A Framework for Patient-Centric Medical Image Management using Blockchain Technology

Abdulaziz Aljaloud
College of Computer Science and Engineering, University of Ha'il, Saudi Arabia

***Abstract*—In smart systems context, the storage and distribution of health-critical data – medical images, test reports, clinical information etc. that is processed and transmitted via web portal and pervasive devices which requires a secure and efficient management of patients' medical records. The reliance on centralized data centers in the cloud to process, store, and transmit patients' medical records poses some critical challenges including but not limited to operational costs, storage space requirements, and importantly threats and vulnerabilities to the security and privacy of health-critical data. To address these issues, this research proposes a framework and provides a proof-of-the-concept named Patient-Centric Medical Image Management System (PCMIMS). The proposed solution PCMIMS utilizes the Ethereum blockchain and Inter-Planetary File System (IPFS) to enable secure and decentralized storage capabilities that lack in existing solution for patients' medical image management. The PCMIMS design facilitates secure access to Patient-Centric information for health units, patients, medics, and third-party requestors by incorporating the Patient-Centric access control protocol, ensuring privacy and control over medical data. The proposed framework is validated through the deployment of a prototype based on smart contract executed on Ethereum TESTNET blockchain that demonstrates efficiency and feasibility of the solution. Validation results highlight a correlation between (i) number of transactions (i.e., data storage and retrieval), (ii) gas consumption (i.e., energy efficiency), and (iii) data size (volume of Patient-Centric medical images) via repeated trials in Microsoft Windows environment. Validation results also indicate computational efficiency of the solution in terms of processing three most common types of Patient-Centric medical images namely (a) Magnetic resonance imaging (MRI) (b) X-radiation (X-Rays), (c) Computed tomography (CT) scan. This research primarily contributes by designing, implementing, and validating a blockchain based practical solution for efficient and secure management of Patient-Centric medical image management in the context of smart healthcare systems.**

Keywords*—Smart healthcare; medical imaging; blockchain; ethereum; distributed storage

I. INTRODUCTION

Information and Communication Technologies (ICTs) and infrastructures have brought significant advancements to the healthcare industry – enabling efficient healthcare delivery – to a number of stakeholders such as medical units, patients, and medics [1]. In smart healthcare context, patient information systems have revolutionized the healthcare sector via medical information systems, pervasive technologies, internet of things driven sensors to tackle healthcare challenges effectively and efficiently [2]. Numerous studies have established a strong correlation between storage, analytics, and transmission of advanced clinical information and communication systems to improve healthcare quality, safety, and patient-centeredness [3]. However, the fragmented nature of health-critical information (i.e., medical images, test reports, clinical information etc.) poses challenges correspond to an effective utilization of personal health information to promote effective and efficient treatment [4]. This fragmentation often results in cumbersome data management and compromises overall patient safety, as health information systems within hospitals, medical clinics, laboratories, and pharmacies remain separate entities that are prone to data security threats or compromised health-critical information [5].

Smart healthcare systems have become increasingly integrated into various aspects of healthcare, including hospital information systems, internet of medical things (IoMTs) and pervasive healthcare technologies [6]. Specifically, as the fundamental unit of smart healthcare, hospital management information systems play a critical role in managing patient data, streamlining workflows, and improving overall healthcare delivery [7]. These systems encompass a range of functionalities, including Electronic Health Records (EHRs), Computerized Physician Order Entry (CPOE), and Picture Archiving and Communication Systems (PACS). PACS has emerged as an essential component of modern radiology departments, enabling the efficient storage, retrieval, and distribution of medical images, including MRI scans [8]. By digitizing and organizing images, PACS eliminates the need for traditional film-based methods and enables rapid access to patient imaging data. It provides radiologists and healthcare professionals with a centralized platform for image interpretation, collaboration, and reporting, leading to improved diagnostic accuracy and patient care outcomes [9].

The integration of ICT in smart healthcare systems, such as hospital information systems and PACS, offers numerous advantages related to cost-efficiency, operational readiness, along with security and privacy of health-critical data [10]. It enables seamless communication and exchange of patient information between various healthcare units (e.g., hospital and labs), medics (e.g., doctors, nurses) and other stakeholders such as patients or healthcare authorities [11]. Such an automated and connected healthcare facilities improve healthcare coordination, faster access to critical information, and enhanced decision-making processes, ultimately benefiting patient outcomes and satisfaction. Despite the outlined benefits as above, the implementation and integration of IT systems, particularly PACS, present various challenges and such challenges include but are not limited to issues related to interoperability, data security, privacy concerns, and the need for efficient data storage and management solutions [12]. Overcoming these challenges is crucial to ensure the effective utilization of ICT for smart healthcare and maximize its potential for improving patient care [13]. This research aims to address these challenges by proposing a novel approach for enhancing the integration and utilization of ICT systems, specifically focusing on hospital information systems and PACS in the context of MRI imaging. By leveraging existing method and algorithms of blockchain technology, this study aims to optimize data management, improve interoperability, and enhance overall efficiency in healthcare settings.

Context and Challenge(s): Medical images pose a significant challenge in terms of their size and storage requirements, surpassing the capacities typically available on public blockchains [14]. In recent years, blockchain-based solutions have started to gain significant attention with their use-cases and applicability in healthcare data management [15]. In response to the need for decentralized storage, Protocol Labs developed the InterPlanetary File System (IPFS) [16]. IPFS is designed as a distributed web solution that enables the sharing and storage of hypermedia that is managed as peer-to-peer (P2P) file system. It offers an alternative off-chain storage option that can be seamlessly integrated with different blockchain networks, enhancing interoperability [17]. IPFS provides a distributed data access system that offers several advantages, including persistence, improved efficiency, and faster online services. By utilizing content addressing, IPFS ensures that data can be accessed and retrieved from multiple locations, enhancing redundancy and availability [18]. The peer-to-peer nature of IPFS allows for efficient data sharing among participants, reducing the reliance on centralized servers and improving data transfer speeds [8-18]. Moreover, IPFS introduces a more intelligent approach to online services by enabling the creation of decentralized applications (dApps) that leverage its distributed storage capabilities [8-18].

However, despite the advantages offered by distributed storage options, there are notable challenges and barriers when it comes to storing sensitive medical images. One of the primary concerns is ensuring the privacy and security of patient images, while also preventing unauthorized access [21]. The sensitive nature of medical data necessitates robust privacy measures to protect patient confidentiality and complying with necessary regulations including but not limited to Health Insurance Portability and Accountability Act (HIPAA) [22]. Furthermore, a key requirement for a secure data management and its ability to handle large volumes of data across various stakeholders, including medics, health units, patients, and institutions [23].

Solution Overview: To address these challenges, we design and implement a proof-of-the-concept for a distributed framework called a Patient-Centric image management (PCMIMS). PCMIMS is a blockchain-based solution that is architected to enable secure and private management of Patient-Centric medical images within an open distributed network. We elaborate on a step-wise and incremental design, implementation and validation of the PCMIMS solution in dedicated sections and outline the key contributions and salient features of the proposed solution below. The implications of this research and proposed solution aims to complement the research and development on exploiting blockchain technologies synergized with the IPFS to enable secure management of health-critical data. The proposed solution PCMIMS in terms of a framework, its implemented prototype, and validations could help researchers and developers to incrementally design and develop a blockchain-based Patient-Centric medical image management in a secure and efficient way. Specifically, the solution aims to improve state-of-the-art by offering:

- Blockchain-based framework (i.e., PCMIMS) that provides a structural representation of the overall solution that sketches a blue-print and guides software designers and developers about how the system operates and facilitates effective healthcare management.
- Smart contract-based implementation of Patient-Centric access to PCMIMS that ensures controlled access to medical image data for stakeholders, i.e., medics and patients. The implemented prototype employs specific functions to enable data transfer via Ethereum blockchain and establishes access privileges between relevant parties. This enhances privacy and security in the management of medical data.
- Experimental validation of the functionality of the proposed solution PCMIMS through test cases, focused on key performance metrics. These metrics include (i) number of transactions (i.e., data storage and retrieval), (ii) gas consumption (i.e., energy efficiency), and (iii) data size (volume of Patient-Centric medical images) via repeated trials in Microsoft Windows environment. This evaluation ensures the effectiveness and efficiency of the proposed framework in handling medical data and provides insights for future enhancements.

Structure of the paper: Section II provides context and background of the proposed research. Section III discusses the most relevant existing research. Section IV presents research method and motivating scenario. Section V discusses prototype-based implementation of the proposed solution. Section VI presents results of the solution validation. Section VII concludes the paper and summarizes the key findings and contributions of this research.

II. RESEARCH CONTEXT AND BACKGROUND

In this section, we provide a broader perspective and overall context of the proposed research. The context provides necessary background information in terms of some core concepts of healthcare management, distributed system, and healthcare data management. We have introduced the concepts and terminologies introduced in this section that are used throughout the paper to explain the technical concepts. Fig. 1 illustrates the core concepts and complements the theoretical description presented in this section.

A. Digital Healthcare Systems

Healthcare systems heavily rely on medical image systems for diagnosis, treatment, and monitoring of various medical conditions. These systems encompass the storage, retrieval, and analysis of medical images, specifically addressing X-rays, CT scans, MRI scans, and ultrasound images. The effective utilization of medical image systems plays a vital role in improving patient outcomes and optimizing healthcare delivery. However, the widespread adoption and integration of medical image systems in healthcare settings pose numerous challenges. One significant challenge is the sheer volume and complexity of medical images generated daily, leading to storage and management issues [12]. The exponential growth in medical image data requires robust infrastructure and storage solutions to ensure efficient access, retrieval, and secure archiving.

B. Medical Image Data

Another critical challenge lies in the interoperability and integration of medical image systems within the broader healthcare ecosystem [13]. Healthcare providers, hospitals, clinics, and other stakeholders often employ different systems and technologies, resulting in fragmented data silos. This fragmentation hinders seamless data exchange, collaboration, and comprehensive patient care. Moreover, privacy and security concerns are paramount in healthcare systems, especially when it comes to sensitive patient information contained within medical images [14]. The protection of patient privacy, compliance with regulatory requirements (e.g., HIPAA), and safeguarding against unauthorized access are essential considerations in the design, development, and operational context of medical image systems. Addressing these challenges requires innovative approaches and technologies to enhance the efficiency, interoperability, and security of medical image systems. Solutions such as distributed storage, blockchain technology, and advanced data analytics have shown promise in overcoming these hurdles [15, 16, 17]. By leveraging these advancements, healthcare organizations can optimize the management and utilization of medical images, leading to improved patient care, streamlined workflows, and enhanced decision-making processes.

Fig. 1 provides a comprehensive illustration of medical image-based data management in a distributed environment. The system ensures that user authorization is a prerequisite for accessing its functionalities. The user base comprises medics, patients, and individuals undergoing lab tests. In the patient registration process, users are required to request permission to utilize the system. Once the authorization is granted, users who have undergone lab tests can proceed to upload their test results. The MRI and radiologist specific data can be accessed via a designated web portal. It is important to note that access to the report's data is limited only to patients and doctors who have been specifically granted permission. A rigorous access control mechanism and implementation ensures that health-critical data remains private and secure and is only accessible to authorized individuals involved in patient care and treatment. The system's design and implementation prioritize data privacy and confidentiality while enabling efficient and secure sharing of medical information within a trusted and authorized user community.

III. RELATED WORK

This section reviews the most relevant existing research in terms of discussing state-of-the-art on (i) medical image data management in centralized system in Section III A and medical image data in distributed and peer-to-peer systems in Section III B. A critical review of the most relevant existing work helps us to comparatively analyze the scope of proposed solution and justify its contributions. Table I provides the comparative analysis and act as a catalogue to distinguish between most relevant existing works and proposed solution PCMIMS.

A. Medical Imaging Data in Centralised Systems

The management of medical health records is a critical aspect of healthcare systems. Traditional paper-based records have been gradually replaced by electronic health records (EHRs), which offer numerous advantages in terms of accessibility, interoperability, and data sharing [18]. EHR systems have transformed the way patient information is stored and accessed, enabling healthcare providers to have comprehensive and real-time access to patient data. Advanced medical imaging techniques, such as CT scans, MRI scans, and X-rays, play a pivotal role in diagnosing and monitoring various medical conditions. These imaging modalities generate large volumes of data, and efficient storage and retrieval systems are essential for their effective utilization in healthcare [19]. Imaging systems need to handle the complexities of different image formats, metadata, and associated clinical information. The management of medical images involves storing, organizing, and accessing various types of images, including CT scans, MRI scans, and X-rays. With the increasing volume and complexity of medical images, there is a growing need for efficient storage, retrieval, and analysis solutions [20]. Centralized and decentralized approaches have been explored to address the challenges of managing and sharing medical images.

Centralized systems, such as cloud-based storage and data centers, have been widely used in healthcare for storing and managing medical images. These systems offer centralized control, efficient storage, and accessibility but raise concerns regarding data security, privacy, and single points of failure [21].

B. Medical Imaging in Peer-to-Peer Distributed Systems

In contrast to the centralized management of medical images, decentralized approaches, such as distributed file systems and blockchain technology, have gained attention as potential solutions for medical image management [22].

Distributed file systems, like the InterPlanetary File System (IPFS), offer a decentralized architecture for efficient and secure storage and sharing of medical images [23]. Blockchain technology provides a distributed and immutable ledger that ensures data integrity, transparency, and privacy in medical image systems [24].

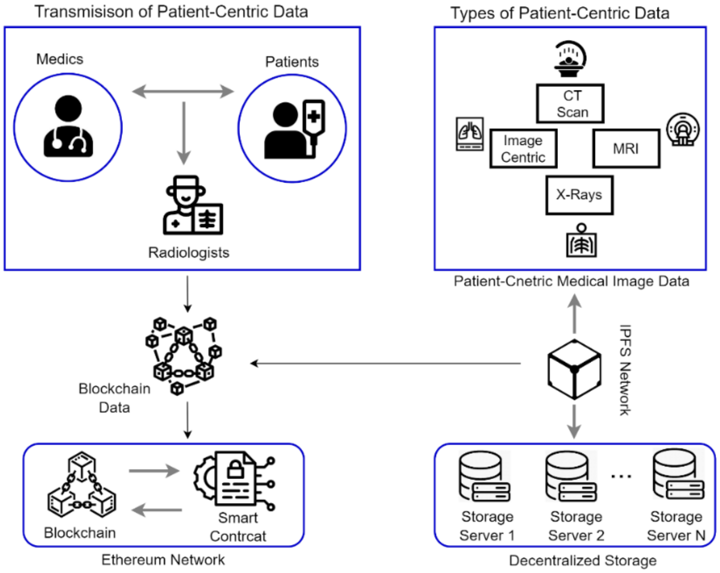


Fig. 1. Context: decentralized management of medical image data.

Researchers have explored the integration of centralized and decentralized approaches to strike a balance between efficiency, scalability, security, and privacy in medical image systems [25]. These studies aim to leverage the benefits of decentralized systems while addressing the challenges associated with data management, privacy, and interoperability.

Fig. 1 provides a comprehensive illustration of the entire system, depicting each step and process involved. The system ensures that user authorization is a prerequisite for accessing its functionalities. The user base comprises the medics (doctors, nurses, etc.), patients, and individuals undergoing lab tests. During the patient registration process, the users are required to request permission to utilize the system. Once the authorization is granted, users who have undergone lab tests can proceed to upload their test results and MRI radiologist image data through the designated website. It is vital to mention that access to the report's data is limited only to patients and doctors who have been specifically granted permission. This strict access control mechanism ensures that sensitive medical information remains secure and is only accessible to authorized individuals involved in patient care and treatment. The system's design and implementation prioritize data privacy and confidentiality while enabling efficient and secure sharing of medical information within a trusted and authorized user community.

Comparative Analysis and Summary: Table I provides a concise comparison of the proposed framework with other existing blockchain-based medical imaging and health data management systems. The table highlights the advantages offered by the PCMIM system over its competitors. It is evident that the PCMIM system outperforms the alternatives in terms of various benefits and features.

The table serves as a valuable reference, showcasing the superiority of the PCMIM system in comparison to the existing alternatives, thereby reinforcing its potential as an innovative and promising solution for effective medical health record management.

TABLE I. COMPARISON BETWEEN THE EXISTING AND PROPOSED PCMIMS SYSTEM

Scheme	[3]	[12]	PCMIMS System
Source Data Storage	Dedicated	Server	Immutable IPFS Storage
Encryption	Symmetric Encryption	✓	Asymmetric Encryption
Server Attack Resistance	×	×	✓
Database Management	Centralized	Centralized	Decentralized
Smart-Contract	×	✓	✓
Data-Access	×	×	✓

IV. RESEARCH CONTEXT AND BACKGROUND

This section presents the research method that is employed to conduct this research study, outlining the design specifics of the proposed solution. Fig. 2 provides an overview of the research methodology, which comprises four distinct stages. These stages follow an incremental approach, allowing for the assessment, development, and validation of the solution.

A. *Steps of Research Method*

The research methodology followed a structured process consisting of four distinct steps.

- Phase I: Literature Review involved a thorough examination of a diverse range of literature sources, including peer-reviewed research articles, technological road maps, and technical reports, to identify existing solutions and their limitations.

```
01: function AddImageCentric(string memory patientUserId, uint appointment_id,
02: string memory description, string memory filehash) public{
03: imgCount ++;
04: GetImageCentric_Id [_appointment_id] = ImageCentric(imgCount, appointment_id, _description, _filehash, now);
05: PatientRecordAccess [_patientUserId][_appointment_id] = ImageCentric (imgCount, appointment_id, _description, filehash, now);
06: emit ImageCentricCreated(imgCount, appointment_id, _description, filehash, now);
07: }
```

Listing 1. Code snippet for adding image to the chain.

To gather the most relevant papers in the field, a systematic literature review was conducted. This comprehensive review of existing research and development solutions helped establish the research scope and streamline the necessary solutions.

- Phase II: System Design focuses on architectural design of the proposed solution. Here, the proposed solution was meticulously modeled and simulated in accordance with established standards, such as the ISO/IEC/IEEE 42010:2011 standard [26].
- Phase III Algorithmic Implementation encompassed the implementation of algorithms, which involved executing the solution through computational and storage-intensive phases. The solution was broken down into modular algorithms that could be customized by users with specific inputs, adhering to executable standards and underlying source code.
- Phase IV Algorithmic Evaluation steps revolve around validating the solution by assessing its functionality and quality using the ISO/IEC-9126 model [26]. Well-established assessment metrics were employed to evaluate the system's usability and efficiency. While the first two steps required manual effort and human decision-making, the latter two phases involved human interaction and tool support. The validation phase provided insights for potential algorithm enhancements to improve efficiency or modify functionality based on the evaluation results. Overall, this methodology, as depicted in Fig. 2, ensured a comprehensive and systematic approach to solution development and evaluation.

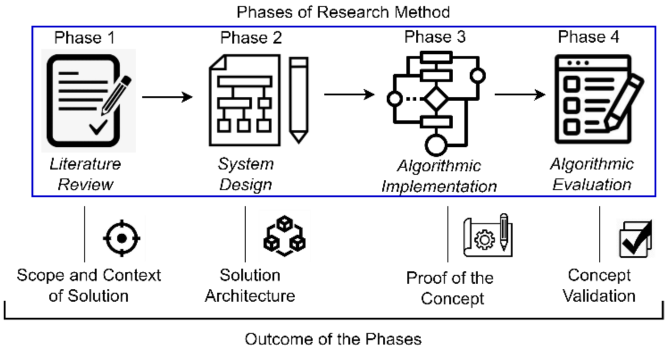


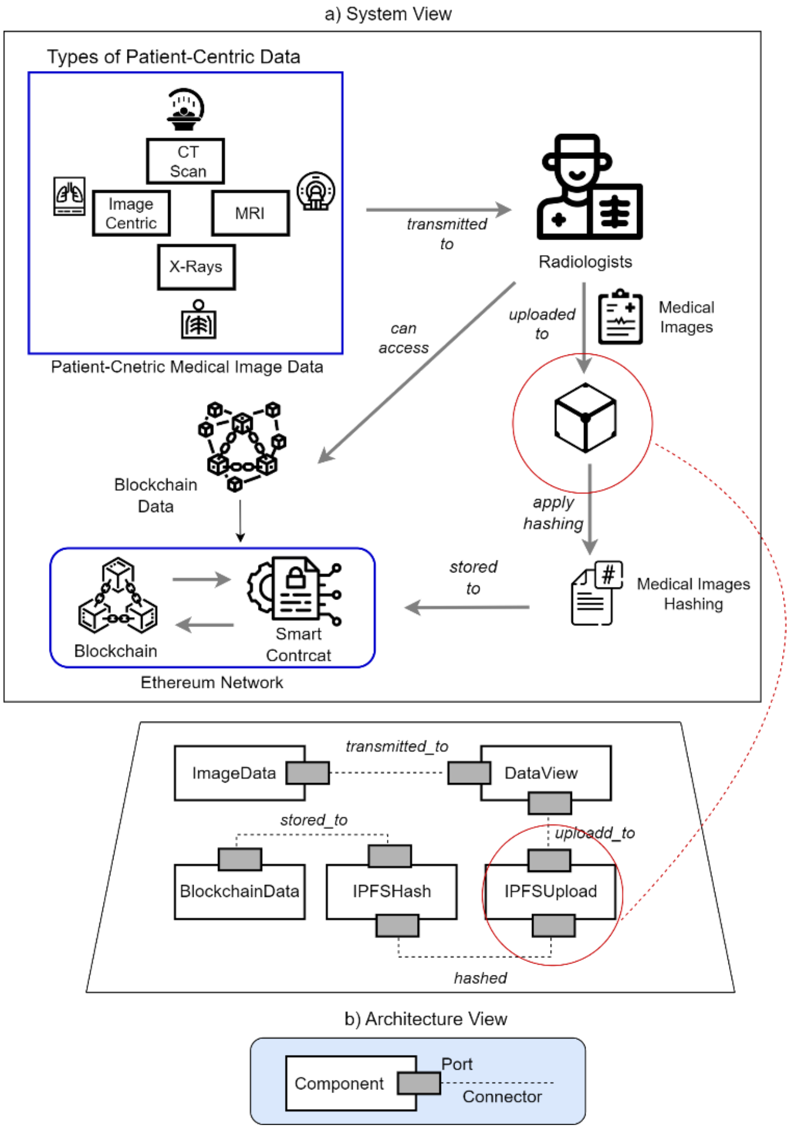
Fig. 2. An overview of four phases of research method.

B. Motivating Scenario

Fig. 3 illustrates a comprehensive process involved in storing and managing medical imaging and test reports within the proposed framework. The medical images are managed and stored via IPFS by the radiologist, who is responsible for the image acquisition and interpretation within the lab. The radiologist uploads the medical image data to IPFS, and in return, receives a unique hash key associated with the stored image. This hash key, along with other necessary information, is then linked and stored within the blockchain. It is important to note that the processes for medical image uploading are distinct from each other. The file hash of the medical image is then linked to the relevant details and stored within the blockchain. This systematic approach ensures the secure and efficient storage of medical images while maintaining the integrity and traceability of the data within the proposed framework.

The process of medical image data sharing is triggered via the creation of metadata for the original data file, which includes essential information such as the file's name, type, description, and size (Line 1 – Line 2) in Listing 1. Once the metadata is complete, it is uploaded to the IPFS along with the corresponding data file. To achieve this, a smart contract is created for the storage of the data in the blockchain by means of a function named ‘AddImageCentric’ (Line 4) with required parameters (Line 1). In order to streamline the data mapping process, two separate mappings are employed. The first mapping enables retrieval of a comprehensive list of all blood tests that are linked to a patient's appointment ID and the second mapping facilitates access to data specific to individual patients based on two parameters namely patient ID and appointment ID. To provide a seamless user experience and enhance data traceability, the ‘ImageCentricCreated’ event is triggered, signaling the successful creation of the image-centric data entry. This robust and organized approach ensures efficient data sharing and retrieval within the proposed framework while leveraging the advantages of blockchain technology and IPFS.

Blockchain-based management and IFPS based transmission of data ensures secure and transparent storage and transfer of medical image-centric data. Fig. 4 depicts two distinct categories of medical data uploading within the Decentralized Application (DApp) framework.



a) System View

b) Architecture View

Fig. 3. Patient-Centric data storage process.

(a) Overall System View, b) Architecture View

It pertains to medical images, which are connected to other examinations and tests by a radiologist. The radiologist utilizes the DApp system to upload the medical images to IPFS. Alongside the image upload, the radiologist provides the remaining essential details that include patient ID and appointment ID that are stored and retrieved via blockchain. This integrated approach ensures that medical images are seamlessly linked to the relevant patient and appointment data, enabling efficient retrieval and analysis.

The service cycle depicted in Fig. 4 continues to repeat itself at fixed intervals or auto triggered via receipt of medical image data, provided by the server. The dashboard serves as a platform that offers access to both doctors and patients acting as a web-accessible portal, enabling PCMIMS users to access, view, customize and download the medical images over the network. The web portal provides a convenient means of retrieving the health critical data (medical imaging, test reports etc.), with data retrieval based on customized parameters such as patient ID and appointment ID mappings [27] [28].

V. IMPLEMENTATION OF THE ALGORITHMS AS SOLUTION PROTOTYPE

This section discusses the implementation details in terms of the developed algorithms that provide a proof-of-the-concept prototype in Section VA. The discussion on algorithms is complemented with the details of tools and technologies for implementing the algorithms in Section V B. A precise discussion of the tools and technologies used for the implementation can help designers and developers to gain insight into the software tools that can be used to implement the solution [29].

A. Algorithmic View of the Developed Solution

The algorithms provide a modular implementation of the designed solution as in Fig. 3. Each of the two algorithms presented below are detailed in terms of their *inputs*, *processing*, and *outputs*, each elaborated below.

Algorithm 1 shows a step-wise and incremental this section demonstrates and describes the uploading feature for medical data. The technique specifically focuses on uploading medical image data to the IPFS and also applies hashing to the medical image data file for an extra security feature before its representation as a smart contract and storage in the blockchain. The uploaded data is associated with a number of parameters that include but are not limited to user and appointment identities (UserID, Appointment ID) along with description (Description), and data of the appointment (Date).

Algorithm 1 Decentralizing Medical Image

```
Parameters:
    U_ID: User ID
    A_ID: Appointment ID
    Des: Description
    Img = Image
---------------------------------------------------------------
Income: U_ID, A_ID, Des, Img
Outcome: O                              //Returning Result
procedure DATACENTRICMODULE             // Function
if U_ID is Valid then                   //Decentralizing Image
File_Stream ← File(Img)                 //Get File stream FS
File_Buffer ← Buffer.form (File_Stream)    //Convert
File_Hash ← IPFS.Add (File_Buffer)
O ← SBC(U_ID, A_ID, Description, File_Hash)   // Store Image hash and Data to Blockchain
end if
end procedure
```

- Income: The input to the algorithm involves mapping the parameters with a unique hash key of the medical image file. This mapping process occurs as part of the input. The input parameters include User ID, Appointment ID, and Description of the appointment and Medical Image. Combinedly, these parameters provide information about an individual user and their medical related information. The parameters provide customization and parametrized input to the solution.
- Processing: During the processing stage, the medical image data is being retrieved and processed for its conversion into a buffer package. The buffered data, comprising of medical image data is stored as IPFS as a medical data file that in turn hashes the data and generates a hashed key for data access. The additional parameters that include user and appointment identities (UserID, Appointment ID) along with description (Description), and data of the appointment (Date) are associated to the hash key. These parameters are subsequently are part of the smart contract that are privately stored on the blockchain.
- Outcome: Finally, the output stage involves managing and storing the processed medical image data in the blockchain. The mapped date, along with the associated parameters, is stored as the output of the algorithm, ensuring the secure and traceable storage of the uploaded medical data.

Algorithm 2 focuses on validating data accessing capabilities. The algorithm's primary purpose is to access the data in a secure way and make it accessible to authorized entities. By utilizing this algorithm, users can access specific data stored on the blockchain, driven by customized parameters. Notably, there are multiple types of data access available within the algorithm's processing stage. As an example, a user can access their data via user and appointment identities (UserID, Appointment ID) along with description (Description), and data of the appointment (Date).

Algorithm 2 Presentation Layer

```
Parameters:
    U_ID: User ID
    A_ID: Appointment ID
    U_Type: User Type
    T_Type= Test Type
---------------------------------------------------------------
Income:  U_ID, A_ID, U_Type, T_Type
Outcome: O
procedure Interface_Module
    if  U_Type ==  D then                 //Image Access
        Ɛ ←  Get_Report(T_Type)           // Test Type
    end if
R ←Update_Dashboard(Ɛ)                    //Data Dashboard
end procedure
```

- Income: During the input stage of the algorithm, the settings for data access are mapped, enabling the algorithm to determine the appropriate parameters for retrieval. The input parameters include User ID, Appointment ID, User Types and the medical Test Type. Combinedly, these parameters provide information about an individual user and their medical test being performed.
- Processing: The processing stage of the algorithm revolves around granting various forms of data access. This includes allowing users to access their data based on the mapping between their user and appointment identities (UserID, Appointment ID). Moreover, the medics such as the doctors or nurses can readily access the medical image data and reports by utilizing the appointment ID associated with the user (UserID).
- Outcome: As a result of the algorithm's execution, the output consists of publicly accessible data that has been mapped according to the defined parameters. This ensures that authorized users, such as patients and doctors, can retrieve the relevant data from the blockchain.

B. Tools and Technologies for Algorithmic Implementation

In this section, we present a concise overview of the complementary tools and technologies employed in the proposed solution, aiming to enhance the reader's comprehension of the underlying technology.

The combination of stacked tools and technologies, as depicted in Fig. 4, offers a comprehensive solution. For instance, if a radiologist accesses the portal, they can securely upload encrypted medical image files to the IPFS platform, receiving a hash key for subsequent validation of the proposed solution [30] [31].

VI. VALIDATION AND RESULTS

After presenting the implementation of the solution, we now discuss details on validation of the solution. To discuss the validation results objectively, we present the evaluation environment in Section VI A. We than elaborate on validation of the solution based on correlation between the number of transactions, gas consumption, and block data size. Finally, we also present computational efficiency of the solution in terms of processing three most common types of Patient-Centric medical images namely (a) Magnetic resonance imaging (MRI) (b) X-radiation (X-Rays), (c) Computed tomography (CT) scan.

A. Setting up the Evaluation Environment

The evaluation environment was carefully designed to include a combination of hardware and software resources that were essential for effectively executing and monitoring the different phases and outcomes of the solution. For the hardware-based evaluation experiments, a Windows platform was utilized, featuring a powerful core i7 processor and 16 GB of RAM. This robust hardware configuration provided the necessary computing power and memory capacity to handle the demanding tasks involved in the evaluation process. On the software front, a set of evaluation scripts was developed using NodeJS and ReactJS, two widely used technologies in the software industry. These scripts were executed within the popular integrated development environment, Visual Studio Code, allowing for efficient code development and testing. The scripts were specifically designed to automate system testing and incorporated various libraries, such as React, Web3, and IPFS.HTTP. These libraries provided essential functionalities and streamlined the evaluation process.

To thoroughly analyze the CPU consumption during the evaluation, a specialized JavaScript performance library script was employed. This script enabled detailed assessment of CPU usage during critical tasks, including the uploading of medical image data to IPFS, storing it securely on the blockchain, and retrieving data from the blockchain. This analysis provided valuable insights into the system's performance and efficiency.

Furthermore, the evaluation environment included the utilization of the Ganache suite, a comprehensive toolset for establishing a local Ethereum blockchain environment. The Ganache suite allowed for the creation of a personalized blockchain network, facilitating testing, command execution, and observation of the blockchain's state. To enable connectivity with the distributed web and interact with the Ethereum network, the Metamask extension was employed within the browser. This extension seamlessly connected local Ethereum accounts to the Ganache suite, enabling smooth and reliable system functions while considering gas transaction costs.

B. Discussion I - Data Transmission and Gas Consumption

In our suggested solution, we specified the cost of executing the contract migration, which was presented in Table II. This cost was denominated in Ether, and the amount of gas spent during the execution was recorded. To determine the value of Ether, the amount of gas utilized was multiplied by the current gas price. It is important to highlight that the gas price can fluctuate in response to network dynamics and changes in the value of Ether. This dynamic adjustment ensures that the gas cost accurately reflects the ongoing computational expenses within the system, providing a fair and efficient pricing mechanism. During the evaluation process, one of the crucial parameters tested was the time required for users to upload and store data to IPFS and the blockchain ledger. This test parameter encompassed the overall time spent on data. The findings of a series of experiments conducted on an average data size are depicted in Fig. 4. This indicates that the suggested methodology is capable of handling larger data sizes without incurring a notable impact on fuel consumption.

TABLE II. SUMMARY OF THE EXECUTION COST ANALYSIS

Parameter Serial	**Computation Efficiency (Execution Time)**	**Energy Efficiency (Gas Utilisation)**	**Ether Cost (Overhead)**
1	Contract Initialisation	225 (in thousands)	0.058
2	Contract Instantiation	286	0.053
3	Contract Call Initation	42	0.045
4	Contract Migration	27	0.084
Average		145	0.061

These results validate the effectiveness of the proposed solution in efficiently managing the uploading and storing of medical data to IPFS and the blockchain ledger, even as the data size increases. However, it is important to note that despite the increase in data size, the suggested methodology for uploading medical data to IPFS showcased consistent and efficient fuel usage. The difference in fuel consumption between uploading 450-byte data and 1000-byte data was not found to be significantly significant. This indicates that the suggested methodology is capable of handling larger data sizes without incurring a notable impact on fuel consumption. These results validate the effectiveness of the proposed solution in efficiently managing the uploading and storing of medical data to IPFS and the blockchain ledger, even as the data size increases. The suggested methodology ensures a reliable and streamlined process, enabling users to securely upload and access their medical data with minimal impact on fuel consumption.

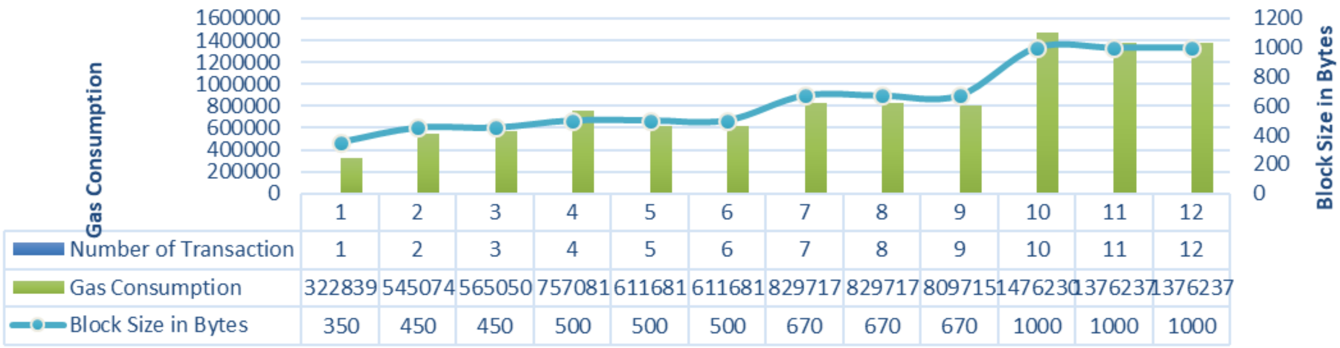


Fig. 4. Gas consumption calculated based on the size of block and number of transactions.

C. Discussion II – Query Response Time

When it comes to storing medical images in IPFS and recording relevant information in the blockchain, efficient data querying becomes a crucial aspect. The query response time plays a vital role in assessing the solution's effectiveness in storing and retrieving data from the blockchain. Fig. 5 provides a visual representation of the execution time involved in accessing the data within this context. The data can be classified into two distinct types. The first type pertains to medical images that are fetched from IPFS using their respective file hashes. This approach ensures a decentralized and distributed storage mechanism for medical images. However, in the case of example number six, it is observed that the execution time is and review, collectively referred to as data uploading and accessing time. The findings of a series of experiments conducted on an average data size are depicted in Fig. 5.

However, it is important to note that despite the increase in data size, the suggested methodology for uploading medical data to IPFS showcased consistent and efficient fuel usage.

The difference in fuel consumption between uploading 450-byte data and 1000-byte data was not found to be significantly significant. However, in the case of example number six, it is observed that the execution time is relatively high compared to other cases. This can be primarily attributed to the larger file size of the medical image associated with this particular scenario. As the file size of the medical image increases, it naturally requires more time for display or download from IPFS. The larger data volume associated with the larger file size contributes to an extended retrieval time. This phenomenon aligns with the intuitive understanding that larger files necessitate more data to be transferred, resulting in a slightly longer execution time. This observation highlights the impact of file size on the retrieval process and emphasizes the need to consider the trade-off between file size and retrieval time when dealing with medical images stored in IPFS. Finding the right balance between image resolution and file size can play a significant role in optimizing the execution time for accessing and displaying medical images in the given solution.

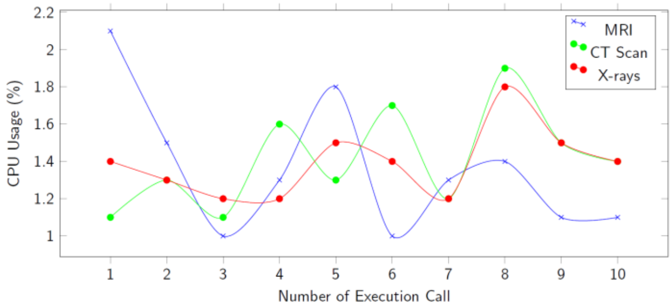


Fig. 5. Computation efficiency and function execution to store the data in IPFS and blockchain.

VII. CONCLUSION AND FUTURE WORK

Decision support and intelligence in healthcare care systems can greatly enhance the cost and efficiency of the healthcare systems. More specifically, the intelligence embedded in electronic healthcare systems relies on efficient processing of medical health data. However, the dispersion of these images across multiple systems poses a challenge for effective and integrated healthcare. Additionally, centralized hosting solutions for picture data, such as cloud-based platforms, can be vulnerable to security breaches. Recognizing the distributed nature of healthcare, there has been increasing attention towards decentralized designs and system interoperability. This research design and implements a proof-of-the-concept for a decentralized Patient-Centric Medical Image Management System (PCMIMS). Built upon the Ethereum blockchain and IPFS, this framework aims to address the storage and distribution challenges associated with medical images. PCMIMS empowers medical images users with secure and private control over their medical images and test reports (such as blood reports, lipid reports) through a DApp web application portal.

1) Evaluation of the proposed solution: To evaluate the efficiency, feasibility, and practicality of the proposed scheme, we conducted an experimental implementation. The suggested system not only facilitates the sharing of medical images but also provides patients with access to an immutable medical database, thereby enhancing efficiency, data provenance, and effective auditing. By employing a decentralized data storage and exchange mechanism, the need for intermediaries or administrative entities is eliminated. Overall, the PCMIMS system presents a unique solution that prioritizes patient rights and control over their medical data. Through decentralization and the utilization of blockchain and IPFS technologies, this system offers enhanced security, privacy, and accessibility in the management of medical images and test reports.

2) Vision for future research: In the current scope of the proposed solution, there is a need for future research to increase the pervasiveness of the proposed solution and rigor of its validation. More specifically, the future work is focused on:

- Developing, deploying, and validating the proposed solution in mobile health (mHealth) context. Mobile devices can offer pervasive healthcare but pose significant challenges related to resource poverty of mobile devices along with security and privacy of health critical data.
- Evaluating the proposed solution via survey or trials with the domain experts, i.e., medics and healthcare professionals. An incorporation of the domain experts' feedback can help us to analyse and improve the solution based on practitioner' perspective.

3) Implications for research and practices: The implications can be attributed to the relevance and benefits of the proposed solution in an academic and industrial context. Blockchain-based framework (i.e., PCMIMS) that provides a structural representation of the overall solution that sketches a blue-print and guides software designers and developers about how the system operates and facilitates effective healthcare management. Academic researchers can exploit architectural design to design and develop emerging solution for blockchain systems in healthcare context. Practitioners can rely on the algorithms and relevant tools to develop solutions that rely on blockchain solutions for managing electronic healthcare systems.

REFERENCES

[1] Aljedaani, Bakheet, Aakash Ahmad, Mansooreh Zahedi, and M. Ali Babar. "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.

[2] Aljedaani, Bakheet, Aakash Ahmad, Mansooreh Zahedi, and Muhammad Ali Babar. "An empirical study on secure usage of mobile health apps: The attack simulation approach." Information and Software Technology 163 (2023): 107285.

[3] Casalino L, Gillies RR, Shortell SM, Schmittdiel JA, Bodenheimer T, Robinson JC, Rundall T, Oswald N, Schauffler H, Wang MC. External incentives, information technology, and organized processes to improve health care quality for patients with chronic diseases. Journal of the American Medical Association. 2003.

[4] Aljedaani, Bakheet, Aakash Ahmad, Mansooreh Zahedi, and M. Ali Babar. "An Empirical Study on Developing Secure Mobile Health Apps: The Developers' Perspective." In 2020 27th Asia-Pacific Software Engineering Conference (APSEC), pp. 208-217. IEEE, 2020.

[5] Ahmad, Aakash, Muhammad Waseem, Peng Liang, Mahdi Fahmideh, Mst Shamima Aktar, and Tommi Mikkonen. "Towards human-bot collaborative software architecting with chatgpt." In Proceedings of the 27th International Conference on Evaluation and Assessment in Software Engineering, pp. 279-285. 2023.

[6] Aljedaani, Bakheet, Aakash Ahmad, Mansooreh Zahedi, and M. Ali Babar. "Security awareness of end-users of mobile health applications: an empirical study." In MobiQuitous 2020-17th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, pp. 125-136. 2020.

[7] Detmer DE, Munger BS, Lehmann CU. Clinical informatics: principles, practice, and products. Washington, DC: American Medical Informatics Association; 2019.

[8] Garg R, Aggarwal A, Gupta N, Sharma A. Picture archiving and communication systems (PACS): A systematic review of published literature of the last decade and future directions. J Med Syst. 2018;42(2):25. doi: 10.1007/s10916-017-0916-4.

[9] Johnson CD. Radiology Picture Archiving and Communication Systems (PACS): An Introduction. J Digit Imaging. 2018;31(3):283-291. doi: 10.1007/s10278-018-0073-0.

[10] Bates DW, Gawande AA. Improving safety with information technology. N Engl J Med. 2003;348(25):2526-2534. doi: 10.1056/NEJMsa020847.

[11] Kruse CS, Kristof C, Jones B, Mitchell E, Martinez A. Barriers to Electronic Health Record Adoption: a systematic literature review. J Med Syst. 2016;40(12):252. doi: 10.1007/s10916-016-0628-9.

[12] Halamka, J.D.; Lippman, A.; Ekblaw, A. The Potential for Blockchain to Transform Electronic Health Records. Harvard Bus. Rev. 2017, 3, 2–5. Available online: https://hbr.org/2017/03/the-potential-for-blockchain-to-transform-electronic-health-records (March 20, 2020).

[13] Benet J. IPFS - Towards a Permanent Web. In: ACM SIGCOMM Computer Communication Review. 2015;45(3):1-2.

[14] Wang Z, Choo KKR. Medicalchain: A Secure and Lightweight Blockchain-Based Framework for Medical Data Sharing. J Med Syst. 2018;42(8):136. doi: 10.1007/s10916-018-1004-9.

[15] Maldjian PD, Lee JH. Advances in PACS: Picture Archiving and Communication Systems. Radiol Clin North Am. 2009;47(6):1051-1064. doi: 10.1016/j.rcl.2009.07.009.

[16] Zhang Y, Liu H, Guo Y. Research on privacy protection technology of medical image. In: 2017 2nd International Conference on Cloud Computing and Big Data Analysis (ICCCBDA). IEEE; 2017. p. 36-39. doi: 10.1109/ICCCBDA.2017.8073701.

[17] Hu F, Cai W, Feng D, Chen M. Challenges of medical big data analysis in developing intelligent healthcare. J Healthc Eng. 2018;2018:5061561. doi: 10.1155/2018/5061561.

[18] Lin H, Huang H, Zhang R, Zhang S, Xie G. Integrated medical image management and analysis system using big data technologies. IEEE J Biomed Health Inform. 2017;21(1):143-154. doi: 10.1109/JBHI.2016.2633738.

[19] Robson C. Privacy and security of electronic health records. In: Liu D, editor. Medical Imaging Informatics. Springer; 2020. p. 75-93. doi: 10.1007/978-3-030-16547-4_5.

[20] Dou D, Wang X, Zhang X, Zeng X. Privacy-Preserving and Scalable Medical Data Sharing Through Blockchain. IEEE Trans Serv Comput. 2021;14(3):666-680. doi: 10.1109/TSC.2020.2974521.

[21] Li J, Yu J, Zhang C, Cao J, Zhang L, Xia F. A Medical Image Retrieval Approach Based on Blockchain Technology. IEEE Access. 2019;7:98952-98960. doi: 10.1109/ACCESS.2019.2924085.

[22] Yu S, Chen Q, Wu L, et al. Intelligent Medical Data Management Using Blockchain Technology. J Med Syst. 2018;42(7):130. doi: 10.1007/s10916-018-0990-y.

[23] Menachemi N, Collum TH. Benefits and drawbacks of electronic health record systems. Risk Manag Healthc Policy. 2011;4:47-55. doi: 10.2147/RMHP.S12985.

[24] Huang HK. PACS and Imaging Informatics: Basic Principles and Applications. 2nd ed. Wiley; 2015.

[25] Zhou X, Liu B, Yu L, Wang T, Jiang M, Zhang Y. Medical Image Retrieval: A Multimodal Approach. J Healthc Eng. 2017;2017:9348252. doi: 10.1155/2017/9348252.

[26] Zvárová J, Hřebíček J, Kolářová J. Security and privacy issues in electronic health records: A systematic literature review. Health Informatics J. 2020;26(1):30-45. doi: 10.1177/1460458219852984.

[27] Dou D, Wang X, Zhang X, Zeng X. Privacy-Preserving and Scalable Medical Data Sharing Through Blockchain. IEEE Trans Serv Comput. 2021;14(3):666-680. doi: 10.1109/TSC.2020.2974521.

[28] Benet J. IPFS - Content Addressed, Versioned, P2P File System. arXiv preprint arXiv:1407.3561. 2014.

[29] Dagher GG, Mohler J, Milojkovic M, Marella PB. Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. Sens Smart Cities. 2017;97:1-8. doi: 10.1109/SESC.2017.7940157.

[30] Meena M, Yadav AK. Blockchain based Secured Electronic Health Record Sharing System. In: 2020 International Conference on Smart Systems and Inventive Technology (ICSSIT). IEEE; 2020.

[31] C. Manville, G. Cochrane, J. Cave, J. Millard, J. K. Pederson, R. K. Thaarup, A. Liebe, M. Wissner, R. Massink, B. Kotterink, Mapping smart cities in the eu (2014).