Towards a Blockchain-based Medical Test Results Management System: A Case Study in Vietnam

Phuc Nguyen Trong, Hong Khanh Vo, Luong Hoang Huong, Khiem Huynh Gia, Khoa Tran Dang, Hieu Le Van, Nghia Huynh Huu, Tran Nguyen Huyen, Loc Van Cao Phu, Duy Nguyen Truong Quoc, Bang Le Khanh, Kiet Le Tuan
FPT University, Can Tho City, Viet Nam

***Abstract*— The role of the testing process cannot be denied in the diagnosis and treatment of patients' diseases in medical facilities today. The results from this process help doctors and nurses in medical centers make a preliminary and detailed assessment of symptoms and provide a specific course of treatment for their patients. In addition, these results are stored as a patient's medical record that serves as a reference for subsequent therapies. However, the storage of this information (i.e., paper-based, electronic-based) faces some difficulties for both approaches. Especially for developing countries (i.e., Vietnam), this process encounters some major obstacles at health centers in rural areas. Many centralized/decentralized storage methods have been proposed to solve the above problem. Besides, the current popular method is patient-centered (all information shared is decided by the patient) can solve the above problems and be applied by many research directions. However, these methods require the user (i.e., patient) to have a background in security and privacy as well as the cutting-edge technologies installed on their phones. This is extremely difficult to apply in rural areas in developing countries where people are not yet conscious of protecting their personal information. This paper proposes a mechanism for storing and managing test results of patients at medical centers based on blockchain technology - applicable to developing countries. We build a proof-of-concept based on the Hyperledger Fabric platform and exploit the Hyperledger Caliper to evaluate a variety of scenarios related to system performance (i.e., create, query, and update).**

Keywords*—Blockchain-based system; hyperledger fabric; medical test results; medical institution at developing countries

I. Introduction

All current treatments are based on the results of the clinical examination/test of the patient's symptoms and medical history. Indeed, doctors and nurses give their diagnosis about the patient's condition (i.e., consultation) and treatment. In other words, the testing process plays an extremely important role in the entire treatment of the patient [1]. In addition, these test results are recorded to build the patient's medical history. Nurses and doctors have a more general view of symptoms from early (i.e., first detected) to the current stage.

However, the storage of medical test results varies widely depending on the region (i.e., city or rural) and the country (i.e., developed or developing). Most hospitals in large cities and or in developed countries, adopt electronic records to store medical test results and patient medical records (aka electronic-based). While rural hospitals or some hospitals in developing countries still use paper records (aka paper-based). Paper records are extremely risky for the healthcare system because i) it is easy for patients to lose the medical test records due to natural issues (e.g., flood, fire) or their failure (e.g., lost); ii) it is very difficult to back up those results because of technology and equipment limitations [2]. Due to these risks, some patients often take pictures of the medical test results to give to doctors for their next visit. For the recent model, almost all hospitals or medical centers in Vietnam applied manual input for the medical test record (see III-A for more details). Besides, determining timelines based on this approach is extremely difficult. For example, in addition to taking pictures, the patient must annotate all information related to those photos. Nevertheless, this method also carries risks, as loss of the device or memory card/memory limitations are the main barriers to this approach [3].

A study that collected patient responses to interviews about the role of using paper and electronic records was conducted by [4]. Their findings clearly indicate that electronic records are considered more reliable than paper records. Specifically, about 51% of interviewees indicated that they are less burdened in preserving paper records, and in case of loss of their records, they have to tell all their medical records to all. hospitals they visit if using paper records. An interesting finding of the author is that patients are willing to spend extra money each month to keep their health records in electronic form. In addition to the above reasons, the study by Muchangi and Nzuki [5] conducted a survey in medical centers in developing countries (i.e., India) that showed that patients did not trust the treatment. Using electronic records will reduce the risk of privacy invasion. They argue that the methods of building a user-centric health data sharing system are facing a lot of difficulties due to the limitations of the method of building a centralized data system (i.e., data) stored and processed centrally in cloud servers).

The risks that such systems may face come from unintended events such as natural disasters, fires or possible attacks by hackers to exploit sensitive patient information. For the first risk, studies[1] have shown that lost health information must be recreated, requiring in-depth time and resources. Because critical data such as patient health must require an electronic record using secure information systems to store and access patient health information and to ensure that the information contained updated and available when needed [2]. In addition, being attacked by hackers is inevitable. These hackers take advantage of existing security holes from the system to get personal information of patients and use them for purposes of violating privacy (e.g., selling personal information) [6]. It is impossible to recover stolen information. We can only find ways to overcome the current risks (i.e., centralized storage).

[1] https://www.hl7.org/FHIR/

The transition from centralized to decentralized medical data processing storage brings a lot of risks as well as benefits [7]. Nghia et al. [8] has argued that the challenges may outweigh the benefits, such as scalability, availability, data transparency (i.e., for the field). building systems on Blockchain), as well as giving more rights to users. Specifically, the authors argue that users can see who is working on their data and what benefits they have.

For the second approach (i.e., applying electronic record method to store patient information), in large cities in developing countries (e.g., Vietnam) archival methods are only centrally stored on a server of a center or a hospital in big cities (e.g., Ho Chi Minh City, Can Tho). Therefore, patients face a great challenge when they want to share medical data (i.e., test results, medical history) from previous facilities to the new facility [9]. Centralized data processing and storage systems exhibit at least one of the following disadvantages: instability due to a faulty central point, lack of security due to greater vulnerability, and greater potential for malicious attacks (i.e., unethical activities) due to the presence of central authority [10]. In contrast, the decentralized system has no central authority; instead, permissions are shared between each computer (node), each with equal permissions [11]. Instead of all processing and storage requirements being centralized in a central machine (i.e., cloud server), the distributed system divides computations into smaller computations to be performed by multiple nodes as well as storing the collected data in many different memory areas [12]. Thereby, increasing the processing and storage capacity for the whole system. This also increases interaction with users (i.e., patients, nurses, doctors) and reduces the risk of attacks from hackers because of the lack of a central point to attack [13]. This feature also makes them stable and fault tolerant since each node has the same role (i.e., regardless of Client-Server); thereby, privacy-invading operations are unlikely to be performed [14]. The peer-to-peer system uses these features and benefits to allow the network to remain fully operational even if one node fails.

In addition, because of the requirements for supporting equipment and supplies, the current testing procedures are all done in hospitals or medical centers (i.e., it is difficult to meet a large number of requests. patient testing at the same time). Patients have to wait a long time for testing and consultation results before their disease can be identified. Therefore, there is a need for a mechanism to support patients in storing and sharing medical records (e.g., test results, medical history) as well as limiting waiting time for results at centers. medical center. Besides, security and privacy issues depend greatly on the context in which the system is deployed. For example, in developing countries (i.e., Vietnam), exploitation and risk assessment and privacy have not been given due attention [15]. The developing countries' citizen do not have the concept of protecting personal privacy (especially countryside people). This argument is completely correct and can be applied to developed countries, where the education level is high and there are many supporting facilities and infrastructure.

To solve the problems mentioned above, this paper proposes a medical test result management model based on blockchain technology. Methods to prove the effectiveness of applying Blockchain technology to medical facilities to solve problems related to supply chain (e.g., blood and its produces [16], [17]) curative problem (e.g., emergency data assessment) that current health care systems have not fully addressed. Another example demonstrating the effectiveness of applying the strengths of Blockchain technology and patient care is introduced by Roehrs et al. [18]. Specifically, they emphasized non-functional requirements such as network usage, disk space, response time, CPU usage, and memory footprint, and their importance in implementing a pool management system. Health records based on blockchain technology. They evaluated the performance of both systems (i.e., traditional archiving system and blockchain-based storage system) by deploying two models on two hospital databases (i.e., 40,000 patients) adult person). Analyzing the results obtained, they concluded that the results achieved were much more effective than traditional practices in maintaining integrity, security, ownership, and decentralization. Various technologies can be used to create patient-centered healthcare systems where blockchain-based approaches provide a single solution [19]. Specifically, Blockchain uses features (security, stability, fault tolerance) to allow a network to remain fully functional even if a node fails [20]. However, these approaches (listed in the II section) suffer from many user-related (i.e., patient) limitations, which are highlighted in the Prior Work section.

Therefore, the research problem of this article is to introduce the blockchain-based approach for medical test result management used for developing countries (i.e., Vietnam) For the objective of this article, our contribution is threefold: i) proposing a model for managing test results for patients in developing countries (i.e., Vietnam); ii) building a proof-of-concept based on the proposed model via Hyperledger Fabric satisfying the specific properties of the regions/applicable areas; and iii) evaluate the system's capabilities based on how well it supports initialization, retrieval, and update requests (i.e., overall rating based on system performance - number of successful and failed requests; system-wide latency) based on exploiting Hyperledger Caliper.

The next section presents the state-of-the-art. Sections III and IV present our approach, processing model, and system implementation. Section V builds an environment for evaluating proposed models and makes comments on their strengths and weaknesses as well as future directions in Section VI. Finally, we summarize the study in Section VII.

II. Related Work

There are many approaches that have proposed methods for remote diagnosis and treatment of diseases, which are data mining and other practical applications based on medical data by exploiting the strengths of the blockchain technology. For example, Chen et al. [21] proposes a model for storing and controlling personal data in a healthcare environment based on Blockchain technology. This system can collect information from IoT devices (i.e., medical devices in real time). To improve the security of the system, the authors build an anonymous data sharing environment and encrypt the patient's personal data before storing them on cloud servers. Similarly, Du et al. [22] and Son et al. [23] used medical centers (i.e., hospitals) to store data and manage access and those hospitals. Specifically, they categorize two types of medical data protection policies: global for all data shared outside

of the medical center, and local, which is accessed only by individuals at the medical center. medical (i.e., doctor, nurse).

However, one of the major limitations is that through this solution, patients do not have full control over their data as the data and policies are stored in the hospital. Patra et al. [24] proposes a cloud-based model to build an information system at the national level, providing a more convenient solution for patients in rural areas at the lowest cost. Specifically, instead of having to go to health care centers in large companies, they propose a solution to diagnose and treat diseases remotely. Specifically, citizens are encouraged to provide their personal healthcare information, which will be stored in the health cloud and accessed by health professionals and policymakers to provide more medical services. Similarly, Rolim et al. [25] proposes a framework that covers the process from data collection to cloud-based data delivery. Using sensors mounted on medical equipment, data can be collected and stored directly in the cloud, which can be accessed by authorized medical professionals.

Some other approaches build a user-centric (i.e., patient) model, who has full discretion to share their personal data with providers/health care facilities. economic (i.e., in a medical setting). For example, Makubalo et al. [26] has summarized the above approaches in their publication. They argue that the methods of building a user-centric health data sharing system are facing a lot of difficulties due to the limitations of the method of building centralized data system (i.e., data) stored and processed centrally in cloud servers). Yin et al. [27] introduced a patient-centric system built in the cloud with a data collection layer, data management layer, and medical service delivery layer based on medical records of the patient. To protect data privacy, many approaches have adopted attribute-based encryption (ABE), one of the most common encryption schemes used in cloud computing, to define patient data object. Depending on the context, the policy tells to lose (or not) grant the corresponding access rights. For example, Barua et al. [28] proposes an ABE-based access control model based on patience and privacy protection; Chen et al. [29] described a new framework with a cloud-based, privacy-aware Role-Based Access Control model that can be used for control, data traceability, and access allowed access to healthcare data resources. Methods for applying the Access Control model are also introduced for dynamic policies [30], [31] or protection policies for both security and privacy [32].

In addition, Madine et al. [33] has introduced a Smart Contract-based system that provides patients with reliable, traceable and secure control over their medical data (i.e., which is stored non-invasively). concentrate). To increase the security and privacy of medical data, they used the decentralized storage feature of the interplanetary file system (IPFS) to store and share patient medical data safely. For practical applications, HealthBank has proposed a healthcare system and surrounding ecosystems that allow users (i.e., patients) to manage and control their data.[2] This solution is recommended to be able to comply with strict security and privacy regulations (e.g., GDPR) and to assist users in using their services. In addition, the system also proposes solutions for storing personal data with complex data encryption algorithms, immutability and accountability. Similarly, HealthNautica and Factom Announce Partnership have used blockchain technology to ensure the integrity of patient medical data while providing transparency based on blockchain technology and encryption of sensitive data (e.g., personal information, health status).[3]

With the same approach based on Blockchain technology and IPFS, Misbhauddin et al. [34] introduced the MedAccess platform, A Scalable Architecture for Blockchain-based Health Record Management. The platform supports on-chain storage and processing allowing doctors, lab technicians and patients to securely manage medical records. However, these systems face some problems in the processing and storage of personal data. Specifically, Le et al. [35] has argued that not all data collected must be processed on-chain. Instead, Son et al. [2] argues that personal data that is either not directly related to treatment or diagnosis may be stored off-chain (i.e., offchain). Similar to the above approach, to increase the processing capacity for the whole system, Zyskind et al. [36] presented an approach based on in-chain and out-of-chain processing. Onchain processes require all entities of a typical personnel management system, where patient and medical staff information is stored; in contrast, encrypted medical data is stored on a separate centralized storage server to enable faster access and low cost. However, the above methods have major limitations, including that any information that is validated must be executed on-chain instead of local processing. This only benefits storage but does not change data handling (i.e., since all information still executes on-chain) [17].

To solve the on-chain storage problem, Zhang et al. [37] have proposed FHIRChain (Fast Healthcare Interoperability Resources), a blockchain-based system that allows patients to securely share their clinical data in a medical setting. For this approach, users are allowed to share their personal data directly with hospitals and medical centers instead of having all their personal information stored directly on the banana. Another approach suggested by Patel et al. [38] has empowered hospitals to be the creators of medical records and patients to be owners of their records. In this approach, all medical data processing and updating are done off-chain (e.g., medical record sharing, and all query requests to patient data). In addition, the issue of threading while exporting medical data is also very important because data stored on the same system can be accessed by a malicious user on the same system [39], [14]. Therefore, Iryo is introduced as a healthcare ecosystem that uses blockchain technology to decentralize access to medical records.[4] Specifically, it uses the NuCypher KMS key management system (i.e., [40]) to address the limitations of adopting the peer2peer model for storing and executing on encrypted data. Also adopting an advanced cryptographic-based approach and blockchain technology, Chen et al. [41] proposed a system that only stores the searchable index of records on the blockchain. The patient information is organized as Key-Value. Where "key" contains records presented as hash (i.e., reduced index) while actual patient data (i.e., "value") is encrypted and stored on a public cloud server.

Tith et al. [42] proposed a system based on blockchain technology to ensure privacy, scalability, and availability of

[2]https://www.healthbank.coop/2018/10/30/healthbank-creates-the-first-patient-centric- healthcare-trust-ecosystem/

[3]https://www.factom.com/company-updates/healthnautica-factom-announce-partnership/

[4]$https://iryo.network/iryo_whitepaper.pdf$

patient data in the medical environment combined with data encryption methods. patient data using the public key. It uses a proxy re-encryption mechanism on a centralized server to transfer encrypted data from the patient to the doctor. In this solution, the patient-centered aspect is still lacking because the medical records are under the control of the hospitals. Another limitation is that the re-encryption is done on a single server. During the Covid-19 pandemic, there are several approaches to exploiting blockchain technology as a workaround in providing telemedicine support services (e.g., [43]). Specifically, they proposed a blockchain-based model to solve 5 problems at that time, including i) Managing patient consent for unwanted accesses from service providers health care service/center; ii) Traceability of remote diagnoses and treatments; iii) Traceability of home medical supplies and equipment; iv) Secure access to individual health records (i.e., combined with an IPFS-based approach); and v) Automated billing for all telehealth services (e.g., drug bills).

Instead of focusing only on the two main target groups in the medical environment, patients and staff at the healthcare facility (i.e., nurses, doctors), Kassab et al. [44] has expanded its blockchain-based medical data processing and storage system to include (insurance companies and regulatory agencies). In addition, the processed data is also extended to the supply chain of equipment and drugs from the suppliers/hosting agencies to the respective hospitals and pharmacies. However, the role of the patient is not mentioned as a major contribution of the paper. Similar to Xiao et al. [45] has proposed Healthcare Data Gateway (HGD) that allows patients to easily and securely own, control, and share their own data without violating privacy. This article presents a direction to combine Blockchain and Machine learning systems to achieve the system's ability to quickly handle "emergency" situations and ensure the privacy of medical data. [46] proposes a review, demonstrating how the inherent properties of the blockchain (e.g., synchronous processing, decentralized storage) can enhance or hinder current healthcare systems in improving healthcare services in healthcare facilities.

However, the above approaches (i.e., state-of-the-art) have brought many solutions to today's traditional healthcare systems. But those approaches only consider the general problem rather than consider a specific area (i.e., country). Thereby, in developing countries (e.g., Vietnam) where medical equipment and supplies are one of the barriers that directly affect people's healthcare process. In addition, the above approaches require a certain knowledge of information technology as well as the risks related to security and privacy. It is for the above reasons that a few case studies (i.e., applied to a specific geographical area - country, region) address the upper limits of [47]. In this article, we provide Blockchain-based support for the management of test results in medical centers.

III. The Blockchain-based Medical Test Results Management System

A. Traditional Model

To build the traditional model, we conducted a survey of 10 hospitals and medical centers in Can Tho city. We act as the medical check-up patient and the interviewer taking information directly from the test patients. We also surveyed

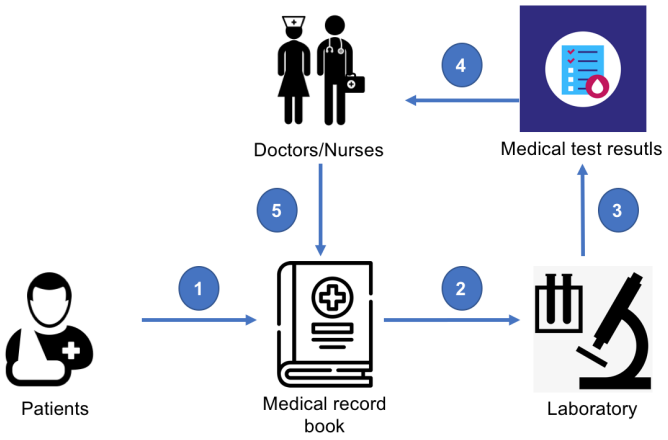

Fig. 1. The Traditional Process for Medical Test Results Management System.

medical opinions on the diagnosis process of a doctor who used to work at Children's Hospital - Can Tho. The traditional model surveys were conducted from June to August 2022. All the collected procedures are evaluated and graded step-by-step by the team before building the medical test results management model as shown in Fig. 1.

Fig. 1 shows the basic steps of the traditional medical test results management process. This model describes the five main steps, excluding the risks of losing medical test results. In other words, this process will be repeated for each patient whenever they have a routine checkup or a health-related reason. Specifically, in the first step, the patient registers for a medical test result, which includes basic information about the patient, such as full name, address, phone number, or medical condition. The medical test result number is also the patient number at that hospital. In the second step, the patient brings the medical test result to a specialist at the hospital, called a laboratory (e.g., eye, blood, urine) for sampling. This procedure requires a very long wait time from the patient. The patient then receives information about this form in the third step before forwarding this information to the doctors and nurses for consultation in the fourth step. Finally, the consultation results are updated in the medical test result of the patient in the fifth one.

For the process of storing patient information, the storage of their information is completely manual. Only a few major medical centers in major cities support the storage of medical results on their centralized database. This demonstrates that it is not feasible to share a patient's medical result between different healthcare facilities. It is easy to see that there are many inconveniences for both patients and hospital staff when using the current testing/receiving process, respectively. The first limit comes from the patient, all information stored on the medical test result must be ensured carefully, and the medical test result must not be lost otherwise, all procedures will have to be repeated from the beginning with a new medical test result. Changing the place of treatment/examination is extremely difficult because the patient has to bring the medical test results issued at the previous medical facility to a new one. In addition, the loss of medical test results is extremely risky, besides the reason for having to repeat the entire sampling

process, since they relate to the diagnosis process. Regarding the responsibility of physicians (i.e., doctors/nurses), they must reread a patient's entire medical history each time their patient has a follow-up visit. This is similar to the process of examining a new patient.

B. Proposed Model

To solve the above problems, we introduce a model based on Blockchain technology, where all information related to the testing process and the storage of patient's medical test results are updated and shared freely in the healthcare environment. Fig. 2 shows our proposal system based on Blockchain technology and distributed ledger (i.e., Distributed Ledger). As a first step, the patient initializes a global ID for not only a certain healthcare facility but also for others ones (e.g., the hospital in the same city). Unlike the traditional process, in another word, this ID will identify the user globally, which means that the patient can be examined at another medical facility without affecting the diagnosis process. Specifically, doctors/nurses can retrieve information about a patient's medical history based on their global ID (this will be covered in more detail in the next steps). From the initial global ID, users can generate more than 1 medical test result (i.e., per medical facility or healthcare service). These records store all test results and related patient information (i.e., similar to a medical test result in the paper). The data stored on the medical test result is always updated to Distributed Ledger (step 3). Users will then go to the respective Laboratories to take samples (step 4) before seeing a doctor in person to receive advice on their health status (step 6). This is the biggest difference between our model compared to the traditional model. Patients do not need to wait a long time at the facility; instead, an appointment is delivered to their device (e.g., smartphone) whenever their result is available. Meanwhile, the remaining steps will be executed independently at the system under the confirmation of the relevant parties. Specifically, after testing, the results are updated to the Distributed Ledger, and this information includes the user's corresponding medical test results and metadata about the time and location of the test as well as the doctors participating in the consultation. In case the patient goes to another medical facility, the patient's permission (or the patient's family member's/relatives in some special cases) must be obtained before accessing the patient's medical data (i.e., over-privileged permission). After receiving the request from the system, the doctors will enter the diagnostic results into the system (i.e., Distributed Ledger). The whole process will be confirmed by the stakeholders during the execution. The data will be encrypted when there is no request for access or update from the relevant parties (e.g., patient, nurse, doctor). The next section presents our approach based on Hyperledger Fabric.

IV. Implementation

A. Permission Diagram

Fig. 3 presents the working mechanism of the request authentication process in this paper. Specifically, we built two organizations with corresponding encrypted material certificates, each organization includes two users and two peers. Each peer is responsible for maintaining the version of the ledger so that the network and data can be maintained even if other peers are shut down.

When the user initiates a request and sends it to the service. The back-end service processes the data and sends it to the smart contract API. When receiving the request and the data, the smart contract sends this to the peers in the network for authentication and data interaction purposes. During the creation, querying or updating data processes, peers check the identity of the request to decide whether to allow access to the data at the distributed ledger. If the identified user of the request is not defined in the data collection, the system denies access and sends a message to the back-end API to notify the user; the system allows access and proceeds with further processing steps.[5]

B. Hyperledger Component

The model in this paper is implemented on the Hyperledger Fabric platform. Fabric is a permissionless blockchain platform that integrates smart contracts, the storage of data to the distributed ledger is controlled through the smart contract APIs, from which the data is simplified and easily traced. Each request that goes through the smart contract is verified with public and private key pairs. In other words, if the user does not exist in the system, the system is better protected from malicious requests outside the system.

The Fabric system in this paper includes two organizations. Each organization consists of 2 peers to store smart contracts, where each peer registers two users and is authenticated with public and private key pairs. The components of the model are shown in Fig. 4

When user devices access the system to initiate/query or update data for a particular transaction, requests are sent from the client to the services of the existing system. Then, these services send access information to the peers belonging to the organization located in the blockchain network. At this step, the peers conduct verification of that user's key pairs, and if the successful peer authentication process proceeds to send information to the smart contract with the transaction type declared in a smart contract requested by the user, the smart contract will go through the designed features function to access the distributed ledger to initiate/query or update specific data.

C. Our Proposed Model's Diagram

One of the most important parts of the model lies in the validation and interaction with the patient's global ID and their medical data described in Fig. 5 and 6. In particular, the main functions include initializing and querying the patient's global ID and their medical data.

Fig. 5 depicts the process of storing new record data (e.g., patients' global ID and their medical data). In step 1, when the user initializes information about a certain ID, the data is sent to the back-end service of the health center's information management system. In the next step, the back-end APIs (i.e., backend) check, authenticate, and initialize the

[5]For more detail of the basic Blockchain following https://ethereum.org/en/whitepaper/ and https://www.hyperledger.org/learn/white-papers for Ethereum and Hyperledger Fabric, respectively

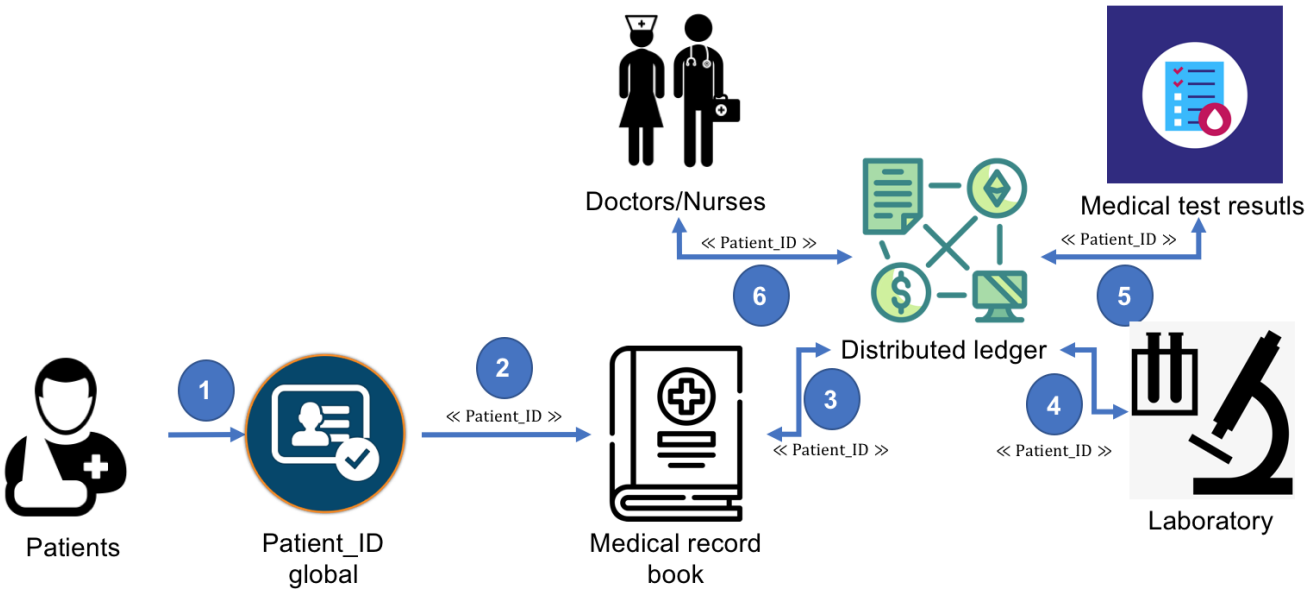

Fig. 2. The Proposed Model for Blockchain-Based Medical Test Results Management System.

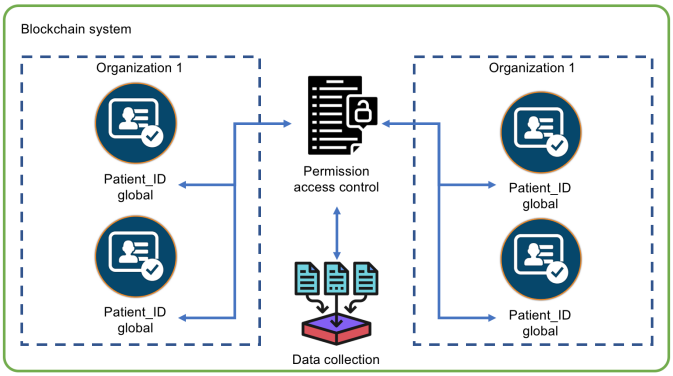

Fig. 3. Permission Diagram.

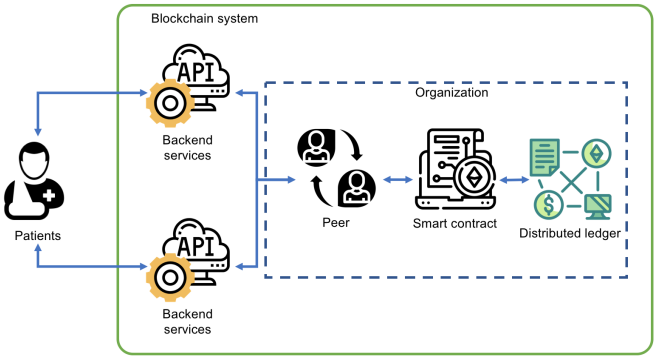

Fig. 4. Hyperledger Fabric Component.

default values, then pass the parameters to the API inside the smart contract. At this point, a smart contract transfers data and stores transactions to the distributed ledger of the blockchain network. The default values for parameters sent from the request are intended to minimize errors caused by null field data.

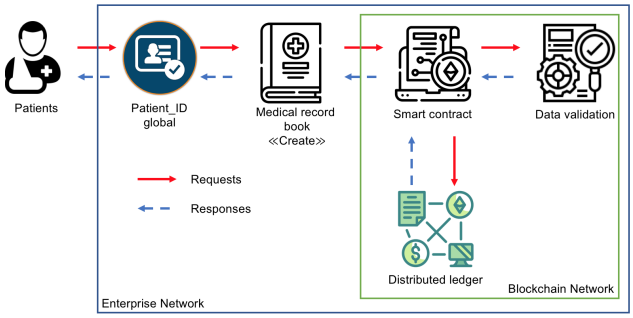

Fig. 5. Initializing and Storing the New Data.

Fig. 6 presents the process of retrieving data of a particular (e.g., patients' global ID and their medical data). When the user sends a query request to the system, the service query data checks and confirms whether the parameter ID of their medical data exists or not. Then, the smart contract's APIs are called and passed into the corresponding parameter. Next, the smart contract's APIs check for the existence of data in the request before querying. In the case that the ID does not exist, the smart contract sends an error notification to the user's device; otherwise, it returns the relevant data/record of the patient corresponding to the requested ID.

V. Evaluation Scenarios

A. Environment Setting

Our paradigm is deployed on the Hyperledger Fabric network maintained inside docker containers. In this section, we measure the performance of chaincode in the two scenarios: initializing (i.e., creating data) and accessing data. The experiments are deployed on Ubuntu 20.01 configuration, core i5 2.7Ghz, and 8GB RAM.

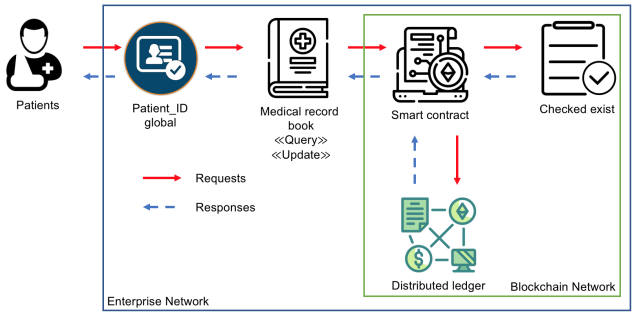

Fig. 6. Retrieving/Querying Data Process.

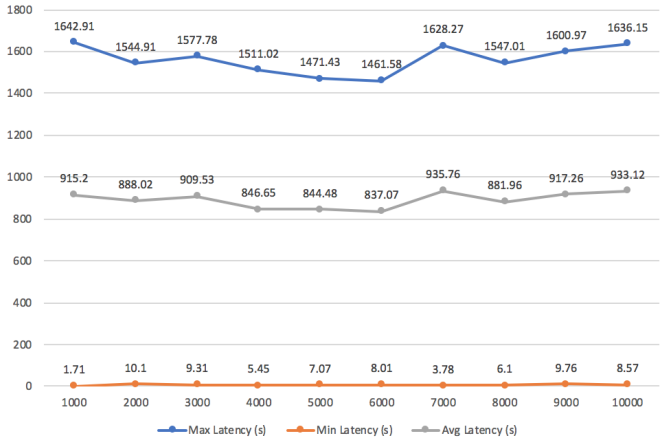

Fig. 7. Data Creation/Initialization for the Medical Test Results of the Patient in Terms of Latency.

To prove the effectiveness of our model, we also define several experiments by exploiting the Hyperledger Caliper[6] that is used to design the test scenarios and collect all the information regarding the performance.

B. Evaluation Results

As introduced in the whole article, we consider the three main execution tasks for the blockchain-based system, namely data creation, data access, and data update. The three following sub-section will target our evaluation of the ten scenarios in terms of the supported performance of the system.

1) Data Creation: In this scenario, the study measures the performance of the data initialization function/data created (e.g., medical record book) performed through smart contracts. The number of requests sent simultaneously from two users[7]. Table I shows the execution results of the data initialization/creation function in terms of the success and fail requests. The data initialization/creation script is conducted with two users concurrently making 1000 - 10000 requests to the system. Based on the execution results in Table I, it can be seen that the number of successful and failed requests is stable (except in the case of 10000 requests/second). Specifically, the number of failed requests is limited to less than 15,000 requests (i.e., on average 11.4K requests - 23.32%). Meanwhile, the

[6]https://www.hyperledger.org/use/caliper

[7]We set up one organization with two users and two peers

TABLE I. Data Creation/Initialization for the Medical Test Results of the Patient in Terms of the Success and Fail Requests

#Request/second	Success	Fail	Percentage of the fail requests
1000	38506	10524	21.4644%
2000	37289	9918	21.0096%
3000	38754	8128	17.3371%
4000	35208	14705	29.4613%
5000	36699	12872	25.9668%
6000	37098	11833	24.1830%
7000	38405	10847	22.0235%
8000	37769	11535	23.3957%
9000	37392	12456	24.9880%
10000	37852	11516	23.3269%

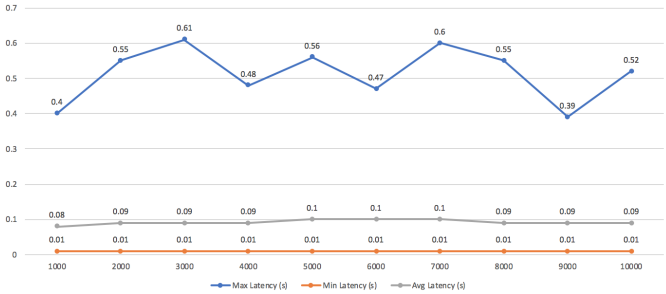

Fig. 8. Data Access (i.e., Retrieving/Querying) for the Medical Test Results of the Patient in Terms of Latency.

lowest case was with only 17.34% (8,128 requests at 3K requests/second). The maximum of failed request rate is in the fourth row 4,000/s request with 14,705 requests - 29.46%. In contrast, the system is more stable in terms of data creation with only an average of approximately 37.5K success requests for each scenario (from 1K requests to 10K).

We also measure the parameters of the system latency for each request (i.e., max, min, avg) in Fig. 7. In particular, for system-wide latency, we recorded the number of requests with response delays per 1,000 requests/second to 10,000 requests per second. The data in Fig. 7 demonstrate that the highest latency ranges from 1,461.58 to 1,642.91 seconds. The minimum is less than 10 seconds. The average delay when creating new data is less than 940 seconds. This is acceptable because creating thousands of new records at the same time is very unlikely in medical centers. The results observed in this scenario also demonstrate that the system supports very well with the continuous generation of new profiles.

2) Data Access (Retrieving/Querying): In the second experiment, we consider the data access (e.g., medical record book). We also set up 6 scenarios from 1000 to 10000 requests which access the medical record book from two users. Table II shows the execution results of the data access function (e.g., medical record book). Compared with the creation tasks, the results of 10 scenarios to evaluate the data accessibility of our proposed blockchain-based system are more balanced. Given the number of successful and failed requests, we also collect the number of requests at every 1000 to 6000 requests per second. The number of successful and failed requests is fairly balanced, with only 21 fail request for 10 scenarios (especially without the fail request at the seventh and ninth scenarios) around 99.99% of the requests are successful in all 6 scenarios.

TABLE II. DATA ACCESS (RETRIEVING/QUERYING) FOR THE MEDICAL TEST RESULTS OF THE PATIENT IN TERMS OF THE SUCCESS AND FAIL REQUESTS

#Request/second	Success	Fail	Percentage of the fail requests
1000	104435	2	0.0019%
2000	105102	3	0.0029%
3000	105103	1	0.0010%
4000	105294	4	0.0038%
5000	105348	4	0.0038%
6000	105373	1	0.0009%
7000	105119	0	0.0000%
8000	105222	1	0.0010%
9000	105104	5	0.0048%
10000	105122	0	0.0000%

TABLE III. DATA EDIT/UPDATE FOR THE MEDICAL TEST RESULTS OF THE PATIENT IN TERMS OF THE SUCCESS AND FAIL REQUESTS

#Request/second	Success	Fail	Percentage of the fail requests
1000	23018	23509	50.5277%
2000	21503	25012	53.7719%
3000	22642	25497	52.9654%
4000	22042	24782	52.9258%
5000	24547	23376	48.7782%
6000	22499	24091	51.7085%
7000	21775	23820	52.2426%
8000	22690	22972	50.3088%
9000	22496	23656	51.2567%
10000	25557	20470	44.4739%

Retrieval of stored data is extremely important. Indeed, considering health data retrieval time directly affects the patient's health care. To solve this problem, we consider the latency of the system (i.e., the maximum/average/minimum time it takes to process the request of data accessed from the system) which presented in Fig. 8. Specifically, the maximum time to wait for a data retrieval request is 0.6 seconds at the third scenario with on average 0.513 seconds. [8] The minimum wait time is almost instant response (i.e., with only 0.01 seconds for the whole scenarios - from 1K to 10K requests/second). The average time for each data retrieval request is less than 0.1 seconds - between 0.08 and 0.1 seconds.

3) Data Edit/Update: Finally, we look at the user's ability to update the medical test result's data. This parameter reflects whether a doctor or nurse updates information about a patient's medical record (e.g., new symptoms, diagnoses). In this scenario, we also conduct a review of 10 different scenarios, each of which will require processing from 1000 to 10000 requests per second. We also measure two parameters, similar to the two scenarios above, the number of successful and failed requests in Table III and the overall latency, which is shown Fig. 9.

For the first aspect (i.e., #request for success and fail), The number of failed requests was also higher than the success requests in all 10 scenarios (with an average of about 51%). On average, there are 22,876.9 request is success and this amount for fail requests is 23,718.5. Generally, the number of fail requests in data update task is higher than that in the two above tasks (see section VI for the details of reason).

For the latency aspect of the data update requirement, we

[8]Note: all of our simulation scenarios use single information retrieval/querying data - not concluding complex access requirements, such as join, and group by commands like database management systems on SQL.

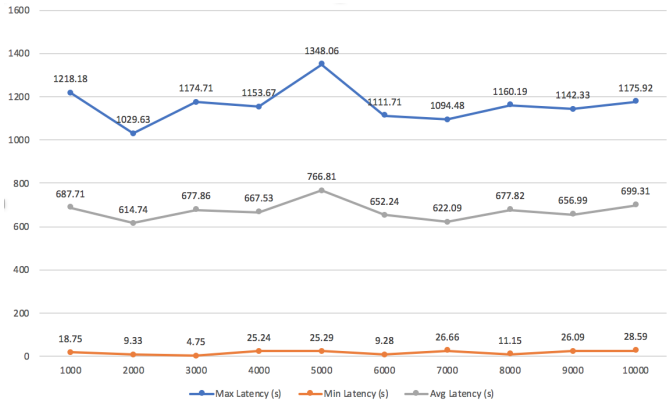

Fig. 9. Data Edit/Update for the Medical Test Results of the Patient in Terms of Latency.

present the collected performance in Fig. 9. In terms of time for execution, updating data is more complex than the previous two previous tasks (i.e., creation and access data). Specifically, we must determine if user information exists in Distributed ledger, then we determine which information needs updating (e.g., symptoms, disease diagnoses). Because of the above requirement, the execution time for the update task is longer. Specifically, the latency of all scenarios ranges from 1029.63 to 1348.06 seconds in the maximum case. The minimum latency ranges from 4.75 seconds to 28.59 seconds, while the average latency required by an application to process ranges from 614.74 seconds to 766.81 seconds.

VI. DISCUSSION

Comparing all three evaluation scenarios, we find that real-time is acceptable. We also describe why there is a difference between the time lag in the execution of requests from the system depending on the complexity of the query. Specifically, the most prolonged time lag was recorded in data initialization due to updating to Hyperledger. This is different from the traditional way of storing data, where the information is only stored in tables and is done by the system administrator. On the contrary, initiating a medical test result requires confirmation from all relevant parties. In addition, defining constraints in an update request is more complex than in a retrieval request. The update time clearly defines the information the requester wishes to add/update to the existing medical test results. Finally, the fastest execution time is the data retrieval request which offers more promise for a Blockchain-based system than traditional storage systems.

However, Section V provides a marked change in all three data creation, retrieval, and update scenarios regarding the number of success and failed requests. Specifically, in the update scenario, the failure rate of requests is much higher than in the data initialization scenario (with more than 50% compared to less than 20%). A similar method occurs when comparing initialization/data creation and access/data retrieval with more than 20% and nearly 0% of failed requests, respectively. This happens because we build a system that simulates the interactions between the parties (e.g., patient, nurse, doctor). In particular, the update and retrieval request must require the data to be initialized before. Otherwise, the request is

considered a failure. For the update scenario, the system also requires that the updated information be initialized before being replaced with new data (e.g., patient information and medical history). Initializing a dummy data system according to the above requirements is extremely difficult because we do it on two separate user groups.

For the system specification, we have not included encryption and decryption times for the data stored on Hyperledger. We assume that a trusted third party will take care of this. In terms of execution time, including the user critical generation time, as well as encryption and decryption, will increase the execution time for the whole system. This is hard to meet on our simulation system. In addition, this proposed model is also the first attempt to build a blockchain-based system that aims to offer a test management model in medical centers in developing countries.

For future work, we intend many potential research directions to follow after this work. One of the mandatory requirements for health systems is confidentiality (i.e., authentication and authorization). We apply the proposed models based on the dynamic data support the environment of IoT devices [11], [48]. For authorization, a model based on ABAC [31], [30] and supporting dynamic policy [49], [50] is an appropriate choice in the context of the current health system. For encryption requirements, we use a trusted authority that provides a solution to store and protect patient data on Hyperledger [51]. Moreover, we plan to combine the NFT and IPFS to define the medical test result for the patients.

VII. Conclusion

We have built a blockchain-based system for healthcare facilities in developing countries (i.e., Vietnam) to manage and store patient medical test results. Our proposed model is based on a balance between many unique criteria including limitations of medical facilities in developing countries (i.e., in terms of equipment), patient effort (i.e., waiting time, requirement background about security and privacy as well as technique), sharing information about test results and patient medical records between different healthcare centers; and system transparency. In addition, we build a proof-of-concept based on the Hyperledger Fabric platform. To demonstrate the feasibility of the proposed model, we evaluate the actual w.r.t performance of the system (i.e., create, access and update) based on 10 scenarios that change the number of requests per second (i.e., 1000 requests increaing for each scenario) by exploiting Hyperledger Caliper. The review highlighted our findings based on a review of the system as well as of the proof-of-concept; thereby suggesting possible future development directions.

References

[1] R. A. McPherson and M. R. Pincus, *Henry's clinical diagnosis and management by laboratory methods E-book*. Elsevier Health Sciences, 2021.

[2] H. T. Le, L. N. T. Thanh, H. K. Vo, H. H. Luong, K. N. H. Tuan, T. D. Anh, K. H. N. Vuong, H. X. Son *et al.*, "Patient-chain: Patient-centered healthcare system a blockchain-based technology in dealing with emergencies," in *International Conference on Parallel and Distributed Computing: Applications and Technologies*. Springer, 2022, pp. 576–583.

[3] L. N. T. Thanh *et al.*, "Toward a unique iot network via single sign-on protocol and message queue," in *International Conference on Computer Information Systems and Industrial Management*. Springer, 2021.

[4] N. Mostert-Phipps, D. Pottas, and M. Korpela, "Improving continuity of care through the use of electronic records: a south african perspective," *South African Family Practice*, vol. 54, no. 4, pp. 326–331, 2012.

[5] D. M. Mugo and D. Nzuki, "Determinants of electronic health in developing countries," 2014.

[6] H. X. Son and E. Chen, "Towards a fine-grained access control mechanism for privacy protection and policy conflict resolution," *International Journal of Advanced Computer Science and Applications*, vol. 10, no. 2, 2019.

[7] N. Duong-Trung, H. X. Son, H. T. Le, and T. T. Phan, "Smart care: Integrating blockchain technology into the design of patient-centered healthcare systems," in *Proceedings of the 2020 4th International Conference on Cryptography, Security and Privacy*, ser. ICCSP 2020, 2020, p. 105–109.

[8] ——, "On components of a patient-centered healthcare system using smart contract," in *Proceedings of the 2020 4th International Conference on Cryptography, Security and Privacy*, 2020, p. 31–35.

[9] H. X. Son, T. H. Le, N. T. T. Quynh, H. N. D. Huy, N. Duong-Trung, and H. H. Luong, "Toward a blockchain-based technology in dealing with emergencies in patient-centered healthcare systems," in *International Conference on Mobile, Secure, and Programmable Networking*. Springer, 2020, pp. 44–56.

[10] L. N. T. Thanh, N. N. Phien, H. K. Vo, H. H. Luong, T. D. Anh, K. N. H. Tuan, H. X. Son *et al.*, "Sip-mba: A secure iot platform with brokerless and micro-service architecture," 2021.

[11] N. T. T. Lam, H. X. Son, T. H. Le, T. A. Nguyen, H. K. Vo, H. H. Luong, T. D. Anh, K. N. H. Tuan, and H. V. K. Nguyen, "Bmdd: A novel approach for iot platform (broker-less and microservice architecture, decentralized identity, and dynamic transmission messages)," *International Journal of Advanced Computer Science and Applications*, 2022.

[12] T. T. L. Nguyen, H. K. Vo, H. H. Luong, H. T. K. Nguyen, A. T. Dao, X. S. Ha *et al.*, "Toward a unique iot network via single sign-on protocol and message queue," in *International Conference on Computer Information Systems and Industrial Management*. Springer, 2021, pp. 270–284.

[13] L. N. T. Thanh, N. N. Phien, H. K. Vo, H. H. Luong, T. D. Anh, K. N. H. Tuan, H. X. Son *et al.*, "Uip2sop: a unique iot network applying single sign-on and message queue protocol," 2021.

[14] N. Duong-Trung, X. S. Ha, T. T. Phan, P. N. Trieu, Q. N. Nguyen, D. Pham, T. T. Huynh, and H. T. Le, "Multi-sessions mechanism for decentralized cash on delivery system," *Int. J. Adv. Comput. Sci. Appl*, vol. 10, no. 9, 2019.

[15] C. Frazzoli, O. E. Orisakwe, R. Dragone, and A. Mantovani, "Diagnostic health risk assessment of electronic waste on the general population in developing countries' scenarios," *Environmental Impact Assessment Review*, vol. 30, no. 6, pp. 388–399, 2010.

[16] H. T. Le, T. T. L. Nguyen, T. A. Nguyen, X. S. Ha, and N. Duong-Trung, "Bloodchain: A blood donation network managed by blockchain technologies," *Network*, vol. 2, no. 1, pp. 21–35, 2022.

[17] N. T. T. Quynh, H. X. Son, T. H. Le, H. N. D. Huy, K. H. Vo, H. H. Luong, K. N. H. Tuan, T. D. Anh, N. Duong-Trung *et al.*, "Toward a design of blood donation management by blockchain technologies," in *International Conference on Computational Science and Its Applications*. Springer, 2021, pp. 78–90.

[18] A. Roehrs, C. A. da Costa, R. da Rosa Righi, V. F. da Silva, J. R. Goldim, and D. C. Schmidt, "Analyzing the performance of a blockchain-based personal health record implementation," *Journal of biomedical informatics*, vol. 92, p. 103140, 2019.

[19] X. S. Ha, T. H. Le, T. T. Phan, H. H. D. Nguyen, H. K. Vo, and N. Duong-Trung, "Scrutinizing trust and transparency in cash on delivery systems," in *International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage*. Springer, 2020, pp. 214–227.

[20] X. S. Ha, H. T. Le, N. Metoui, and N. Duong-Trung, "Dem-cod: Novel access-control-based cash on delivery mechanism for decentralized marketplace," in *2020 IEEE 19th International Conference on Trust,*

Security and Privacy in Computing and Communications (TrustCom). IEEE, 2020, pp. 71–78.

[21] Z. Chen, W. Xu, B. Wang, and H. Yu, "A blockchain-based preserving and sharing system for medical data privacy," *Future Generation Computer Systems*, vol. 124, pp. 338–350, 2021.

[22] M. Du, Q. Chen, J. Xiao, H. Yang, and X. Ma, "Supply chain finance innovation using blockchain," *IEEE Transactions on Engineering Management*, vol. 67, no. 4, pp. 1045–1058, 2020.

[23] H. X. Son, M. H. Nguyen, H. K. Vo *et al.*, "Toward an privacy protection based on access control model in hybrid cloud for healthcare systems," in *International Joint Conference: 12th International Conference on Computational Intelligence in Security for Information Systems (CISIS 2019) and 10th International Conference on EUropean Transnational Education (ICEUTE 2019)*. Springer, 2019, pp. 77–86.

[24] M. R. Patra, R. K. Das, and R. P. Padhy, "Crhis: cloud based rural healthcare information system," in *Proceedings of the 6th International Conference on Theory and Practice of Electronic Governance*, 2012, pp. 402–405.

[25] C. O. Rolim, F. L. Koch, C. B. Westphall, J. Werner, A. Fracalossi, and G. S. Salvador, "A cloud computing solution for patient's data collection in health care institutions," in *2010 Second International Conference on eHealth, Telemedicine, and Social Medicine*. IEEE, 2010, pp. 95–99.

[26] T. Makubalo, B. Scholtz, and T. O. Tokosi, "Blockchain technology for empowering patient-centred healthcare: A pilot study," in *Conference on e-Business, e-Services and e-Society*. Springer, 2020, pp. 15–26.

[27] Y. Zhang, M. Qiu, C.-W. Tsai, M. M. Hassan, and A. Alamri, "Healthcps: Healthcare cyber-physical system assisted by cloud and big data," *IEEE Systems Journal*, vol. 11, no. 1, pp. 88–95, 2015.

[28] M. Barua, X. Liang, R. Lu, and X. Shen, "Espac: Enabling security and patient-centric access control for ehealth in cloud computing," *International Journal of Security and Networks*, vol. 6, no. 2-3, pp. 67–76, 2011.

[29] L. Chen and D. B. Hoang, "Novel data protection model in healthcare cloud," in *2011 IEEE International Conference on High Performance Computing and Communications*. IEEE, 2011, pp. 550–555.

[30] N. M. Hoang and H. X. Son, "A dynamic solution for fine-grained policy conflict resolution," in *Proceedings of the 3rd International Conference on Cryptography, Security and Privacy*, 2019, pp. 116–120.

[31] H. X. Son and N. M. Hoang, "A novel attribute-based access control system for fine-grained privacy protection," in *Proceedings of the 3rd International Conference on Cryptography, Security and Privacy*, 2019, pp. 76–80.

[32] Q. N. T. Thi, T. K. Dang, H. L. Van, and H. X. Son, "Using json to specify privacy preserving-enabled attribute-based access control policies," in *International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage*. Springer, 2017, pp. 561–570.

[33] M. M. Madine, A. A. Battah, I. Yaqoob, K. Salah, R. Jayaraman, Y. Al-Hammadi, S. Pesic, and S. Ellahham, "Blockchain for giving patients control over their medical records," *IEEE Access*, vol. 8, pp. 193 102–193 115, 2020.

[34] M. Misbhauddin, A. AlAbdulatheam, M. Aloufi, H. Al-Hajji, and A. Al-Ghuwainem, "Medaccess: A scalable architecture for blockchain-based health record management," in *2020 2nd International Conference on Computer and Information Sciences (ICCIS)*. IEEE, 2020, pp. 1–5.

[35] N. T. T. Le, Q. N. Nguyen, N. N. Phien, N. Duong-Trung, T. T. Huynh, T. P. Nguyen, and H. X. Son, "Assuring non-fraudulent transactions in cash on delivery by introducing double smart contracts," *International Journal of Advanced Computer Science and Applications*, vol. 10, no. 5, pp. 677–684, 2019.

[36] G. Zyskind, O. Nathan *et al.*, "Decentralizing privacy: Using blockchain to protect personal data," in *2015 IEEE Security and Privacy Workshops*. IEEE, 2015, pp. 180–184.

[37] P. Zhang, J. White, D. C. Schmidt, G. Lenz, and S. T. Rosenbloom, "Fhirchain: applying blockchain to securely and scalably share clinical data," *Computational and structural biotechnology journal*, vol. 16, pp. 267–278, 2018.

[38] V. Patel, "A framework for secure and decentralized sharing of medical imaging data via blockchain consensus," *Health informatics journal*, vol. 25, no. 4, pp. 1398–1411, 2019.

[39] H. X. Son, M. H. Nguyen, N. N. Phien, H. T. Le, Q. N. Nguyen, V. Dinh, P. Tru, and P. Nguyen, "Towards a mechanism for protecting seller's interest of cash on delivery by using smart contract in hyperledger," *International Journal of Advanced Computer Science and Applications*, vol. 10, no. 4, pp. 45–50, 2019.

[40] M. Egorov, M. Wilkison, and D. Nuñez, "Nucypher kms: decentralized key management system," *arXiv preprint arXiv:1707.06140*, 2017.

[41] L. Chen, W.-K. Lee, C.-C. Chang, K.-K. R. Choo, and N. Zhang, "Blockchain based searchable encryption for electronic health record sharing," *Future generation computer systems*, vol. 95, pp. 420–429, 2019.

[42] D. Tith, J.-S. Lee, H. Suzuki, W. Wijesundara, N. Taira, T. Obi, and N. Ohyama, "Application of blockchain to maintaining patient records in electronic health record for enhanced privacy, scalability, and availability," *Healthcare informatics research*, vol. 26, no. 1, pp. 3–12, 2020.

[43] R. W. Ahmad, K. Salah, R. Jayaraman, I. Yaqoob, S. Ellahham, and M. Omar, "The role of blockchain technology in telehealth and telemedicine," *International journal of medical informatics*, vol. 148, p. 104399, 2021.

[44] M. Kassab, J. DeFranco, T. Malas, P. Laplante, G. Destefanis, and V. V. G. Neto, "Exploring research in blockchain for healthcare and a roadmap for the future," *IEEE Transactions on Emerging Topics in Computing*, vol. 9, no. 4, pp. 1835–1852, 2019.

[45] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control," *Journal of medical systems*, vol. 40, no. 10, pp. 1–8, 2016.

[46] M. Kassab, J. DeFranco, T. Malas, G. Destefanis, and V. V. G. Neto, "Investigating quality requirements for blockchain-based healthcare systems," in *2019 IEEE/ACM 2nd International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB)*. IEEE, 2019, pp. 52–55.

[47] K. L. Quoc, H. K. Vo, L. H. Huong, K. H. Gia, K. T. Dang, H. L. Van, N. H. Huu, T. N. Huyen, L. Van Cao Phu, D. N. T. Quoc *et al.*, "Sssb: An approach to insurance for cross-border exchange by using smart contracts," in *International Conference on Mobile Web and Intelligent Information Systems*. Springer, 2022, pp. 179–192.

[48] H. H. Luong, T. D. Anh, K. N. H. Tuan, and H. X. Son, "Ioht-mba: An internet of healthcare things (ioht) platform based on microservice and brokerless architecture," 2021.

[49] S. H. Xuan, L. K. Tran, T. K. Dang, and Y. N. Pham, "Rew-xac: an approach to rewriting request for elastic abac enforcement with dynamic policies," in *2016 International Conference on Advanced Computing and Applications (ACOMP)*. IEEE, 2016, pp. 25–31.

[50] H. X. Son, T. K. Dang, and F. Massacci, "Rew-smt: a new approach for rewriting xacml request with dynamic big data security policies," in *International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage*. Springer, 2017, pp. 501–515.

[51] M. Uddin, "Blockchain medledger: Hyperledger fabric enabled drug traceability system for counterfeit drugs in pharmaceutical industry," *International Journal of Pharmaceutics*, vol. 597, p. 120235, 2021.