's treatment process. The key advantages of EHRs include streamlining records in form to simplify data management across various healthcare providers. Additionally, EHR platforms enable healthcare professionals to collaborate on treatment plans, thereby reducing errors in medical practices and enhancing the overall quality of care.

Despite their advantages, EHRs face numerous challenges. Patient data is susceptible, making EHRs vulnerable to data breaches and unauthorized access. Securing EHRs is crucial, requiring encryption techniques and strict access controls. A key obstacle with EHR systems is their lack of standardization, which impacts interoperability and the ability of systems to exchange and interpret shared data accurately. With interoperability, the full benefits of EHRs can be fully realized since data cannot be seamlessly shared across platforms or among healthcare providers. Furthermore, centralization in EHRs involves storing or managing data in a location under one entity. This raises concerns about monopoly control, points of failure, the potential misuse of information and increased vulnerability to cyber-attacks. Centralization may also create bottlenecks when accessing or processing data, impacting healthcare services' efficiency.

Moreover, usability and adoption pose another challenge. The complexity of EHR systems can lead to usability issues that result in resistance from healthcare professionals. This resistance can hinder the adoption rates of EHR systems and diminish their benefits.

3- Advanced Solutions Adopted for Healthcare Security

3-1- Related Studies

Research has emphasized improving healthcare systems' security and effectiveness by incorporating advanced technologies. Table 1 highlights the main advancements in this area, including the incorporation of blockchain, artificial intelligence, and the metaverse. This section explores this area's key progressions, applications, and limitations.

Table 1. Relevant Studies Related to Healthcare/EHRs Security Using Blockchain and Advanced Technologies

Paper	Contribution	Method	Results	Challenges
Ma & Zhang (2024) [12]	The authors proposed a system using blockchain technology to manage electronic medical records, aiming to overcome the issues of data protection and availability in the healthcare sector. This system utilizes zero knowledge rollups (ZK-Rollups) to improve the effectiveness and safety of data exchanges.	- Zk-Rollups environment - Smart contracts - Zk-Snarks - Ethereum main network	-Improved Security -Enhanced scalability and efficiency	- Requirement for key exchange
Benaich et al. (2024) [13]	The authors proposed a blockchain-based solution to secure EHRs using the Algorand blockchain, decentralized identifiers and PPoS consensus	- Inclusion of Pure Proof of Stake consensus - Algorand Blockchain - ChaCha20-Poly1305 - Token-based Access control	-Improved Security -Fast transactions (6,5 seconds)	- Scalability - Interoperability
Awan et al. (2024) [7]	The authors developed a framework for incorporating digital twins into the Metaverse in healthcare, focusing on ensuring data synchronization and security.	- The inclusion of Blockchain technology, Web 3.0 functionalities, and cutting-edge consumer gadgets for experiences and data safeguarding.	- Enhancement of data synchronization efficiency by 20%. - Optimization resource usage by 15%.	- Implementation challenges of VR, AR and IoT
Kang et al. (2023) [14]	The authors proposed a user-centric privacy-preserving framework for healthcare metaverses based on decentralized Federated Learning (FL) and blockchain.	- User-centric privacy-preserving framework using decentralized, federated learning for healthcare metaverses - Hierarchical cross-chain architecture - Employment of Age of Information (AoI) as a data-freshness metric - Presented a contract theory model based on the Area of Information (AoI) within Prospect Theory (PT), to encourage sharing sensing data in a way that prioritizes the user's perspective.	-Simplifies secure and private decision-making and data analytics for users in healthcare metaverses. -Improved efficiency	- Challenges related to sensing data security and freshness
Ali et al. (2023) [15]	The authors introduced a hybrid deep learning approach using homomorphic encryption and consortium Blockchain designed for the Industrial Internet of Medical Things (IIoMT) to tackle the security issues surrounding Electronic Medical Records. This model combines HE with the IIoMT system to ensure statistical and machine-learning processes on encrypted EMR data.	Consortium Blockchain Homomorphic encryption Pre-trained hybrid deep learning model in the cloud	- Resistance to collusion and phishing attacks - Secure statistical and machine learning operations on encrypted medical data - High efficiency - Low end-to-end latency	- Centralized servers connected to the cloud can be vulnerable to DDoS attacks.
Liu et al. (2024) [16]	The authors developed a blockchain-based remote smart healthcare system that ensures healthcare data security and achieves the minimum Age of Information.	- Blockchain layer (energy-efficient DPoS-based cooperative game achieving Nash equilibrium) -Sensing communication layer (Energy-aware Whittle Index-based Algorithm	- Low energy consumption - Improved security	- Latency issues - Scalability challenges
Guduri et al. (2024) [17]	The authors proposed a blockchain-based lightweight encryption combined with federated learning to address scalability and trust in EHRs systems.	- Smart contracts - Proxy re-encryption - Ethereum blockchain - Decentralized cloud	- Enhanced security	- High computational requirements - Complexity of federated learning
Chen et al. (2023) [18]	The authors introduced an innovative searchable encryption scheme for cloud-assisted EHRs. This scheme mitigates privacy concerns about searching for sensitive data in the cloud. By leveraging blockchain and hash-proof chains, the system allows for public verification of search results without relying on a trusted authority. Additionally, it supports dynamic datasets, providing enhanced security through a unique hidden data structure.	- Hash-proof chain - Blockchain	- Robust data protection	- High computational requirements - Latency
Singh et al. (2022) [19]	The authors proposed an architecture designed to protect privacy in healthcare by incorporating Blockchain and Federated Learning technologies. This novel architecture integrates Blockchain-based cloud platforms to enhance security and privacy in healthcare systems. By utilizing Federated Learning, the architecture supports large-scale machine learning applications, allowing users to utilize trained models without sending their data to the cloud, thereby preserving data privacy.	- Cloud platforms - Blockchain - Federated learning - Token-based access control	- Granular access over data access - Enhanced security	-Management complexity
Benaich, et al. (2023) [20]	The authors proposed a blockchain-based method combined with an Advanced Encryption Standard and zero-knowledge proof protocol to ensure the security of health records.	- Ethereum Blockchain - Smart contracts - Advanced Encryption Standard - Zk-Snarks	- Improved security - Low costs - Enhanced privacy	- Interoperability challenges - Transactions delays
Jiang et al. (2022) [21]	The authors proposed a scheme that enhances EHR security by enabling the confidential transmission of treatment information and leveraging blockchain to ensure data integrity and traceability. It also supports fine-grained attribute revocation in ciphertext management, which improves key generation and decryption performance while reducing computational overhead compared to other algorithms.	-Attribute-based encryption	- Decentralization - Tamper-resistant - Transparency	-Network consensus delays
Mishra et al. (2022) [22]	The authors introduced an innovative consortium blockchain-based EHR storage model for cloud-assisted healthcare. This model integrates EHR operations into a consortium blockchain to ensure the confidentiality, integrity, and correctness of outsourced EHRs. It utilizes collaborative multi-cloud storage to enhance durability and availability and organizes transactions by EHR type to enable efficient block deletion.	- Consortium blockchain	- Enhanced data security - Enhanced interoperability	- High energy consumption - Scalability issues - Regulatory issues
Zhang et al. [23]	Using blockchain technology, the authors proposed a secure e-health system for managing patient EHRs. This system employs pairing-based cryptography to create tamper-proof records, safeguarding EHRs from tampering or unauthorized access. These secure records are integrated into blockchain transactions, ensuring their verifiability and protection against illegal modifications. Furthermore, the system incorporates secure payment protocols through blockchain-based smart contracts for diagnostic and storage services.	- Smart contracts - Pairing-based cryptography	- Tamper-proof records - Improved Security	- Scalability challenges
Kumar et al. (2022) [24]	The authors introduced a secure data-sharing framework for the industrial healthcare system to transform healthcare data and improve attack detection.	- Permissioned blockchain - Smart contracts -Zero-knowledge proof protocol) -Deep learning (stacked sparse variational autoencoder and self-attention-based bidirectional long short-term memory model)	-Robust security against various threats	- Integration complexity - High costs - Requirement of specialized knowledge
Zou et al. (2021) [25]	The authors developed a blockchain-based system called SPChain to enhance the sharing and privacy of electronic medical records. This system accelerates data retrieval and incentivizes healthcare institutions to participate through a distinctive reputation mechanism.	- Proxy re-encryption - Blockchain	- Promotes security of medical data sharing	- Energy consumption

3-2- Limitations

Despite the progress in managing and securing healthcare data, research gaps still hold back the potential of safe and effective healthcare systems. This section delves into these gaps thoroughly, looking at the shortcomings in research and the areas that need exploration. While many studies have delved into blockchain, artificial intelligence and the Internet of Medical Things in healthcare, they often focus on one technology at a time. The synergies from combining these technologies have yet to be fully explored. We need frameworks that combine blockchain, AI and IoMT to create solutions. This involves building systems that smoothly integrate technologies to boost data security, patient involvement and system efficiency. Moreover, the absence of electronic health records systems poses challenges for interoperability among healthcare providers and systems; this lack of uniformity results in data silos that hinder the sharing of health information. Establishing protocols and frameworks for EHR systems is crucial to support interoperability efforts. Research should concentrate on establishing accepted standards that enable exchanges of health data across diverse platforms and organizations.

Furthermore, integrating technologies into healthcare often needs to be improved due to usability challenges and the complexity associated with learning systems. Research studies should explore how well people in the healthcare sector accept technologies with a focus on creating user interfaces and offering proper training to healthcare professionals. By understanding what factors influence users' willingness to adopt these technologies, we can design systems more likely to be embraced by the end users. Additionally, the rapid progress of healthcare technologies raises regulatory issues, especially concerning data privacy, patient approval and ownership. It is essential to develop frameworks that can keep up with advancements by addressing ethical concerns related to patient approval and data ownership while ensuring that new technologies comply with existing privacy laws. Some current solutions rely either on security approaches or quantum cryptography, which can create vulnerabilities. Traditional methods are becoming more susceptible to quantum attacks, whereas post-quantum methods are still developing and may not cover all security aspects effectively. A combined approach using both post-quantum cryptographic methods is necessary to ensure security measures. Research efforts should concentrate on integrating these methods to capitalize on their strengths for protection against both present and future threats. Addressing these research gaps is vital for enhancing the management and security of healthcare data.

4- Background of the Proposed Approach

This section introduces our healthcare system design, combining pioneering technologies to enhance care and patient interactions. The core of this design incorporates layers that merge a user interface with advanced devices such as smartphones, tablets, computers, and VR headsets to provide users with easy access and immersive experiences. This interface connects to an application layer deeply integrated into the Metaverse. AI-driven healthcare assistants, a reward system, and a decentralized autonomous organization work together to create an interactive healthcare environment. To ensure the security of health information, a robust blockchain layer is utilized with private and public chains and tailored to different data sensitivity levels. Additionally, the storage layer employs post-quantum cryptography for ultimate data protection against existing and future cyber threats. Together, these components establish a health ecosystem that prioritizes user engagement and has the potential to transform healthcare delivery and patient care management.

4-1- Blockchain Technology

Blockchain technology has become a game changer in healthcare, especially when handling and safeguarding sensitive information [26, 27]. Unlike centralized databases, blockchain broadcasts data across a network of computers, reducing the chances of a point of failure and boosting data security. This decentralization prevents any entity from having control over the entire database, thereby enhancing trust among users. Once a transaction is logged on a blockchain, it cannot be removed (Figure 2). This unchangeable record of information ensures that medical records remain unaltered, strengthening the data's credibility and promoting trust between patients and healthcare providers. While providing patient privacy, blockchain also offers transparency in transactions, which can be particularly beneficial in scenarios like tracking drug supply chains for authenticity verification or managing health insurance claims openly. Moreover, blockchain revolves around a distributed ledger that logs all transactions across a network of computers called nodes. Each node stores a ledger copy, ensuring network consistency and validation. This architecture eliminates the need for an authority, reducing susceptibility to attacks or fraud. Furthermore, data on the blockchain is safeguarded using encryption methods to protect health information from unauthorized access. Every block includes a hash of the preceding block, forming a solid chain that cannot be tampered with undetected. This aspect is crucial for adhering to data protection laws and upholding patient confidentiality.

Different types of blockchains vary in accessibility, control, and usage. Public blockchains are known for their decentralization level, allowing anyone to participate and see transactions, ensuring transparency and security. However, they often encounter challenges related to scalability and privacy. On the other hand, private blockchains are controlled by an entity or a group, offering greater privacy and efficient performance but sacrificing some decentralization and transparency. Hybrid blockchains combine the features of both private blockchains, providing a solid solution for managing healthcare data (Figure 3).

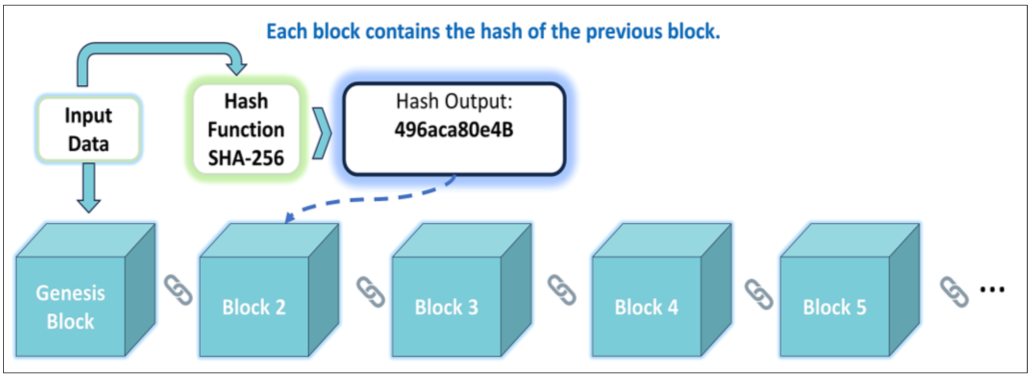


Figure 2. Example of Blockchain

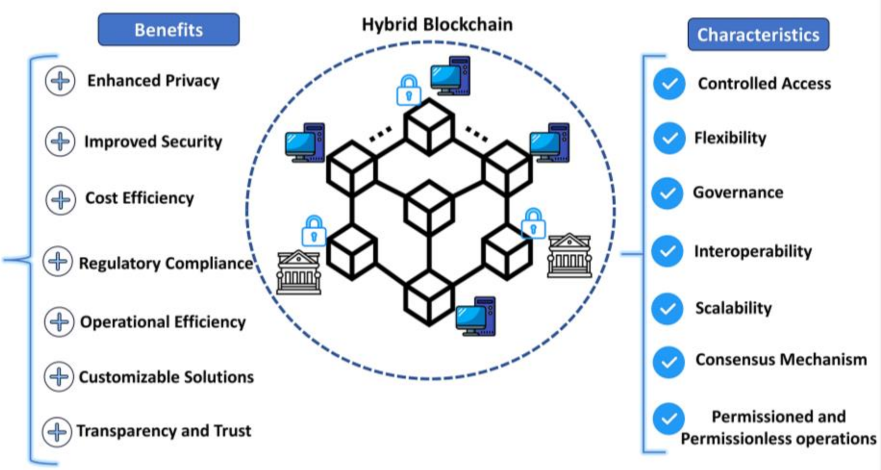


Figure 3. Characteristics and Benefits of Hybrid Blockchain

They offer the needed privacy for information while ensuring transparency and immutability for public health records and research data. This balance makes blockchains suitable for the healthcare sector by addressing security and efficiency needs while supporting compliance with regulations. Through blockchain technology, healthcare institutions can enhance data security, promote interoperability, and encourage trust and collaboration within the healthcare field. This is demonstrated in the comparative Table (Table 2).

Table 2. Primary Differences Between Blockchain

Attribute	Public Blockchain	Private Blockchain	Hybrid Blockchain
Accessibility	Open to anyone	Restricted to specific participants	Public elements are open and accessible, and private ones are restricted
Decentralization	Highly decentralized	Centralized control	The public blockchain is decentralized, and the private blockchain is controlled.
Security	Very high	High	Public ensures integrity; private ensures confidentiality
Data Privacy	Low	High	Sensitive data private, non-sensitive data public
Control	No single entity control	Controlled by one entity	Control over private, decentralized public governance
Immutability	Strong	Strong	The public blockchain provides immutability, and the private ensures security and control.
Scalability	Limited	Generally scalable	Public blockchain handles broad and large data, while private blockchain processes sensitive data.
Transparency	High	Limited	Public transparent, private confidential
Regulatory Compliance	Challenging	Easier	The public blockchain helps compliance, and the private ensures data privacy.
Interoperability	High privacy concerns	Limited	The public blockchain shares broadly, while the private blockchain maintains secure sharing
Cost	Potentially high	Optimized	Public blockchain reduces broad costs; private one optimizes sensitive data.

4-2- Metaverse Technology

The concept of the metaverse, a connected world utilizing augmented reality (AR) and virtual reality (VR), has the potential to support the security of health records and manage healthcare data effectively. Medical professionals can establish safe environments for storing and retrieving electronic health records within this realm. The metaverse uses AR and VR technologies to enable real-time interactions between patients and healthcare providers. Virtual consultations and medical simulations can be conducted within controlled settings to safeguard health information during these engagements. These virtual environments have firm access controls to ensure authorized individuals can access or modify health records. Moreover, the metaverse facilitates the development of training programs for healthcare practitioners. These programs simulate real-life scenarios in a setting that offers an environment for training without compromising patient data security. This does not enhance the expertise of healthcare providers, but it safeguards health records throughout the training process.

The structure of the metaverse has the potential to transform healthcare by boosting security, managing data effectively and improving interactions. The foundational *Infrastructure Layer* uses high-speed internet like Wi-Fi 6 and 5G to back services, remote monitoring and safe data transfer. The *Human Interface Layer* integrates cutting-edge interfaces such as voice-activated systems, smart glasses and tactile feedback to facilitate hand access to information and real-time display during medical procedures. The decentralization layer ensures the confidentiality and security of health records through the storage and access of data by employing secure distributed databases and AI assistants. The *Spatial Computing Layer* utilizes AR and VR for simulations, training sessions, and virtual consultations to enhance precision and interactivity. Meanwhile, the *Creator Economy Layer* encourages creating and sharing content to nurture an environment for healthcare professionals. Moreover, the *Discovery Layer* enhances the accessibility of healthcare services and information through search tools while offering personalized recommendations for patients. Lastly, the *Experience Layer* emphasizes patient engagement by incorporating gamification elements, social media support and immersive experiences for health therapy. By harnessing the capabilities of the metaverse, healthcare institutions can enhance health record security, reinforce confidentiality, and promote the sharing of healthcare data.

4-3- AI Assistance

Artificial intelligence is paramount in improving healthcare, especially security and data management. AI-driven systems can analyze volumes of data to detect security risks, safeguarding the privacy and confidentiality of EHRs. By adopting machine learning algorithms, AI can spot abnormal patterns and behaviours that may signal cyber threats, allowing for rapid and effective measures against security breaches is instrumental in automating information encryption and decryption processes within environments, ensuring that only authorized individuals can access sensitive data. Sophisticated AI platforms also oversee access controls to ensure healthcare professionals view permitted data. Additionally, AI enables communication between patients and providers through natural language processing (NLP) and voice recognition technologies, preserving the confidentiality of interactions. Furthermore, AI-powered predictive analytics aid in pinpointing weaknesses in healthcare IT systems, enabling updates and fixes to prevent security vulnerabilities. Moreover, AI strengthens patient authentication procedures by incorporating verification methods like recognition and fingerprint scanning to ensure that only legitimate users gain entry into healthcare platforms.

Figure 4 explains how artificial intelligence is used in healthcare, from when a patient provides information to when AI assists in decision-making. At the beginning, there is the Environment where a patient shares their symptoms and medical history, asking questions like "***Do I need to consult a specialist based on my symptoms and medical history? If yes, which specialist should I see?***" The AI Health Assistant analyzes this information using natural language processing to understand the patient's query and relevant data. It suggests, "***Considering your symptoms and medical history alongside guidelines, it's advisable to consult with a cardiologist***."

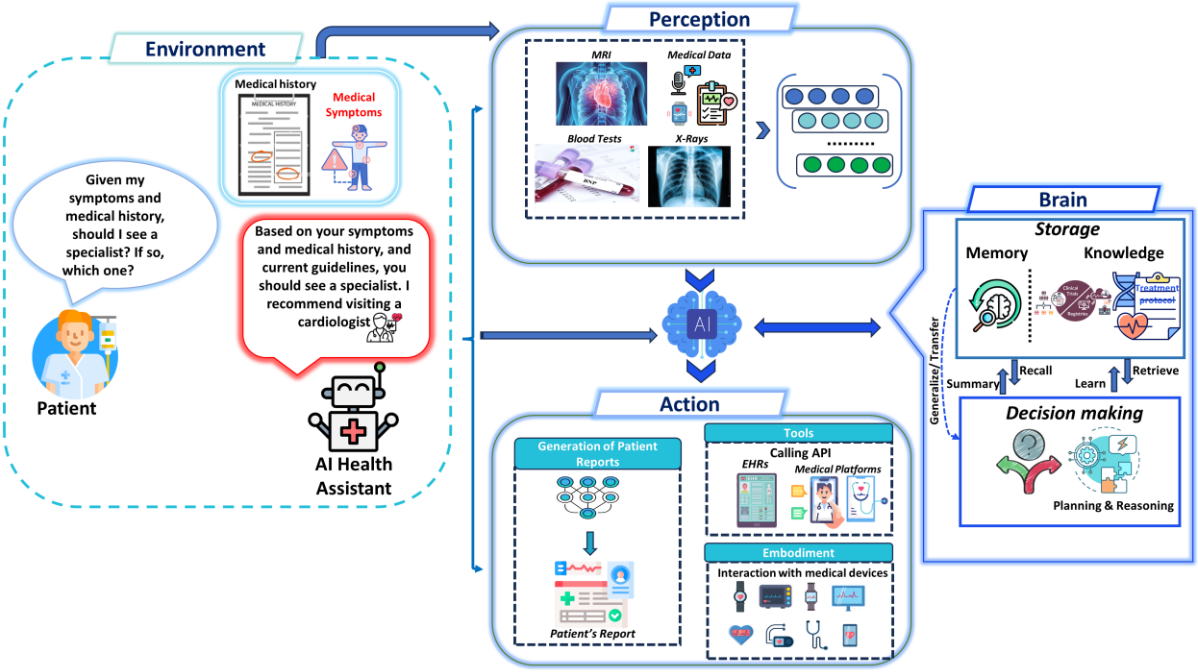


Figure 4. Example of AI Health assistant in the Healthcare Domain

Moving on to the Perception phase, various medical data such as MRI scans, blood tests, X-rays and other inputs are gathered. These inputs undergo preprocessing steps like normalization and noise reduction before feature extraction. Sophisticated machine learning models such as networks (CNNs) for image analysis and recurrent neural networks (RNNs) for sequential data are employed to analyze these inputs for patterns and correlations. This process is crucial for transforming data into insights that aid in decision-making. Subsequently, in the Brain section lies Storage, where memory and knowledge are stored. Patient information is stored in memory, which includes records, while the knowledge base houses medical guidelines, clinical trial data and treatment protocols. The brain's operations utilize a variety of machine learning and deep learning algorithms to learn from data and extract information. Essential methods involve supervised learning for forecasting outcomes based on labelled data, unsupervised learning, and uncovering hidden patterns. Decision-making employs algorithms like decision trees and reinforcement learning to create treatment plans. Planning and reasoning modules utilize these algorithms to optimize treatment strategies in line with standards.

When taking action, the AI generates reports using NLP to convert data into easily understandable text for humans. This involves providing recommendations and follow-up instructions. The AI assistant integrates with tools like EHR systems and medical platforms via API calls, ensuring data exchange and care coordination. The embodiment aspect entails interacting with devices like sensors and robotic surgery systems, enabling real-time data processing to improve patient care. This framework e illustrates how AI is integrated into healthcare by showcasing the flow from input to AI-driven recommendations and actions. The technical processes prioritize accuracy, efficiency and personalized care, ultimately enhancing healthcare delivery.

4-4- Decentralized Autonomous Organizations

The incorporation of DAOs in the healthcare sector has emerged as a brilliant method to boost patient involvement, simplify healthcare procedures and enhance data protection. A DAO (Figure 5) uses smart contracts on a blockchain, facilitating decision-making, transparent operations and automated reward systems. This groundbreaking structure nurtures an atmosphere where patients, healthcare professionals and other parties can interact smoothly and securely. DAOs distribute the management of electronic health records across entities to ensure all entities have complete control over the data. This distribution helps reduce the risks associated with data breaches and improves data integrity and stakeholder trust. Additionally, a vital aspect of a healthcare DAO is its incentivization system. This mechanism encourages engagement, data sharing, and adherence to treatment plans by granting tokens or rewards via blockchain technology for specific actions such as participation in clinical trials. Patients who contribute their data or participate in clinical trials can earn tokens as compensation. Moreover, patients following their treatment plans consistently can receive tokens to promote health outcomes. Besides, patients sharing their health information with researchers or healthcare providers can be motivated through token rewards promoting advancements in medical research driven by data.

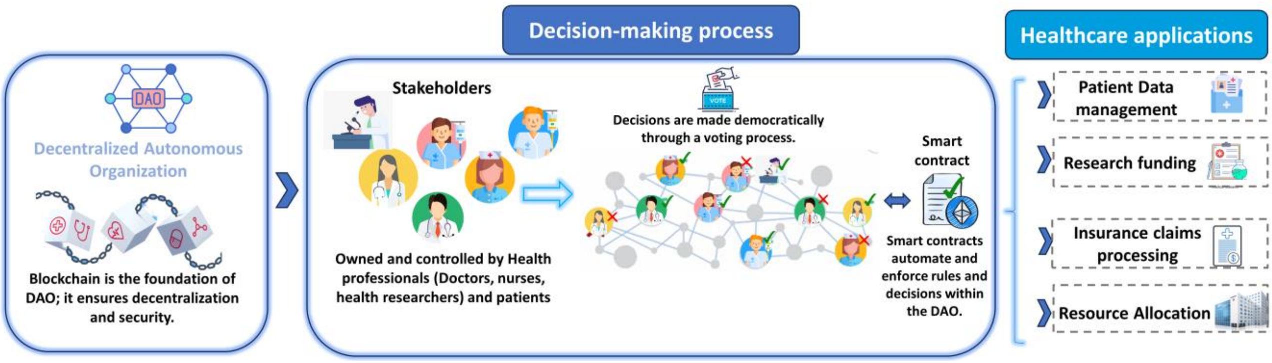

DAO
Decentralized Autonomous Organization
Blockchain is the foundation of DAO; it ensures decentralization and security.
Decision-making process
Stakeholders
Owned and controlled by Health professionals (Doctors, nurses, health researchers) and patients
VOTE
Decisions are made democratically through a voting process.
Smart contract
Smart contracts automate and enforce rules and decisions within the DAO.
Healthcare applications
Patient Data management
Research funding
Insurance claims processing
Resource Allocation

Figure 5. Decentralized Autonomous Organization Process and Applications

Moreover, the DAO's transparency guarantees that every transaction and choice can be easily traced on the blockchain. This openness helps establish trust among patients, healthcare professionals, and other involved parties, allowing them to confirm the legitimacy and equity of reward allocation independently. Additionally, The DAO promotes patient engagement by including patients in decision-making and incentivizing their involvement, leading to a patient-focused approach. Patients are no longer recipients of care but active contributors to their healthcare experience.

- **DAO reward system**

A Decentralized Autonomous Organization is a unique entity governed by rules encoded in a computer program. It is characterized by its transparency, member control, and independence from authority. DAOs are typically built on technology, ensuring openness and safety. The reward system within a DAO is designed to motivate participants for their contributions and align their interests with the organization's objectives. The DAO reward system combines three types of rewards: tokens for contributions, reputation points for enhancing influence, and a blend of token-based and reputation-based rewards to balance incentives with community engagement. This innovative reward system is a key feature of a DAO, as it encourages active participation and ensures that all stakeholders' interests are aligned with the organization's goals.

Token-based Rewards: Participants in a DAO earn tokens as rewards that can be utilized within the ecosystem or traded externally.

Reputation-based Rewards: Participants accumulate reputation points that boost their standing within the organization and may benefit them.

Hybrid Rewards: These reward systems combine token-based and reputation-based systems to balance incentives and community involvement.

In EHRs, the DAO reward system offers advantages over traditional centralized setups. Its scalability, transparency, heightened security measures and cost-effectiveness position it as a solution for managing health records while motivating contributions.

- ***Scalability*****:** By utilizing DAOs' automated aspects, healthcare institutions can enhance data management and build participant trust, improving healthcare outcomes. DAOs' scalability is inherent in their design, allowing many individuals to engage and contribute without bottlenecks. Scalability can be grasped through network effects, where the network's value grows as more participants join. With increasing data and users, the system can accommodate this growth by adding capacity and redundancy to each node.

- ***Transparency*****:** Regarding transparency, all transactions and reward distributions in the DAO are securely recorded on the blockchain. Hash functions uphold the DAO's transparency. Each transaction undergoes hashing before being included in a block that links back to blocks, creating a chain known as the blockchain.

The hash function **H(x) = y** ensures that any alteration in transaction data will modify the hash value, making tampering evident, where **x** is the transaction data, and **y** is the hash output.

- ***Security*****:** The DAO Reward System leverages the blockchain's cryptographic security features to safeguard data and rewards effectively. Public key cryptography safeguards data using private keys for encryption and decryption:
  - E_{public} (message)=ciphertext
  - $D_{private}$ (ciphertext)=message

Each participant possesses these keys, with the key used for encrypting data and the private key for decrypting it.

- ***Decentralization*****:** In a DAO Reward System, control is distributed among participants without relying on an authority. Decentralization minimizes the risk of a point of failure, as demonstrated in distributed systems theory, where the system remains operational even if some nodes fail. Consensus algorithms like Proof of Stake ensure agreement among participants.

- ***Automation*****:** Automation is integral to DAO Reward Systems, where smart contracts automate reward distribution based on predefined rules. Smart contracts execute themselves based on code instructions. They utilize statements to trigger actions: **(if (condition) then (action)**). For instance, if a participant's data contribution is validated, they receive a reward. These contracts aim to enhance cost efficiency by reducing the reliance on middlemen and cutting down transaction expenses.

- ***Cost-efficiency*****:** In DAO, reward systems and disintermediation are crucial in analyzing transaction cost reduction. This concept involves eliminating intermediaries to facilitate transactions among parties. As the number of intermediaries n approaches zero, the overall transaction cost C decreases according to the formula: $C = k \times (1-n)$, where k represents a factor related to the base transaction cost.

The reward system of DAO brings multiple advantages compared to reward systems, especially in the healthcare field. Unlike centralized reward systems, DAO reward systems are easily scalable, allowing them to efficiently manage the amounts of data generated in healthcare. They offer transparency by recording every transaction and distributing rewards on the blockchain, enabling all participants to verify data integrity and operations. Security is significantly improved by ensuring that sensitive health records remain protected from access. The decentralized nature of DAOs eliminates the risk of a point of failure. Reduces reliance on a central authority, increasing system reliability and resilience. Automation via contracts reduces burdens, cuts costs, and guarantees prompt reward distributions without manual interference. Moreover, decreasing intermediaries leads to cost-effectiveness, making the system financially viable. These advantages collectively enhance trustworthiness, efficiency and security when managing electronic health records and establishing a foundation for incentivizing contributions and maintaining data integrity. Table 3 presents the primary advantages of DAO reward systems over centralized reward systems. The DAO reward system usually provides benefits compared to the centralized reward system, especially regarding scalability, transparency, decentralization, automation, cost-effectiveness, and engaging participants. While the centralized system is secure and can enhance decision-making processes, it lacks flexibility, transparency, and efficiency.

Table 3. Comparative Table of DAO and Centralized Reward Systems

Technical Benefits	DAO Reward System	Traditional Centralized Reward System
Scalability	✓	✗
Transparency	✓	✗
Security	✓	✓
Decentralization	✓	✗
Automation	✓	✗
Cost Efficiency	✓	✗
Real-time reward distribution	✓	✗
Reduced administrative overhead	✓	✗
Enhanced trust among participants	✓	✗
Immutable transaction records	✓	✗
Improved decision-making processes	✓	✓
Lower risk of fraud and manipulation	✓	✗
Improved participant engagement	✓	✗
Efficient use of resources	✓	✗
Flexibility in reward structures	✓	✗

4-5- Security Mechanisms: Post-Quantum Cryptography and Advanced Encryption Standard

In our proposed solution, ensuring security is the primary concern. To tackle the changing landscape of cybersecurity risks with the rise of quantum computing, we utilize a mix of post-quantum cryptography (PQC) and traditional symmetric encryption. This strategy establishes a forward-looking security framework. By merging the capabilities of quantum algorithms, like CRYSTALS-Kyber and CRYSTALS-Dilithium, with the widely recognized Advanced Encryption Standard (AES), we guarantee a comprehensive shield against present-day and future cyber threats.

4-5-1- Quantum Resistance: CRYSTALS-Kyber and CRYSTALS-Dilithium

The security of EHRs is a primary concern in today's healthcare systems. Traditional encryption methods, which have long been essential for data security, face challenges with the rise of quantum computers. These advanced systems can break classic encryption algorithms, risking health information. Moreover, quantum computers use principles like superposition and entanglement from quantum mechanics to perform calculations faster than traditional computers can manage. This speed threatens traditional encryption techniques such as RSA (Rivest Shamir Adleman) [28], Elliptic Curve Cryptography (ECC), and Diffie Hellman Key Exchange. Shors algorithm, created by mathematician Peter Shor, allows quantum computers to factor numbers and solve logarithm problems efficiently. This breakthrough means that quantum computers could decrypt data protected by RSA and ECC, making these traditional encryption methods outdated. In response to this quantum threat, post-quantum cryptography has emerged as a field of study.

Post-quantum encryption focuses on creating encryption methods that can withstand attacks from both quantum computing systems. These methods are crafted to function on computers while fending off the threats of quantum computers. Post-quantum encryption includes a range of building blocks rooted in challenges thought to be complex for quantum machines to crack. There are four quantum cryptographic algorithms, each utilizing various complex mathematical challenges to safeguard against quantum attacks. These categories include lattice-based cryptography, code-based cryptography, hash-based cryptography and multivariate quadratic equations. Each category has advantages and drawbacks, making them suitable for various applications and scenarios. Our solution integrates CRYSTALS-Kyber and CRYSTALS-Dilithium to enhance security at every system level, effectively safeguarding against quantum threats.

- **CRYSTALS-Kyber:**

CRYSTALS-Kyber represents a reliable method for securing key exchange in the quantum era. It leverages lattice problems like Learning With Errors (LWE) to prevent quantum attacks [29]. Regarding its foundation, Learning With Errors poses a challenge: deriving the vectors from a matrix **A**, secret vector **s**, and error vector **e**, given **(A, As + e)**, proves computationally difficult. This difficulty stems from the Equation:

$$\mathrm{As} + \mathrm{e} \equiv \mathrm{b} \pmod{q} \tag{1}$$

CRYSTALS-Kyber enables secure, resilient key exchanges against potential quantum threats in quantum cryptography. Kyber is an algorithm created for key encapsulation methods (KEMs) in post-quantum cryptography. It forms a component of the CRYSTALS suite, known for emphasizing structures based on lattices to resist potential threats from quantum computers. Kyber works as a key encapsulation method through three significant steps represented in Figure 6:

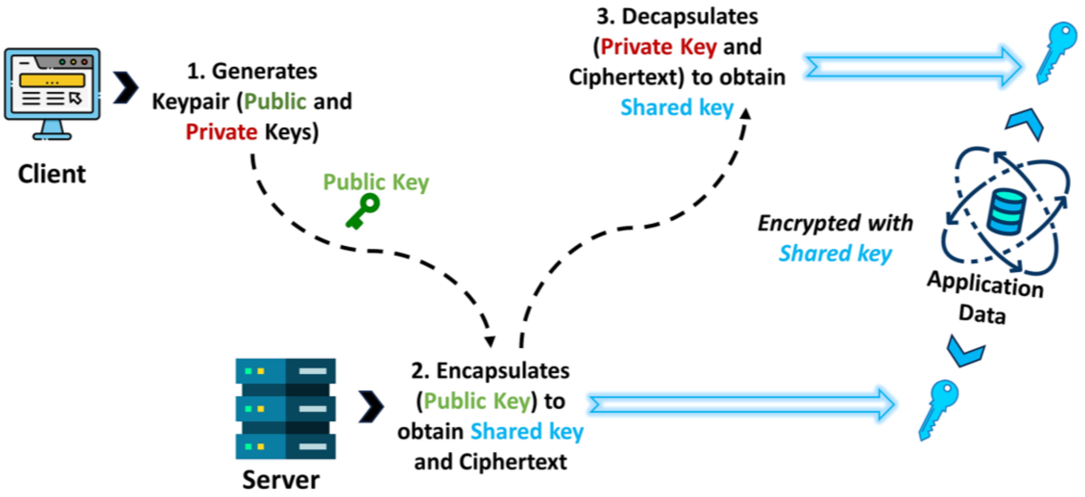

Client
1. Generates Keypair (Public and Private Keys)
Public Key
3. Decapsulates (Private Key and Ciphertext) to obtain Shared key
Encrypted with Shared key
Application Data
Server
2. Encapsulates (Public Key) to obtain Shared key and Ciphertext

Figure 6. Steps of Key Encapsulation Method

Step 1: Key Generation

- , while the private key remains confidential for decryption.
- Utilizing Lattice-Based Structures: Kyber generates keys using lattice-based structures. Specifically, it utilizes a form of a module lattice, deemed efficient and secure for quantum cryptography.

Step 2: Encryption Process

- Generating Random Seed: A random Creating Private Keys: In Kyber, the generation process involves generating public and private keys. This is achieved by selecting polynomials and using them to calculate the keys. The public key is used for encryption, and a seed is produced to facilitate the creation of the ciphertext.
- Sampling Polynomials and Compression: With the aid of the seed, polynomials are. Compressed. These polynomials encrypt a key that is then enclosed within the ciphertext.
- Deriving Symmetric Key: The symmetric key is derived through a hash function and the seed. This particular key will be used for encryption during communication sessions.
- Constructing Ciphertext: The ciphertext combines the key with the public key. Subsequently, this ciphertext can be transmitted through an insecure channel.

Step 3: Decryption Process

- Decomposing Ciphertext: Upon receiving the ciphertext, decryption takes place using the key. This method includes breaking down the encrypted text to retrieve the key.
- Recovering the Symmetric Key: The symmetric key is regained by undoing the encapsulation process and decrypting the ciphertext using the key.
- Message Verification: A hash function is employed to verify the integrity and credibility of the message. If the hash aligns, the symmetric key is deemed legitimate. This can be utilized for communication.

- **CRYSTALS-Dilithium**

Moving on to CRYSTALS-Dilithium, this cryptographic scheme is designed for signature validation in the quantum landscape. It relies on lattice problems such as Short Integer Solutions (SIS) and Learning With Errors to safeguard the genuineness and integrity of communications [30]. Expanding further on its underpinnings Short Integer Solution (SIS), Finding an integer vector $\boldsymbol{z}$ that satisfies the Equation:

$$Az \equiv u \pmod{q} \tag{2}$$

when given a matrix $\boldsymbol{A}$ and a vector $\boldsymbol{u}$ is a computational task. In post-quantum cryptography, this process is essential for securing signatures. It is utilized to generate and authenticate signatures that can withstand quantum attacks, thereby safeguarding the completeness and integrity of data. CRYSTALS-Dilithium Digital Signature Scheme follows the following steps: Figure 7 depicts the CRYSTALS-Dilithium signature procedure, which comprises the creation, signing, and validation stages. Each stage is depicted with steps and guiding arrows in Figure 7, which showcase data transfer and actions between a user and server.

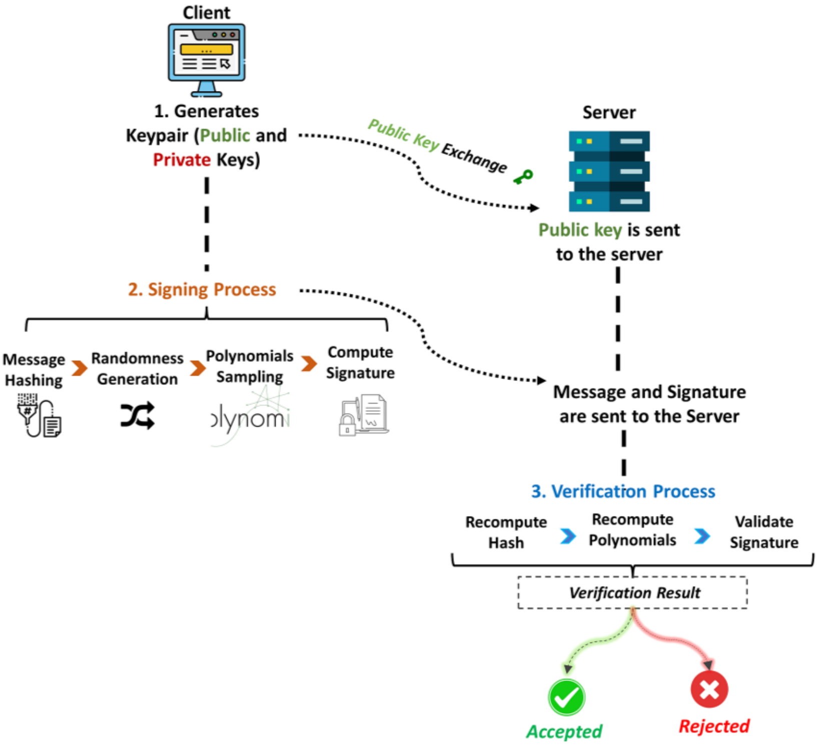


Figure 7. CRYSTALS-Dilithium Signature Procedure

Step 1: Creating Keys

- Generating Public and Private Key Pair: Random polynomials are used to create and calculate public and private keys. The public key is employed for verifying signatures, while the private key remains confidential and is used for signing messages.

Lattice-Based Approach: Like Kyber, Dilithium employs lattice-based methods that hinge on the complexity of lattice problems to ensure its security.

Step 2: Signing Process

- Hashing Messages: The message undergoes hashing to generate a fixed-length digest before signing.
- Randomness Generation: Randomness is produced using the key and the message.
- Sampling Polynomials: Polynomials are sampled using the generated randomness. These polynomials create the signature.
- Signature Calculation: The signature is computed by combining the sampled polynomials with the key, resulting in a collection of polynomials.

Step 3: Verification Procedure

- Rehashing Message: The verifier recalculates the hash of the message that needs verification.
- Recomputing Polynomials: The verifier recomputes polynomials by utilizing the key and recalculated hash.
- Validity Check: To verify whether a signature is authentic, the verifier compares these recomputed polynomials with those from received signatures, and a match indicates a signature.

4-5-2- Data Encryption: Advanced encryption standard

The Advanced Encryption Standard is well known for its effectiveness and security in encryption. It processes data in fixed blocks of 128 bits using keys of 128, 192 or 256 bits. AES works on a 4x4 array of bytes known as the state. The algorithm involves transformations carried out over rounds, with the number of rounds varying based on the key size:

- AES 128: 10 rounds
- AES 192: 12 rounds
- AES 256: 14 rounds

Key operations in each round consist of:

SubBytes: A non-linear substitution process where each byte is substituted with another byte through an S box table.

- **ShiftRows:** Rows within the state matrix are cyclically shifted by a numberal bytes.
- **MixColumns:** A mixing operation that manipulates columns by combining four bytes in each column.
- **AddRoundKey:** Each byte in the state is XORed with a key derived from the original encryption key.

Encryption Procedure of AES:

Given a plaintext block P and a key K, AES executes the following steps:

1. **Key Expansion:** Generating round keys from the cipher key.
2. **Initial Round:** Add the key through the AddRoundKey operation.
3. **Main Rounds:** In each round except the last round, apply SubBytes, ShiftRows, MixColumns and AddRoundKey.
4. **Final Round:** In the last round, only SubBytes, ShiftRows, and AddRoundKey are used without MixColumns.

AES was selected for our solution because of its security features, performance, broad acceptance and flexibility. AES has been thorough. It is known for its high level of security, making it resistant to attacks when correctly implemented. This robust security is vital for safeguarding information.

Regarding speed and efficiency, AES excels in supporting encryption and decryption processes. Its adaptability to hardware and software applications allows system integration without compromising speed or resource utilization. Moreover, AES has become a recognized standard in protocols and systems globally. Its widespread adoption ensures integration into existing setups, enhancing reliability and user-friendliness.

Furthermore, AES's versatility makes it well-suited for data encryption requirements. It guarantees data confidentiality across platforms and devices. By leveraging the capabilities of advanced encryption algorithms such as CRYSTALS-Kyber and CRYSTALS-Dilithium alongside the recognized Advanced Encryption Standard, we establish a defense mechanism against present and future security threats. The comparison Table 4 illustrates how our proposed approach stacks up against encryption techniques and other post-quantum methodologies.

Table 4. Comparison of Different Security Approaches and Methods Adopted In Our Approach

Criteria	Classical Cryptography	Post-Quantum Cryptography	Our Proposed Solution (Kyber + Dilithium + AES)
Security Against Quantum Attacks	Vulnerable (✗)	Resistant (✓)	Resistant (✓)
Key Exchange	RSA, ECC (vulnerable to quantum attacks) (✗)	Lattice-based (resistant) (✓)	CRYSTALS-Kyber (✓)
Digital Signatures	RSA, ECC (vulnerable to quantum attacks) (✗)	Lattice-based, Hash-based (resistant) (✓)	CRYSTALS-Dilithium (✓)
Data Encryption	AES (✓)	Varied (e.g., symmetric encryption combined with PQC) (✓)	AES (✓)
Performance	Efficient in current hardware (✓)	Less efficient, higher computational needs (✗)	Efficient with AES (✓)
Standardization	Widely standardized (✓)	Emerging standards (e.g., NIST PQC) (✓/✗)	Standardized components (✓)
Maturity	Highly mature (✓)	Less mature, ongoing research (✗)	Emerging but standardized (✓/✗)
Compatibility	Highly compatible (✓)	May require significant changes (✗)	Compatible through hybrid approach (✓)

Our proposed solution combines CRYSTALS-Kyber, CRYSTALS-Dilithium, and AES to create a dependable framework that effectively overcomes the limitations of individual post-quantum cryptographic techniques. By combining the advantages of each element, we guarantee protection against upcoming risks, making our solution ideal for long-lasting security requirements. This holistic strategy ensures defense against quantum threats and upholds the efficiency and adaptability needed for real-world healthcare applications.

5- Proposed Approach

This research adopts a pioneering theoretical approach by combining quantum-resistant cryptography, hybrid blockchain, decentralized governance, and user-centered engagement technologies to address critical gaps in EHR security. Traditional healthcare systems rely on centralized databases and classical encryption, which are vulnerable to quantum threats and lack interoperability. By integrating CRYSTALS-Kyber and CRYSTALS-Dilithium, our approach strengthens resilience against future quantum-based attacks, addressing long-term security concerns rarely tackled in healthcare data management. The hybrid blockchain architecture enables selective transparency by storing sensitive data on private blockchains while maintaining transparency for non-sensitive data on public blockchains, balancing privacy with accessibility. Incorporating Decentralized Autonomous Organizations (DAOs) further decentralizes data control, empowering patients in data governance, which aligns with ethical standards in patient-centered care. Additionally, AI and metaverse integration enhance engagement, offering an interactive platform for virtual consultations and real-time decision support, enabling patient involvement and trust. This multi-faceted framework sets a new benchmark by addressing scalability, security, and ethical data governance, filling a vital gap in EHR frameworks and advancing theoretical understanding in quantum-resistant healthcare solutions.

5-1- Architecture

Despite its progress and vital role in society, the healthcare industry continues encountering obstacles hindering its efficiency and effectiveness. Key among these challenges are concerns about data security, a widespread lack of involvement and notable inefficiencies in healthcare delivery. These issues impact the quality of care offered and influence the healthcare experience for both patients and providers. In light of the increasing challenges faced by the healthcare domain, including issues such as data breaches, limited patient involvement and systemic inefficiencies, there is a pressing demand for a healthcare system that is cohesive, secure and focused on the requirements of patients. The proposed approach solves these obstacles by leveraging advanced technologies to establish a practical, safeguarded, patient-focused healthcare setting. The focus of the approach incorporated the following:

- ***Integrative technological strategy***: At the heart of this novel approach lies a strategy that harmoniously integrates blockchain technology, artificial intelligence and immersive metaverse environments. This integrated approach tackles technological and operational hurdles and transforms the healthcare landscape for providers and patients.
- ***Blockchain adoption for enhanced security and transparency*****:** This framework acknowledges the significance of data security and patient confidentiality and adopts a blockchain model. This model efficiently separates health data from sensitive information to ensure robust security where necessary while upholding transparency and accessibility for general health-related data.
- ***AI for personalized care and simplified processes*****:** AI is pivotal in this architectural design. It analyzes extensive health data to offer customized health guidance, predictive analytics, and real-time decision support. This improves the precision and efficiency of healthcare services and significantly reduces the time needed for diagnosing and planning treatments.
- ***Engagement and accessibility in the metaverse***: The metaverse aspect of the structure transforms involvement by creating a virtual healthcare environment where patients can interact naturally with healthcare providers. This virtual environment enhances access to healthcare services in areas and encourages patients to actively participate in managing their health through engaging interactive tools.
- ***Scalability and flexibility*****:** at its core, the design prioritizes scalability and flexibility, allowing it to grow with an expanding user base and seamlessly integrate with existing healthcare systems. This adaptability ensures that the proposed solution can adapt to healthcare demands and technological advancements.
- ***Enabling a collaborative community***: By incorporating decentralized organizations (DAOs) and incentive programs, the structure promotes an ecosystem where all stakeholders, including patients, medical professionals and healthcare institutions, have a position (voice) in system management and continual enhancement.

The proposed system is structured into four layers (user interface layer, application layer, blockchain layer, and storage layer), each playing a crucial role in healthcare management. These layers work harmoniously to provide a secure and engaging healthcare service, as illustrated in Figure 8, providing a clear understanding of the system's structure.

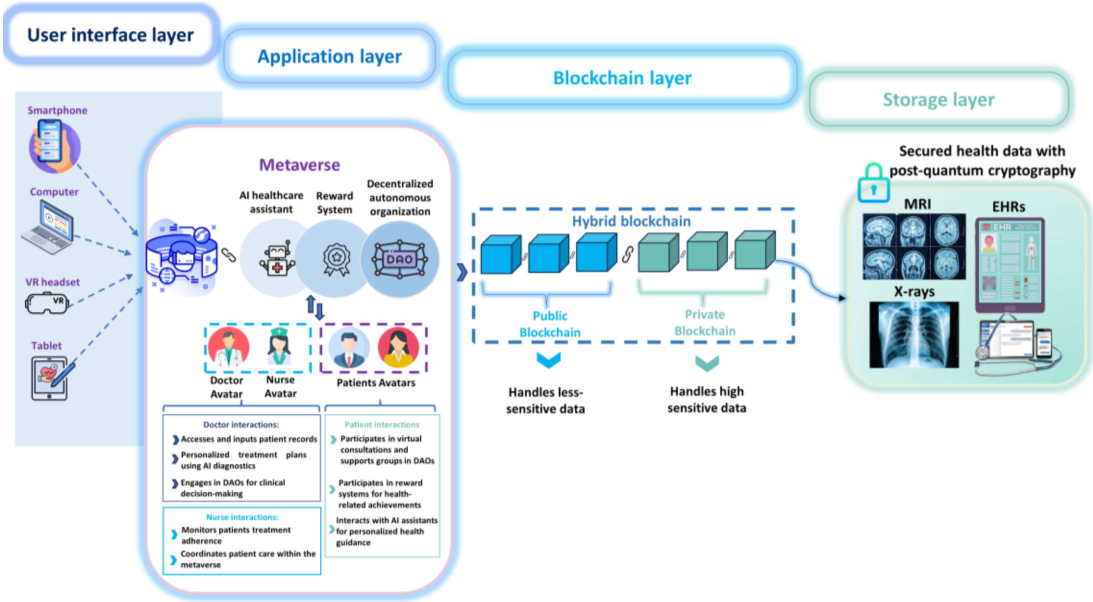

User interface layer
Application layer
Blockchain layer
Storage layer
Smartphone
Computer
VR headset
VR
Tablet
Metaverse
AI healthcare assistant
Reward System
Decentralized autonomous organization
DAO
Doctor Avatar
Nurse Avatar
Patients Avatars
Doctor interactions:
Accesses and inputs patient records
Personalized treatment plans using AI diagnostics
Engages in DAOs for clinical decision-making
Nurse interactions:
Monitors patients treatment adherence
Coordinates patient care within the metaverse
Patient interactions
Participates in virtual consultations and supports groups in DAOs
Participates in reward systems for health-related achievements
Interacts with AI assistants for personalized health guidance
Hybrid blockchain
Public Blockchain
Private Blockchain
Handles less-sensitive data
Handles high sensitive data
Secured health data with post-quantum cryptography
MRI
EHRs
EHR
X-rays

Figure 8. Architecture of the Quantum-Resistant Hybrid Blockchain Framework for Securing EHRs

1. *User interface layer:*

This particular layer acts as the point of contact for users, including patients and healthcare professionals, to engage with the system. A variety of devices support it, fulfilling function:

- **Smartphones** are utilized to access healthcare applications on the go. Users can receive alerts, view records, and communicate directly with healthcare providers through their devices.
- **Healthcare professionals frequently use computers** for in-depth tasks such as analyzing patient data, interpreting diagnostic details, and devising treatment strategies.
- **VR Headsets:** These devices offer immersive experiences for therapy sessions, detailed consultations, and simulations. Patients could virtually visit a doctor's office, while doctors could visualize conditions in 3D.
- **Tablets** function as tools for both healthcare providers and patients. They are portable and user-friendly, suitable for telemedicine consultations, patient education sessions, and health record management.

Each device improves the connection between the healthcare system and its users, making healthcare more reachable, effective, and tailored to individual patient requirements. This strategy utilizes technology to reduce obstacles and enhance healthcare results by integrating cutting-edge tools into healthcare interactions.

2. *Application layer*

By utilizing the functions of these devices, the application layer goes a step further in enhancing user experience by incorporating applications and virtual environments that use artificial intelligence within an engaging Metaverse framework. The following are the primary components of the application layer:

- **AI Healthcare Assistant:** This type of assistant offers automated, intelligent assistance for healthcare services. It analyzes data for recommendations, devises personalized treatment strategies, tracks patient health indicators, and promptly alerts healthcare professionals of critical changes in patient status.
- **Incentive System:** This system encourages involvement and adherence to treatment plans through rewards. It grants points or badges for completing health-related tasks, offers benefits for adhering to medication schedules, and motivates patients with engaging health-related challenges.
- **Decentralized Autonomous Organization (DAO):** This supports decentralized decision-making processes driven by the community. It is integrated to Empower patients and healthcare professionals in governance decisions, facilitate virtual health consultations and support groups, and coordinate collaborative care initiatives within the Metaverse.
- **Doctor Avatars:** Represent healthcare experts. They access and update records, conduct consultations, create customized treatment plans, and contribute to clinical decision-making processes within the virtual setting.
- **Nurse Avatars:** They are involved in patient care and monitoring. In the Metaverse, patient treatment adherence is monitored, patients receive education, care activities are coordinated, and doctors are supported during consultations.
- **Patient avatars** serve as representations of patients in the Metaverse. They engage in consultation support groups, interact with AI assistants for health guidance, and monitor health metrics.

The primary objective of this application layer is to enhance healthcare experiences by utilizing applications and virtual environments to boost outcomes and engagement through interactive systems.

3. *Blockchain layer*

This section oversees the transfer and preservation of data in a blockchain setup that includes both public and private blockchains. The following are the main components:

- **Public Blockchain:** manages information that is not highly confidential and requires openness to an audience. It records health details, maintains health records, and tracks healthcare transactions that do not involve sensitive data but benefit from transparency and traceability.
- **Private Blockchain**: This blockchain handles confidential data to ensure its protection and confidentiality. It stores patient information, records health transactions, maintains secure access records, and manages encrypted medical files. The private blockchain establishes a transparent system for managing healthcare data transactions and storage by leveraging blockchain technology capabilities to safeguard data integrity and privacy.

Encrypted and authenticated data from the blockchain layer is securely moved to the storage layer for long-term archiving and retrieval.

4. Storage layer

The storage layer securely stores health information by using a mix of cryptography methods and AES encryption. This layer is responsible for upholding the confidentiality, accuracy and trustworthiness of stored health information to safeguard against access while ensuring its availability for medical purposes. This layer can gather the following components.

- **MRI Scans** are used to retain imaging data for medical diagnoses. Keeping MRI images safe through robust encryption guarantees that these high-quality scans are stored securely and can only be accessed by personnel.
- **X-rays:** are used to store X-ray images for diagnoses and treatment planning. Safeguarding X-ray images in storage, enabling radiologists and doctors to access them while ensuring data confidentiality.
- **Electronic Health Records are** used to maintain patient health records securely. They store patients' complete histories, lab results, medication lists, treatment plans, and ongoing health monitoring data.

5-2- Data Workflow

At the User Interface Layer, users start logging into their devices like smartphones, computers, VR headsets or tablets by verifying their identity through user authentication. After authentication, the device begins a key exchange by sending its public key to the application server. The server then reciprocates with its key to enable both sides to create a shared secret for communication. The data is digitally signed on the device for authenticity and encrypted for protection against access before being sent to the application layer. Security features in this layer include utilizing CRYSTALS-Kyber for exchanges and AES for data encryption to ensure data confidentiality.

In the Application Layer, incoming data is first checked for integrity. Then, it is re-encrypted during processing to uphold security standards. Users engage in activities within realms using avatars and AI helpers to ensure authenticated sessions. Transactions are encrypted and signed before being sent to the layer. To ensure security, CRYSTALS-Dilithium is used for data verification and signing interactions, while AES is employed for data encryption (Algorithm 1).

Algorithm 1. Pseudocode for user interface layer

```
function UserAuthentication(user_credentials):
    if VerifyCredentials(user_credentials):
        session_key = CRYSTALS_Kyber_KeyExchange()
        return session_key
    else:
        return "Authentication Failed"
// Data Encryption before Transmission
function EncryptData(session_key, data):
    roundKeys = AESKeyExpansion(session_key)
    encrypted_data = AESEncrypt(data, roundKeys)
    return encrypted_data
function TransmitData(encrypted_data):
    SendToApplicationLayer(encrypted_data)
```

In the Blockchain Layer, nodes exchange keys using CRYSTALS-Kyber to facilitate communication within the network. Signed transactions are. They are stored on the blockchain to maintain a ledger. Before data is stored, it undergoes encryption for confidentiality and integrity purposes. Security measures include using CRYSTALS-Kyber for exchanges and AES for encrypting data to storage. The **ReceiveData** function obtains encrypted data from the user interface layer. The **ProcessData** function decrypts this data using the session key, processes it, and prepares it for transaction. The **CreateTransaction** function then signs the processed data using CRYSTALS-Dilithium and creates a transaction object. Finally, the **SendTransaction** function sends this transaction to the blockchain layer (Algorithm 2).

Algorithm 2. Pseudocode for Blockchain layer

```
function ReceiveData():
    encrypted_data = GetDataFromUserInterfaceLayer()
    return encrypted_data

function ProcessData(encrypted_data, session_key):
    roundKeys = AESKeyExpansion(session_key)
    data = AESDecrypt(encrypted_data, roundKeys)
    // Further processing of the data
    processed_data = AnalyzeAndProcess(data)
    return processed_data

function CreateTransaction(processed_data, private_key):
    signature = DilithiumSign(private_key, processed_data)
    transaction = { "data": processed_data, "signature": signature }
    return transaction
function SendTransaction(transaction):
    SendToBlockchainLayer(transaction)
```

In Algorithm 3, the **BlockchainNodeKeyExchange** function generates a node key using CRYSTALS-Kyber for secure key exchange. The **RecordTransaction** function encrypts the transaction with this node key and stores it on the blockchain, ensuring the transaction is securely recorded.

Algorithm 3. Pseudocode for blockchain layer

```
function BlockchainNodeKeyExchange():
    node_key = CRYSTALS_Kyber_KeyExchange()
    return node_key

function RecordTransaction(transaction, node_key):
    encrypted_transaction = EncryptTransaction(node_key, transaction)
    StoreOnBlockchain(encrypted_transaction)
    return "Transaction Recorded"
```

The Storage Layer focuses on storing health information like MRI scans, X-rays and EHRs. Data is signed with CRYSTALS- Dilithium to guarantee authenticity and integrity before being stored. The final steps involve securing the storage of signed and encrypted health data to ensure secure access and verification of data. This layer utilizes CRYSTALS-Dilithium for signing purposes and AES for decrypting data when accessed to allow authorized personnel to view the stored information (Algorithm 4).

Algorithm 4. Pseudocode for storage layer

```
function SignDataForStorage(data, private_key):
    signature = DilithiumSign(private_key, data)
    signed_data = { "data": data, "signature": signature }
    return signed_data
function StoreData(signed_data):
    StoreInSecureStorage(signed_data)
    return "Data Stored Securely"
function AccessData(data_id, private_key):
    signed_data = RetrieveFromStorage(data_id)
    if DilithiumVerify(signed_data["data"], signed_data["signature"], private_key):
        return signed_data["data"]
    else:
        return "Verification Failed"
```

Adhering to this organized process and implementing security measures at every level guarantee safeguarding healthcare information against unauthorized entry and potential online risks. The distinct security measures at each level are essential in creating an effective system that instils trust in the reliability and privacy of patient data. The upcoming section presents a scenario of patient interaction in the architecture and how the different components of the approach work jointly to offer a magnified healthcare ecosystem and ensure robust security levels.

5-3- Use Case Scenario

Our healthcare virtual world provides a comprehensive platform for patient care, as demonstrated through the medical history of the patient, a 41-year-old woman dealing with hypertension and Type 2 diabetes. Figure 9 presents a scenario where a patient integrates their health portal via phone and VR headset to have a virtual consultation with the doctor securely.

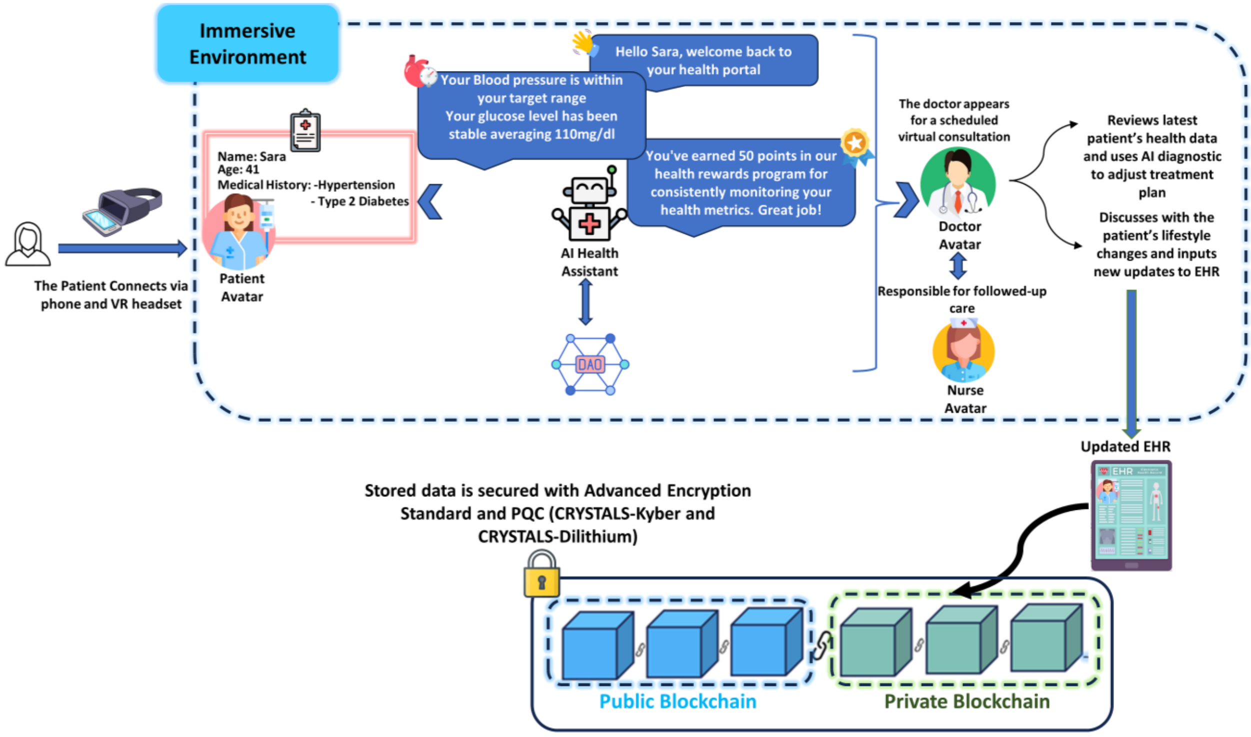

Immersive Environment
The Patient Connects via phone and VR headset
Name: Sara
Age: 41
Medical History: -Hypertension
- Type 2 Diabetes
Patient Avatar
Your Blood pressure is within your target range
Your glucose level has been stable averaging 110mg/dl
Hello Sara, welcome back to your health portal
You've earned 50 points in our health rewards program for consistently monitoring your health metrics. Great job!
AI Health Assistant
DAO
The doctor appears for a scheduled virtual consultation
Doctor Avatar
Reviews latest patient's health data and uses AI diagnostic to adjust treatment plan
Discusses with the patient's lifestyle changes and inputs new updates to EHR
Responsible for followed-up care
Nurse Avatar
Updated EHR
EHR
Stored data is secured with Advanced Encryption Standard and PQC (CRYSTALS-Kyber and CRYSTALS-Dilithium)
Public Blockchain
Private Blockchain

Figure 9. Use Case Scenario of Our Proposed Approach

On the other hand, the nurse checks the patient's adherence to treatment plans, ensuring she sticks to medications and exercises while planning care steps. The patient electronic health record is regularly updated to ensure that all of her health information remains current and easily accessible. Our system uses private blockchain technologies to protect patient's data and the newly added changes by the doctor. Then, this record is stored in the private blockchain, which safeguards highly confidential information such as EHRs and medical images. For this process, robust encryption methods such as Advanced Encryption Standard and Post-Quantum Cryptography using CRYSTALS-Kyber and CRYSTALS-Dilithium are employed to secure the data against access. At the same time, the public blockchain manages less sensitive data, such as general health tips. This example showcases how our healthcare virtual environment delivers personalized, timely and consistent care by integrating artificial intelligence blockchain technology and immersive settings to elevate the experience and improve treatment effectiveness.

Remaining within the benefits of our proposed solution, the following section presents an extensive overview of its primary advantages. The following section focuses on the aspects of our proposed solution, illustrating how it tackles obstacles and integrates contemporary to improve the entire health services.

6- Key Benefits of the Proposed Solution

The novel proposed system combines pioneering technologies like blockchain artificial intelligence and metaverse settings to tackle the issues surrounding the management and security of electronic health records. The following are the primary advantages of this solution (Figure 10).

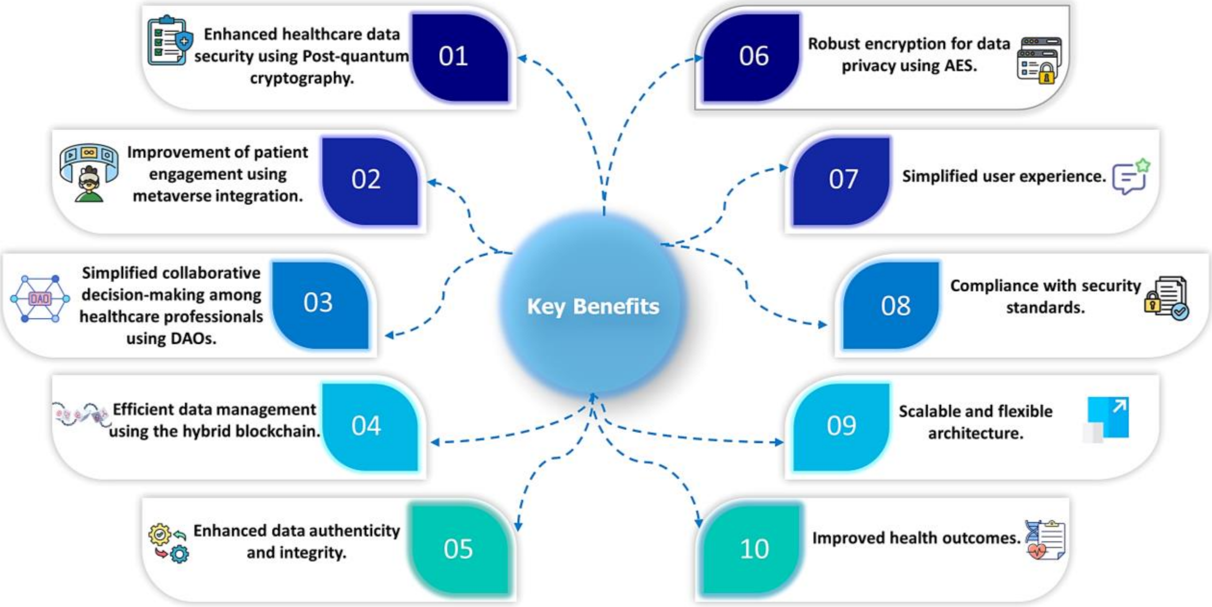

Key Benefits
01 Enhanced healthcare data security using Post-quantum cryptography.
02 Improvement of patient engagement using metaverse integration.
03 Simplified collaborative decision-making among healthcare professionals using DAOs.
DAO
04 Efficient data management using the hybrid blockchain.
05 Enhanced data authenticity and integrity.
06 Robust encryption for data privacy using AES.
07 Simplified user experience.
08 Compliance with security standards.
09 Scalable and flexible architecture.
10 Improved health outcomes.

Figure 10. Benefits of the Proposed Solution

- **Enhancing Security Measures for Healthcare Data through Advanced Cryptography:** With the advancement of quantum computing, there is a growing concern over the vulnerability of traditional encryption methods. To address this, we have proposed post-quantum cryptography utilizing algorithms specifically designed to withstand potential attacks from quantum computers. This ensures the safety and confidentiality of data even in the evolving landscape of quantum technology. By adopting this approach, we safeguard healthcare information from future threats, bolstering patient confidence and compliance with strict data protection regulations.

- **Enhancing Patient Engagement through Integration with Metaverse Technology:** The metaverse provides a space where patients can engage with healthcare professionals and services more personally and interactively through virtual consultations and interactive health education. Customized wellness experiences are offered on metaverse platforms. This adopted approach to engagement can increase satisfaction levels, adherence to treatment plans, and overall health outcomes by engagingly enhancing access to healthcare services.

- **Facilitating Collaborative Decision-Making for Healthcare Professionals Using DAOs:** Decentralized Autonomous Organizations empower healthcare professionals to participate in decision-making processes without control. By leveraging technology, DAOs facilitate transparent and inclusive governance structures within healthcare teams. Improved teamwork among healthcare providers results in effective patient care decision-making, enhancing service quality and nurturing a collaborative healthcare environment.

- **Efficient Data Management through Hybrid Blockchain Technology:** Hybrid blockchain technology merges the privacy elements of blockchains with the security and transparency of blockchains. This unique approach allows confidential patient data to be securely stored and shared with parties while maintaining a clear and unchangeable record of transactions. Healthcare institutions can handle data effectively and securely, ensuring its integrity and minimizing the risks associated with access or data breaches. Our proposed method is a major improvement over current EHR systems as it integrates quantum cryptography with a hybrid blockchain framework. In contrast to existing frameworks that use classical encryption, which is susceptible to quantum attacks, our method uses both the CRYSTALS-Dilithium and CRYSTALS-Kyber algorithms to produce encryption that is resistant to quantum attacks. This guarantees that EHR data is safe from future quantum attacks, which is a degree of security that is unmatched by conventional systems. Furthermore, to maximise security and transparency, our hybrid blockchain design separates sensitive and non-sensitive data across private and public blockchains. While non-sensitive data can be kept on a public blockchain to provide transparency for authorised parties, sensitive patient data is safeguarded on a private blockchain with restricted access. Our system can adaptably handle the complexity of healthcare data thanks to this dual-layered protection, which requires accessible transparency and refined security. Our hybrid blockchain architecture guarantees that sensitive EHR data is kept on a private blockchain and overseen by Decentralised Autonomous Organisations, which offer improved data management and governance, in contrast to traditional systems that rely on centralised databases that are vulnerable to breaches. This implies that since sensitive data is divided on a different private blockchain, it will not be compromised in the event of a breach on the public blockchain. By providing improved scalability, interoperability, and user involvement through metaverse integration, this framework performs better than existing systems.

- **Enhancement of Data Integrity:** It utilizes hybrid blockchain technology to document every data exchange in a ledger. This guarantees that healthcare-related information, from records to studies, remains unchanged and genuine. Upholding the authenticity and integrity of data is crucial for diagnosis, treatment procedures, and adherence to regulatory standards. Ultimately, this promotes trustworthiness and reliability within healthcare systems.
- **Robust Data Privacy Encryption Utilizing Advanced Encryption Standard:** Advanced Encryption Standard (AES) is a trusted encryption technique for safeguarding data. Our solution incorporates AES to encrypt patient details and other sensitive information during transmission and at rest. We adopted the AES encryption system, which offers data protection and safeguards it from unauthorized access and security breaches. This helps healthcare providers with regulations and boosts patient trust in data security measures.
- **Improved User Experience:** For a user experience, our solution features an intuitive interface designed for both healthcare professionals and patients. With workflows, easy navigation, and responsive design, users can efficiently. Utilize the system functions. This simplified approach reduces learning curves and minimizes errors. It improves satisfaction, allowing healthcare professionals to focus on patient care rather than complex system management. Our solution is meticulously crafted to meet or exceed healthcare industry security standards to ensure compliance with these requirements. Integrating these standards into the system's foundation aligns all data-handling processes with the regulations. Adhering to security standards not only aids in avoiding penalties but also upholds patient privacy and maintains a reputable image in the healthcare sector.
- **Increased Scalability and Flexibility:** Our solution, built with scalability and flexibility at its core, empowers healthcare organizations to adapt and expand to meet evolving needs. The architecture supports integrating existing systems while effectively handling technological advancements and increased data loads. The ability to adjust and evolve guarantees that organizations can grow their capabilities without necessitating changes or interruptions, ensuring long-term sustainability and cost-effectiveness.
- **Enhanced Health Results:** Our solution empowers healthcare providers to offer patients more precise, timely and customized care by incorporating technologies and maintaining data handling and security measures. Enhanced health outcomes result from increased involvement, efficient operations and informed medical choices, ultimately delivering superior quality care and boosting patient contentment.

7- Comparative Analysis

In this section, we compare our suggested framework with research. We aim to showcase our method's contributions, illustrating how it tackles constraints and enhances the approaches detailed in academic works. By assessing the merits and drawbacks of our framework and established solutions, we offer an insight into its influence and real-world uses. Table 5 outlines how the proposed system enhances security compared to traditional cryptographic techniques, especially in preparation for future quantum computing threats.

Table 5. Comparison of Traditional Systems and Our Solution

Security Aspect	Proposed Framework	Traditional cryptographic Techniques
Data Security	It includes a hybrid blockchain for dual-layer protection.	It uses traditional centralized databases, which are more vulnerable to cyber threats.
Cryptographic Robustness	It offers an elevated level of protection against quantum computing attacks due to the employment of PQC.	They are exposed to quantum attacks because no reinforced security measures against these new-age vulnerabilities exist.
Encryption Algorithms	It incorporates classical encryption algorithms (AES) and Post-quantum cryptography, offering a dual level of protection.	It mainly relies on classical encryption algorithms such as AES, which is considered secure; however, with the advent of quantum computing risks, it is considered vulnerable.
Decentralization	It relies on blockchain technology, which offers an advanced level of decentralization.	Primarily, it relies on centralized databases, which make these systems prone to cyber-attacks.
Data Integrity	With blockchain employment, immutability and transparency are ensured, making unauthorized data tampering complex.	Ensures integrity through cryptographic hash functions, but centralization introduces risks of undetected tampering.
User Authentication	Decentralized identity management is employed in the metaverse to boost security by utilizing identities and AI support.	Classical approaches rely on passwords and two-factor authentication, which are susceptible to phishing and social engineering threats.
Scalability	The system scales by integrating hybrid blockchain and metaverse interactions, ensuring substantial data volumes are processed.	Centralized systems frequently encounter bottlenecks and limited scalability due to the requirement for infrastructure.
Resilience against Quantum Attacks	The solution is crafted to withstand risks posed by quantum computing by implementing post-quantum cryptography.	They are exposed to the vulnerabilities posed by quantum computing, which can easily crack methods.
Patient Control & Privacy	Provides patients with control over their data through decentralized autonomous organizations (DAOs) in the metaverse.	Central authorities often control patient data, with less transparency and control for the patient.
Interoperability	Due to its hybrid nature, it can integrate with existing healthcare systems and future quantum-resistant systems.	It often needs more flexibility in integration with quantum-resistant systems.

Moreover, Table 6 compares relevant studies in blockchain-based healthcare solutions, outlining how each addresses essential aspects of electronic health record security and management. From Table 6, our proposed system stands out as a forward-thinking solution. It tackles the fundamental security and privacy issues. It guarantees scalability and compatibility, which is vital for healthcare solutions' widespread acceptance and efficiency in a progressively digital and interconnected environment. By incorporating technologies like quantum cryptography and Decentralized Autonomous Organizations, your system is poised to tackle present and future obstacles in the healthcare industry.

Table 6. Comparative Table of Our Approach vs Existing Studies

Criteria	Sharma et al. (2023) [31]	Dong et al. (2023) [32]	Babu et al. (2023) [33]	Our proposed System
Decentralized Application	✓	✓	✓	✓
Blockchain Integration	✓	✓	✓	✓
Proof of work consensus	✓	✗	✗	✗
Permissioned Blockchain	✗	✓	✓	✓
Unique Identification for Medical Certificates	✓	✗	✗	✓
Patient-Controlled Security and Privacy	✓	✗	✗	✗
Anonymity of Patient Data	✗	✓	✓	✓
Integration of AI and Metaverse	✗	✗	✗	✓
Decentralized Autonomous Organizations	✗	✗	✗	✓
Comprehensive EHR security	✓	✓	✓	✓
Resilience to Quantum Attacks	✗	✗	✗	✓
Enhanced User Engagement and Compatibility	✗	✗	✗	✓
Scalability	✗	✓	✓	✓
Interoperability	✗	✓	✓	✓
Lower Cost across Care	✗	✗	✓	✓

Furthermore, Table 7 presents an analysis of various critical security adaptive metrics of either a traditional EHR system or our alternate hybrid solution resistant to quantum attacks driven by distributed ledger technology. These metrics emphasize the security, data accuracy, interaction, and adherence to improvement as a result of employing quantum-resistant cryptography, distributed management, and a hybrid of blockchain systems. This comparison does justice in gauging the advantages that our solution presents over traditional systems especially in tackling quantum threats and securing healthcare data.

Table 7. Security Metrics of Traditional systems and our Proposed System

Security Metric	Traditional EHR Systems [34-36]	Our Proposed Solution
Quantum Attack Resistance	Vulnerable (0%)	99.9%
Data Integrity (Tamper-Resistant)	85%	99%
Encryption Strength	AES 128-bit or RSA	AES 256-bit + CRYSTALS-Kyber & CRYSTALS-Dilithium
Data Breach Frequency (Incidents/Year)	2-3 per year (average)	<1 per year
Access Control Effectiveness	75-80%	95%
Interoperability with Legacy Systems	60%	90%
System Downtime	5-10 hours/year	<1 hour/year
Data Privacy Compliance (HIPAA Score)	80%	98%
Scalability (Users Supported)	Up to 10,000	Up to 100,000
User Trust/Transparency	70%	90%
Overall Security Score	75%	95%

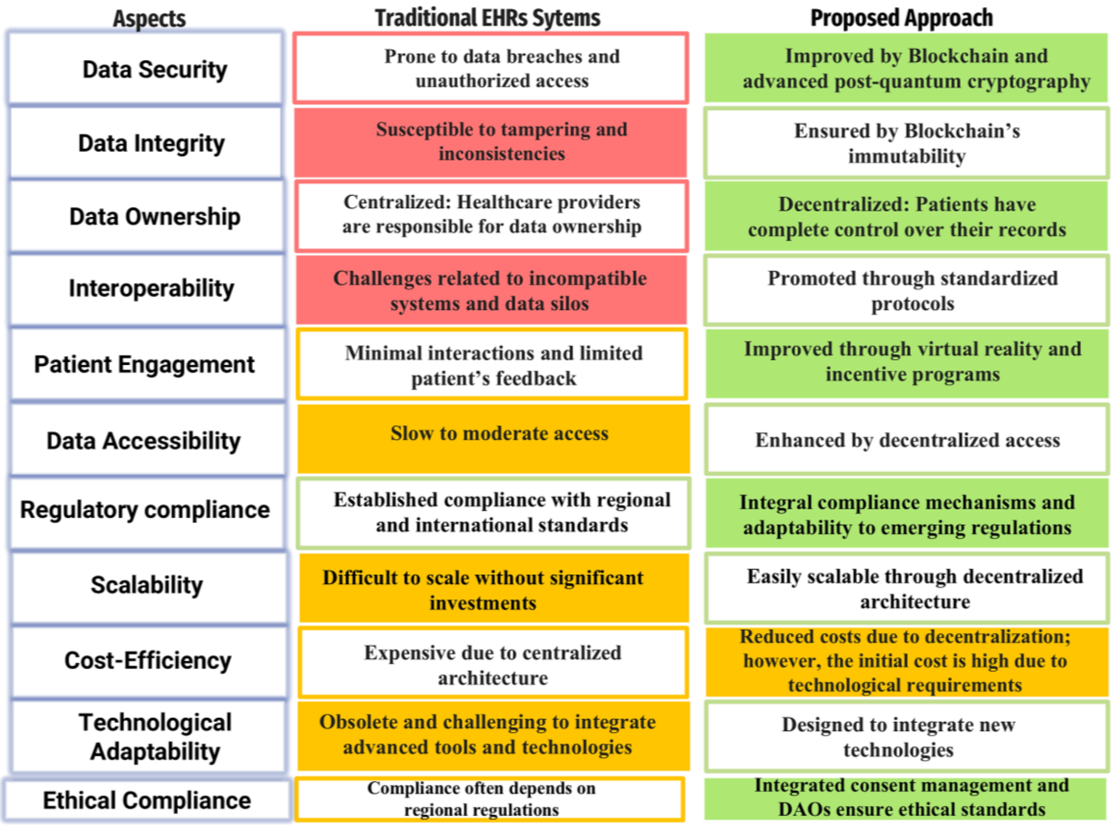
- **Quantum Attack Resistance:** The classical EHR systems are inherently weak and cannot resist quantum attacks, hence they are at risk of breaches from the prospective quantum computers. The CRYSTALS-Kyber and CRYSTALS-Dilithium algorithms which are both considered quantum proof are incorporated into our solution creating an effect of almost complete protection from quantum attacks. This addition also enhances security in the long run by safeguarding against risks that the growth of technology would have posed on healthcare-sensitive information to keep it safe for many years.

- **Data Integrity:** Traditional EHR systems, the majority of which use centralized databases, exhibit a very low capacity for tampering that is about 85% efficient due to many centralized vulnerability points. Our approach is based on the use of an immutable blockchain, where for every transaction there is a record created and no alteration is possible without detection. The advancement in Data Integrity assurance enables it to reach 99% levels which guarantees that electronic health records EHRs will not change with time and will be protected to the utmost levels which is very important in keeping the patients' records safe as well as meeting various laws and regulation requirements.
- **Data breach frequency:** An attack on traditional systems is highly likely to occur more than once every year since they have a centralized structure which bears single points of attack and can easily attacked. Unlike this, the distributed layout of the blockchain technology used in our solution and the strong encryption system that goes along with it minimizes the risk as data cannot be lost and the level of security is more so that it is not easy to break into core data. This reduces the incidence of annual healthcare data breaches to below even one occurrence in a year thus creating an exceedingly safe environment for data in the healthcare sector.
- **Access Control Effectiveness**: Traditional systems often achieve 75-80% access control effectiveness, due to single-layer access protocols and limited encryption methods. In contrast, our solution improves this effectiveness to 95% by implementing decentralized access controls through Decentralized Autonomous Organizations, where permissions are managed more granularly, and by using advanced encryption techniques. This dual approach ensures that only authorized individuals access specific data segments, enhancing security and user trust.
- **Interoperability with Legacy Systems**: Traditional EHR systems struggle with compatibility across different platforms, resulting in data silos and limited communication between systems. Our framework’s modular architecture, supported by standardized APIs, promotes interoperability, achieving 90% compatibility. This design allows seamless integration with legacy systems and healthcare platforms, enabling efficient data exchange and reducing administrative burdens, particularly in diverse healthcare environments.
- **System Downtime**: Due to the centralized nature of conventional systems, they frequently encounter more downtime, averaging 5-10 hours per year, which can disrupt healthcare operations. Our solution's distributed blockchain design enhances resilience by eliminating single points of failure and enabling continuous operations. This reduces downtime to less than one hour per year, providing higher availability and reliability, crucial for real-time healthcare needs.
- **Data Privacy Compliance**: While conventional EHR systems generally meet regulatory requirements, they often face challenges in ensuring real-time auditing, transparency, and adherence to strict privacy standards. Our system enhances compliance by leveraging blockchain's transparency and incorporating DAO governance for real-time data monitoring and auditing capabilities. This approach boosts privacy compliance to 98%, aligning with stringent regulatory standards and fostering patient trust in data privacy protections.

8- Discussion

Our proposed system combines blockchain, AI and virtual reality to tackle the security, accessibility and engagement issues in healthcare setups. Blockchain technology ensures the security and transparency of records by decentralizing them, reducing the chances of data breaches. Using permissionless blockchains allows for separating non-sensitive data to balance openness with privacy requirements. This strategy aligns with healthcare technology advances, like tamper-proof records and secure consent management. Incorporating post-quantum cryptography into our system addresses concerns about methods being vulnerable to quantum computing attacks. Combining encryption standards with post-quantum cryptographic techniques safeguards our system against current and future cyber threats. This two-layered approach guarantees the security of EHRs and medical imaging data while upholding top-notch data protection standards. Previous research has emphasized the significance of advancements in protecting health information using post-quantum methods.

Integrating the metaverse into our system introduces an approach to boost engagement and interaction. By establishing an environment where patients can communicate with healthcare providers through avatars, our system creates an immersive and interactive healthcare experience. Integrating AI-powered diagnostics in this environment enhances the precision and effectiveness of patient care. Moreover, implementing reward structures in the metaverse encourages patients to manage their healthcare, potentially boosting adherence to treatment plans and overall health outcomes. This strategy tackles systems' shortcomings that often need more real-time communication avenues and patient involvement. Interoperability poses a hurdle in healthcare information systems leading to data silos that obstruct data sharing. Our proposed framework promotes interoperability by establishing protocols and frameworks for Electronic Health Record (EHR) systems. This ensures health data sharing across platforms and healthcare providers, enabling coordinated care and enhancing patient outcomes. Furthermore, our emphasis on user interfaces aims to overcome usability challenges by designing interfaces for smartphones, tablets, computers and VR headsets. This ensures interaction with the system for healthcare providers and patients, promoting adoption and effective utilization. We must address regulatory concerns as we incorporate top-notch technologies into healthcare practices. Our system includes processes for obtaining consent and managing data ownership to comply with privacy laws and ethical standards. Leveraging Decentralized Autonomous Organizations within the metaverse establishes a transparent framework for handling patient data interactions responsibly. Figure 11 presents a comparison to showcase the benefits of our proposed approach compared to traditional electronic healthcare systems. This schema outlines factors like data protection, patient involvement, compatibility and other features with colour-coded columns for enhanced understanding. Where Red Indicates the Gravity of the Risk, Orange Indicates Moderate Risk, and Green Indicates Low Risk.



Aspects	Traditional EHRs Sytems	Proposed Approach
Data Security	Prone to data breaches and unauthorized access	Improved by Blockchain and advanced post-quantum cryptography
Data Integrity	Susceptible to tampering and inconsistencies	Ensured by Blockchain's immutability
Data Ownership	Centralized: Healthcare providers are responsible for data ownership	Decentralized: Patients have complete control over their records
Interoperability	Challenges related to incompatible systems and data silos	Promoted through standardized protocols
Patient Engagement	Minimal interactions and limited patient's feedback	Improved through virtual reality and incentive programs
Data Accessibility	Slow to moderate access	Enhanced by decentralized access
Regulatory compliance	Established compliance with regional and international standards	Integral compliance mechanisms and adaptability to emerging regulations
Scalability	Difficult to scale without significant investments	Easily scalable through decentralized architecture
Cost-Efficiency	Expensive due to centralized architecture	Reduced costs due to decentralization; however, the initial cost is high due to technological requirements
Technological Adaptability	Obsolete and challenging to integrate advanced tools and technologies	Designed to integrate new technologies
Ethical Compliance	Compliance often depends on regional regulations	Integrated consent management and DAOs ensure ethical standards

Figure 11. Comparison of EHR Systems and Our Proposed Approach

9- Challenges and Implementation Solutions

The deployment of a quantum-resistant hybrid blockchain architecture for electronic health records presents distinct challenges, from integration obstacles and processing needs to user acceptance and practicality. Addressing these challenges requires both technological adjustments and strategic planning. For instance, incorporating advanced cryptographic techniques like CRYSTALS-Dilithium and CRYSTALS-Kyber into our quantum-resistant framework involves specific operational and technical difficulties, especially in ensuring smooth functionality and interoperability within healthcare information systems. Although resistant to quantum attacks, these lattice-based algorithms demand considerable computational power. To balance data flow with security, we minimized redundant encryption processes, optimized algorithmic cycles, and integrated a hybrid blockchain framework. These modifications ensured that system performance remained efficient while maintaining the highest encryption levels.

Quantum cryptography, despite its potential, still requires extensive testing in real-world healthcare settings. Major obstacles to practical implementation include compatibility with existing hardware and the computational load, particularly in regions with limited infrastructure. To evaluate scalability and enhance performance across diverse infrastructures, we aim to pilot the framework in a variety of healthcare environments. Furthermore, by emphasizing modular architecture, our system remains flexible enough to accommodate incremental advancements in quantum technology and cryptographic standards, which we believe will eventually improve operational viability.

Moreover, integration and interoperability are essential in regions with limited technological infrastructure. Our framework is designed to seamlessly interact with existing healthcare systems and overcome compatibility issues with legacy systems by using standardized APIs and data protocols. To facilitate this, we adopted a dual-blockchain approach: the private blockchain securely manages sensitive EHR data, while the public blockchain supports broader transparency, even on less sophisticated systems. This approach ensures that critical services remain accessible even when system resources are constrained.

We also acknowledge that the introduction of new technology may initially encounter resistance from users, including patients and healthcare professionals. To ease this transition, we proactively implemented strategies such as targeted training programs, interactive onboarding, and ongoing support. Stakeholder feedback highlighted the importance of usability and transparency, leading us to emphasize practical, approachable applications in our training. Additionally, to empower users in data management decisions and build trust in the system's security and transparency, we incorporated DAO governance features. Our goal is to provide a seamless and secure transition for all parties by aligning our technology with user needs and existing healthcare workflows.

10- Conclusion

In the current era of rising cyber threats and the growing requirement for virtual consultations, our proposed system presents an innovative solution to the critical issues encountered by traditional healthcare information systems. By harnessing the capabilities of blockchain, artificial intelligence, and metaverse, we established an efficient and interactive healthcare environment that emphasizes safeguarding patient information and meeting patients' requirements. This integration enhances data security through encryption techniques and patient engagement and interaction using the metaverse, setting a new benchmark for managing electronic health records. Using blockchain guarantees records and transparent consent management processes, while AI-driven diagnostics and virtual reality settings create a more immersive and precise healthcare experience. Our systems focus on interoperability and user-friendliness and tackle challenges in existing healthcare setups by facilitating data exchange and providing easy-to-use interfaces for healthcare providers and patients. Nevertheless, it is important to recognize limitations. The application of quantum cryptography holds immense promise but requires further validation in real-world scenarios to ensure its practicality and effectiveness. Moreover, adopting these pioneering technologies may encounter resistance from individuals (patients and doctors) to advancements, highlighting the need for comprehensive training schemes and user education efforts.

While the proposed framework shows satisfactory promise in improving the security and efficiency of Electronic Health Records, further research is crucial to validate its practicality; in future works, we aim to tackle implementation obstacles and understand its impact on the healthcare field. This involves creating and testing a prototype to assess its effectiveness in terms of security, scalability, and efficiency. Collaborating on pilot projects with healthcare organizations can offer insights into this proposed solution's real-world challenges and advantages. Additionally, we aim to explore the integration of decentralized autonomous organizations in healthcare, which requires rigorous investigation. In future studies, we will concentrate on designing governance models and smart contracts specifically tailored to meet healthcare management needs and examining case studies on how DAOs are used for decision-making and data sharing among healthcare providers can provide helpful insights and best practices.

11- Declarations

11-1- Author Contributions

Conceptualization, R.B.; methodology, R.B.; software, R.B.; validation, Y.G. and S.M.; formal analysis, Y.G.; investigation, S.M.; resources, R.B.; data curation, R.B.; writing—original draft preparation, R.B.; writing—review and editing, R.B.; visualization, R.B.; supervision, Y.G. and S.M.; project administration, Y.G. All authors have read and agreed to the published version of the manuscript.

11-2- Data Availability Statement

The data presented in this study are available in this paper.

11-3- Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

11-4- Acknowledgements

The authors express gratitude to the National School of Applied Sciences of Kenitra.

11-5- Institutional Review Board Statement

Not applicable.

11-6- Informed Consent Statement

Not applicable.

11-7- Conflicts of Interest

The authors declare that there is no conflict of interest regarding the publication of this manuscript. In addition, the ethical issues, including plagiarism, informed consent, misconduct, data fabrication and/or falsification, double publication and/or submission, and redundancies have been completely observed by the authors.

12- References

[1] Alder, S. (2024). Security Breaches in Healthcare in 2023. The HIPAA Journal, Michigan, United States. Available online: https://www.hipaajournal.com/security-breaches-in-healthcare/ (accessed on December 2024).

[2] Nowrozy, R., Ahmed, K., Kayes, A. S. M., Wang, H., & McIntosh, T. R. (2024). Privacy Preservation of Electronic Health Records in the Modern Era: A Systematic Survey. ACM Computing Surveys, 56(8), 1-37. doi:10.1145/3653297.

[3] Atal, D.K., Tiwari, V., Anjali, & Berwer, R.K. (2024). The Intersection of Blockchain Technology and the Quantum Era for Sustainable Medical Services. Quantum and Blockchain-based Next Generation Sustainable Computing. Contributions to Environmental Sciences & Innovative Business Technology. Springer, Cham, Switzerland. doi:10.1007/978-3-031-58068-0_2.

[4] Lalova-Spinks, T., Saesen, R., Silva, M., Geissler, J., Shakhnenko, I., Camaradou, J. C., & Huys, I. (2023). Patients' knowledge, preferences, and perspectives about data protection and data control: an exploratory survey. Frontiers in Pharmacology, 14. doi:10.3389/fphar.2023.1280173.

[5] Shinde, R., Patil, S., Kotecha, K., Potdar, V., Selvachandran, G., & Abraham, A. (2024). Securing AI-based healthcare systems using blockchain technology: A state-of-the-art systematic literature review and future research directions. Transactions on Emerging Telecommunications Technologies, 35(1), 4884. doi:10.1002/ett.4884.

[6] Murala, D. K., Panda, S. K., & Dash, S. P. (2023). MedMetaverse: Medical Care of Chronic Disease Patients and Managing Data Using Artificial Intelligence, Blockchain, and Wearable Devices State-of-the-Art Methodology. IEEE Access, 11, 138954–138985. doi:10.1109/ACCESS.2023.3340791.

[7] Awan, K. A., Din, I. U., Almogren, A., & Rodrigues, J. J. P. C. (2024). MediTwin: A Web 3.0-Integrated Digital Twin for Secure Patient-Centric Healthcare in the Metaverse. IEEE Transactions on Consumer Electronics, 5654-5661. doi:10.1109/TCE.2024.3409845.

[8] Treiblmaier, H., Rejeb, A., Gault, M., Khurshid, A., Norta, A., Poteet, J., & Sivagnanam, S. (2024). Harnessing Blockchain to Transform Healthcare Data Management: A Comprehensive Research Agenda. Blockchain in Healthcare Today, 7(1), 10 30953 7 301,. doi:10.30953/bhty.v7.301.

[9] Keshta, I., & Odeh, A. (2021). Security and privacy of electronic health records: Concerns and challenges. Egyptian Informatics Journal, 22(2), 177–183. doi:10.1016/j.eij.2020.07.003.

[10] Vivekananda, G. N., Ali, A. R. H., Arun, S., Mishra, P., Sengar, R., & Krishnamoorthy, R. (2022). Cloud Based Effective Health Care Management System With Artificial Intelligence. 2022 IEEE 7th International Conference for Convergence in Technology, I2CT 2022, 1–6. doi:10.1109/I2CT54291.2022.9825457.

[11] vellore pichandi, K., Janarthanan, V., Annamalai, T., & Arumugam, M. (2024). Enhancing healthcare in the digital era: A secure e-health system for heart disease prediction and cloud security. Expert Systems with Applications, 255, 124479. doi:10.1016/j.eswa.2024.124479.

[12] Ma, S., & Zhang, X. (2024). Integrating blockchain and ZK-ROLLUP for efficient healthcare data privacy protection system via IPFS. Scientific Reports, 14(1), 11746. doi:10.1038/s41598-024-62292-9.

[13] Benaich, R., El Mendili, S., & Gahi, Y. (2024). Securing EHRs With a Novel Token-Based and PPoS Blockchain Methodology. IEEE Access, 12, 83183–83204. doi:10.1109/ACCESS.2024.3412793.

[14] Kang, J., Wen, J., Ye, D., Lai, B., Wu, T., Xiong, Z., Nie, J., Niyato, D., Zhang, Y., & Xie, S. (2024). Blockchain-Empowered Federated Learning for Healthcare Metaverses: User-Centric Incentive Mechanism With Optimal Data Freshness. IEEE Transactions on Cognitive Communications and Networking, 10(1), 348–362. doi:10.1109/tccn.2023.3316643.

[15] Ali, A., Pasha, M. F., Guerrieri, A., Guzzo, A., Sun, X., Saeed, A., Hussain, A., & Fortino, G. (2023). A Novel Homomorphic Encryption and Consortium Blockchain-Based Hybrid Deep Learning Model for Industrial Internet of Medical Things. IEEE Transactions on Network Science and Engineering, 10(5), 2402–2418. doi:10.1109/TNSE.2023.3285070.

[16] Liu, Y., Wang, X., Zheng, G., Wan, X., & Ning, Z. (2024). An AoI-Aware Data Transmission Algorithm in Blockchain-Based Intelligent Healthcare Systems. IEEE Transactions on Consumer Electronics, 70(1), 1180–1190. doi:10.1109/TCE.2024.3365198.

[17] Guduri, M., Chakraborty, C., Maheswari, U., & Margala, M. (2024). Blockchain-Based Federated Learning Technique for Privacy Preservation and Security of Smart Electronic Health Records. IEEE Transactions on Consumer Electronics, 70(1), 2608–2617. doi:10.1109/TCE.2023.3315415.

[18] Chen, B., Xiang, T., He, D., Li, H., & Choo, K. K. R. (2023). BPVSE: Publicly Verifiable Searchable Encryption for Cloud-Assisted Electronic Health Records. IEEE Transactions on Information Forensics and Security, 18, 3171–3184. doi:10.1109/TIFS.2023.3275750.

[19] Singh, S., Rathore, S., Alfarraj, O., Tolba, A., & Yoon, B. (2022). A framework for privacy-preservation of IoT healthcare data using Federated Learning and blockchain technology. Future Generation Computer Systems, 129, 380–388. doi:10.1016/j.future.2021.11.028.

[20] Benaich, R., El Mendili, S., & Gahi, Y. (2023). Advancing Healthcare Security: A Cutting-Edge Zero-Trust Blockchain Solution for Protecting Electronic Health Records. HighTech and Innovation Journal, 4(3), 630–652. doi:10.28991/HIJ-2023-04-03-012.

[21] Jiang, Y., Xu, X., & Xiao, F. (2022). Attribute-Based Encryption With Blockchain Protection Scheme for Electronic Health Records. IEEE Transactions on Network and Service Management, 19(4), 3884–3895. doi:10.1109/TNSM.2022.3193707.

[22] Mishra, R., Ramesh, D., Edla, D. R., & Qi, L. (2022). DS-Chain: A secure and auditable multi-cloud assisted EHR storage model on efficient deletable blockchain. Journal of Industrial Information Integration, 26, 100315. doi:10.1016/j.jii.2021.100315.

[23] Zhang, G., Yang, Z., & Liu, W. (2022). Blockchain-based privacy preserving e-health system for healthcare data in cloud. Computer Networks, 203, 108586. doi:10.1016/j.comnet.2021.108586.

[24] Kumar, R., Kumar, P., Tripathi, R., Gupta, G. P., Islam, A. K. M. N., & Shorfuzzaman, M. (2022). Permissioned Blockchain and Deep Learning for Secure and Efficient Data Sharing in Industrial Healthcare Systems. IEEE Transactions on Industrial Informatics, 18(11), 8065–8073. doi:10.1109/TII.2022.3161631.

[25] Zou, R., Lv, X., & Zhao, J. (2021). SPChain: Blockchain-based medical data sharing and privacy-preserving eHealth system. Information Processing & Management, 58(4), 102604. doi:10.1016/j.ipm.2021.102604.

[26] Benaich, R., El Mendili, S., & Gahi, Y. (2024). Securing the Future: Harnessing Blockchain's Power Against New-Age Vulnerabilities. 2024 4th International Conference on Innovative Research in Applied Science, Engineering and Technology (IRASET), 1–8. doi:10.1109/iraset60544.2024.10549415.

[27] Benaich, R., El Mendili, S., & Gahi, Y. (2023). Moving Towards Blockchain-Based Methods for Revitalizing Healthcare Domain. The 4th Joint International Conference on Deep Learning, Big Data and Blockchain (DBB 2023), 16–29. doi:10.1007/978-3-031-42317-8_2.

[28] Calderbank, M. (2007). The RSA Cryptosystem: History, Algorithm, Primes. Fundamental Concepts of Encryption, University of Chicago: Chicago, United States.

[29] Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J. M., Schwabe, P., Seiler, G., & Stehle, D. (2018). CRYSTALS - Kyber: A CCA-Secure Module-Lattice-Based KEM. 2018 IEEE European Symposium on Security and Privacy, 353–367. doi:10.1109/eurosp.2018.00032.

[30] Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G., & Stehlé, D. (2018). Crystals-dilithium: A lattice-based digital signature scheme. IACR Transactions on Cryptographic Hardware and Embedded Systems, 238-268. doi:10.13154/tches.v2018.i1.238-268.

[31] Sharma, P., Namasudra, S., Gonzalez Crespo, R., Parra-Fuente, J., & Chandra Trivedi, M. (2023). EHDHE: Enhancing security of healthcare documents in IoT-enabled digital healthcare ecosystems using blockchain. Information Sciences, 629, 703–718. doi:10.1016/j.ins.2023.01.148.

[32] Dong, Y., Mun, S. K., & Wang, Y. (2023). A blockchain-enabled sharing platform for personal health records. Heliyon, 9(7), 18061. doi:10.1016/j.heliyon.2023.e18061.

[33] Babu, E. S., Yadav, B. V. R. N., Nikhath, A. K., Nayak, S. R., & Alnumay, W. (2023). MediBlocks: secure exchanging of electronic health records (EHRs) using trust-based blockchain network with privacy concerns. Cluster Computing, 26(4), 2217–2244. doi:10.1007/s10586-022-03652-w.

[34] Kokila, M. L. S., Fenil, E., Ponnuviji, N. P., & Nirmala, G. (2024). Securing cloud-based medical data: an optimal dual Kernal support vector approach for enhanced EHR management. International Journal of System Assurance Engineering and Management, 15(7), 3495–3507. doi:10.1007/s13198-024-02356-1.

[35] Chinnasamy, P., & Deepalakshmi, P. (2022). HCAC-EHR: hybrid cryptographic access control for secure EHR retrieval in healthcare cloud. Journal of Ambient Intelligence and Humanized Computing, 13(2), 1001–1019. doi:10.1007/s12652-021-02942-2.

[36] Ishaq, A., Qadeer, B., Shah, M. A., & Bari, N. (2021). A Comparative study on Securing Electronic Health Records (EHR) in Cloud Computing. 26th International Conference on Automation and Computing (ICAC-2021), 1–7. doi:10.23919/icac50006.2021.9594178.