IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.///Access-Template-1 <- the file name …

Digital Object Identifier 10.1109/ACCESS.2017.Doi Number

Development of an Internet-of-Healthcare System Using Blockchain

SUPARAT YONGJOH[1], CHAKCHAI SO-IN[2] (Senior Member, IEEE), PEERAPOL KOMPUNT[1], PAISARN MUNEESAWANG[1] (Senior Member, IEEE), ROY I. MORIEN[3]

[1]Department of Electrical and Computer Engineering, Faculty of Engineering, Naresuan University, Phitsanulok 65000, Thailand

[2]Applied Network Technology Laboratory, Department of Computer Science, Faculty of Science, Khon Kaen University, 40002, Thailand

[3]Naresuan University Graduate School, Phitsanulok 65000, Thailand

This work was supported by the National Broadcasting and Telecommunication Commission (NBTC), Thailand; and in part by the Thailand Research Fund through the International Research Network Program under Grant IRN61W0006.

ABSTRACT The Internet-of-Healthcare-Systems is a highly distributed special emulation of the Internet of Things technology using web agents as front-ends to the many and varied internal patient information systems of the participating hospitals, providing a canonical interface to all those diverse hospital systems. Extending on previously developed and distributed health care apps, blockchain technology has been applied for the storage of sensitive patient data that requires a high degree of security that is imperative for patient data and medical histories. Data sourced from participating hospitals are integrated with a decentralized storage system using blockchain technology, guaranteeing secure access and control, and veracity of that data over time. Web agents, accessed using the Message Queueing Telemetry Transport protocol, efficiently handle potentially thousands of recognised local systems without loss of network timeliness. Mobile device apps have been developed that enable secure direct access to patient data in a central blockchain with download capability to a mobile device, under strict access control using Amazon Web Services under fully managed access control, with permissions controlled by the Key Management System. The Internet-of-Healthcare-Systems model is an exemplar for many different types of secure networks that could be generically called an Internet of Special Things; a network of web agents programmed for a special purpose. Security analysis, and feedback from participating medical staff, indicates security improvements and a high level of satisfaction with all aspects of the system: ease of use, ease of installation, maintenance and update, and, importantly, the security of the system.

INDEX TERMS blockchain data storage, Internet of Things (IoT), Electronic Health Care System (eHCS), Internet of Health Care System (IoHCS).

I. INTRODUCTION

Electronic Health Care Systems, generally termed eHealth systems, are now seen as being very important in national public health administration systems. The World Health Organization (WHO) has highlighted the importance of, and motivation for, Electronic Health Care Systems (eHCSs) [1]. The system presented in this paper was developed within the broader national development strategy promulgated by the Thai Government Ministry of Public Health, termed Thailand 4.0 [2], the overall intention of which is to digitally create a national, fully integrated, public health information system.

For simplicity of reference, the terminology of Electronic Health Record (EHR) will be used to refer to the data package elicited by the web agents. The patient information systems used internally by participating hospitals are termed Hospital Information Systems (HIS), and the terminology of e-Health Care Systems (eHCS) is used to refer generally to any electronic health information system in use or available, however referred to in the literature.

Traditionally, health service providers, even large hospitals, kept medical records of patients in manual form in card indexes or manually updated folders. There has been a significant move towards computerized patient information systems which have replaced the manual systems which were error-prone and time-consuming to manage and to retrieve patient information, and both the manual systems and the computerized systems that replaced them are discrete bounded

systems local to their location. The variety of these systems also presented an obstacle to overall, national, integration.

Acknowledging the strategic public health administration policy of the Thai Ministry of Public Health, researchers and medical practitioners, and academics at the Naresuan University (NU) Faculty of Medicine and Naresuan University Hospital, together with researchers and developers in the Faculty of Computer Engineering at NU, collaborated on the development of a sophisticated system whose purpose was to provide an e-consultation facility to enable specialist medical, surgical and ICU personnel to virtually participate in crisis situations at remote hospitals and medical centers where such specialist knowledge was unavailable. This prior work has been presented in previous publications [3], [4], [5].

The system previously developed also enabled the networking of health services providers, hospitals, and medical centers, which allowed full patient medical histories to be available on an Anywhere / Anytime / Anydevice basis, thereby providing information continuity and, importantly, continuity of patient care when patients move between medical service providers. Enhancements to this system to strengthen the security and privacy aspects regarding patient medical data are the central focus of this paper.

Medical records have a special status requiring confidentiality, privacy protection, and secure storage and handling. Any system designed to network patient data must be designed, developed, and promulgated with this in mind. This was the first of three major factors that confronted the researchers in this project.

The second major factor was the variety of these local patient information systems, with different application software suites from different providers, with different DBMS and database schemas, different languages, different hardware, and different utility software. A way needed to be found to enable these diverse systems to have a single, canonical network interface for data accessing to seamlessly networking them together.

Thirdly, inherent in the intentions of the researchers for the ultimate use of the system as a nationwide network linking all hospitals, health clinics, and medical practitioners, the system requirements demanded high-speed, ultra-efficient processing and networking connectivity able to network potentially thousands of medical facilities nationwide while maintaining a high level of timeliness and response times. As well, given the intended extent of the system in the future, the aspects of ease of implementation and ease of maintenance required appropriate attention.

In this paper, we elaborate on, first, the new architecture which we have termed the Internet-of-Health-Care-Systems (IoHCS) that securely manages the historical patient records gathered from all participating hospitals in a network. This was achieved by applying blockchain technology as a method for recording patient data, where sharing, distribution, communication, and agreement protocols can be applied to make the gathered patient data highly secure and immutable.

Second, we describe the way that the hospital Health Information Systems (HIS) of all of these hospitals have been networked together using software agents via Message Queueing Telemetry Transport (MQTT) protocol. This is a central aspect of the IoHCS as each hospital has its own HIS, each of which may have different system and data structure characteristics that are opaque to the network.

As well, we discuss our efforts at ensuring ease of installation and maintenance, and useability and ease of use, or the system.

While achieving these required factors, the security of access to, and storage of, patient medical data, wherever held, was always considered to be of the highest order. Responses from medical personnel from all participating hospitals and health centers, indicated that the security issue is the most important aspect of concern, and the privacy and confidentiality of patient data must be maintained. Data integrity and veracity is essential, and the data must be protected against being tampered with in any way. The central cloud server is potentially a solution to the safe and secure storage of data in an integrated network, but is still subject to threats from bad actors.

Changes to data that may have been tampered with may not be noticed, and, where noticed, may not be recoverable. As well, the integrity of the providers of cloud servers and services is also not guaranteed, and the misuse, monitoirng and even sale, of data is still a likelihood of concern. Patient data must be stored in a manner that provides high reliability and fault tolerance, and ensures the immutability of the data. Blockchain technology is a way to overcome these problems. The distributed or decentralized network and data structures characteristic of blockchains makes tampering with stored data extremely difficult, if not impossible.

Historical data can be recovered from the blockchain intact and unchanged because of the distributed peer-to-peer network characteristics of blockchains that guarantees data integrity throughout the network. Furthermore, a blockchain network has a consensus mechanism that requires the agreement of all participants in the blockchain for all changes to the blockchain.

We also developed an Application Programming Interface (API) for reading and writing data for each hospital on the blockchain. A mobile app was developed that can access patient data with a secured channel using a Key Management System (KMS). This app was then included in the existing HIS of the 350 participating hospitals.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3103443, IEEE Access

So the system and research being presented here builds on previous research and development in the electronic health systems dimension, introduced above as a collaborative development between researchers at Naresuan University and major local tertiary care hospitals. The interface to this system is illutrated in Figure 1.

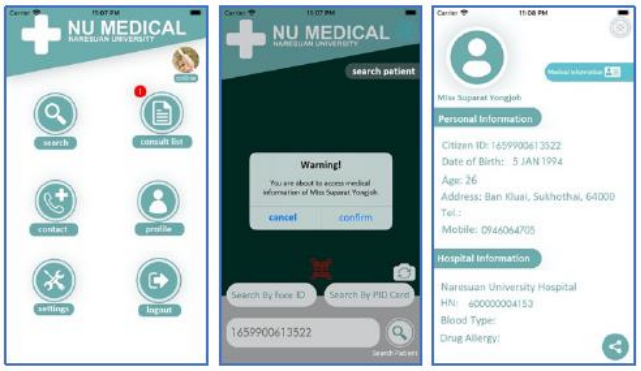


FIGURE 1. NUMED home page (left), patient search (center) and patient information display (right) pages.

This system is termed the NUMED System and 'The Doctor Knows You' system app, which were specifically developed for the 2nd Health Region in central Thailand, with the assistance and cooperation of the Administrator of that Health Region, which encompasses an area stretching from the eastern border, with Laos, to the western border with Myanmar, of Upper Central Thailand and encompassing 5 provinces.

With that system and suite of apps, 350 hospitals and medical facilities are currently networked for the purpose of integrating their patient medical information records such that their medical staff has full availability of patient medical histories regardless of the service provider for each or any of these services, and individual patients could download their individual medical history into storage on their smartphone or mobile device and carry that data with them, disconnected from the Internet.

Those previously developed apps included significant information gathering and communication abilities linking the lowest level of health care involvement; village health volunteers, who number quite literally in the millions, to the highest levels of the Health Region Administration, as well as being a patient history and information-sharing network to support the public health administrative tasks at all levels within the community and the health practitioners.

Prominent in these systems was the use of HoloLens® technology, and haptics, enabling the remote control of medical devices and enabling virtual specialist consultations in remote hospitals. Information regarding these systems has been published previously in journals and at international conferences. [3], [4], [5] op. cit.

The subsequent system development that is the subject of this current paper, builds on that previous system and apps to achieve improvements particularly in the security of the patient data and prevention of unauthorized access to patient data and information tampering. This was successfully achieved by the application of blockchain technology in a central data repository, and the development of software agents that provide the canonical interface to the many diverse hospital patient information systems. These software agents are implemented as front-ends to the hospitals' patient information systems.

The extensions to those apps, incorporating blockchain technology, have been done independently of the 2nd Health Region administration, and the extended system is now installed, at the time of writing, in 350 hospitals in 3 provinces in the Central North region of Thailand. However, during the development of the blockchain extensions, data from the original 157 participating hospitals were used.

The rest of this paper is organized as follows: Section II discusses the related work on blockchain, electronic health records, and the Internet of Things (IoT). Section III presents the architecture of the IoHCS and also presents the details of the technology used by this system and the implemented system. General discussion is presented in Section IV, security analysis in Section V, and Conclusions in Section VI.

II. RELATED WORK

Blockchain is a shared database storage technology also known as Distributed Ledger Technology (DLT). Data is recorded in such a way that guarantees the safety, security and veracity and immutability over time, including the full recording of changes, edits and deletions, of that data. This means that original data 'blocks' in the blockchain remain intact and verifiable, and the blockchain also acts as an unchangeable complete journal or log of data updates separate from the original entry. The beginnings of blockchain technology were in 2008, with the presentation of Satoshi Nakamoto (apparently an alias, but irrelevant to the discussion) in a seminal paper regarding the cryptocurrency Bitcoin where ultra-secure data storage is imperative [6]. In that paper, the author presented the idea of creating a platform that can secure the exchange of cryptocurrency of Bitcoin using the theory of Cryptography and Distributed Computing.

Since its inception in 2008, blockchain technology has been of great interest to developers and researchers for use in various fields, of which medical systems and associated health-related systems are examples [7]. MEDShare [8] was developed with the purpose of protecting the privacy of patients and reducing the risk of misuse of patient medical records. The developers of MEDshare applied blockchain-based data storage for the control and auditing of shared medical data in the Cloud. Medshare records all operations and data in the system in a tamper-proof manner and can monitor the entities that access data from their data custodian system.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3103443, IEEE Access

A cloud storage system, reported in [9], proposed patient privacy protection for electronic patient records by distributing partial components of electronic patient records amongst a number of cloud servers and an efficient process for reconstruction of those records. This novel cloud storage system fully ensured data privacy. by employing the Shamir's secret sharing (an algorithm in cryptography created by Adi Shamir [10]). This was essentially an Internet of Things (IoT) based system.

Another design of a cloud-based Electronic Health Record (EHR) systems was proposed by Fatos Xhafa [11] which included attribute-based encryption. The system enabled the combining of the separated components of the data from each remote cloud server for easy access and viewing by a physician, preserving the privacy of the patient information using attribute-based encryption. The system structure included components for Physician Authorization and Access and Patient Health Record Storage and Access which allowed patients their health records to be shared among physicians.

An Internet of Things (IoT) based system proposed by [12], which the researchers termed HealthChain, was an application of IOT technology for remote patient data monitoring. However, it was recognized that the data retrieved from the IoT device and stored in a centralized data store was not guaranteed to be secure and therefore there was the possibility of leakage of patient information and loss of patients' privacy. As well, there was always the possibility of the irretrievable loss of patient data in the event of a server failure. These researchers overcame these problems by collecting patient health information using the blockchain, thus the name HealthChain. In the HealthChain system, connections between the blockchain and IoT devices were designed to prevent data deletion or correction in order to prevent medical disputes. This is, of course, the primary characteristic of blockchain technology: the immutable aspect of data once in the blockchain so the data is never changed, but changes to the data are included in the blockchain as a record or log of changes which, themselves, are immutable.

As reported in [13], health data-sharing on the permissioned blockchain from HyperLedger Fabric was proposed and developed, along with a mobile application that enabled the data owners to control access from other healthcare providers and health insurance companies. Wearable devices were also integrated with the system to collect user's health data. The health data would be synced to the cloud server and was processed before storing it on the blockchain. Due to the size of health data collected from wearable devices, the Merkle tree was adopted to store only the Merkle root on a blockchain transaction to ensure scalability and efficiency of the system. (A Merkle root is a simple mathematical way to verify the data on a Merkle tree and are used in cryptocurrency to make sure data blocks passed between peers on a peer-to-peer network are whole, undamaged, and unaltered. They are central to the computation required to maintain cryptocurrencies like bitcoin and ether).

The blockchain also stored medical treatment data, insurance claims, and other activities such as data requests, etc. Channeling was also proposed with the scheme to ensure privacy protection.

Cloud-assisted EHR consortium blockchain was proposed in [14]. The blockchain was developed on the Ethereum platform with Proof-of-Authorization as the consensus mechanism. They proposed searchable encryption and proxy re-encryption for the security of data. The system enabled the storage of encrypted patient EHR on the cloud server. The shared EHR must be authorized by their data owner first. The blockchain was for storing keyword ciphertext along with the data owner's account address in order to grant permission for accessing data from the data requester. The data requester could search for keywords in the blockchain and ask for permission from the data owner. If the permission was granted, the data will be encrypted again using the data owner's re-encrypted key before sending it to the data requester which could be a government, laboratory, clinic, etc. The scheme achieved security goals and had high computational efficiency.

A proposed framework from [15] could be a role model for the implementation of blockchain technology on EHR. They also provided a scalable solution with the off-chain storage by implementation from Inter-Planetary File System (IPFS) technology. Each file uploaded in the system contained lab results or other medical records. The IPFS technology uses peer-to-peer network to store data and not allow any data alteration and redundancy because the technology will generate a unique cryptographic hash for each file as an identifier. These hashes are used to store in the blockchain along with their patient ID, name, co-morbid, and blood group. Only authenticated users can access the blockchain data due to the smart contract functionality. The security was ensured in many levels with the blockchain characteristics along with the IPFS, and the role-based access functionality on the smart contract, etc. Transactions were also performed faster because detail medical records are stored in the IPFS rather than the blockchain. The proposed framework was developed on Ethereum platform with Proof-of-work as the consensus mechanism.

A further blockchain-based eHCS was proposed in [16]. In this system, blockchain technology was applied to securing patient data that were shared in a mobile Cloud-based eHCS. The collaboration between mobile applications and cloud computing facilitated data sharing between patients and health care providers, but patient privacy and security of the patient data stored in the Cloud could not be guaranteed. Therefore, in order to reduce the risk of these problems the solution proffered in that paper was to share the data in the blockchain with a decentralized interplanetary file system

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3103443, IEEE Access

(IPFS) (a protocol and peer-to-peer network for storing and sharing data in a distributed file system[1]) on a mobile cloud platform. The implementation used the Ethereum[2] blockchain which is a public blockchain that also works with Amazon Web Services (AWS). This approach enabled safe, controlled and efficient access to patient information, and was a significant step towards efficient management of electronic patient health records in a secure eHCS.

In our system, we store encrypted patient data in a special format which we refer to as the patient's Electronic Heal Record (an EHR) on a blockchain per user. Only patient-of-interest information will be stored on the blockchain in the central location rather than storing all available patient information which can cause tremendously high storage volume.

The main usage of our system is for medical personnel to view patient EHR for further diagnosis and treatment. A doctor/nurse/medical staff can retrieve patient EHR in nearly realtime if the EHR is already stored on the blockchain. If they meet a new patient, It would take less than 1 minutes depending on how many records would be stored on the blockchain for the patient, up to a maximum of 10 of the most recent medical incidences for that patient (stated in TABLE II). This process is possible because of the MQTT protocol which can retrieve the patient information from all available participating hospitals. This ensures that the doctor/nurse/medical staff can retrieve and view patient EHRs as required at or by the time that they meet the patient.

III. SYSTEM MODEL

Since the inception of the Internet, new terminology for various usages of the Internet have evolved. Prominent among these is The Internet of Things (IoT) which refers to the addressing of devices of many kinds by their IP address, ranging from 'intelligent' household appliances to individual communication devices on soldiers in the field, and to machinery in remote railway and mining operations. We have taken this terminology and extended the concept to create a more specific term, The Internet-of-Health-Care-Systems (IoHCS) comprising specifically the patient medical information systems located at participating hospitals and other medical facilities, connected in an integrated network of web services.

The obvious difference between the IoT and the IoHCS is that IoT devices are addressed by an IP, and usually exchange a single interaction or single command or item of data whereas the IoHCS presents a canonical interface to the Internet by software agents, or web agents, which have an IP address, and exchange complex data. As previously acknowledged, in our system, we refer to that set of data as an Electronic Health Record (EHR), the format of which is discussed below.

Figure 2 shows a schematic of the system that we developed. We achieved this integration of the variety of local hospital information systems and successfully promulgated the system to the original 157 hospitals and other medical service providers, a user base that has now grown to over 300. The IoHCS guarantees the secure and verifiable storage of immutable data by applying blockchain technology.

This data is added to by the downloading of new data, the EHR, from the hospitals and other medical service providers via Internet software agents that present a canonical network-facing structure in front of a wide variety of different patient information systems based on the many different operating systems (Windows, Linux), different DBMSs with different schema, different application suites, and so forth.

As can be seen in the diagram, each participating hospital has its own patient information system, the structure and content of which is essentially hidden from the network. Embedded in each of those systems is the software agent that presents a canonical view of each hospital's patient information system.

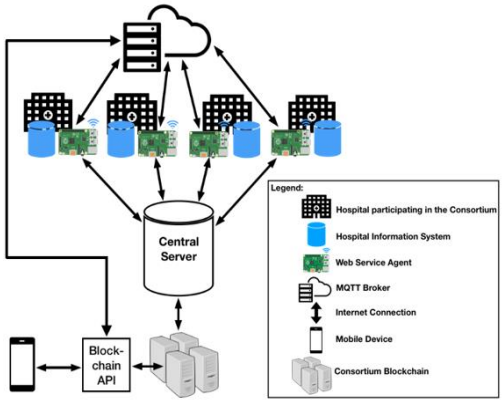


FIGURE 2. The overall structure and design of the system, highlighting the IoHCS component.

The network of these software agents, also termed web agents, comprises the Internet-of-Health-Care-Systems, the IoHCS. These software agents, which are addressed by their IP address, are accessed using the MQTT protocol. The function of the software agents is to transmit a complex set of patient data in a package, which has a defined structure and content, in response to the network request. We term this complex data package as the Electronic Health Record (EHR) to differentiate it from the Hospital Information System (HIS) of the participating hospital.

[1] https://en.wikipedia.org/wiki/InterPlanetary_File_System

[2] Ethereum.org

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3103443, IEEE Access

We discuss the various components of the overall system including the purpose, the processes, and technology applied in each component.

• Hospital Information System (HIS)

This component is not part of our system but it is very important and needs to be considered for designing the interface (an agent) for interacting with patient data. The designed agent has to support the different patient information systems in different hospitals for their data structures and configutations.

Each participating hospital or medical center has their own patient information system which we term their Hospital Information System (HIS) and each HIS is potentially a different software package, such as iMed in Windows Server with SQL Server, HosXP in Linux (CentOS) with MySQL, and PatientInfo in Windows Server with SQL Server.

Because of the many and various Hospital Health software and database configurations, it was necessary to provide a common interface to the network to 'front' these systems. This means that, essentially, the particular hospital patient information system itself is not part of our system but is viewed through a web agent, or software agent, that was defined and developed by the research team. The web agents will be discussed in detail below.

• The Central Server

The patient data that is stored in a variety of ways in each HIS, and is opaque to the network, must be converted into a single format for storage on the blockchain. The EHR returned from a hospital via the web agent comprises all of the available information about that patient which is then stored in the Central Server, which acts as a data buffer. That data is then sorted in the Central Server and the 10 most recent records of the patient are then selected and inserted into the blockchain which resides on a dedicated system, located, in fact, at Naresuan University. The Google Database-as-a-Service (DBaaS) technology is used here. Only authenticated users can access the information on the server.

Message Queueing Telemetry Transport (MQTT) Broker

The MQTT protocol is implemented in the web agents which return all of the patient's records from the HIS to be stored on the Central Server.

MQTT technology is used for communicating between machines or machine to machine (M2M). For developing the system, 2 main components were required:

- Clients
  - Publisher – publish PID of patients to the MQTT broker
  - Subscriber – or listener, receive the PIDs published and query patient records for each PID
- MQTT Broker - a medium for queueing and communicating between devices (clients).

The process of MQTT is illustrated in Fig. 3.

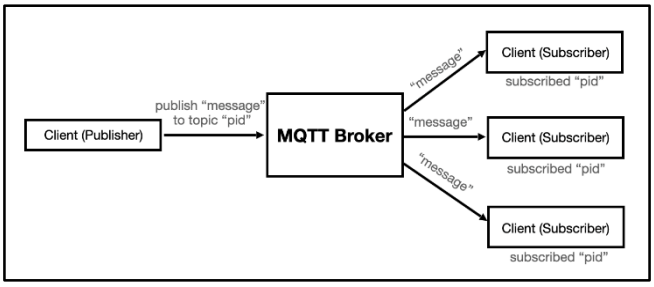


FIGURE 3. MQTT technology diagram

In our case, publishers are mobile phones and API, and subscribers are agents. A web agent (termed a subscriber), will be installed in the computer system of each participating hospital.

Web / Software Agents

For the process, the patient's national ID number is used as the globally unique Patient ID (PID). The PID is the key for retrieving patient records from the different hospitals they have visited. Patients will also have a local ID allocated by each hospital that they have visited, but this is irrelevant for our purposes. No updates to an HIS are made from our system, so the HIS is a read-only system for our purposes.

Each HIS has a query module, written by the developers for this purpose, that can retrieve and format the patient information that has been requested via the web agent, for the specific patient of interest. This is a read-only process that does not update or modify the patients data in the HIS. These web agents request the patient information after receiving the PID via MQTT protocol, and the data is retrievd and returned to the web agent by the query module mentioned.

Agents are software processes developed in Python that are either installed as embedded processes in the hospital's system or run on a Raspberry Pi computer-on-a-board that can be installed as a front-end and are connected to the hospitals server machine via their Local Area Network (LAN). The installation and maintenance of this hardware and software was handled by the development team.

One process carried out by each Agent is to format and restructure the patient information data extracted HIS to form the EHR. and encrypt that data before sending it to the Central Server.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3103443, IEEE Access

The EHR is formatted by the Agent by separating the data into different parts i.e. patient, visit, laboratory, diagnosis, and drug order information, and all parts are encrypted by the Advanced Encryption Standard (AES) 256 Algorithm for each field and transmitted to the Central Server Database in JSON format. The overall structure of the network is illustrated in Fig. 4.

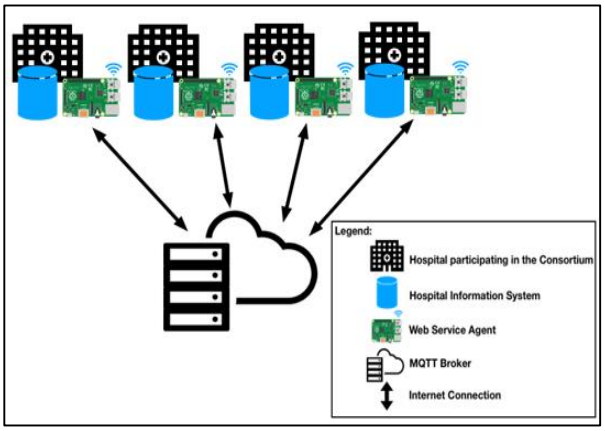


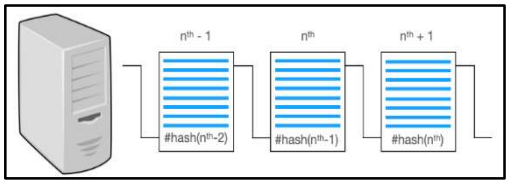
FIGURE 4. The Web / Software Agents and MQTT Broker Structure and design of the system

Blockchain Architecture Design

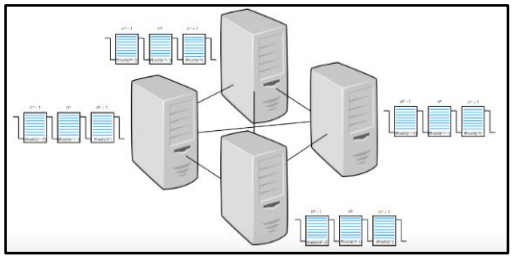
The blockchain system was introduced to increase the data security levels and safety and security of the data retrieved from the participating hospitals. By storing that data in a blockchain at the Central Server, the level of security was raised to the highest level possible. By adopting the hash algorithm for linking the data in each block of the blockchain, and the consensus mechanism, to the distributed peer-to-peer network, the data is stored at a super-secure level.

In a blockchain, each block of data contains a hash of its previous block which can link all blocks together to form a chain of blocks in the order of their arrival in the blockchain. Any change to the data in a block will result in a different hash value being generated which will immediately indicate that change, and the original data is retrieved from the otiginal block. So the hashing concept is a change flagging mechanism. Fig. 5 (a) shows a blockchain node with its block data and Fig. 5 (b) shows several blockchain nodes connected to each other with the hash value propagated from one block to the next.

As cited previously [14], the blockchain was developed on the Ethereum platform. The Proof-of-Stake concept was implemented as a consensus mechanism to replace the traditional Proof-of-Work concept in which all the mining nodes had to solve a cryptographic puzzle to generate a new block. This required a lot of computational power to solve the problem and thus higher electricity consumption, which became a significant cost of processing. Proof-of-Stake, however, acknowledges accounts with a higher priority, or stake, to create a new block without having to solve any puzzles, thus being a faster process at a lower cost.



(a)



(b)

FIGURE 5. Blockchain data structure

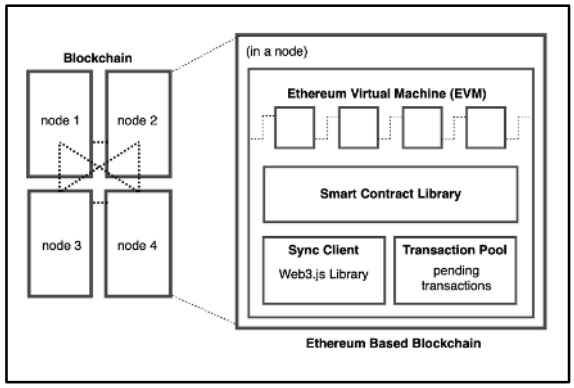


FIGURE 6. Ethereum based blockchain node

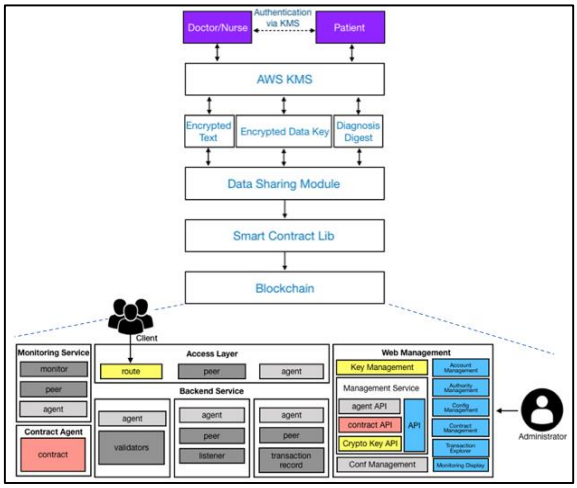


FIGURE 7. The Overall Structure of the Network

The blockchain interface API for connecting and interacting with the Ethereum blockchain was developed using the web3.js library. This library is a JavaScript library that provides multiple functions for interacting with the blockchain. While the nodes of the blockchain could be

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3103443, IEEE Access

deployed on physical servers located at each hospital, in our system we have constructed four blockchain nodes, each deployed on separate servers located at a physically central location.

The Data Layer

At the data layer, the data will be recorded and shared in a consortium blockchain via its block producer node. Based on the blockchain's features, once data has been recorded in the blockchain, it will be immutable forever.

In order to unify the data and have a better authorization mechanism and control of access to the data layer, the application layer manages the authentication and interaction with the data layer by its Data Sharing Module.

The information reader and writer need to interact with the data layer via the application layer. The read and write interfaces in the application layer will be post/get, and the Data Sharing Module will convert them into the data structure required for the blockchain.

The Amazon Web Services (AWS) Key Management Service (KMS) is used to create and manage the encryption of the data. The Master Key that is used to encrypt the Data Key and the encrypted data generated from the Data Center, which will then be stored in the blockchain, never leaves the KMS environment.

The Data Sharing Module

The Data Sharing Module is the interface to control the receipt of the data input from the Application Logic layer as well as controlling the transmission of data sent to the Smart Contract mobile phone app (discussed next).

The Smart Contract library is the template for controlling writing the data into the blockchain and the Ethereum Virtual Machine (EVM) and has an Interpreter compatible with the Solidity language. The blockchain is a full stack of services, including a web service, with access management, a data monitoring service, transaction verification, and block validation.

Smart contact

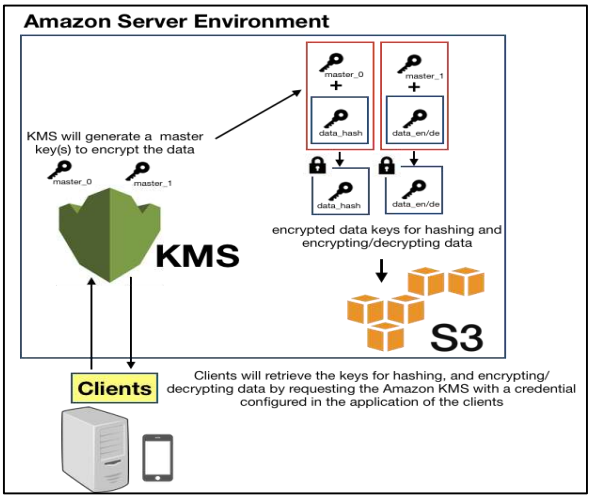
The Smart Contract is a software module for reading data from, and writing data to, the blockchain. The Smart Contract provides information to the mobile device as a 10 record patient information list.

The patient information is structured in 6 parts, which are personal information, visit information, laboratory tests information, drug order information, and a hash value created by the encryption module. The smart contract for our Ethereum blockchain platform is developed with Solidity language.

When the system wants to access patient information for a specific PID, the mapping object will be used to store patient information in the form of a dictionary which requires the PID to access the patient information. For the patient information creation function, the system will check the hash constructed for the new visit and compare it to the hash of the latest existing visit information for the patient. If that hash value exists, the new visit information will not be written in the system storage as that implies the new data is a duplicate.

•Application Programing Interface

The Application Programming Interface (API) is for connecting to and interacting with the blockchain. The API functions can read or write patient data from the mobile application. The API is developed in Node.js, integrated with the Amazon Web Service: Key Management System and Simple Storage Service (AWS KMS and S3), to encrypt 2 keys which are the hash key (salt) used for searching and the encrypt/decrypt key used to encrypt/decrypt patient data retrieved from an HIS. This data is forever encrypted and



cannot be accessed by any means unless specifically authorized to be decrypted with the AWS KMS.

FIGURE 8. The process of storing the hashing and decrypting key

As illustrated in Figure 8, in the system, 2 master keys will be generated from the Amazon Key Management System (Amazon KMS). These keys are stored in the Amazon server with a very high-security system. These keys will be used to encrypt the hashing and encrypting/decrypting of the data keys of our application. The hashing key is used for searching patient information in the blockchain system, and the encrypting/decrypting key is used for encrypting/decrypting the information from the Data Center blockchain for the API Server and the mobile application.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3103443, IEEE Access

Mobile Device Systems

The Mobile Device Systems are for clients (medical personnel) to access patient information from the blockchain. We developed the mobile application using the XCode framework and the Swift language. This application sends requests for data from the blockchain and receives responses via the blockchain API.

FIGURE 9. The Mobile Device App Interfaces

Figure 9(a)-(c) shows the mobile device app screens. 9(a) is the Application home page, 9(b) the patient search screen, and 9(c) is the patient information display. Fig. 9(d) to 9(f) show detailed patient information.

The main menu (Fig. 9(a)) has 2 main tasks which are writing or updating and reading patient information from the blockchain system. The app was tested by running on an iOS iPhone emulator, and the actual iPhone device.

The PID is entered on the top of the mobile application page and searching is performed by pressing the "Search" button. The patient information will be returned in the form of a list object containing information up to the last 10 visits. This limit of 10 was considered sufficient to allow a physician to have all necessary patient history to aid in their diagnosis. Each visit contains information on the visit, laboratory work, diagnoses, drug orders, and other general information. All visits are displayed on one page and a user can scroll through the list, if necessary.

The various information sections are displayed in a form of tabs, but the general information will be displayed in the form of a popup after pressing the "…" button. These are illustrated in Figure 10 which shows the patient information pages.

FIGURE 10. Patient information pages on the mobile device

The visit section information contains the date and time of the visit, the hospital name, symptoms, and the information needed for a diagnosis at a primary level: Chief Complaint (CC), Present Illness (PI), Physical Examination (PE), Blood Pressure (BP), Pulse Rate (PR), Body Weight (BW), Height (HT), Body Temperature (BT), Respiratory Rate (RR), Body Mass Index (BMI), and Oxygen Saturation (O_2Sat). The laboratory information will be displayed if the patient needs to provide a blood sample. The diagnosis is as described by the attending doctor. The drug order covers all medications and drugs prescribed by the doctor. Blood type, and drug allergies are also shown. The general information for each visit, shown in the popup, contains the PID, date of birth, age, address, home telephone number, and mobile phone number, together with the hospital name.

Amazon Key Management System (KMS), and Amazon S3 (Simple Storage Service) provide a stack of security levels which we have integrated into our system, assuring an extremely high level of data and process security.

If the patient information does not exist in the blockchain, the blockchain API will perform the process of writing the patient information from the Data Center where the patient's data is temporarily buffered after being downloaded from the hospitals, and writes that data into the blockchain system. The data is then sent to an appropriate mobile device by the Smart Contract app.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3103443, IEEE Access

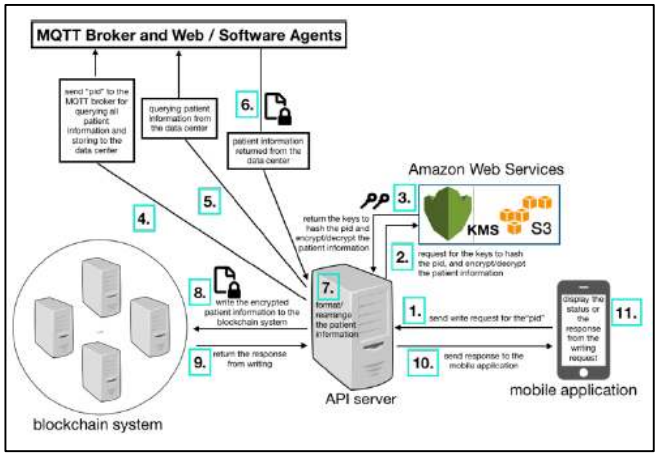


FIGURE 11. The process of writing patient information to the blockchain system via the mobile application

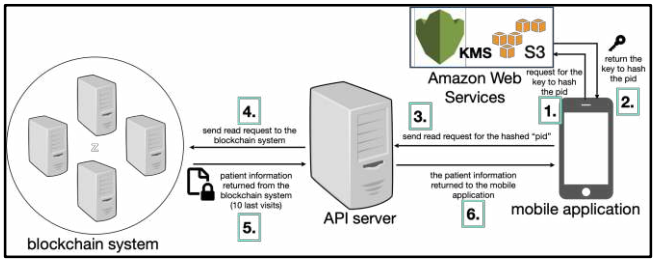


FIGURE 12. Reading patient information from the blockchain system via the mobile application

The data from more than 8,500 patients from the original 157 hospitals that were stored in the blockchain when the system was being tested and verified. (This number had significantly increased from that time with more than 300 hospitals now participating) With that number of patients, and each block in the blockchain containing the information for the 10 most recent visits for the PID, there were 221,269 blocks in the system, and the storage taken are 194GB. The average elapsed time for writing each patient record to the blockchain is about 3.245 seconds per record (visit), or 3.245 s/block. Each block has an average of 0.89MB per block.

For the real-time data, if there is no patient record for a specific PID in the blockchain, the system will retrieve data from all agents to be stored in the data center, which acts as a data buffer, and the data will then be formatted before uploading it to the blockchain. Thus, the patient information is updated as and when required. If the patient information for a specific PID exists, the system will then return the latest 10 visits at most, and a user can also update the patient information in the blockchain system via the mobile application.

Implementation with real case scenario

Currently, an application is used for implementation on those technologies, led by Faculty of Medicine and Faculty of Engineering, Naresuan University. The application is targeted for a mobile application, and the name is NU Medical. Doctors, nurses and medical staffs from 157 hospitals in Thailand are using the application for consultation on patient cases, which mostly are not very urgent cases. The application helps medical staffs in need of consulting a professional, but they are far away apart from the professional such as in rural or remote area.

When the medical staff needs to consult, they need permission to access the patient medical information and patients also need to sign an official document if they want to permit their medical information to be accessed.

The medical information of the patient will be attached to the created case of the staff in order that the doctor/professional can read, and analyze for further diagnosis.

The doctor/professional will respond in the case by writing what should the staff do and choosing drugs to order for the patient if needed. If the staff is not clear with the doctor instruction and do not want to mess with the case too much, they can directly contact the doctor from the application.

A medical staff member searches for a patient's medical information to retrieve the specific medical information for the consulting doctor. This information includes the prior consultation cases in the consult list menu. They can also contact doctors directly for example message chat, phone, or video call, and do some settings about the online/offline status, profile, and login/logout.

FIGURE 13. NU Medical application's home page.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3103443, IEEE Access

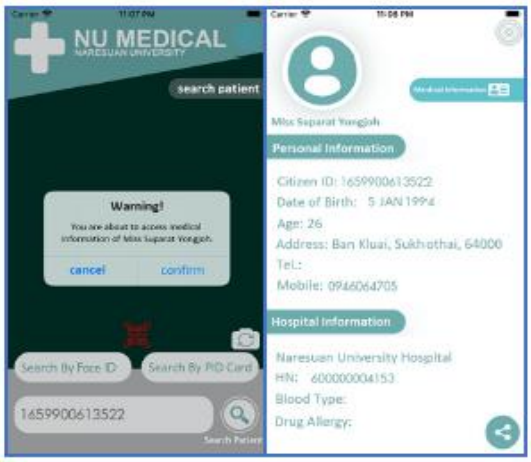


FIGURE 14. NU Medical application's searching and displaying patient information pages

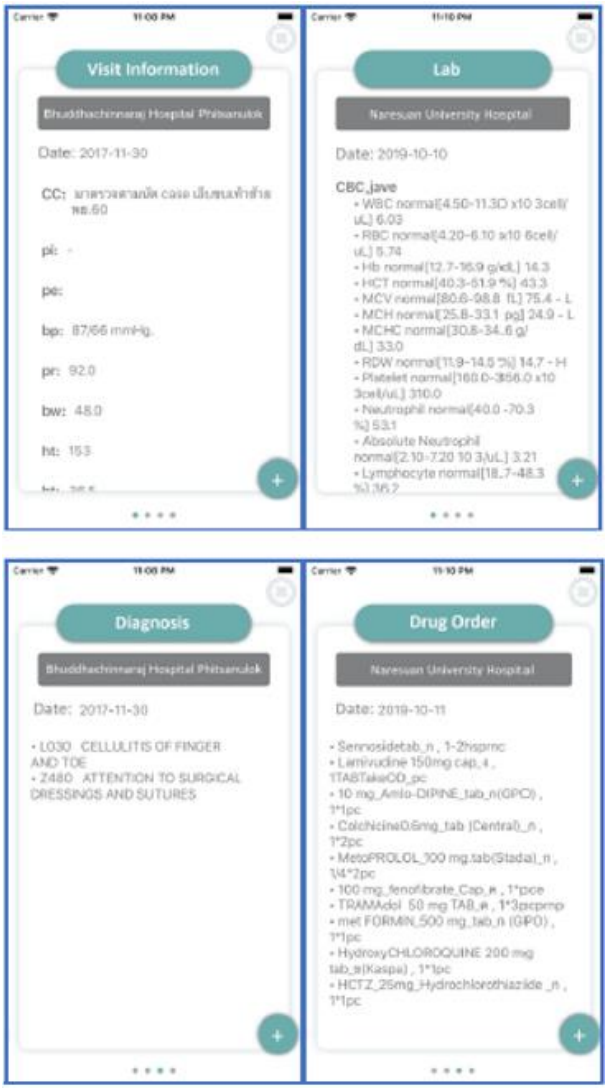


FIGURE 15. More on patient medical information via the Medical Information menu

The staff can search by taking a photo of a patient/ citizen PID card or entering the patient PID directly and if the staff is permitted to search and access the patient information, they will be prompt with the alert for the staff to confirm. The staff needs to accept and confirm the privacy policy. The first page of the search result is the patient general information page and the staff can take a look for more medical information via the Medical Information menu button.

The staff can check the visit, laboratory, diagnosis, and drugs order information for further diagnosis.

TABLE I

CURRENT STATE OF OUR BLOCKCHAIN SYSTEM

Topic	amount
Number of people	8,578
Number of total blocks	221,269
Storage taken (GB)	194
Average elapsed time for writing per 1 block (second)	3.245
Average block size (MB)	0.89

TABLE II

CURRENT STATE OF OUR BLOCKCHAIN SYSTEM INCLUDING WRITING AND READING THE DATA

Topic			amount
Number of people			8,578
Number of total blocks			221,269
Storage taken (GB)			194
API Elapsed Time (in seconds)	Writing	*MQTT	10
		*Retrieving and Formatting data from Data Center	3.089
		*Actual writing to blockchain	0.156 * n
		Handling Request and Response Threads	0.465
	Reading	Actual reading from blockchain	0.401
		Handling Request and Response Threads	0.465

1. For MQTT system, the patient data needs to be queried and retrieved from all hospitals, in order to get all data updated in the data center. For making sure that all data is updated, we set the time for 10 seconds

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3103443, IEEE Access

2. For Retrieving and Formatting data from Data Center, the time is depending on how many visits of that particular patient and the average time is 3.089 seconds
3. For Actual writing to blockchain, the average time to write 1 block is 0.156 second and n is the number of visits for that particular patient.

IV. GENERAL DISCUSSION

Table III shows a comparison between the technology applied in our system and that of related work. This shows the differences in capabilities of each system.

Citations in the comparison include:

[8] formulation of a data-sharing mechanism used by the blockchain-based data sharing among untrusted parties for data security and provenance.

[9] employs Shamir's secret sharing concept where the EHR is divided into multiple segments by a healthcare center, and the segments are distributed to numerous cloud servers. When retrieving the health record, the healthcare center captures segments from partial cloud servers and reconstructs the EHRs.

[11] designed a secure cloud-based EHR system, which guarantees security and privacy of medical data stored in the cloud, relying on cryptographic primitive but not the full trust over cloud servers.

[12] Healthchain, a large-scale health data privacy preserving scheme based on blockchain technology, where health data are encrypted to conduct fine-grained access control.

[13] Permissioned blockchain for storing users' wearable device data via the mobile application synced to the cloud server. The Merkle Tree is adopted to ensure scalability and efficiency. The blockchain also stores data from healthcare providers and health insurance companies. Users (data owners) can control access from the organizations with channeling.

[14] Storing encrypted keywords on Ethereum blockchain for searching their related EHR on the cloud server. The data provider encrypted EHR before storing it on the cloud server. The cloud server will re-encrypt the EHR before sending it to the data requester after getting the patient (data owner) authorization.

[15] proposed a framework developed from Ethereum blockchain with role-based access mechanism integrated with off-chain storage developed from IPFS technology to solve the blockchain scalability problem.

[16] presents an implementation using Ethereum blockchain in a real data sharing scenario on a mobile app with Amazon cloud computing.

TABLE III

COMPARISON BETWEEN OUR BLOCKCHAIN AND RELATED WORK

Metric	[8]	[9]	[11]	[12]	[13]	[14]	[15]	[16]	Our System
Blockchain-based	Y	N	N	Y	Y	Y	Y	Y	Y
Decentralized access	Y	N	N	Y	Y	Y	Y	Y	Y
Mobile Application	N	N	Y	N	Y	N	N	Y	Y
Actual Medical Data	Y	Y	Y	Y	- N/A	- N/A	- N/A	N	Y
Consortium Blockchain Type	Y	- N/A	- N/A	Y	* N	Y	- N/A	Y	Y

1. For the [13], the blockchain type was permissioned blockchain which with some additional configurations was similar to the type of consortium.

From the comparison stated in Table III, the other previous research systems have some limitations. Our system provides more aspects which are consortium blockchain-based, using actual medical data, accessible via the mobile application, and decentralized access.

Below we summarize the contribution of our work to this area of research under the headings Actual Medical Data, Mobile Application, and Decentralized access.

Actual Medical Data

During the development of the blockchain extensions to the NU-MED system, we used real data from 157 hospitals to develop the blockchain system for patient EHR storage. We used real data because we were aware of the real problems of data collection from various sources with its high risk of data error. Collecting the data storage formats of each hospital enabled us to appropriately modify our data collection structure and enabled us to write the data into the blockchain system in a consistent and correct format.

Mobile Application

The Mobile Application is designed to be used by all the parties to a patient visit: the patient, perhaps the triage nurse, and the consulting doctor, all of whom can immediately retrieve patient information via the Mobile Application. Also, patients can do the same independently. This is the flexibility provided by the system for simplifying contacts between patients and hospitals and enables continuity of medical information and continuity of medical service, both highly desirable factors.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3103443, IEEE Access

Decentralized access

Our objective was to provide a decentralized storage structure to ensure the safety and security of patient information. This was achieved by the implementation of the blockchain system with multiple nodes. As indicated above, those blockchain nodes could be both physically and virtually stored at each hospital, but in our system, we have 4 blockchain nodes stored on separate physical servers.

Blockchain Type and Blockchain-based

Our decision to use blockchain technology was based on our perception of the need for a high level of security and safety for medical data, processed with a robust and efficient system that was available to appropriate interested parties on an Anywhere / Anytime / Anydevice basis with inherent safeguards to protect patient privacy. Prior work, such as cited above, demonstrated blockchain technology as a highly secure technology, suitable to meet high-level data storage security requirement, convinced us that a blockchain solution was required. With the consortium blockchain, the data will be distributed to their trust authorities which enables more tamper-proof and also maintains data integrity.

Essential Factors for a Nationwide Roll-out

It is our hope and ambition that this system will one day be rolled out as the nation-wide eHCS in Thailand. This implies the possibility of probably more than 3,000 hospitals and medical centers would be present in the network. We are confident that the technology used in this would be fully able to handle that number of hospitals and ensure fast, error-free communications and data transmission.

However, the technology is only part of the requirements for such a system. Basic factors such as ease of implementation, ease of installation of the web agent, the ease with which the web agent can be configured for a new installation, the ease of providing updates to the web agent software, and the ease with which decisions by any hospital to change their internal patient information system to other hardware or another software package, can be accommodated, must be considered.

For installing the web server, The Raspberry Pi computer-on-a-board with the appropriate software would be installed on systems in smaller hospitals with less IT expertise, and so can be couriered to the hospitals for a simple 'plug-in' action. For larger hospitals with more sophisticated IT configurations and more expert IT personnel, the implementation can be done remotely as a software package installation process. One simplifying factor is that some 60% of hospitals in Thailand run the HosXP package in Linux (CentOS) so the same web agent can be remotely installed on that majority of systems. A further 25% run the JHCIS open source

TABLE IV

USERS' SATISFACTION

Topic	Satisfaction					Total	Mean	SD
	5	4	3	2	1			
1. Designing and Layout of the Graphic User Interface								
1.1 Beautiful and interesting	71	53	18	1	-	623	4.36	0.79
1.2 Clearly to read and use layout	68	54	20	1	-	618	4.32	0.73
1.3 The menu is easy for searching patient information and saving data	63	56	22	2	-	609	4.26	0.76
1.4 User friendly	61	58	21	3	-	606	4.24	0.78
2. Functionalities								
2.1 Login	51	63	27	2	-	592	4.14	0.76
2.2 Reset password and verification	51	67	23	2	-	596	4.17	0.74
2.3 Search for patient information	69	60	13	1	-	626	4.38	0.68
2.4 Consultation on patient cases	63	57	19	3	1	607	4.24	0.77
2.5 Creating group and group chat	49	60	31	3	-	584	4.08	0.80
2.6 Saving notes	48	61	31	3	-	583	4.08	0.79
2.7 Settings	51	59	31	2	-	588	4.11	0.79
3. Utilities								
3.1 Accessing patient history and information	74	48	19	2	-	623	4.36	0.76
3.2 Increasing potential for understanding each patient's situation	67	56	19	1	-	618	4.32	0.73
3.3 Increasing potential in communication between medical personnel	59	60	23	1	-	606	4.24	0.74
3.4 Increasing efficiency in patient treatment	61	55	26	1	-	605	4.23	0.76
3.5 Decreasing tasks from inputting or saving data for consultation	44	58	36	4	1	569	3.98	0.82

The users' evaluation was collected from 143 medical staffs. There were 2 professional physicians, 7 family medicine physicians, 28 nurses from different hospitals, 82 nurses from subdistrict health promotion hospitals, and the other 24 medical staffs.

V. SECURITY ANALYSIS

• Access Control from System Administrators

This can be considered as the very first level of security. All of the participants (medical personnel) have to sign a formal document with the policy for registering in the system. The administrators take care of the registration process. They check through each individual and each participant has to be with the administrators throughout the process of registration. This ensures only authenticated participants can join the system.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3103443, IEEE Access

• Privacy of Data

The medical personnel needs permission to access patient data and patients have to sign an official document if they want to authenticate them to access their data.

Also with the help of the smart contract, only authenticated users can access the data on the blockchain. All transactions will be checked or validated. If there is an invalid or malicious transaction from unknown sources or any third parties, the system will reject this transaction and not perform any further processes. Furthermore, no one can change the smart contract stored in the EVM within the decentralized network.

• Confidentiality of Data

There is no plaintext of patient data on the blockchain. All the patient data is stored in encrypted form and never leaves the blockchain system without still encrypted. The algorithm for encryption is AES256. The data key for encryption/decryption is stored in the AWS KMS with S3. This increases the security levels of the system.

• Managing Cryptographic Keys with AWS KMS and S3

The data key is stored in the AWS KMS along with the S3. Those services are governed by hardware security modules validated under the Federal Information Processing Standard (FIP) 140-2. The key is stored securely in the AWS environment and can only be accessed by the AWS credentials. The key is also trackable on its usage.

• Integrity of Data

The patient data needs to always be intact throughout the decentralized system. Data Integrity is one of the blockchain characteristics due to its data structure with the hash algorithm that creates all blocks cryptographically linked and its distributed peer-to-peer network of nodes and consensus mechanism to maintain the data integrity.

• Secure Searching

The primary key for searching patient information from the blockchain is stored in a cryptographic hash form. The personnel who performs searching only knows the original value of a patient's PID. The salt key is also combined with the PID to make the resulting hash value to be more complex and unpredictable because the hash(PID) is already extremely complex and if the salt is added, the hash(PID+salt) will be even more complex. The salt key is also stored securely in the AWS KMS. The hash makes the patient data unidentifiable. This combination of unidentifiable data and encryption of the data increases the complexity and security levels.

VI. CONCLUSION

In our system, the Internet of Health Care System integrating with the blockchain concept and implementation have been proposed in order to tackle problems that come with centralized storage and for securely sharing patient data among participating hospitals in the network. There are 3 primary factors that need to be considered for the development. First, data transmission and processing must be secure at the highest level along with data storage. Second, the variety of different internal hospital patient information systems must be supported by our proposed system. Third, our system must efficiently cater for a large number of participants in the network.

The Central Server has been designed for storing patient information as a buffer before sending it to the blockchain via the Application Programming Interface (API). For each participating hospital, we have an agent installed in order to retrieve patient data from their internal hospital information system. Message Queueing Telemetry Transport protocol (MQTT) is adopted for communication between machines (internal hospital information systems and agents). The blockchain has been developed on Ethereum platform with the Proof-of-Stake as the consensus mechanism. The blockchain is for storing encrypted 10 recent records of patient information for each patient. The blockchain smart contract has been developed in Solidity language to ensure that only authenticate medical personnel can access the data on the blockchain. The smart contract can be interacted via the API with help from web3.js JavaScript library. The Amazon Web Service: Key Management System (AWS KMS) is adopted for storing data key and salt key for data encryption and indexing. Only authenticated users can access these keys via AWS credentials. The mobile application has been developed for medical personnel to access patient data for diagnosing and performing a further treatment.

From comparison with some related works and users' evaluation in the GENERAL DISCUSSION section, our proposed system provides more functionalities due to some previous research limitations. From the SECURITY ANALYSIS section, our system has achieved the first factor of the 3 primary factors that need to be concerned for the development which is about the security of data transmission and processing with the data storage. For the second and the third factors, an agent installed for each hospital has been configured to support available internal hospital patient information systems and our developed system can handle a large number of participants in the network with the help of MQTT protocol.

Furthermore, EHRs have increasingly replaced the traditional method of storing patient information which relied on paper-based records stored locally at the health provider's premises. Information retrieval was challenging, prone to data loss, often insecure with no backup data in the case of loss, and subject to long-term storage issues such as physical deterioration and physical damage.

In our system, the patient information is maintained in electronic form, secured in the blockchain, which can be accessed on mobile devices and can be shared among the hospitals. In the development activity enhancing our eHCS, the EHRs for 8,578 patients were received from 157 hospitals using Message Queueing Telemetry Transport or MQTT protocol: the completed system has been installed at 350 hospitals at the time of writing.

The technology was integrated with the mobile application to enable easier access to the patient information. offering simple and fast searching on an Anytime / Anywhere / Anydevice basis by the patient or authorized hospital staff. In addition, Key Management Service (KMS) from Amazon Web Services (AWS) was used for securing the search through the mobile application.

The blockchain technology, has overcome the challenges faced in eHCSs found in other published systems. As stated in the Introduction, these challenges were, first, that medical records have a special status requiring confidentiality, privacy protection and secure storage and handling. The second major factor was the system requirement of being a high-speed, ultra-efficient processing system with universal networking connectivity. Thirdly, a way needed to be found to enable the diverse hospital patient information systems to appear to have a single, canonical network interface for data accessing and updating.

We are confident that all three challenges have been met by our use of imaginative, State-of-the-Art contemporary blockchain and internet communications technology and, when called upon in the future, would perform efficiently as a nationwide integrated health care system, which we have terms an Internet of Health Care Systems (IoHCS). We are equally confident that the system is ready to be rolled out even nationwide technically and with great ease of installation in the potentially thousands of hospitals and medical centers that that implies.

REFERENCES

[1] World Health Organization (WHO) (2012), Management of patient information: Trends and challenges in Member States, Available at

https://apps.who.int/iris/bitstream/handle/10665/76794/9789241504645_eng.pdf?sequence=1

[2] Thai Government Ministry of Public Health (2017) e-Health Strategy 2017-2026,

eHealth_Strategy_ENG_141117.pdf, *ehealth.moph.go.th*

[3] Sirilak, Sirikasem and Paisarn Maneesawang (2018), A New Procedure for Advancing Telemedicine Using the HoloLens, IEEE Access, Vol. 6, pp. 60224 – 60233, October, 2018

[4] Maneesawang, Paisarn and Roy I. Morien (2019), Applying Augmented Reality to Telemedicine in Thailand, using the HoloLens, KSII The 14th Asia Pacific International Conference on Information Science and Technology(APIC-IST), Beijing, China, 2019.

[5] Thongsanik, Songsak and Roy I. Morien (2019) The Doctor Knows You": A Telemedicine System to bring medical services to rural and remote villages in Thailand, KSII The 11th International Conference on Internet (ICONI), Hanoi, December 2019

[6] Nakamoto, Satoshi (2008), Bitcoin: A Peer-to-Peer Electronic Cash System, Available at https://bitcoin.org/bitcoin.pdf

[7] Yang Yilong, Li Xiaoshan, Nafees Qamar, Liu Peng, Ke Wei, Shen Bingqing (2018), MedShare: Medical Resource Sharing among Autonomous Healthcare Providers, Available at

https://www.researchgate.net/publication/327027574_MedShare_A_Novel_Hybrid_Cloud_for_Medical_Resource_Sharing_among_Autonomous_Healthcare_Providers

[8] Xia, Q. I., Sifah, E. B., Asamoah, K. O., Gao, J., Du, X., & Guizani, M. (2017). MeDShare: Trust-less medical data sharing among cloud service providers via blockchain. IEEE Access, 5, 14757-14767.

[9] H Zhang, J Yu, C Tian, P Zhao, G Xu, J Lin (2018), Cloud storage for electronic health records based on secret sharing with verifiable reconstruction outsourcing, IEEE Access 6, 40713-40722

[10] Vault12 (2018), Understanding Shamir's Secret Sharing, Available at https://medium.com/vault12/understanding-shamirs-secret-sharing-6a4bd27768c9

[11] Xhafa, F., Li, J., Zhao, G., Li, J., Chen, X., & Wong, D. S. (2015). Designing cloud-based electronic health record system with attribute-based encryption. Multimedia Tools and Applications, 74(10), 3441-3458.

[12] Xu, J., Xue, K., Li, S., Tian, H., Hong, J., Hong, P., & Yu, N. (2019). Healthchain: A Blockchain-Based Privacy Preserving Scheme for Large-Scale Health Data. IEEE Internet of Things Journal, 6(5), 8770-8781

[13] Liang, X., Zhao, J., Shetty, S., Liu, J., & Li, D. (2017, October). Integrating blockchain for data sharing and collaboration in mobile healthcare applications. In 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC) (pp. 1-5). IEEE.

[14] Y. Wang, A. Zhang, P. Zhang and H. Wang, "Cloud-Assisted EHR Sharing With Security and Privacy Preservation via Consortium Blockchain," in IEEE Access, vol. 7, pp. 136704-136719, 2019, doi: 10.1109/ACCESS.2019.2943153.

[15] A. Shahnaz, U. Qamar and A. Khalid, "Using Blockchain for Electronic Health Records," in IEEE Access, vol. 7, pp. 147782-147795, 2019, doi: 10.1109/ACCESS.2019.2946373.

[16] Nguyen, D. C., Pathirana, P. N., Ding, M., & Seneviratne, A. (2019). Blockchain for secure EHRs sharing of mobile cloud-based e-Health systems. IEEE access, 7, 66792-66806.

Paisarn Muneesawang (M'14–SM'14) received the B.Eng. degree in Electrical Engineering from the Mahanakorn University of Technology, Bangkok, Thailand, in 1996, and subsequently the M.Eng.Sci. Degree in Electrical Engineering from the University of New South Wales, Sydney, NSW, Australia, in 1999, and the Ph.D. Degree from the School of Electrical and Information Engineering, University of Sydney, Sydney, NSW, Australia. He was a Post-Doctoral Research Fellow with Ryerson University, Toronto, ON, Canada, from 2003 to 2004, and an Assistant Professor with the College of Information Technology, University of United Arab Emirates, Al Ain, United Arab Emirates, from 2005 to 2006. He has been a Visiting Professor with Nanyang Technological University, Singapore, since 2012, and Ryerson University, Toronto, since 2013. He was the Vice President of Administrative Affairs, Naresuan University, Phitsanulok, Thailand, where he is currently a Professor and the Dean of the Graduate School. He has co-authored Multimedia Database Retrieval: A Human-Centered Approach (Springer, 2006), and Unsupervised Learning—A Dynamic Approach (Wiley–IEEE Press, 2013), and Multimedia Database Retrieval: Technologies and Applications (Springer, 2014), and also co-edited Advances in Multimedia Information Processing-PCM 2009 (Springer, 2009) and Visual Inspection Technology in the Hard Disk Drive Industry (Wiley–ISTE, 2015). His current research interests include multimedia signal processing, computer vision, and machine learning. He has served as the Registration Co-Chair for the International Conference on Multimedia and Expo 2006. He was the Technical Program Co-Chair of the Pacific-Rim Conference on Multimedia 2009.

Chakchai So-In (SM'14) is currently an Associate Professor in the Department of Computer Science at Khon Kaen University, Thailand. He received the Ph.D. degree in Computer Engineering from Washington University in St. Louis, USA, in 2010. He was an Intern at CNAP/NTU (NTU, SG), Cisco Systems, WiMAX Forum, and Bell Labs (Alcatel Lucent) (USA). His research interests include computer networking and the Internet, wireless and mobile networking, wireless and sensor networks, Internet of Things, and Cyber Security. He has served as an Editor member IEEE Access, PeeJ (Computer Science), PLOW ONE, and ECTI-CIT, and a Committee Member for conferences/journals, such as Globecom, ICC, VTC, WCNC, ICNP, the IEEE TRANSACTIONS WIRELESS COMMUNICATIONS, the IEEE TRANSACTIONS ON COMPUTERS, the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, the IEEE TRANSACTIONS ON MOBILE COMPUTING, the IEEE TRANSACTIONS ON INFORMATION FORENSICSAND SECURITY, the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, the IEEE Communications/Network Magazine, and the IEEE Communications Letters. He has authored 10 books and has 100 international publications in the IEEE JSAC, Communications Magazine, Wireless Communications Magazine, Android Application Development, and Computer Networks and Security, Mobile and Wireless Networking Labs. He is a Senior Member of the ACM.

Suparat Yongjoh received the B.Eng. degree in Computer Engineering in 2016 from Narasuan University, Phitsanulok, Thailand. He is studying in studying in a Ph.D. program in Computer Engineering from Narasuan University. He has experienced in mobile application development. He is interested in the integration of IoT and Blockchain, Augmented Reality, Virtual Reality, and Mixed Reality, A.I., and Game Development.

Peerapol Kompunt received the B.S. degree in Industrial Computing from Pibulsongkram Rajabhat University, in 2018. She is studying in a Ph.D. program in Computer Engineering from Narasuan University, Phitsanulok, Thailand. His research interests include computer vision, image processing and machine learning. She has experience in hard disk dive inspection with Western Digital (Thailand) Co. Ltd. She has published at 3 national conferences and has 2 articles in Thai Journal Citation Index Centre.

Mr. Roy I. Morien is currently an English Language Specialist, Academic Editor and Language Teacher in the Naresuan University Graduate School. He has a M. Information Systems (with Distinction), a Post-Graduate Diploma (Information Systems) and two Undergraduate Degrees in Business (Corporate Law and Corporate Administration, and Management and Accounting). He has had more than 25 years' experience as a Teaching Academic in the areas of Computer Science, Business Computing and Information Technology, teaching Database Development, Programming, Systems Analysis and Design, and Software Project Management, usually from an Agile Development / Agile Programming perspective, and extensive system consulting experience. He is an Australian who has taught extensively in Australia, Singapore, Jakarta and Hong Kong, as well as in Thailand since 2006. Roy has presented at over 40 international conferences and has published 8 articles in international journals, 2 book chapters, a textbook on Programming, and an unpublished textbook on Agile Database Development.

BIBLIOGRAPHY

[1] Zhang, P., Walker, M. A., White, J., Schmidt, D. C., & Lenz, G. (2017, October). Metrics for assessing blockchain-based healthcare decentralized apps. In 2017 IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom) (pp. 1-4). IEEE.

[2] Park, Y. R., Lee, E., Na, W., Park, S., Lee, Y., & Lee, J. H. (2019). Is blockchain technology suitable for managing personal health records? Mixed-methods study to test feasibility. Journal of Medical Internet Research, 21(2), e12533.

[3] Zhao, H., Bai, P., Peng, Y., & Xu, R. (2018). Efficient key management scheme for health blockchain. CAAI Transactions on Intelligence Technology, 3(2), 114-118.

[4] Talukder, A. K., Chaitanya, M., Arnold, D., & Sakurai, K. (2018, October). Proof of disease: A blockchain consensus protocol for accurate medical decisions and reducing the disease burden. In 2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI) (pp. 257-262). IEEE.

[5] Tang, F., Ma, S., Xiang, Y., & Lin, C. (2019). An efficient authentication scheme for blockchain-based electronic health records. IEEE access, 7, 41678-41689.

[6] Jin, H., Luo, Y., Li, P., & Mathew, J. (2019). A review of secure and privacy-preserving medical data sharing. IEEE Access, 7, 61656-61669.

[7] [8] Wang, S., Zhang, D., & Zhang, Y. (2019). Blockchain-Based Personal Health Records Sharing Scheme with Data Integrity Verifiable. IEEE Access, 7, 102887-102901.

[9] Liu, X., Wang, Z., Jin, C., Li, F., & Li, G. (2019). A Blockchain-Based Medical Data Sharing and Protection Scheme. IEEE Access, 7, 118943-118953.

[10] Wang, Y., Zhang, A., Zhang, P., & Wang, H. (2019). Cloud-Assisted EHR Sharing with Security and Privacy Preservation via Consortium Blockchain. IEEE Access, 7, 136704-136719.

[11] Shahnaz, A., Qamar, U., & Khalid, A. (2019). Using Blockchain for Electronic Health Records. IEEE Access, 7, 147782-147795.

[12] Ismail, L., Materwala, H., & Zeadally, S. (2019). Lightweight Blockchain for Healthcare. IEEE Access, 7, 149935-149951.

[13] Daraghmi, E. Y., Daraghmi, Y. A., & Yuan, S. M. (2019). MedChain: A Design of Blockchain-Based System for Medical Records Access and Permissions Management. IEEE Access, 7, 164595-164613.

[14] Patel, V. (2019). A framework for secure and decentralized sharing of medical imaging data via blockchain consensus. Health Informatics Journal, 25(4), 1398-1411.

[15] Hylock, R. H., & Zeng, X. (2019). A Blockchain Framework for Patient-Centered Health Records and Exchange (HealthChain): Evaluation and Proof-of-Concept Study. Journal of Medical Internet Research, 21(8), e13592.

[16]Angraal, S., Krumholz, H. M., & Schulz, W. L. (2017). Blockchain technology: applications in health care. Circulation: Cardiovascular Quality and Outcomes, 10(9), e003800.

[17] Jamil, F., Hang, L., Kim, K., & Kim, D. (2019). A Novel Medical Blockchain Model for Drug Supply Chain Integrity Management in a Smart Hospital. Electronics, 8(5), 505.

[18] Kuo, T. T., Kim, H. E., & Ohno-Machado, L. (2017). Blockchain distributed ledger technologies for biomedical and health care applications. Journal of the American Medical Informatics Association, 24(6), 1211-1220.

[19] Fan, K., Wang, S., Ren, Y., Li, H., & Yang, Y. (2018). Medblock: Efficient and secure medical data sharing via blockchain. Journal of Medical Systems, 42(8), 136.

[20] Shabani, M. (2019). Blockchain-based platforms for genomic data sharing: a de-centralized approach in response to the governance problems? Journal of the American Medical Informatics Association, 26(1), 76-80.

[21] Kuo, T. T., Zavaleta Rojas, H., & Ohno-Machado, L. (2019). Comparison of blockchain platforms: a systematic review and healthcare examples. Journal of the American Medical Informatics Association, 26(5), 462-478.

[22] Johnson, M., Jones, M., Shervey, M., Dudley, J. T., & Zimmerman, N. (2019). Building a Secure Biomedical Data Sharing Decentralized App (DApp): Tutorial. Journal of Medical Internet Research, 21(10), e13601.

[23] Latifi, S., Zhang, Y., & Cheng, L. C. (2019, July). Blockchain-Based Real Estate Market: One Method for Applying Blockchain Technology in Commercial Real Estate Market. In 2019 IEEE International Conference on Blockchain (Blockchain) (pp. 528-535). IEEE.

[24] Eung Seon Kang, Seung Jae Pee, Jae Geun Song, Ju Wook Jang (2018), A Blockchain-Based Energy Trading Platform for Smart Homes in a Microgrid, 3rd International Conference on Computer and Communication Systems (ICCCS)

[25] Maslove, D. M., Klein, J., Brohman, K., & Martin, P. (2018). Using blockchain technology to manage clinical trials data: a proof-of-concept study. JMIR Medical Informatics, 6(4), e11949.

[26] Sylim, P., Liu, F., Marcelo, A., & Fontelo, P. (2018). Blockchain technology for detecting falsified and substandard drugs in distribution: pharmaceutical supply chain intervention. JMIR Research Protocols, 7(9), e10163