A Framework for Blockchain-based Secure Management of Mobile Healthcare (mHealth) Systems

Adel Alkhalil[1], Abdul Razzaq[2,*], Aakash Ahmad[3], Magdy Abdelrhman[4], Yaser Altameemi[5], Mohammed Altamimi[5] and Zhang Tao[2,*]

[1]*Department of Software Engineering, College of Computer Science and Engineering, University of Ha'il, Ha'il, 81481 Saudi Arabia*
[2]*School of Software, Northwestern Polytechnical University, Xi'an, 710072, Shaanxi, P.R. China*
[3]*School of Computing and Communications, Lancaster University Leipzig, 01459, Germany*
[4]*Department of Foundation of Education, College of Education, New Valley University, Egypt*
[5]*Applied College, University of Ha'il, Ha'il, Saudi Arabia*
E-mail: a.alkalel@uoh.edu.sa; dr.razzaq@zju.edu.cn; a.ahmad13@lancaster.ac.uk; y.albakry@uoh.edu.sa; mh.altamimi@uoh.edu.sa; tao_zhang@nwpu.edu.cn
[*]*Corresponding Author*

Received 04 October 2024; Accepted 10 March 2025

Abstract

In recent years, several research and development initiatives have focused on developing secure and trustworthy systems for the healthcare industry via pervasive and mobile healthcare (mHealth) solutions. State-of-the-art mHealth solutions primarily rely on centralized storage, such as cloud computing servers, which may escalate the maintenance costs, require ever-increasing storage infrastructure, and pose privacy and security risks to the health-critical data produced, consumed, and transmitted over ad hoc

Journal of Web Engineering, Vol. 24_3, 317–354.
doi: 10.13052/jwe1540-9589.2431

networks. To overcome these limitations, we conducted this study intending to synergize mobile computing (devices to process health-critical data) and blockchain technology (infrastructure to secure storage and retrieval of health-critical data), specifically addressing data security and privacy using a blockchain mHealth system. The research employs an incremental method by (i) developing a framework that acts as a blueprint to architect blockchain-enabled mHealth systems, (ii) implementing a suite of algorithms as a proof-of-concept to automate the framework, and (iii) experimental evaluations to validate the scalability, computation, and energy efficiency of the proposed solution. The proposed framework has been implemented as a frontend using a mobile application interface that exploits the backend via the InterPlanetary File System (IPFS) system and Ethereum blockchain for secure management of mHealth data. We use a case-study-based approach demonstrating how health units, medics, and patients can securely access and distribute health-critical data. For evaluation, we deployed a smart contract prototype on the Ethereum TESTNET network in a Windows environment to test the proposed framework. Results of the evaluation indicate (a) scalability with query response time (range: 10–41 ms), (b) computational performance (CPU utilization: 1.5% – 2.5%), and (c) energy efficiency (gas consumption: 40000 units for 1000 bytes). The proposed solution – framework, algorithms, and experimental evaluation – aims to advance state-of-the-art architecting and implementing cybersecurity mHealth solutions using blockchain technology.

Keywords: Blockchain, mobile computing, smart health, security, smart contracts.

1 Introduction

Information and computing technologies (ICT) can utilize a plethora of systems including but not limited to mobile systems, pervasive sensors, and context-sensing devices to revolutionize scalable and efficient delivery of healthcare services [28]. The adoption and availability of sophisticated clinical information systems have been supported by mobile and pervasive healthcare solutions that advance healthcare care quality, safety, and patient-centeredness [1]. In smart healthcare systems, mobile health (mHealth for short) exploits mobile and context-sensitive technologies mobile technologies to offer healthcare services including, but not limited to, monitoring

heartbeats, analyzing blood-pressure levels, and capturing medical images to enable cost-effective and time-efficient digitized healthcare services. Mobile devices integrate (i) hardware sensors (monitoring context data), (ii) software applications (app to process the data), and (iii) networking technologies (protocol to send and receive data). In 2019, 67% of the global population (5.2 billion people) used mobile services, expected to rise to 70% by 2025 [29]. Mobile devices contributed US$4.1 trillion (4.7% of GDP) in 2019, projected to grow to 4.9% by 2024. The mHealth app market expanded in 2017 with 78,000 new apps, foreseeing a digital health market revenue of US$31 billion by 2020 [29]. Despite centralized management benefits, fragmented data poses challenges in personal health info utilization. Effective security requires human-centric practices beyond technical features. While mobile devices incorporate various security measures like device locks and encryption, a study by [32] underscores that even advanced security features cannot guarantee protection against human behaviors, such as privacy leakage or unauthorized access, which may enhance or compromise device and data security [32].

Research motivation: The use of ICT has yielded new difficulties in the context of the cybersecurity of mHealth systems [31]. The security breaches to which health facilities are exposed have become a high-impact strategic problem [5]. Electronic medical records, electronic health records, and personal health records are some of the systems that are likely to be breached [6]. These systems manage a multitude of secure and private data including but not limited to patient records and images of X-rays, injuries, operations, medicines, etc. To analyze image data, clinical institutions require significant storage capacity to maintain safe and completely accessible medical images. Current methods for transmitting medical images and information about a patient are mainly focused on centralized data centers [7]; however, these alternatives raise problems related to accessibility, privacy, security, and storage of data [8]. Furthermore, over the past few decades, significant issues with medical image processing technology have been brought about by breaches of medical record data in large medical data centers [9]. The term "Blockchain" describes an innovative technology to support cryptocurrencies like bitcoins [2, 3]. This technology aims to develop blockchain platforms for many enterprises through an open-source project, allowing industry-based distributed transactions through a distributed ledger technology that enables transactions to be handled in a distributed and consensus-based practice [4].

Ethereum is a digital platform that embraces blockchain technology and extends its use to a wide range of systems and applications. Its native coin, ether, is currently the second-biggest cryptocurrency available. Ethereum's goal is to create a distributed system for executing smart contracts. Decentralized technologies are becoming more popular in the health business [10, 11]. They have emerged as a significant trend with the potential to provide new ground for overcoming barriers and enabling more widespread adoption of a patient-centric system. Although distributed solutions such as the InterPlanetary File System (IPFS) [12] provide shared storage solutions, there has been little discussion on using decentralized technologies to store sensitive medical images. Decentralized solutions also have questions about their ability to handle massive volumes of data among patients, hospitals, general practitioners, and medical institutions while lowering the possibility of privacy violations. The primary objective of this research is to investigate the answer to the following three research questions (RQs):

RQ 1: How do we design a framework that can leverage block chain technology to enable secure management of health-critical data in mobile health systems?

Rationale: Synergize research and development on block chain technology with mobile healthcare solutions to ensure health-critical data that is produced, consumed, and/or processed by mobile.

RQ 2: What algorithms and tools can be developed to support the implementation of the proposed framework?

Rationale: To develop algorithms and a prototype that supports automation and parameterized customization (user input to algorithms) to develop a proof-of-the-concept for the proposed.

RQ 3: Why there is a need for experimental evaluation for criteria-based evaluation of the proposed framework?

Rationale: To define a criteria such as efficiency, energy consumption, scalability and performance to qualitatively and objectively evaluate the usefulness of the proposed framework.

Proposed contributions: In the context of mobile and smart healthcare systems, the contemporary landscape of research and development on mHealth

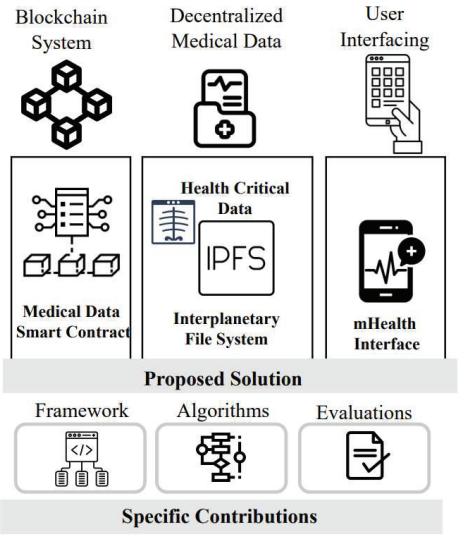


Figure 1 A layered overview of the proposed solution.

solutions heavily relies on centralized storage systems, typically utilizing cloud computing servers [30]. While effective, this approach presents challenges such as the cost of maintenance, increased computation and storage infrastructure, and inherent privacy and security risks associated with health-critical data transmitted over mobile networks [30].

In response to these limitations, the focus of this research is to synergize mobile computing (for processing health-critical data) and blockchain technology (as an infrastructure for secure storage and retrieval of health-critical data). To fulfil the objective(s), we present the proposed solution, an overview of which is given in Figure 1, a mobile-based system that utilizes decentralized storage in the form of distributed repositories (such as IPFS and blockchain) to register and store clinical images. This metadata is stored on the decentralized storage of IPFS, and the transaction is recorded on the blockchain ledger along with the hash of the file. To access their data, the patient is provided with a smart app that allows them to do so. In the smart app, Google Firebase is used as a platform for pushing notifications of report updates to the patients. Based on the illustrative view in Figure 1, the primary contributions of this research include:

– **An mHealth framework** that synergizes mobile computing systems (context-sensitive devices for health-critical data) and blockchain as a decentralized technology (secure ledger to record the transactions and

retrieval of health-critical data). This solution provides a access management system as a patient-centric system based on a smart contract that allows patients and doctors to access examination reports on a decentralized portal and mobile interface (RQ 1).
- **Algorithmic implementations** that automate and provide a proof-of-concept (PoC) for mobility-driven and secure management and transmission of health-critical data. The algorithms enable the development of a PoC and foundations to evaluate the mHealth prototype for a patient-centric control system on Ethereum (RQ 2).
- **Experimental evaluations** by deploying a prototype of smart contracts on the Ethereum TESTNET network within a Windows environment. The evaluation outcomes highlight three critical aspects in terms of scalability, computational efficiency, and energy efficiency. These evaluation results affirm the effectiveness and practicality of our blockchain-enabled mHealth system (RQ 3).

The source code for the algorithmic implementations as a prototype of the mHealth system is provided via GitHub: https://github.com/razzaq786/BC-HealthCare.

Nomenclature	
$\cup(\iota \mathrm{d})$	User ID
$\partial(\iota \mathrm{d})$	Patient appointment ID
$\Delta \mathrm{p}$	Description
γP	Meta file (images or reports)
μ	Data variable
$\mathrm{U}(\tau)$	User type (doctor or patient)
τ	Test type (blood test, lipid test)
FS	File stream
FB	File buffer

Study organization: Section 2 provides background details and research method to conduct this study. Section 3 overviews the related work to justify the scope and proposed contributions. Section 4 presents the proposed framework and algorithms. Section 5 details solution implementation and evaluation. Section 6 presents future work. Section 7 details the discussion section. Section 8 concludes this research study.

2 Research Background and Method

This section introduces the background details to contextualize the proposed solution (Section 2.1) and provides details about the method of conducting

this research (Section 2.2). We introduce the core concepts in this section that are being used throughout the paper.

2.1 Background: Blockchains and mHealth Systems

2.1.1 Blockchain systems

Blockchain is a distributed ecosystem in which each node is independent in terms of interests or willingness to perform tasks of maintaining a single ledger through competition or collaboration [13]. Each confirmed transaction is included in a block that connects to the most recent block by using the prior block's hash as one of the inputs for calculating the current block's hash. This transaction can only be added to the blockchain ledger once most miners have reached a consensus. Blockchain platforms can be divided into two groups: permissionless and permission [14]. Permissionless means that any entity can join or leave at any time. In contrast, permission adds a membership management module where only pre-designated members have the right to view and modify the blockchain ledger. The permission blockchain is, therefore, partially decentralized but attracts much more interest in the business community than the permissionless blockchain.

In smart grid management, blockchain simplifies decentralized energy trading, allowing consumers to purchase and sell excess energy without intermediaries. In the same way, in smart city infrastructure, blockchain can advance data security and transparency in governance, empowering tamper-proof records for urban planning, public services, and utility management. By integrating blockchain with IoT systems, smart cities can secure real-time data exchange while minimizing the risks of cyber threats. Blockchain plays a critical role in security management, principally in identity verification, access control, and cybersecurity. With decentralized identity solutions, entities and organizations can securely manage their credentials, minimizing the risk of identity theft and fraud. In unmanned aerial vehicles (UAVs), blockchain enables secure and transparent drone operations, including flight data recording, decentralized traffic management, and secure authentication of UAVs for monitoring compliance. The application of blockchain in these domains enhances security, efficiency, and trust, making it an auspicious technology for the future of decentralized digital ecosystems.

2.1.2 Smart contract

Smart contracts, executed on blockchains when conditions are met, automate agreements without intermediaries [15]. They store documentation, enable

electronic signatures, and execute logic based on predetermined instructions [15]. Smart contracts play an active role; not only do they electronically store documentation or enable electronic signatures, but these programs also perform analysis and execute some parts of their internal logic. Ethereum, a decentralized open-source platform, hosts blockchain globally, requiring widespread agreement for network changes [17]. In the Ethereum network, there are two different types of accounts: a smart contract account managed by the compiled program code of a smart contract and an externally owned user account controlled by the private key.

2.1.3 InterPlanetary File System (IPFS

IPFS is a distributed file system that aims to connect all computers to the same file system. Through a P2P system, users can host information in IPFS and access it without needing a single access point. Unlike HTTP, which addresses by location, IPFS uses a content-based addressing system, which can generate benefits in terms of quality of service. Concerning the information managed by IPFS, the data is immutable and content-addressed [12]. In this network, user accounts are empty of code, and the only way to communicate with other accounts is by establishing and signing transactions using their private keys [18]. The receiving account can recognize the sender using the sender's public key. Ethereum uses a nonce to ensure that each transaction can only be performed once. The leading cryptocurrency used by Ethereum for transaction processing and payment is called ether (see Figure 2).

2.1.4 Blockchain in mHealth systems

In terms of smart healthcare systems, traditional healthcare systems use a centralized platform for providing services. We gathered the most useful details on traditional healthcare systems to modernize and decentralize with a new technology that was centralized. Blockchain has received more attention in the healthcare business since it provides creative solutions to data security, interoperability, and trust issues. Blockchain's tamper-resistant and decentralized nature makes it a promising tool for keeping secure sensitive health data and increasing the overall efficiency of healthcare systems [26].

In the context of healthcare, blockchain can be applied to create a secure and transparent system for managing electronic health records (EHRs), ensuring that patient data is stored and shared in a way that maintains privacy

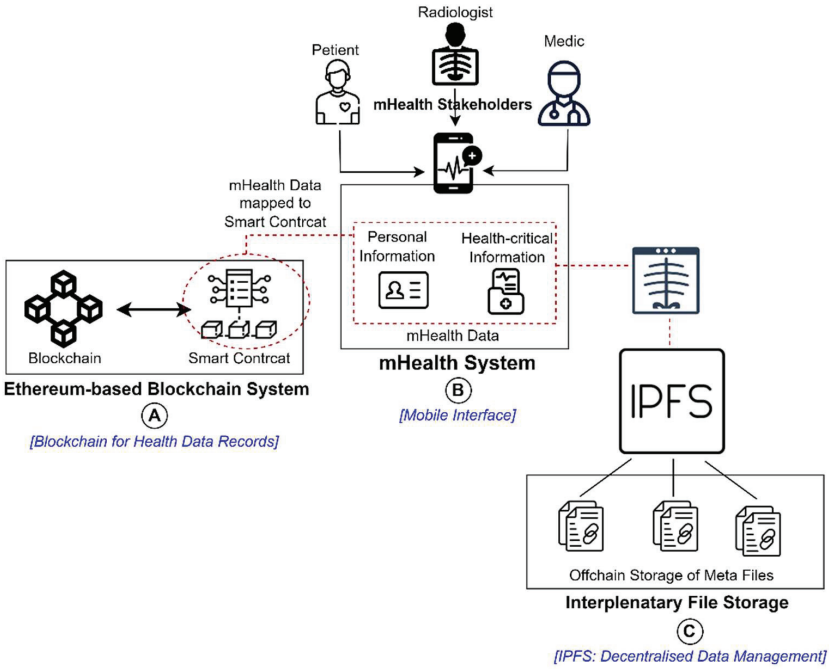


Figure 2 Background with overview of (a) blockchain, (b) IPFS, and (c) mH.

and integrity. Additionally, blockchain's ability to establish a decentralized network of trust facilitates secure and seamless information exchange among healthcare providers, insurers, and patients. Several studies highlight the potential of blockchain to enhance data integrity, reduce fraud, and streamline administrative processes in healthcare [27]. As the healthcare industry continues to grapple with data management and security issues, exploring blockchain technology's applications becomes imperative for realizing a more efficient and secure healthcare ecosystem. The decentralized system developed under the research aims to fill the gap of technology and knowledge in medical field healthcare systems. A decentralized system using blockchain technology is a more secure system than a traditional one. The decentralized web-based system was developed with a mobile-enabled application for healthcare to distribute the patient's details and give access to patients for their reports. We facilitate the patient by developing a mobile app connected to a blockchain ledger. We designed a framework for presenting the developed system of healthcare.

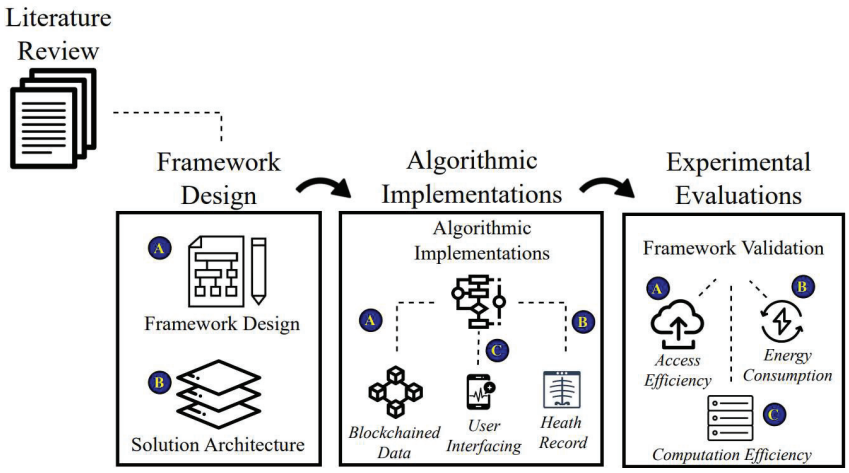


Figure 3 An overview of the steps in the research method.

2.2 Research Method

This section offers an overview of the steps that are executed to conduct this research as methodological details that are offered below and demonstrated in Figure 3. As per Figure 3, the overall research method is divided into a series of well-defined steps, demonstrating the comprehensive nature of the research methodology. It is intended to serve as a roadmap for the reader, guiding them through the systematic approach to conduct this research has been adopted, which is explained in the next section.

2.2.1 Step 1: Literature review and comparative analysis

First, we conducted a comprehensive analysis of several studies (such as [20–23]) to identify the state of the art of our proposal. We systematically analyzed all those studies in line with our proposal to identify opportunities for improvement in terms of the storage of medical images. Details about the review of related work are in Section 3.

2.2.2 Step 2: Developing the proposed framework

The next crucial step in this process is the transfer of knowledge from the theoretical framework put in place in Step 1 to the practical. During this process, we design the architecture at the foundation of the proposed solution. By providing a full understanding of the structural framework that is underpinning our research project from an architectural perspective, we

will be able to demonstrate how it is supported by the research project. As a result, the dataset was created using the results obtained from trials performed using the proposed system. Therefore, we were able to ensure the accuracy and relevance of the data. Moreover, the source code has been made publicly available on GitHub so that researchers and developers can analyze, modify, and enhance the functionality of the system.

2.2.3 Step 3: Implementing the algorithms

This step is all about the modularization of the algorithms that are essential for the successful implementation of our solution. We are designing algorithms for the processing of images using blockchain technology and other technologies related to medical decisions and image processing.

2.2.4 Step 4: Evaluating the framework

To validate the proposal we have developed, we need to define a method that we will use. We chose to focus on evaluating the usability and efficiency of the system to achieve our objectives. To accomplish this, a set of evaluation metrics has been developed to be used in this process.

3 Related Work

This section overviews the existing research, generally classified as (a) patient-centric mHealth systems (Section 3.1) and (b) blockchain technologies in healthcare (Section 3.2). The section concludes by comparing and summarizing the closed available research, presented in Table 1, to justify the conducted research's contributions in this paper.

Chakravorty [19] proposes MobiCare, a mobile patient monitoring system for continuous physiological data collection, aiming to enhance patient care quality offline. Moosavi et al. [20] propose an end-user security solution for healthcare IoT, featuring a robust mobility architecture, secure communication, and user authentication based on datagram transport layer security. As reported in [30], mobile technology's impact on identity and self-efficacy correlates with the espousal of clinically supported mobile health applications. Mobile technology self-efficacy and identity provide insight into the inner factors that influence the acceptance and use of health apps [36]. Using mobile health apps endorsed by clinical settings, the study examines how individuals perceive themselves in the context of mobile technology. As a result of synthesizing self-efficacy theory and identity theory, it gives valuable insights into the understanding of mobile health technology adoption.

Table 1 Comparative analysis: Existing vs proposed research on secure mHealth systems

Security Mechanisms	[20]	[21]	[22]	[23]	Proposed Study
Data encryption	✓	×	×	✓	✓
Data storage	Cloud storage	Blockchain node	Blockchain node	Blockchain node	IPFS storage Blockchain node
Large data support	✓	✓	×	×	✓
Attack resistance of the server	✓	×	×	×	✓
No third-party authentication	✓	✓	×	×	✓
Mobile smart access	×	×	×	✓	✓

Tanwar et al. [21] present an EHR system based on blockchain design with four participants: a patient, a clinician, a lab, and a system administrator. Several assets or smart contracts, such as "CreateMedicalRecord", "GrantAccessToClinician", "GrantAccessToLab", "RevokeAccess", and "RevokeAccessTo Lab", are defined in this system. The authors' suggestion emphasizes the system's central authority. The blockchain-based medical picture retrieval system proposed by Shen et al. [22] includes scenarios and architectural specifications. They demonstrate a layered architecture and threat model. In a blockchain prototype referred to as MedRec, Azaria et al. [23] integrate Ethereum smart contracts to address EHR issues, including permissions, data sharing, and mining, as well as pointers for locating medical records. Blockchain nodes retain only authorization data, not medical records. The studies discussed in this section point out that, in general, medical images should be stored and retrieved by a centralized entity that, through traditional (e.g., cloud) and blockchain approaches, can process image data securely. In contrast to previous studies, our proposal offers a strategy to provide secure access of system in a decentralized architecture.

Table 1 overviews the most relevant existing research and highlights the open research gaps in terms of security mechanisms for blockchain-based mobile health systems. Specifically, Table 1 serves as a comprehensive catalogue, employing criteria-based comparison to delineate the scope and contributions of the proposed solution in contrast to existing methodologies. Derived from existing study classification recommendations, seven criteria are examined. These include the implementation of data encryption techniques for securing grades and certificates on the network, exploration of diverse data storage sources such as decentralized and on-premises options, evaluation of the system's capacity to handle large data with a focus on cost implications, comparison of the security resilience of decentralized versus

centralized storage against potential attacks, and an assessment of the absence of third-party authentication in the system. The exclusion of third-party authentication allows for the seamless design and evaluation of exam systems capable of real-time data collection and analysis. Through these criteria, Table 1 systematically illuminates how the proposed solution excels or aligns with existing approaches, providing insights into key aspects of data security, storage, scalability, and authentication of exam systems.

4 Proposed Framework[1] and Algorithms

As per the research method in Figure 4, this section details the proposed blockchain-based mHealth framework and algorithms that implement the proposed framework. First, the framework is presented along with its components in Section 4.1, which follows the details of algorithms in Section 4.2, both detailed below the framework. This section underpins the design and implementation of a medical healthcare system that relies on blockchain for the secure management of health-critical data.

4.1 Framework for Blockchain-based mHealth Systems

The design of our proposal for processing medical image files and patient lab reports is depicted in Figure 5. Using our solution, an analysis report is converted into textual data, which a lab assistant saves immediately in a blockchain ledger via a smart contract. The radiologist branch of the laboratory uses the IPFS to store medical images. This technique allows the radiologist to upload accessible medical picture data to the IPFS and receive a hash key that corresponds to the uploaded data. It is then entered into the blockchain ledger with other critical information, such as the hash key. IPFS can store medical images, but analysis reports can represent any event. As a record-keeping tool, the hash of the image file is kept with the necessary details in the blockchain.

Our design determines that the first step in the digital data exchange process is the generation of metadata for the original file (see Figure 4). In the

[1]In the general context of software and system engineering, the term framework or architecture are often considered as virtually synonymous and interchangeable concepts. Framework refers to an abstraction that allows unification of architectural blueprint (i.e., design), modules of code (i.e., implementations), and validations (i.e., evaluation) of the solution under consideration. This framework provides a method for constructing mHealth applications, functioning as a versatile and reusable software environment.

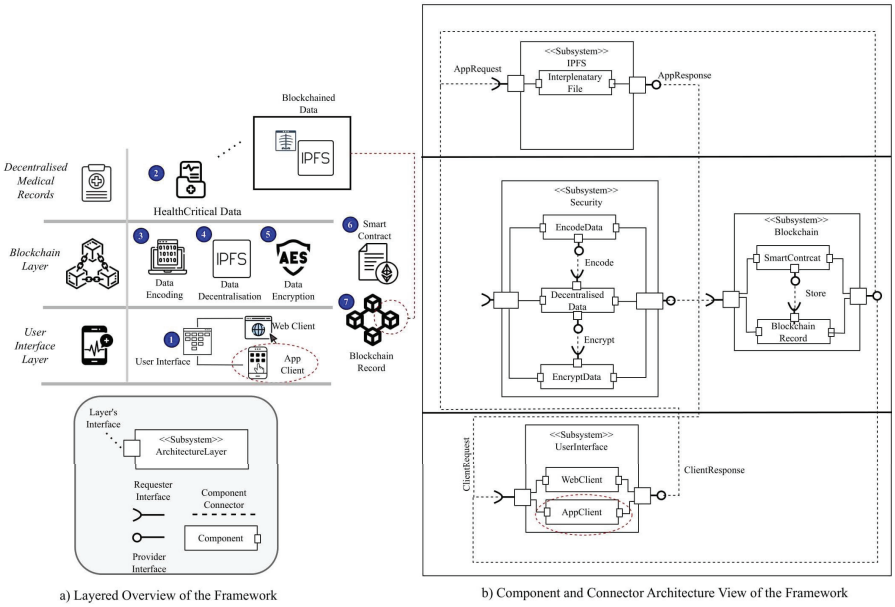


Figure 4 Proposed framework: (a) layered view and (b) component and connectors.

medical data upload process, essential information like file name, description, and size forms the medical image metadata. Once complete, this metadata is merged with the data file and published in the IPFS. Subsequently, the parameters required for blockchain storage are provided through a smart contract. For data retrieval, three parameters are essential: the first for obtaining lipid test lists, the second for retrieving data by citation ID, and the third for accessing patient data using patient and appointment IDs. These datasets are securely stored on the blockchain through smart contracts illustrated in Figure 5; our medical data upload process commences when a patient receives a test notification. A laboratory assistant collects a blood sample, conducts the test, and records results on the blockchain using patient and appointment IDs. Following this, a radiologist associates medical images with relevant assessments, uploads them to the IPFS, and provides necessary details against patient and appointment IDs, both recorded on the blockchain.

- Monolithic healthcare systems use centralized databases or cloud servers, which increases the risk of unauthorized access and breach of data. Using decentralized storage, medical visual data can be stored securely.

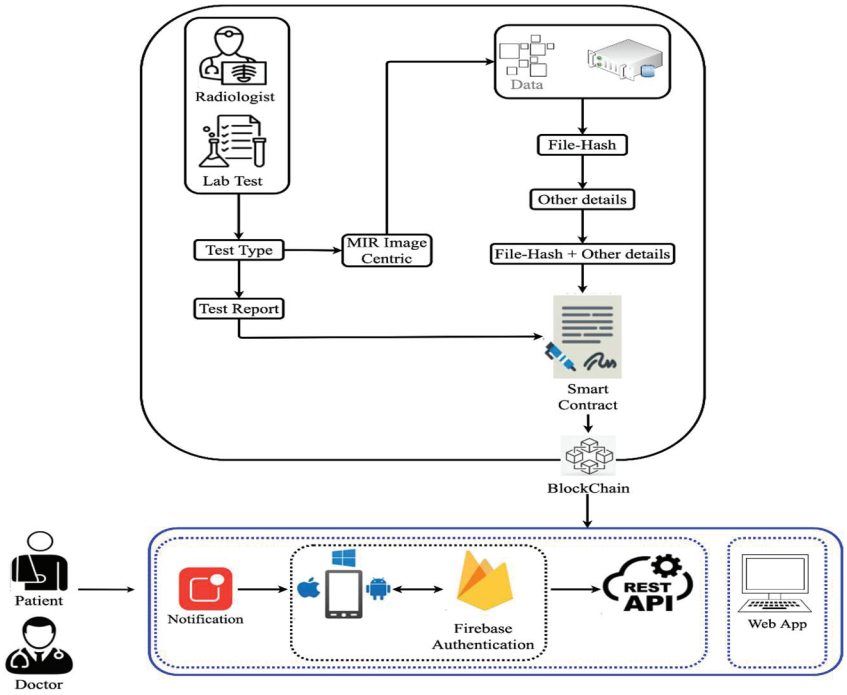


Figure 5 Process flow for blockchain-based uploading of critical health data.

- Example: This framework can be used in the hospital to store data in a ledger through a secure channel, which can be stored on the IPFS decentralized storage.

- The key advantage of this framework is to give patients access to their medical data.
  - Example: Patients can use the web portal decentralized system and mobile smart health app to access their medical data.
  - Example: A patient can access their health record globally, which ensures security and eliminates the need for physical availability.

In a recently published systematic review of engineering blockchain systems, the authors have identified and classified blockchain systems into seven distinct layers, highlighted below. Layering in blockchain systems helps to maintain a logical or physical separation of concerns (Table 2). This separation helps to distinguish different parts of a blockchain system briefly introduced below. As per [37, 38], these layers include:

Table 2 Most prominent attacks corresponding to each layer of the blockchain

Layer 1: Application	
Attacks	Solution
Phishing attacks	Multi-factor authentication (MFA) and user education
Malware injection	Regular security audits
Layer 2: Smart contract	
Attacks	Solution
Reentrancy attack	Use checks-effects-interactions pattern
Integer overflow/underflow	Use SafeMath libraries
Layer 3: Incentive	
Attacks	Solution
Selfish mining	Adjusting mining rewards
Sybil attack	Proof-of-stake (PoS) and identity verification
Layer 4: Consensus	
Attacks	Solution
Sybil malicious	In permissioned blockchains, use the proof of identity to limit the forged nodes
51% Attack	PoW with PoS reduce susceptibilities to 51% attack
Layer 5: Network	
Attacks	Solution
Eclipse malicious	Nodes refresh peer connections to avoid isolation
DDoS	Implement encrypted infrastructures to ease DDoS threats
Layer 6: Data	
Attacks	Solution
Double-spending malicious	Implement finality in consensus protocols to guarantee irrevocable transactions
Off-chain data tampering	Use cryptographic hash to verify data integrity
Layer 7: Physical	
Attacks	Solution
Hardware tampering	Save private keys offline cold wallets to avert physical compromise
Side-channel attacks	Implement intrusion detection systems to detect unauthorized changes

- **The application layer** manages blockchain applications to interact with smart contracts.
- **The smart contract layer** contains the data and logic that manipulates the data that is stored or processed in a block network.
- **The incentive layer** provides the incentivization and rewards to nodes that are part of the chained network.
- **The consensus layer** encapsulates the consensus algorithm for executing the transactions.
- **The network layer** manages the network and communication details of the blockchain network.

- **The data layer** manages the necessary data (e.g., transaction records) as part of the blockchain system.
- **The physical layer** interacts with the hardware and network to execute the blockchain system.

Based on these seven layers, our proposed solution has derived a three-layered framework including the user interface layer, the blockchain layer, and the medical record layer, as shown in Figure 4. Before presenting an algorithmic implementation of these layers, we also highlight the benefits and limitations for each of the three layers of our proposed solution (Table 3).

4.2 Algorithmic Implementations

This section introduces the three most relevant algorithms we have defined for our proposal. To establish the algorithms, we looked into the previous studies and implanted models as a case study to validate and refine our proposal's steps.

4.2.1 Algorithm 1: Securing critical health data with blockchain

The first approach involves uploading data to the IPFS and hashing it in a smart contract using attribute mapping. The deployed data file hash is related to numerous parameters, such as user ID, appt. ID, description, and date.

- **Input**: Hash key file.
- **Processing:** To link parameters to the data provided, a hash key is generated. The medical data image file is read and converted into a buffer package, yielding a hash key. It entails attaching information like as the ID of user as a patient, ID of patient for appointment, patient description, and date to a smart contract for secure storage on blockchain.
- **Output:** The output is the mapped date, which is saved in the blockchain.

Algorithm 1 Uploading radiologist image data

0: Input: $\cup(\iota d), \partial(\iota d), \Delta p, \gamma_{\wp}$ {User ID, Appointment ID, Description, File}
0: Output: $\mathcal{R}$ [Returing Result]
0: **procedure** IMAGECENTRIC {Event based function}
0: **if** User is $\mathcal{L}\sigma\beta$ **then** {Uploading by User OR System}
0: $\mathcal{FS} \leftarrow$ File($\gamma_{\wp}$) {Get File stream $\mathcal{FS}$}
0: $\mathcal{FB} \leftarrow$ Buffer($\mathcal{FS}$) {Convert $\mathcal{FS}$ to Buffer $\mathcal{FB}$}
0: $\mathcal{FH} \leftarrow$ IPFS.Add ($\mathcal{FB}$) {Get Hash of Uploaded Data $\mathcal{FH}$}
0: SAVE($\cup(\iota d), \partial(\iota d), \Delta p, \mathcal{FH}$) {Store Data to Blockchain with file hash}
0: **end if**
0: **end procedure**=0

Table 3 Advantages and disadvantages layers in the proposed system

Interface Layer	Blockchain Layer	Medical Record Layer
Advantages:	**Advantages:**	**Advantages:**
1. Provides user-friendly access based on web and mobile interfaces for patients and healthcare to manage health data. 2. Patients are notified of their medical reports by using Google Firebase. 3. Secure authentication based on an encryption mechanism to prevent unauthorized access. 4. The system is based on the polyglot concept using Xamarin to make it accessible on different platforms.	1. Removes the risk of a single point of failure due to decentralized security and recording data to the blockchain ledger. 2. Due to immutability, data cannot be tampered with. 3. Using smart contracts facilitates the automation. 4. Transparency of data ensures that healthcare professionals can verify data.	1. Data efficiency, IPFS handles the large medical data files (X-rays, MRIs) and access control on blockchain. 2. Patients are able to access data. 3. It allows data sharing interoperability among different healthcare providers and ensures security. 4. Removes the centralized dependency due to decentralized storage.
Disadvantages:	**Disadvantages:**	**Disadvantages:**
• There is a device dependency in remote areas for users that is limiting accessibility. • There could be performance limitations due to interface responsiveness by network latency.	• It takes more energy cost to make a transaction, especially on a public blockchain. • Large data processing on the blockchain may reduce the transaction speed which increases the limitations of scalability.	• To use the external storage, increase the complexity of system management. • Accessing the data from the IPFS could be slower than old central systems which affects the real-time accessibility.

4.2.2 Algorithm 2: Preserving health critical data

The second point of the algorithm pertains to the storing of medical reports. Blood tests and lipid test results are kept in the blockchain ledger using a smart contract. The second algorithm is explained as follows:

- **Input:** Required parameters are linked ID of patient and user appt. ID using the algorithm's input.
- **Processing:** Blockchain securely stores patient IDs, prescription IDs, HDL cholesterol, triglycerides, LDL cholesterol, ratio of total cholesterol, and appt. IDs for lipid and blood test data. Using a blockchain smart contract, the user ID and appointment ID are incorporated into test report parameters and used for data preservation in the blockchain.
- **Output:** The output is the mapped date, which is kept in the blockchain.

Algorithm 2 Saving blood & lipid test data

0: Input: $\mathcal{B}_{(parameters)}, \mathcal{L}_{(parameters)}, \tau$ {List of Parameters (Blood/Lipid), Test Type}
0: **procedure** TESTREPORT {Event based function}
0: **if** $\tau == \mathcal{B} \| \tau == \mathcal{L} \| \tau == \mathcal{N}$ **then** {Test Type}
0: **if** $\tau == \mathcal{B}$ **then**
0: $\mu \leftarrow \mathfrak{Blood}(\mathcal{B}_{(parameters)})$ {Get Data of Blood Test}
0: **end if**
0: **if** $\tau == \mathcal{L}$ **then**
0: $\mu \leftarrow \mathfrak{Lipid}(\mathcal{L}_{(parameters)})$ {Get Data of Lipid Test}
0: **end if**
0: **if** $\tau == \mathcal{N}$ **then**
0: $\mu \leftarrow \mathfrak{Test}(\mathcal{L}_{(parameters)})$ {Get Data of N(Other) Test}
0: **end if**
0: **end if**
0: Save(μ) {Smart Contract Save records in Blockchain}
0: **end procedure**=0

4.2.3 Algorithm 3: User interfacing for the mHealth system

The third algorithm checks the data access capabilities. The algorithm extracts information from the blockchain and makes it public. Users can obtain the data from the blockchain depending on their selected configuration. The algorithm allows access to the data in several ways. For instance, users can obtain information based on their user and appt. IDs. Clinicians can easily view the test report of medical using the user's appt. ID. The third algorithm is described as follows:

- **Input**: Parameters for accessing the data.

- **Processing**: An appointment identifier is obtained for each identified user to access the medical record. If the user is not valid, he or she must register in the system via a cloud database and a two-factor authentication service.
- **Output**: Mapped data available to the user.

Algorithm 3 Interface layer for web & mobile app

0: Input: $\mathcal{U}(\iota d), \varrho(\iota d), \mathcal{U}(\tau), \tau$ {User ID, Appointment ID, User Type, Test Type}
0: Output: $\mathcal{R}$ {Display analytics}
0: **procedure** IINTERFACEMODULE {Event based function}
0: **if** $\mathcal{U}(\iota d)$ is $\mathcal{VALID}$ **then** {Google Fire-base Authentication}
0: **if** $\mathcal{U}(\tau) == \mathcal{D}$ **then** {Doctor To Check Report}
0: **if** $\tau == \mathcal{B} \| \tau == \mathcal{L}$ **then** {Test Type Blood OR Lipid}
0: $\mu \leftarrow$ GetReport$(\varrho(\iota d))$ {Return Test Report}
0: **end if**
0: **end if**
0: **else**
0: **if** $\tau == \mathcal{B} \| \tau == \mathcal{L}$ **then** {Test Type Blood OR Lipid}
0: $\mu \leftarrow$ GetReport$(\mathcal{U}(\iota d), \varrho(\iota d))$ {Return Test Report Map with User ID}
0: **end if**
0: $\mathcal{R} \leftarrow$ UpdatedDashboard(μ) {Show Data on User Screen}
0:
0: $\mathcal{REGISTER}(\mathcal{U}(\iota d))$ {Register account in Firebase}
0: **end if**
0: **end procedure**=0

5 Framework Implementation and Validations

Implementation and validation details are presented of the proposed framework. Specifically, the infrastructure and technologies to implement the proposed framework are elaborated in Sections 5.1–5.2 and described in Figures 6 and 7. Sections 5.3–5.5 provide details on the evaluation of energy efficiency, execution performance, and framework scalability, as demonstrated in Figures 8, 9, and 10, respectively. This section details the proposed system's outputs, which include an environmental assessment (performance, response of query, and efficiency). Threats to research validity and pertinent constraints are also addressed.

5.1 Infrastructure and Technology for Framework Implementation

Implementing the algorithms requires a technology stack and infrastructure compatible with medical imaging and data processing, as well as blockchain and smart contract transactions.

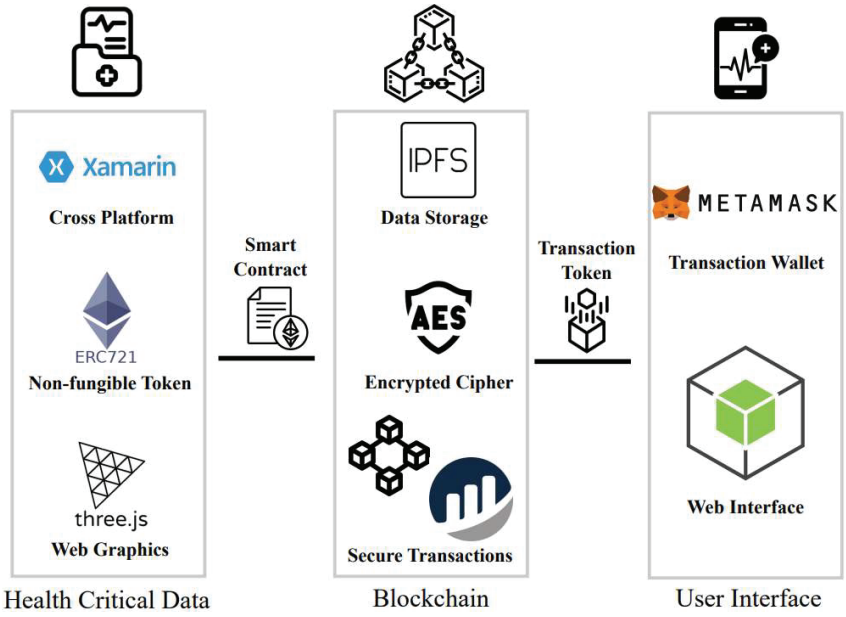


Figure 6 Overview of tools and technologies for framework implementation.

The platform was developed on a client-server architecture using Node.js. To launch the Node.js application, Visual Studio Code was used, and the Ganache Truffle Suite enabled the creation of a personal Ethereum blockchain that could conduct the tests, issue commands, and monitor the state of the blockchain operations. Furthermore, for application development, we opted for Xamarin Cross-platform within Microsoft Visual Studio, focusing on the Xamarin Android Mobile platform (see Figure 7). This approach ensured a seamless and integrated development process, enabling efficient testing and deployment. The choice of these technologies is aimed at fostering a robust and user-friendly environment for the successful execution of the platform's functionalities.

5.2 Configuration of the Validation Environment

We used the Windows operating system to develop a mechanism for delivering lab test results and medical imaging data to the IPFS. Aiming at using the distributed web, we used Ganache to connect with ether blockchain environment. We used the Metamask plugin, which links local Ethereum accounts to Ganache as a private blockchain to perform the operations of our

Figure 7 Data access view on a mobile interface.

proposal using the cost of gas transactions. On the other hand, we developed an API to abstract communications from the blockchain to avoid difficulties when interacting directly with the IPFS and the blockchain ledger. In turn, for formatting and low-level parsing of the Ethereum protocol, we used an Ethereum client and its corresponding libraries.

Figure 8 shows the application's different views on data presentation of blockchain. In a mobile application, the first screen is to register the user as a patient in Google Firebase to access their medical data. After login, the user type will be verified using the Google email authentication service and if the user is a patient they will see the screen with two inputs to access the record, the first input is Patient ID and the second input is Appointment ID by a patient. If the user type is a doctor they will see a single input to access the record of a patient by passing only the Appointment ID, the same at the bottom of the web portal shows the data.

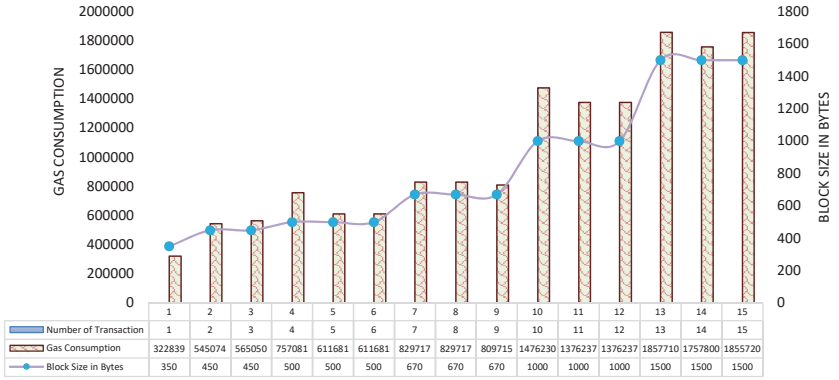


Figure 8 Evaluating energy efficiency: gas consumption per block size and transaction count.

5.3 Evaluation I: Energy Efficiency Based on Gas Consumption for Data Uploading

The gas is used to pay the fee to execute the smart contract in the Ethereum environment. In this regard, we assess the consumption of gas and compare it to that of the data payload. In our validation, we use the Gwei[9] to monitor fuel use. In addition, we defined the cost of carrying out the contract migration (see Table 4). We determined ether price of gas utilized. The ether is calculated by multiplying the petrol use by the petrol price. In turn, the gas reflects the system's calculation expenses. The network described in [17] changed the petrol price to take into account changes in the Ether value. The prototype we developed in our study sets a default gas constraint for validation and analysis purposes.

The migration process involves creating a smart contract with a minimal cost of 0.0054726 ether and ingesting of fuel for 27,363. By minimizing the input data, overall costs can be further decreased. Nevertheless, these expenses remain more economical compared to paying for external storage space or maintaining a centralized database.

Table 4 Smart contract execution cost analysis

Execution Type	Gas Used	Cost in Ether
Creation of SM	2869227	0.05738454
Migration of SM	27363	0.0054726
Initial contract	225237	0.0450474
Initial migration	42363	0.0084726
Final cost		**0.06188928**

5.4 Evaluation II: Computational Efficiency to Up/Download Data to IPFS and Blockchain

To assess our work, we measure the time users spend loading and saving data to the IPFS and the blockchain ledger. This includes determining how long it takes to load medical data, retrieve accessible data, and assess the data, as well as the time required for data search, which is critical for recording medical data transactions in IPFS and keeping log information on the blockchain. The query response time is evaluated to assess the system's efficiency for recording data making transactions from the blockchain. We explore the speed at which medical image data and records with file hashes are stored in the IPFS. The correlation between the number of execution calls and the percentage of CPU usage corresponding to the processing of a report from mobile and web are illustrated in Figure 11. Figure 11 illustrates the scalability of the proposed solution across mobile and web systems in terms of execution calls and processing time.

The environment of evaluation is a set of software resources and hardware used to evaluate the developed system and record various execution phases and outcomes. Hardware trials on the Windows Platform, involving lab test results and medical image data submissions to IPFS (core i7, 16 GB RAM with SSD), were executed. For software evaluation, Node.js code, executed using ReactJS in Visual Studio Code, automated system testing. The assessment utilized various libraries like web3, ipfs for http, and some other for communication. To measure the performance of CPU, JS script is used during processing the medical data in term of accessing and decentralizing. To make the local environment for ether blockchain, we used the Ganache suit kit, and the Metamask addon in the browser integrated local Ethereum accounts into Ganache, operating as a private blockchain for testing. System operations in the testing environment were carried out using the gas transaction cost.

5.5 Evaluation III: Framework Scalability Based on Overall Execution Monitoring

Figure 8 illustrates the relationship between fuel consumption and stored bytes. Loading 450 bytes incurs an average fuel consumption of approximately 555,062 gas units, while storing 1000 byte data results in an average fuel consumption of around 1,409,568. This indicates a direct correlation between data size and gas consumption. Notably, despite an increase in data size, our proposal exhibits consistent fuel usage when loading medical data into the IPFS.

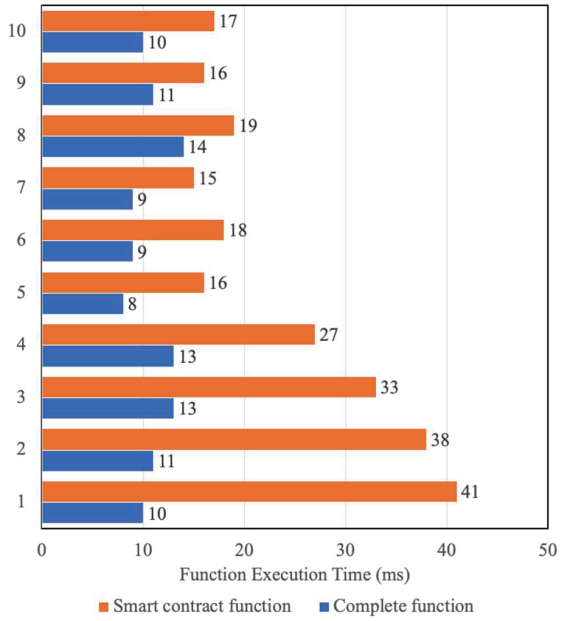


Figure 9 Computational efficiency: time to execute data upload to IPFS and blockchain.

5.6 Advantages and Limitations of the Proposed Study

Once evaluation has been detailed, we also summarize the advantages and the limitations of the proposed research.

Advantages of the proposed mHealth framework

1. **Enhanced security and privacy:** The study proposes a blockchain-based framework for mobile healthcare (mHealth) systems, which significantly improves data security by preventing unauthorized access and ensuring data integrity.
2. **Decentralization and transparency:** By leveraging blockchain and the IPFS, the framework eliminates reliance on centralized server which reduce the allied risk.
3. **Scalability and efficiency:** The experimental evaluation indicates that the system achieves low query response times (10–41 ms), minimal CPU utilization (1.5%–2.5%), and efficient energy consumption (40,000 gas units for 1000 bytes).
4. **Patient-centric control:** Patients have direct control over their health data, for enhancing privacy and user autonomy.

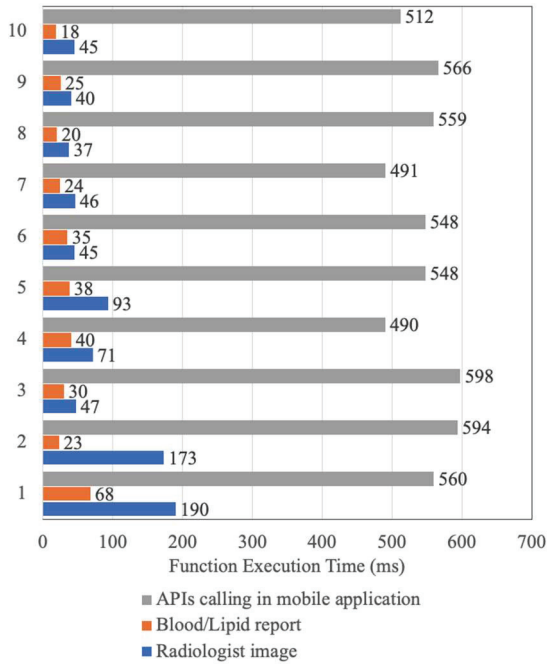


Figure 10 Computational efficiency: time to execute data download to IPFS and blockchain.

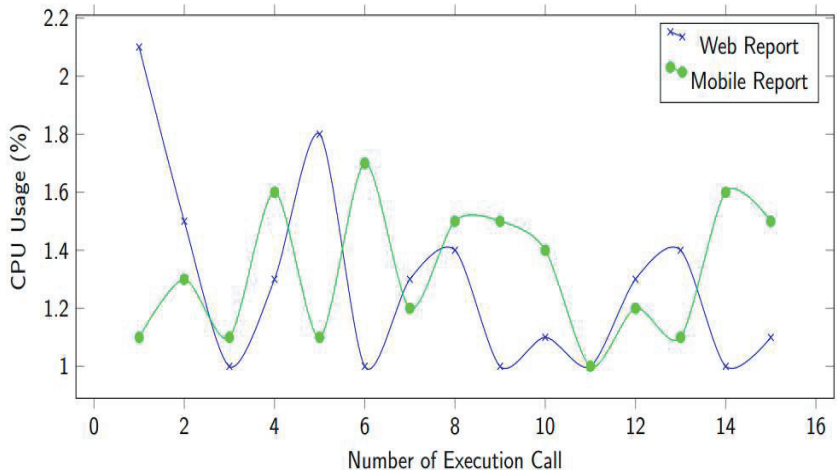


Figure 11 Scalability analysis with overall evaluation: execution calls and processing time.

5. **Smart contract automation:** The use of Ethereum smart contracts facilitates automated, trust-less interactions between stakeholders (patients, doctors, and health units), reducing administrative overhead.
6. **Cost-effectiveness:** Decentralized storage reduces dependency on expensive cloud-based storage infrastructure, potentially lowering long-term operational costs.

Disadvantages of the proposed mHealth framework

1. **Computational and energy costs:** While blockchain ensures security, the study highlights the gas consumption and energy costs associated with smart contract execution, which may limit large-scale adoption.
2. **Limited storage capability:** Storing large medical images on a blockchain is inefficient, necessitating the use of the IPFS. However, the IPFS requires separate management and security measures.
3. **Technical complexity:** The implementation of blockchain and smart contracts requires specialized knowledge, making adoption challenging for healthcare providers with limited expertise.
4. **Regulatory and compliance issues:** The use of decentralized technology in healthcare must adhere to strict legal and regulatory requirements (e.g., HIPAA, GDPR), which may pose barriers to adoption.
5. **Network scalability concerns:** Blockchain networks can face congestion issues, leading to higher transaction costs and slower processing times as the number of users grows.
6. **Dependency on internet connectivity:** Since the system relies on blockchain and cloud-based components, uninterrupted internet access is crucial, which may be a limitation in remote or underdeveloped regions.

6 Future Work

This study presents a decentralized framework for web and mobile-based technology for decentralizing medical data. Our system will, in the future, be enhanced further to the highpoint of current research with the use of a metaverse so that our system can deliver the latest research findings. A diversity of data evaluation will be the focus of future case studies, increasing the rigor of the evaluation.

Case studies and pervasive healthcare: It will also focus on improving the proposed blockchain-enabled mHealth system by enhancing scalability, minimizing transaction costs, and enhancing interoperability with existing

healthcare structures. This research will explore different consensus mechanisms for improved efficiency and integrate unconventional cryptographic techniques to strengthen data privacy. The framework will be extended to incorporate more case studies and applications in several domains, such as smart transportation and smart homes, to evaluate its adaptability and effectiveness in diverse IoT-driven environments, and evaluations will also be conducted to assess usability and adoption in several sectors.

Datasets for mobile healthcare: In the medical domain, the framework can be tested with larger and more diverse datasets for adaptability and effectiveness in real-world applications that can be better evaluated. This framework can be extended to support the interoperability with available systems of healthcare such as HER. To validate PCRIM-Mob, we evaluated the efficiency of our proposal. The results indicate that when storing medical images, our proposal gives patients access to an immutable medical database, obtaining acceptable results regarding data provenance, as no intermediaries or administrative entities are needed.

7 Discussion

This study presents a novel framework for the secure management of mobile health (mHealth) data using blockchain. The research describes the privacy, security, and scalability challenges of monolithic-type centralized mHealth systems by leveraging blockchain and the IPFS for decentralized storage. The proposed framework empowers patients to keep control over their health data and presents a secure and transparent approach compared to existing centralized systems. The framework contributes Ethereum-based smart contracts and decentralized storage to ensure efficient data management and access control. This section confers the key findings, implications, and challenges met during the development and evaluation of the proposed system.

Key findings: The evaluations based on experiments of the framework determine its effectiveness in several critical areas. First, the system scalability was established with query response times reaching from 10 ms to 41 ms, signifying that the decentralized architecture can efficiently handle queries, even when the number of users increases. Second, the computational performance was found to check efficiency with CPU utilization ranging from 1.5% to 2.5%. These results advise that the blockchain-enabled mHealth system is proficient in processing medical transactions with less resource ingesting, a critical factor for extensive implementation in healthcare environments.

Third, the system showed impressive energy efficiency with gas consumption of 40,000 units for 1000 bytes of data, effectively without incurring excessive operational costs.

8 Conclusions and Validity Threats

Recent research has emphasized the development of secure healthcare systems through pervasive mobile healthcare (mHealth) solutions. The current mHealth landscape relies on centralized storage, leading to increased maintenance costs and security risks. This study proposes a blockchain-enabled mHealth system, combining mobile computing and blockchain to enhance data security and privacy. It introduces a framework, implements proof-of-concept algorithms, and conducts evaluations to validate scalability, computation, and energy efficiency. The front end utilizes a mobile application interface, while the backend employs the InterPlanetary File System and Ethereum blockchain for secure data management. Evaluation of the Ethereum TESTNET network indicates promising scalability (10–41 ms), efficient CPU utilization (1.5%–2.5%), and energy efficiency (40,000 gas units for 1000 bytes) (see Figure 8). This comprehensive solution aims to advance cybersecure mHealth implementations using blockchain technology.

The key findings and primary contributions of this research are categorized as:

- A mobile and blockchain integrated smart healthcare framework that synergizes mobile computing systems (context-sensitive devices for health-critical data) and blockchain technology (infrastructure to secure storage and retrieval of health-critical data). The framework provides a patient-centric access management system based on a smart contract that allows doctors and patients to view medical test records on a decentralized web portal and mobile interface.
- A proof-of-concept that automates and provides a proof-of-concept for mobility-driven and secure management and transmission of health-critical data. The algorithms enable the development of a proof-of-concept and foundations to evaluate the mHealth prototype for a patient-centric control system on Ethereum.
- Multi-criteria experimental evaluations by deploying a smart contract prototype on the Ethereum TESTNET network within a Windows environment. The evaluation outcomes highlight three critical aspects in terms of scalability, computational efficiency, and energy efficiency.

These evaluation results affirm the effectiveness and practicality of our blockchain-enabled mHealth system.

Threats to validity: The study has two main validity threats, referred to as *internal* and *external* validity threats that need to be highlighted. Internal validity threats represent limitations that influence how the proposed system is designed and put into practice. For instance, the results could differ in terms of performance if medical data were used to carry out the experiments and produce the output. External validity connects to several pertinent systems and case studies that validate the solution. To illustrate and assess the solution, we used a case study approach, as described in the research method and assessment section. To minimize the effects of external validity, more case studies will be needed in the future.

Acknowledgements

This research has been funded by Scientific Research Deanship at University of Ha'il – Saudi Arabia through project number RG-21 149.

References

[1] Mazhar T, Irfan HM, Khan S, Haq I, Ullah I, Iqbal M, Hamam H. Analysis of Cyber Security Attacks and Its Solutions for the Smart grid Using Machine Learning and Blockchain Methods. Future Internet. 2023; 15(2):83. https://doi.org/10.3390/fi15020083.

[2] Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton University Press, 2016.

[3] F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: A technical survey on decentralized digital currencies," IEEE Communications Surveys & Tutorials, vol. 18, no. 3, pp. 2084–2123, 2016.

[4] T. Aste, P. Tasca, and T. Di Matteo, "Blockchain technologies: The foreseeable impact on society and industry," 2017.

[5] S. Kruse, B. Smith, H. Vanderlinden, and A. Nealand, "Security techniques for the electronic health records," Journal of Medical Systems, vol. 41, no. 8, pp. 1–9, 2017.

[6] Shah, S. F. A., Mazhar, T., Al Shloul, T., Shahzad, T., Hu, Y. C., Mallek, F., and Hamam, H. (2024). Applications, challenges, and solutions

of unmanned aerial vehicles in smart city using blockchain. PeerJ Computer Science, 10, e1776.

[7] Ghadi, Y.Y., Shah, S.F.A., Mazhar, T. et al. Enhancing patient healthcare with mobile edge computing and 5G: challenges and solutions for secure online health tools. J Cloud Comp 13, 93 (2024). https://doi.org/10.1186/s13677-024-00654-4.

[8] G. Márquez, C. Taramasco, and H. Astudillo, "Defining security metrics to evaluate electronic health records systems: A case study in chile," in 2020 IEEE International Conference on Software Architecture Companion (ICSA-C), pp. 173–180, IEEE, 2020.

[9] A. H. Seh, M. Zarour, M. Alenezi, A. K. Sarkar, A. Agrawal, R. Kumar, and R. Ahmad Khan, "Healthcare data breaches: insights and implications," in Healthcare, vol. 8, p. 133, Multidisciplinary Digital Publishing Institute, 2020.

[10] G. Bigini, M. Zichichi, E. Lattanzi, S. Ferretti, G. D'Angelo, et al., "Decentralized health data distribution: A dlt-based architecture for data protection," in 5th IEEE International Conference on Blockchain (Blockchain 2022), IEEE, 2022.

[11] G. Ye, H. Yin, T. Chen, M. Xu, Q. V. H. Nguyen, and J. Song, "Personalized on-device e-health analytics with decentralized block coordinate descent," IEEE Journal of Biomedical and Health Informatics, 2022.

[12] Y. Psaras and D. Dias, "The interplanetary file system and the filecoin network," in 2020 50th Annual IEEE-IFIP International Conference on Dependable Systems and Networks-Supplemental Volume (DSN-S), pp. 80–80, IEEE, 2020.

[13] M. Nofer, P. Gomber, O. Hinz, and D. Schiereck, "Blockchain," Business & Information Systems Engineering, vol. 59, no. 3, pp. 183–187, 2017.

[14] A. Miller, "Permissioned and permissionless blockchains," Blockchain for distributed systems security, pp. 193–204, 2019.

[15] W. Zou, D. Lo, P. S. Kochhar, X.-B. D. Le, X. Xia, Y. Feng, Z. Chen, and B. Xu, "Smart contract development: Challenges and opportunities," IEEE Transactions on Software Engineering, vol. 47, no. 10, pp. 2084–2106, 2019.

[16] Z. Zheng, S. Xie, H.-N. Dai, W. Chen, X. Chen, J. Weng, and M. Imran, "An overview on smart contracts: Challenges, advances and platforms," Future Generation Computer Systems, vol. 105, pp. 475–491, 2020.

[17] G. Wood et al., "Ethereum: A secure decentralised generalised transaction ledger," Ethereum project yellow paper, vol. 151, no. 2014, pp. 1–32, 2014.
[18] W. Ethereum, "Ethereum whitepaper," Ethereum. URL: https://ethereum.org [accessed 2022-09-22], 2014.
[19] Bermúdez, A. G., Carramiñana, D., Bernardos, A. M., Bergesio, L., and Besada, J. A. (2024). A fusion architecture to deliver multipurpose mobile health services. Computers in Biology and Medicine, 173, 108344.
[20] Sarkar, A., and Jhamb, M. (2024). Secure and portable health monitoring system for Cyber Physical Systems in Internet of Things. Engineering Research Express.
[21] Rathore, Nitin, Aparna Kumari, Margi Patel, Alok Chudasama, Dhyey Bhalani, Sudeep Tanwar, and Abdulatif Alabdulatif. "Synergy of AI and Blockchain to Secure Electronic Healthcare Records." Security and Privacy 8, no. 1 (2025): e463.
[22] Vatambeti, Ramesh, ES Phalguna Krishna, M. Ganesh Karthik, and Vijay Kumar Damera. "Securing the medical data using enhanced privacy preserving based blockchain technology in Internet of Things." Cluster Computing 27, no. 2 (2024): 1625–1637.
[23] Tariq, M. U. (2024). Revolutionizing health data management with blockchain technology: Enhancing security and efficiency in a digital era. In Emerging Technologies for Health Literacy and Medical Practice (pp. 153–175). IGI Global.
[24] E. Ahmed, I. Yaqoob, A. Gani, M. Imran, and M. Guizani, "Internet-ofthings-based smart environments: state of the art, taxonomy, and open research challenges," IEEE Wireless Communications, vol. 23, no. 5, pp. 10–16, 2016.
[25] X. Larrucea, A. Combelles, J. Favaro, and K. Taneja, "Software engineering for the internet of things," IEEE Software, vol. 34, no. 1, pp. 24–28, 2017.
[26] Sharma, Aashima, Sanmeet Kaur, and Maninder Singh. "A comprehensive review on blockchain and Internet of Things in healthcare." Transactions on Emerging Telecommunications Technologies 32.10 (2021): e4333.
[27] Pustokhin, Denis A., Irina V. Pustokhina, and K. Shankar. "Challenges and future work directions in healthcare data management using blockchain technology." *Applications of Blockchain in Healthcare* (2021): 253–267.

[28] Aljedaani, Bakheet, et al. "An empirical study on secure usage of mobile health apps: The attack simulation approach." Information and Software Technology 163 (2023): 107285.

[29] Aljedaani, Bakheet, et al. "End-users' knowledge and perception about security of clinical mobile health apps: A case study with two Saudi Arabian mHealth providers." Journal of Systems and Software 195 (2023): 111519.

[30] Balapour, Ali, et al. "Mobile technology identity and self-efficacy: Implications for the adoption of clinically supported mobile health apps." International Journal of Information Management 49 (2019): 58–68.

[31] Kao, Cheng-Kai, and David M. Liebovitz. "Consumer mobile health apps: current state, barriers, and future directions." PM&R 9.5 (2017): S106–S115.

[32] Zhang, Peng, et al. "FHIRChain: applying blockchain to securely and scalably share clinical data." Computational and structural biotechnology journal 16 (2018): 267–278.

[33] Farouk, Ahmed, et al. "Blockchain platform for industrial healthcare: Vision and future opportunities." Computer Communications 154 (2020): 223–235.

[34] CHELLADURAI, Mrs USHARANI, Seethalakshmi Pandian, and Krishnamoorthy Ramasamy. "A blockchain based patient centric electronic health record storage and integrity management for e-Health systems." Health Policy and Technology 10.4 (2021): 100513.

[35] Nanda, Saroj Kumar, Sandeep Kumar Panda, and Madhabananda Dash. "Medical supply chain integrated with blockchain and IoT to track the logistics of medical products." Multimedia Tools and Applications (2023): 1–23.

[36] Sun, Fangmin, et al. "Gait-based identification for elderly users in wearable healthcare systems." Information fusion 53 (2020): 134–144.

[37] Fahmideh, Mahdi, John Grundy, Aakash Ahmad, Jun Shen, Jun Yan, Davoud Mougouei, Peng Wang et al. "Engineering blockchain-based software systems: Foundations, survey, and future directions." *ACM Computing Surveys* 55, no. 6 (2022): 1–44.

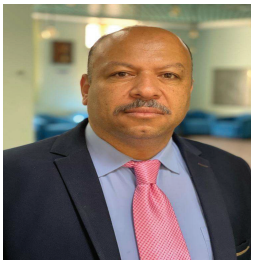
[38] Guggenberger, Tobias, Vincent Schlatt, Jonathan Schmid, and Nils Urbach. "A Structured Overview of Attacks on Blockchain Systems." *PACIS* (2021): 100.

Biographies

Adel Alkhakil received a Ph.D. degree from Bournemouth University, Poole, UK. He joined the College of Computer Science and Engineering, University of Ha'il, Hail, Saudi Arabia, as an Assistant Professor. His research interests include software evolution for mobile and cloud computing systems, decision support systems, and knowledge-based systems.

Abdul Razzaq received a Ph.D. degree from Zhejiang University of China in 2024. He did his M.Sc. in Software Engineering in 2018 at International Islamic University of Islamabad (IIUI), Pakistan. His research of interest areas are software engineering, blockchain, Internet of Things, ocean Internet of technologies, and mobile computing.

Aakash Ahmad is currently working as Assistant Professor in Software Engineering at the School of Computing and Communications, Lancaster University Leipzig, Germany. He is also acting as a Technical Consultant for TeraBluIoT that focuses on the engineering and development of Internet of Things and Quantum computing systems. He received his Ph.D. in Software Engineering from the School of Computing, Dublin City University, Ireland in 2015 respectively.



Magdy Abdelrhman is a professor of educational planning at the Education College, New Valley University, Egypt. He currently works as a quality and development consultant at the Deanship of Quality and Development, University of Hail, Kingdom of Saudi Arabia. His research interests include educational planning, strategic planning, and educational administration.

Yaser Mohammed Altameemi is currently an Assistant Professor with the Department of English, College of Literature and Arts, University of Hai'l. He is interested in critical discourse analysis, discourse studies, and corpus linguistics. His research interests include investigating the use of language with the consideration of institutional, social, and cultural contexts qualitatively and quantitatively through big data analytical tools.

Mohammed Altamimi received a Ph.D. degree from Bangor University, Bangor, Wales, in 2020. He joined the College of Computer Science and Engineering, University of Ha'il, Saudi Arabia, as an Assistant Professor. His research interests include machine learning, deep learning and natural language processing (NLP).

Zhang Tao, Shaanxi Province, was born in April 1976. He is a professor at the School of Software, Northwestern Polytechnical University. His main research directions include software definition, network software, large models, open system architecture, etc. He has published over 10 high-level research papers in prestigious journals such as Information Science, IEEE Software, and Acta Electronica Sinica, authored 1 monograph and 2 textbooks, and holds over 20 software copyrights.