2020 International Conference on Computational Science and Computational Intelligence (CSCI) | 978-1-7281-7624-6/20/$31.00 ©2020 IEEE | DOI: 10.1109/CSCI51800.2020.00161

Health Record Chain (HRC): Implementation of Mobile Healthcare system using Blockchain to enhance Privacy of Electronic Health Record EHR.

Arij Alfaidi
Department of Computer Science
University of Colorado at Colorado Springs
Colorado Springs, USA
aalfaidi@uccs.edu

Edward Chow
Department of Computer Science
University of Colorado at Colorado Springs
Colorado Springs, USA
cchow@uccs.edu

Abstract— Mobile health applications connect to wearable devices with inbuilt sensors to monitor critical human body parameters such as heart rate, pulse rate, body temperatures ,and others. This paper will introduce our system, Health Record Chain HRC, to investigate how to design and implement secure mobile health systems that leverage the smart mobile devices' new authentication and geo-location mechanism. HRC introduces an enhancing framework to ensure the users' security and privacy and conform to the related regulations (General Data Protection Regulation GDPR, Health Insurance Portability and Accountability Act HIPPA) using blockchain. The immutability of blockchain conflicts with GDPR' "Right to be forgotten" when the user can delete all of his/her data. This work implements a blockchain system with a mobile application and a web interface to address this conflict by hashing the Electronic health record EHR to Ethereum based blockchain.

Keywords- Mobile health application, Electronic Health Record EHR, Blockchain, Ethereum, Privacy.

I. INTRODUCTION

In the contemporary context, it has become increasingly essential for health providers to integrate mobile applications into their health care delivery systems to enhance the quality of care. Mobile healthcare (mHealth) is instrumental in enhancing access to care, monitoring, and tracking patients' health status in real-time [1]. It also enhances health information sharing between providers, patients, practitioners, and other stakeholders involved in patient well-being. Notably, health information collection using mHealth tools can be vital in providing essential insights that indicate the causes of diseases and inform the selection of appropriate health interventions. Although the emergence of mHealth to support care delivery is admittedly revolutionary, it is wrought with privacy and security issues regarding patient health information. Since mHealth apps rely on information technology (IT) solutions, cybercriminals can target them through exploitable vulnerabilities with the intent of extracting health information for malicious purposes [7]. Health providers should assess the privacy and security risks mHealth apps pose before selecting appropriate health applications. In this way, they can develop robust systems to detect, prevent, and mitigate unauthorized individuals' attacks, which exploit loopholes to gain access to confidential patient information [10]. This paper introduces a mobile Healthcare system using blockchain and discusses a solution to give the patient the Right to be forgotten using off-chain storage of the EHR encrypted data.

II. PREVIOUS WORK

We are aware of two endeavors ostensibly engaged with clinical records on the blockchain, strikingly Factom [6] and Med-Vault [4]. Both cannot seem to distribute explicit techniques or an outline of specialized work. Supposedly, we are the first to present an efficient model, applying blockchain innovation to mobile applications.
Zyskind et al. have shown the utilization of blockchain conventions for consent to the executives. They

978-1-7281-7624-6/20/$31.00 ©2020 IEEE
DOI 10.1109/CSCI51800.2020.00161

actualize a believed daze escrow administration, putting away encoded information while logging pointers on the blockchain [7]. Kish proposed the blockchain for essential theoretical administration in a clinical setting [9]. We expand on these thoughts and create unique work in disseminated record recovery, keen agreement permission plans, information sharing, and the financial matters of data flexibly and request using blockchain mining.

Azaria and Asaph, in their work "MedRec," [3] implemented a blockchain system, which is Ethereum-based, that links global patient identities to records held by providers. Their work was supported by MIT Digital Currency Initiative and the MIT Media Lab Consortium. They were the first blockchain-based system with many smart contracts to define patient data and patient-provider relationships. We follow their experience in mining in our system, and we will leave it for further investigation. In the following section, we present the design and implementation of our system HRC.

III. BLOCKCHAIN

The blockchain paradigm's role has evolved from keeping a financial ledger to include a generalized framework by which decentralized computer resources can be implemented. Every computer resource could be considered a single state-machine with the ability to transition between multiple states through cryptographically-secured transactions[5]. The nodes effectively encode consensus during the production of the new state-machine. In this case, the consensus is responsible for defining the valid state transition before uploading it to the blockchain. After that, the blocks create numerous valid transactions in succession, provided there is an incremental execution with the state from the preceding block, thus transforming the state-machine into a more current state.

With the underlying peer-to-peer protocol, the proof of work consensus is responsible for securing the state machine's condition and preventing logic tempering. Besides, the protocol and consensus share the information with relevant nodes within the system. Therefore, nodes can pose queries for the state-machines and obtain acceptable results, which are utilized by the whole network with a significant level of certainty[7]. In the end, the general categorization of the blockchain by the transaction-based state-machine is traditionally viewed as a Smart contract. Ethereum became the first to implement the smart contract idea in blockchain fully. In general, the idea involves developing Turing-complete instruction within the blockchain, which facilitates smart contracts programming and has a sufficient capacity for storing the on-chain state. Accordingly, its hugely flexible programming language is considered vital in general EHR management practices[11]. The blockchain's flexibility component encourages advanced functionality, part of multiparty arbitration and bidding, to be coded on the suggested system. This results in the systems conforming to the stakeholders' different needs and the variations in regulatory laws.

IV. CONSORTIUM BLOCKCHAIN

These are blockchains whose consensus is managed by preselected sets of trusted nodes. After a consensus has been reached, a node is added to the chain, and the transaction is validated by a group that is part of the preselected nodes. For instance, in the presence of five trusted or unknown nodes on the chain, the processing or addition of any block on the chain would require at least three entities to corroborate the validation before it can be appended onto the chain. In this case, the right to reach the blockchain can be restricted to selected participants or made public. Besides, consortium blockchains are perceived to be partially-centralized, hence different from private blockchains [2]. Our HRC system uses this type of blockchain since the EHR data need more than one node to be authorized and handle the editing and deleting of EHR. Figure 1 shows how we can use consortium blockchain in the mHealth system when a node wants to add a record as in step 1. It is needed to have all the authorized nodes in the Health system ex(clinic node, insurance node, and Health provider node) as in step 2. When these nodes validate the new block, it can be added to the blockchain as in step 3.

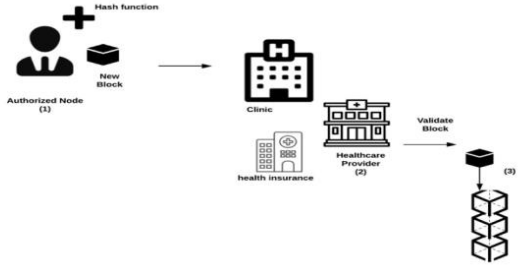

Figure 1. Consortium blockchain in Healthcare system

V. System Implementation

We structure the segments of our framework node to incorporate with the existing Electronic medical record EMR foundation. We expect that numerous nodes, specifically care suppliers, trust-completely external databases with tolerant information, put away workers with organized availability. Our structure presents the following programming segments: Ethereum Client, Backend Library, Database Gatekeeper, and EHR Manager. We give a model usage of these segments that coordinates with the SQLite database and is managed through our web doctor interface and a patient mobile application connected to a wearable device to measure the patient's health data. Ethereum explicit Web3 API of the JSON RPC to make connection possible to mobile applications implemented in Swift XCode.

We implemented a smart contract for every user that will be registered in the system. This smart contract will hold the user information with Ether address. When this contract "Authorization Contract" is implemented, it will make the user's EHR data saved securely in the external database DB. This Ether address will be hashed to this user data that will be saved to the external DB. We used the ABE-encryption method to encrypt the user data in the DB. In this case, the user can edit and delete his data when he requests that. Figure 2 shows the general architecture of our system number 1; when the user registers, the webserver will send it to the W3 node server that communicates with blockchain to create Ether (wallet) address for the user. This will give the user a hash address to encrypt his/her data. This hash address will be the public key to encrypt/decrypt data before saving DB data. Numbers 2 and 3 in the graph will show how the system will create this wallet address for the user, and it will be sent to the webserver to allow registering the user shown in number 4 in the graph. Number 5 shows gathering health data from Apple watch to help making a history of health data for the user to check. After gathering the data, it will be sent to the doctor's website to make the graph's diagnosis shown in number 6. After the doctor makes the diagnosis, it will be sent to the health app to accept adding it or reject it. The user can delete and edit his/her EHR data, shown in number 7 in the graph. If the user accepts adding the health data to history, it will be sent to the webserver, shown in number 8 in the graph. These data will add to the DB encrypted by a hash address, shown in number 9 in the graph.

The user will have the ability to control who will see his/her data by choosing the doctor or health provider to communicate with. If there is any new diagnosis, the user will be notified, and if he/she accepts, this diagnosis will be saved to health record; otherwise, not. The user can sign out from the system. In this case, all health data will be erased. Figure 3 shows the mobile application interface.
The doctor web implemented in HTML, where the doctor can log in to the web page, and the notification will be shown. Doctor can accept/ reject new patient. The doctor can add diagnosis and send it to the user for approval. Doctor web page is shown in Figure 4.

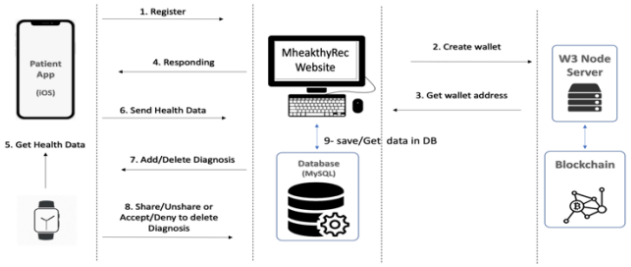

Figure 2. HRC system Architecture

VI. Discussion

Our HRC implementation improved data quality and quantity for medical research by encouraging the developer to use blockchain in the mHealth system. HRC will save the medical data off-chain from addressing blockchain's scalability issue at the same time to save the user right of privacy. GDPR gives the patient the Right to remove all his/her medical records, so when saving data off-chain, we can remove the hash value, and the wallet address will be discarded. The patient controls his/her EHR data, the patient will know where it will be saved and who will have access to it, and he/she has to permit to update the data. At the same time, the patient will have the medical care needed and communicate with health providers at any time. Our interface on the mobile application is easy to use, and the buttons are precise and efficient.

Figure 3. HRC Mobile Application interface

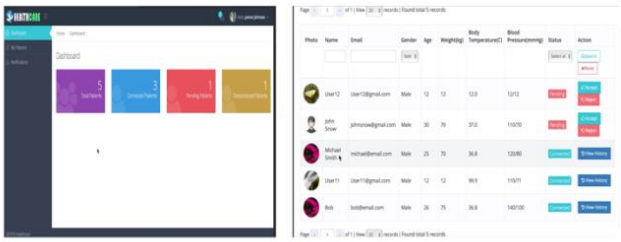

Figure4. HRC Doctor Web interface

Ethereum's exchanges require Ether, a system cash unit, to be prepared by the system. Ether can be earned by mining, granting an adequate measure to a node that solves the computational puzzle. Therefore, care suppliers are boosted to take an interest in mining to support the continuation of their services. In like manner, when patients wish to share their data, they will be required to spend Ether or host the goal get-together reserve them. Giving patients Ether or having them pay for it tends to be controlled by healthcare provider system owners.

VII. Conclusion and Future Work

The use of blockchain technology is instrumental in enhancing the security and privacy of multi-user mHealth applications. Integrating blockchain can allow providers to improve data security and enhance their ability to offer quality care. However, it warrants further research to identify appropriate blockchain technologies that can augment mHealth-based services. HRC is a novel healthcare system that uses mobile applications and wearable devices. It is a blockchain system that gives the patients control of their health data while satisfying the right to be forgotten GDPR's.

We will include our HRC system's installation and configuration steps and deposit it to a GitHub site for broader distribution to have a broader impact. Through this effort, we hope to improve the future mobile healthcare system. We will create a set of representative operational scenarios as a benchmark for evaluating the performance of the prototype system we have developed.

Our next step will be to integrate a redactable blockchain to manage the user health data and requests. We will investigate using a chameleon hash function to make the edit and delete possible inside the blockchain. The impact factors for using redactable blockchain in such mHealth systems will be evaluated in further work.

References

1. Arora, Shifali, Jennifer Yttri, and Wendy Nilsen. "Privacy And Security In Mobile Health (mHealth) Research." Alcohol Research: Current Reviews, vol. 36, no.1, 2014, pp. 143

2. Ateniese, Giuseppe, et al. "Redactable blockchain–or–rewriting history in bitcoin and friends." 2017 IEEE European Symposium on Security and Privacy (EuroS&P). IEEE, 2017.

3. Azaria, Asaph, et al. "Medrec: Using blockchain for medical data access and permission management." *2016 2nd International Conference on Open and Big Data (OBD)*. IEEE, 2016.

4. CoinDesk, "Medical records project wins top prize at blockchain hackathon," 2015. [Online]. Available: \url{http: //www.coindesk.com}

5. Esposito, Christian, et al. "Blockchain: A panacea for healthcare cloud-based data security and privacy?." IEEE Cloud Computing 5.1 (2018): 31-37.

6. Factom, "Healthnautica + factom announce partnership," 2015. [Online]. Available: \url{http://blog.factom.org}

7. G. Zyskind *et al.*, "Decentralizing privacy: Using blockchain to protect personal data," in *Security and Privacy Workshops (SPW), 2015 IEEE*. IEEE, 2015, pp. 180–184.

8. G. Zyskind *et al.*, "Decentralizing privacy: Using blockchain to protect personal data," in *Secure Privacy Workshops (SPW), 2015 IEEE*. IEEE, 2015, pp. 180–184.

9. L. J. Kish and E. J. Topol, "Unpatients– why patients should own their medical data," *Nature biotechnology*, vol. 33, no. 9, pp. 921–924, 2015.

10. Latif, Siddique, et al. "Mobile health in the developing world: Review of literature and lessons from a case study." IEEE Access 5 (2017): 11540-11556.

11. Lin, Iuon-Chang, and Tzu-Chun Liao. "A Survey of Blockchain Security Issues and Challenges." IJ Network Security, vol. 19, no. 5, 2017, pp. 653-659.