Towards a Blockchain-based Medical Test Results Management System

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 test results in the diagnosis and treatment of patients' diseases at medical facilities cannot be ignored. Patients must have a series of tests that are related to their symptoms. This can be repeated as many times as possible, depending on the type of disease and treatment. Seriously, in the cases where the patients lose their medical test record (i.e., patient's medical history), the diagnosis is difficult due to the lack of information about the medical history as well as the symptoms/complications in the previous treatments. Storing this treatment information in medical centers can address risks related to user failure (e.g., loss of medical test records and wet/fire documents). However, users face a bit of difficulty when they change to other medical centers for medical examination and treatment since the data is stored locally, and difficult to share this with others. Current solutions focus on empowering users (i.e., patients) to share medical information related to disease treatment. However, the main barrier to these approaches is the knowledge of the users. They must embrace some background in terms of the technologies, risks, and rights they may share with treatment facilities. To solve this problem, we propose a Blockchain-based medical test result management system where all information is stored and verified by the stakeholder. The data will be stored decentralized and updated throughout the treatment process. We implement a proof-of-concept based on the Hyperledger Fabric platform. To demonstrate the effectiveness of the proposed system, we conduct evaluation methods based on three main tasks of the system: initializing, accessing, and updating data on six different scenarios (i.e., increasing in size of processing requests). The evaluation based on Hyperledger Caliper helped us to have a deeper analysis of the proposed model.**

***Keywords*—Blood donation; blockchain; hyperledger fabric; blood products supply chain**

I. Introduction

The need for health care is extremely urgent for all ages. The diagnosis process has a great influence on the treatment of the patient. To be able to make an accurate diagnosis of the condition, doctors must consider the test results as well as the patient's medical history. This information is usually compiled in a medical test result. Depending on the medical facility, medical test results are provided in the form of paper results or electronic results [1]. One of the biggest difficulties in this traditional process is the long processing time and waiting time, not to mention all the information resulted in the medical test result (i.e., information about the patient's health). In addition, the traditional medical process is not yet capable of reusing the patient's existing test results. Specifically, the current storage methods are only centrally stored in a central or hospital server in the big cities. This situation does not apply to small health facilities in the countryside [2]. For this reason, all resulted information is manually analyzed by the physicians before being resulted in the patient's medical result [3].

This situation is extremely risky for the healthcare system because i) it is easy for patients to lose the medical test results 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. To this end, the previous approaches that have contributed a lot to these risks are based on centralized personal data methods (i.e., where the user is central and is allowed to share any data with the hospital/ medical facility or third party) [4]. In addition, the methods propose a decentralized management mechanism for users, including hospital or medical center staff (e.g., doctors, nurses) and patients and their family members; [5] in special cases (e.g., emergency [6]). These approaches are based on the assessment that health care is needed and prioritized over privacy issues. However, both groups of approaches have encountered a binding mechanism that the patient must be able to use smart devices (i.e., smartphones). They argue that privacy risks are of great concern and that there must be a reasonable mechanism for healthcare-related issues where medical data is exploited/stored/processed. This argument is completely correct and can be applied to big medical institutions where the facility is available for data storage and processing. However, for the other scope (i.e., small medical centers), not many approaches provide the solution in terms of storage and processing of the medical data [7], [8].

This paper is one of the first attempts to address the above issues related to the storage of medical test results from medical/healthcare centers. We aim for a decentralized storage solution that is not bound by data storage and processing equipment in small and medium medical centers. This study opens up a potential approach where decentralized methods of storing and processing patient personal data (i.e., test results) can be applied. In addition to infrastructure barriers, we also consider issues related to data transparency, where all information stored is verified by stakeholders (e.g., patients, the patient's relatives in the emergency situation, and the doctor). This method gives transparency to all stored data. All of the above solutions lead to a Blockchain-based approach, where all data is verified by the parties involved. Furthermore, the data is stored and processed decentralized.

Blockchain technology is known for its outstanding features of transparency and immutable content. Picha Edwardsson et al. studied the possibility of using blockchain technology

to create a secure, community-facing information verification database with the goal of creating a solution that could improve the reliability of verifying information and monitoring each authenticity verification process for digital content, including images and videos. The paper indicates that blockchain is not yet ready to be directly applied to fact-checking processes in a real-world scenario. The study also shows that the application of blockchain to verify a scenario is entirely possible and highly reliable and transparent [9]. Several approaches address these problems by applying Blockchain techniques in the other environment (e.g., cash-on-delivery [10], [11], [12], healthcare [5], [4], [6], supply chain [13], [14], [15], and others [16], [17], [18]). As for the patient's/patient's ability to use technology, we assume that they have the ability to read information about their personal data usage through their phone whenever there is a phone call. access from outside the system.

Rather than emphasizing the role of patients in our system [19], [20], [21], our proposed model aims to propose a decentralized store and process system for the patient's medical test results (see more details in Section II). In other words, our system is device-centric instead of user (i.e., patient) or service provider (i.e., app). All processing requests are guaranteed by the parties (i.e., patients and therapists) and stored on a distributed ledger. An important difference from our system is that our proposed model still uses a trusted third party to manage the encryption and decryption of data before and after processing them. Acknowledging that adopting a model of depending on a trusted third party will compromise the security of the entire system (i.e., third party trust level). However, it also brings benefits when the data is secure and has fewer burdens on users as well as the user's background requirements [22]. Responsibility for the protection of personal data is assigned to a security company (i.e., third party). As for the implementation, we exploited the Hyperledger Fabric platform for our proof-of-concept. The related evaluation to prove the effectiveness (i.e., focusing on initialization, query, and update) was analyzed by Hyperledger Caliper.

Stemming from the research problem of ensuring transparency and decentralized storage for patients' medical test results (see details in the related work section), we propose a model for information management about patients. Test results based on Blockchain technology and Smart contract. Therefore, our main contribution revolves around three aspects: (a) building a medical test result management system based on Blockchain and Smart contract; (b) building proof-of-concept on top of Hyperledger Fabric; and (c) assessing the appropriateness of the approach based on an analysis of three main scenarios (i.e., initialize, retrieve, and update) based on the Hyperledger Caliper platform.

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. [23] 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. [1] and Son et al. [24] 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. [25] 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. [26] 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. [27] 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. [28] 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. [29] proposes an ABE-based access control model based on patience and privacy protection; Chen et al. [30] 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 [31], [32] or protection policies for both security and privacy [33].

In addition, Madine et al. [34] 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.[1] 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).[2] With the same approach based on Blockchain technology and IPFS, Misbhauddin et al. [35] 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. [12] has argued that not all data collected must be processed on-chain. Instead, Son et al. [14] 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) [7].

The above approaches have brought many solutions to today's traditional health care systems. However, in developing countries (e.g., Vietnam) where medical equipment and supplies are one of the barriers that directly affect people's health care 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 [37]. 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

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

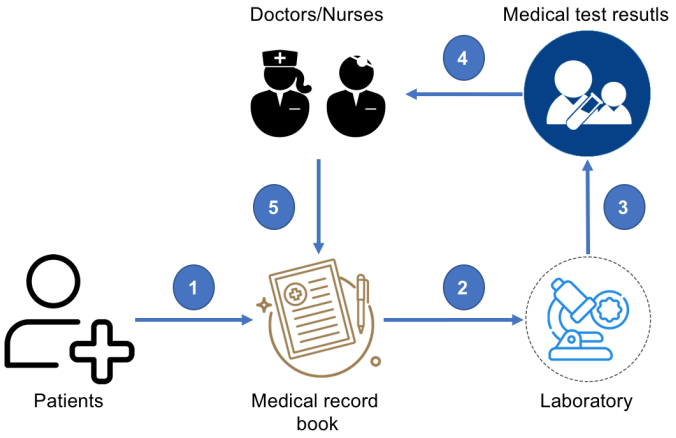

Fig. 1. The Traditional Process for Medical Test Results Management System.

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.

[1]https://www.healthbank.coop/2018/10/30/healthbank-creates-the-first-patient-centric-healthcare-trust-ecosystem/
[2]https://www.factom.com/company-updates/healthnautica-factom-announce-partnership/

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., Hyperledger). 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 Hyperledger (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 Hyperledger, 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., Hyperledger). 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.

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 two 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 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. 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

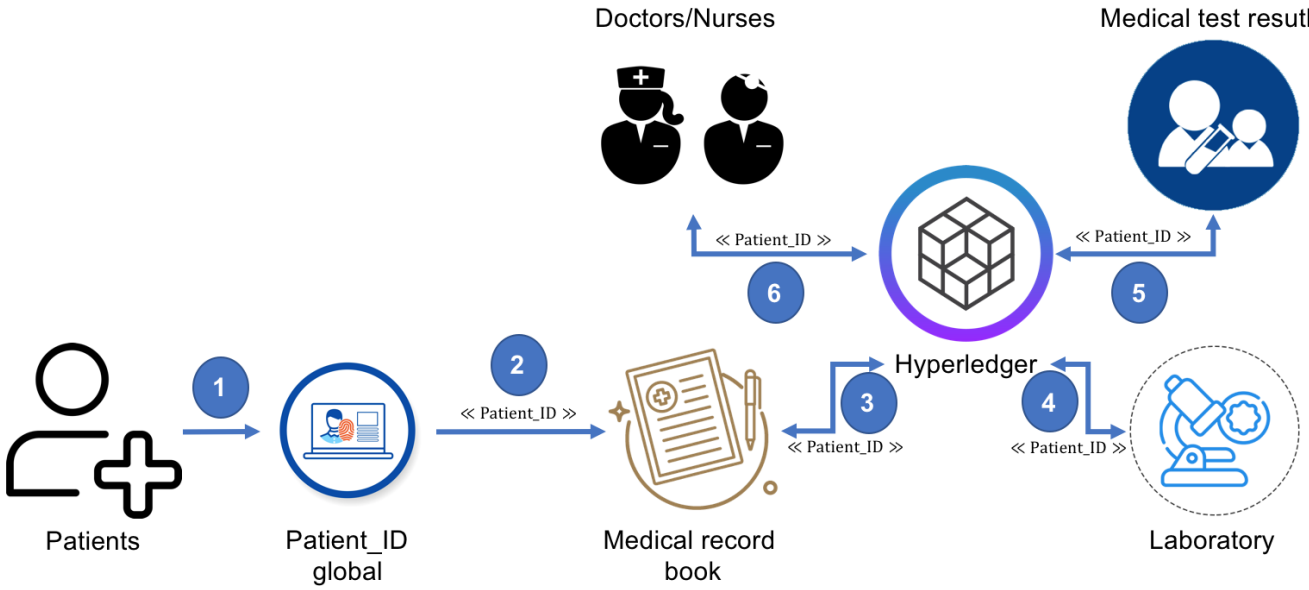

Fig. 2. The Proposed Model for Blockchain-Based Medical Test Results Management System.

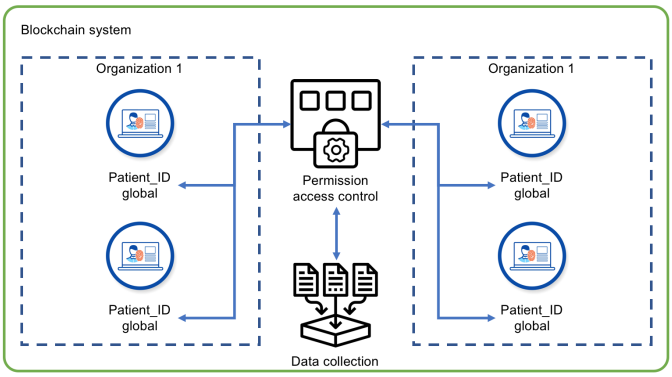

Fig. 3. Permission Diagram.

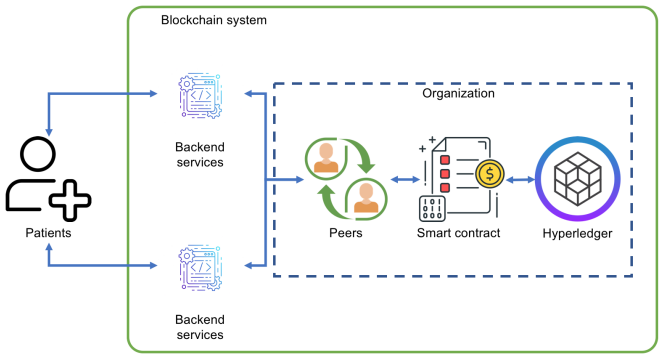

Fig. 4. Hyperledger Fabric Component.

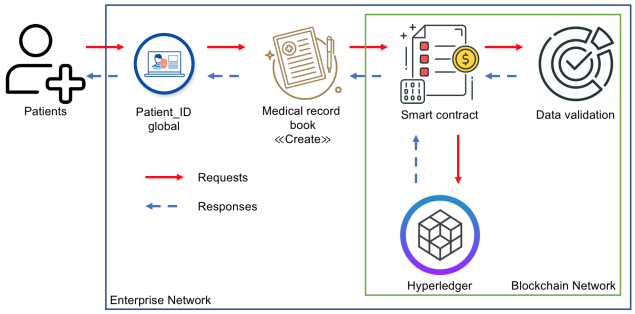

Fig. 5. Initializing and Storing the new Data.

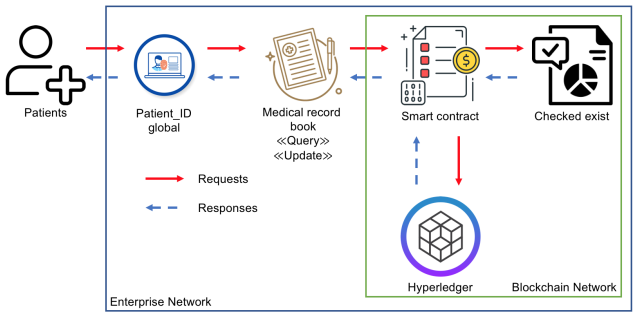

Fig. 6. Retrieving/Querying Data Process

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 exper-

iments are deployed on Ubuntu 20.01 configuration, core i5 2.7Ghz, and 8GB RAM.

To prove the effectiveness of our model, we also define several experiments by exploiting the Hyperledger Caliper[3] that is used to design the test scenarios and collect all the information regarding the performance.

B. Results

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[4]. Table I shows the execution results of the data initialization/creation function (e.g., medical record book). The data initialization/creation script is conducted with two users concurrently making 1000 - 6000 requests to the system. We measure the parameters of command success/failure and system latency (i.e., max, min, avg). 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 6000 requests). Specifically, the number of failed requests is limited to less than 7,500 (i.e., 7,458 requests - 16.24%). Meanwhile, the lowest case was with only 6.57% (2,953 requests). The highest failed request rate is in the first 1,000/s request, the system is more stable in terms of data creation with only an average of 5K errors per scenario (from 2K requests to 6K). For system-wide latency, we recorded the number of requests with response delays per 1,000 requests/second to 6,000 requests per second. Specifically, the data in Table I demonstrate that the highest latency ranges from 1,626.57 to 1,781.15 seconds. The minimum is less than 8 seconds. The average delay when creating new data is less than 900 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 6000 requests which access the medical record book from 2 users. Table II shows the execution results of the data access function (e.g., medical record book). Compared with the first task (i.e., data creation), the results of 6 scenarios to evaluate the data accessibility of our proposed blockchain-based system are more balanced. Retrieval of stored data is extremely important. Indeed, considering health data retrieval time directly affects the patient's health care.[5] 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). Specifically, the maximum time to wait for a data retrieval request is 15 seconds (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). The minimum wait time is almost instant response (i.e., with only 0.06 seconds). The average time for each data retrieval request is about 7.35 seconds. 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, around 80% of the requests are successful in all 6 scenarios.

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 six different scenarios, each of which will require processing from 1000 to 6000 requests per second. We also measure two parameters, similar to the two scenarios above, the number of successful and failed requests and the overall latency, which is shown in Table III. In terms of time, updating data is more complex than the previous two scenarios (i.e., initialization and access). Specifically, we must determine if user information exists in Hyperledger, 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 850 to 950 seconds in the maximum case. The minimum latency ranges from 0.5 seconds to 0.6 seconds, while the average latency required by an application to process ranges from 370 seconds to 400 seconds. Similarly, the number of failed requests was also higher than the success requests in all six scenarios (with an average of about 51%).

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 data retrieval and initialization with more than 20% and less than 20% 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

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

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

[5]In this scenario, we do not include time for encoding and decoding. code the data stored on Hyperledger

TABLE I. DATA CREATION/INITIALIZATION (I.E., MEDICAL RECORD BOOK) FOR THE MEDICAL TEST RESULTS OF THE PATIENT

Number of requests	Max Latency (s)	Min Latency (s)	Avg Latency (s)	Success	Fail
1,000	1,627.11	7.23	817.17	38,479	7,458
2,000	1,781.15	5.21	893.18	41,962	2,953
3,000	1,626.57	5.40	815.99	38,504	5,331
4,000	1,659.02	6.94	832.98	39,375	5,417
5,000	1,744.65	5.93	875.29	39,824	6,347
6,000	1,765.50	6.67	886.09	40,136	5,261

TABLE II. DATA ACCESS (I.E., MEDICAL RECORD BOOK) FOR THE MEDICAL TEST RESULTS OF THE PATIENT

Number of requests	Max Latency (s)	Min Latency (s)	Avg Latency (s)	Success	Fail
1,000	11.78	0.03	7.43	91,127	22,307
2,000	13.99	0.01	7.45	91,307	26,322
3,000	13.35	0.02	7.37	92,325	25,519
4,000	12.54	0.01	7.34	91,674	26,785
5,000	11.56	0.02	7.32	92,047	26,622
6,000	14.35	0.04	7.33	91,408	27,044

TABLE III. DATA UPDATE (I.E., MEDICAL RECORD BOOK) FOR THE MEDICAL TEST RESULTS OF THE PATIENT

Number of requests	Max Latency (s)	Min Latency (s)	Avg Latency (s)	Success	Fail
1,000	852.24	0.56	373.31	12,971	13,835
2,000	856.32	0.59	374.80	12,991	14,099
3,000	889.55	0.55	375.58	12,984	14,083
4,000	919.85	0.60	373.73	13,039	14,129
5,000	931.84	0.51	391.16	13,027	14,178
6,000	852.14	0.59	375.52	12,896	14,052

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. 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 [38], [39]. For authorization, a model based on ABAC [32], [31] and supporting dynamic policy [40], [41] 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 [42].

VII. CONCLUSION

In this work, we propose a test process management system based on Blockchain technology. The main contributions of our solution are threefold: (a) building a medical test result management system based on Blockchain and Smart contract; (b) building proof-of-concept on top of Hyperledger Fabric; and (c) assessing the appropriateness of the approach based on an analysis of three main scenarios (i.e., initialize, retrieve, and update) based on the Hyperledger Caliper platform. Specifically, (**a**) all user-related information as well as test results, diagnoses, and patient medical records are stored on Hyperledger (distributed ledger). All this stored information is authenticated by the relevant parties (i.e., patient, nurse/-doctor). We also offer a traditional test process management system. Thereby, we compared it with our proposed model before implementing proof-of-concept implementation on Hyperleger Fabric platform (i.e., (**b**)). In evaluating the feasibility of the proposed system, we analyze 3 key tasks of a Blockchain-based system (i.e., data initialization, retrieval and update) on six scenarios requiring access from 1,000 to 6,000 requests/second. Comments and future directions are presented in the Discussion section of the paper. Based on the analysis results, we found that our proposed model works stably in the scenario of up to 6,000 incoming requests per second in a simulated environment with limited resources (i.e., (**c**)).

REFERENCES

[1] 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.

[2] W. H. Organization *et al.*, *Increasing access to health workers in remote and rural areas through improved retention: global policy recommendations*. World Health Organization, 2010.

[3] S. S.-L. Tan and N. Goonawardene, "Internet health information seeking and the patient-physician relationship: a systematic review," *Journal of medical Internet research*, vol. 19, no. 1, p. e5729, 2017.

[4] 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.

[5] ——, "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.

[6] 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.

[7] 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.

[8] 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.

[9] M. Picha Edwardsson and W. Al-Saqaf, "Drivers and barriers for using blockchain technology to create a global fact-checking database," *Online Journal of Communication and Media Technologies*, vol. 12, no. 4, p. e202228, 2022.

[10] 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.

[11] 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.

[12] 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.

[13] N. H. Tuan Khoi *et al.*, "Vblock - blockchain based traceability in medical products supply chain management: Case study in vietnam," in *International Conference on Artificial Intelligence for Smart Community*, 2020.

[14] 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.

[15] 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.

[16] H. H. Luong, T. K. N. Huynh, A. T. Dao, and H. T. Nguyen, "An approach for project management system based on blockchain," in *International Conference on Future Data and Security Engineering*. Springer, 2021, pp. 310–326.

[17] N. H. Tuan Khoi *et al.*, "Domain name system resolution system with hyperledger fabric blockchain," in *International Conference on Inventive Computation and Information Technologies*, 2022.

[18] 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.

[19] 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.

[20] 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.

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

[22] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in *2010 proceedings ieee infocom*. Ieee, 2010, pp. 1–9.

[23] 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.

[24] 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.

[25] 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.

[26] 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.

[27] 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.

[28] 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.

[29] 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.

[30] 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.

[31] 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.

[32] 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.

[33] 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.

[34] 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.

[35] 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.

[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] 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.

[38] 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.

[39] 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.

[40] 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.

[41] 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.

[42] 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.