ISBN 978-981-14-4787-7
Proceedings of 2020 the 10th International Workshop on Computer Science and Engineering (WCSE 2020)
Yangon (Rangoon), Myanmar (Burma), February 26- February 28, 2020, pp. 156-161
doi: 10.18178/wcse.2020.02.027

Secure Healthcare System using Blockchain Technology

HtweHtwePyone[+], KhinThan Mya

Faculty of Computer Science, University of Computer Studies (Myitkyina), Myanmar
Faculty of Computer Systems and Technologies, University of Computer Studies (Yangon), Myanmar

Abstract: Due to the popularity of crypto currencies, blockchain technology has gotten valuable for various areas. In the healthcare domain, blockchain became a key component that can drive information streams as significant and adaptable enough to enable continuous secure human services framework. So, this system is proposed as the secure healthcare system by using blockchain technology. To reduce the redundancy from each block of health data, this system proposes the modified mutual information (MMI) method as the contribution. MMI method identifies the quality of relationships between features of various natures without dispersion law limitation. And then, this system uses MD-5 (message-digest-5) hash algorithm for the hash value. Each block with hash value is transmitted through the blockchain. So, this system allows the healthcare providers to easily and securely share health data.

Key Words: Health data, Blockchain, MMI, Hash.

1. Introduction

Today, the premium and advancement of blockchain technology has been driven by the gigantic worth development of crypto-currencies and large investments of venture capital in blockchain start-ups. Crypto-currency is one of the uses of blokchain technology. There are three concepts about crypto-currency. These are blockchain, protocol and currency. In crypto-currency, the blockchain go about as a dispersed record that stores all the performed transactions. In a blockchain, new blocks are added over time. Some of blockchain's potential uses beyond crypto-currency, including for government application, healthcare, identity management and the music industry.

Blockchain can push forward the development of patient-driven medicinal services model. In this model, patients control their healthcare information. Information sharing in both patient-driven and customary models faces the absence of trust and absence of impetuses to share. For sharing data, blockchain can take care of these two issues by going about as a trust layer and presenting the motivating force instruments, for example, remunerating crypto tokens.

The proposed system aims to develop a secure healthcare system by reducing the effect of redundancy within data preprocessing stage. This system can not only reduce the irrelevant and redundant data but also decline the quantity of collinearity issues inside factor examination. To identify optimal subset of health data from the blockchain, this system proposes the modified mutual information (MMI) method. According to the MMI method, mutual information is obtained by subtracting the redundancy from the relevance. Moreover, this system uses the MD-5 hash algorithm for each block of the health data that has to be cryptographically hashed on the header of the block.

For information imparting to other human services suppliers under the user's consent, this system uploads the medical treatment data to the blockchain network. The current healthcare providers can request access to previous medical treatment and health data from the user. Both health information request and this

[+] Corresponding author. Tel.: +95 797603499
E-mail address: htwehtwepyone233@gmail.com

information access are recorded on the blockchain. Because of medical treatment history information is permanently recorded on the blockchain network, the proposed system doesn't allow the users to modify and hide those medical data. So, the integrity and trustworthiness about healthcare data are ensured in this system.

2. Related Work

In 2017, L. Xueping, Z. Juan and S. Sachin [1] presented an innovative user-centric health data sharing solution by using authorization and decentralized blockchain. This system protects privacy using channel formation scheme and enhances the identity management using the membership service that supported by the blockchain. To save the integrity of health information inside each record, a proof of integrity and validation is anchored to the blockchain network. Moreover, they embraced a tree-based information processing and batching method to handle huge data sets of personal health data that are gathered and transferred by the mobile platform.

In 2019, A. R. A. Mohammad, K. Yasar and M. C. E. Yagoub [2] presented a globally integrated healthcare record sharing architecture based on health level seven (HL7) client and blockchain. In this system, the genuine approval process is performed on a unified character the board framework, for example, the Shibboleth. Despite the fact that there are similitudes with personality the executive's frameworks, their framework includes the patient in the authorization procedure and reveals to them the characters of elements got to their health records. This system improves execution, and ensures protection and security by using blockchain and the executive's framework.

In 2019, A. A. Lukman, A. James and A. A. Emmanuel [3] proposed a method for the monitoring and securing of petroleum product distribution records in a decentralized ledger database using blockchain technology. This method is to verify the exchange of circulated records in a database and to shield records from altering, deceitful action, and debasement by the chain members. This framework demonstrated to be effective to keep up as it doesn't allow any person for records altering, however underpins understanding of 75% of members in the chain to make changes.

3. Blockchain

To set up the trust of the considerable number of components in the digital healthcare, blockchain has become as a solution. Blockchain technology uses scientific models for the circulation of encoded data through the chain of blocks. At the real time, blockchain makes the information distribution to be safe [4]. A file is represented as a block. Block can be a text file, video sample and spreadsheet. It can also be any kinds of structured data that consist of records which are storable and readable by machine. To create a chain like a process and govern the transmission of information, blocks are interconnected with nodes. Transaction is a single operation over one node. Nodes are able to communicate and transfer the data from one node to another across the network. Each node acts as a central point that is able to generate and digitally sign the transaction during the transmission process. Figure 1 shows the workflow of blockchain process.

Fig. 1: Workflow of the Blockchain Process [5]

Cryptographic hashing is also used for data transmission. By using hash algorithm, each block of data has cryptographically hashed on the header of the block. Each block contains the hash of its parent. To establish a sequence and to complete the liner list of blocks, each block in the blockchain is connected with the parent (past) block of information put away in the header: timestamp (date-time) and beginning [5].

3.1. Types of Blockchain

Blockchain includes three types that are public, federated and private blockchains. These are as follows:

- Public blockchain: Due to the permission less of public blockchain, anyone can easily validate the transaction. There is the highest level of decentralized trust because the blockchain is maintained by the public community.
- Federated blockchain: Under the leadership of a group, the federated blockchain is a permission blockchain operating. In this blockchain, the transactions may or may not be public.
- Private blockchain: Permission blockchain centralized to one governing organization is the private blockchain. In this blockchain, exchanges are approved inside and might be open lucid. This blockchain for the most part have quicker block occasions. In addition, this blockchain can process higher exchange throughput [6].

3.2. Use of Blockchain in Healthcare

In the healthcare industry, different stakeholders need to organize, access and share health records without any modification in a secure and interoperable way.

Healthcare blockchain is shown in Figure 2. Stakeholder can be practitioners, medical specialists, therapists, patients, payers, etc. To prove the authenticity of records, data provenance is essential for healthcare domain. In this situation, blockchain technology is the important for the healthcare sector. Blockchain is being implemented in different scenarios. By using blockchain, health bank provides a platform for each patient who can safely share their health data [7, 8].

4. Proposed System Design

Framework of proposed system is shown in Figure 3. Firstly, this system accepts the health data from the user. Then, this system separates the health data into each block. Then, this system eliminates the redundant data by using modified mutual information (MMI) method. By using these relevance data, this system hashed with MD5 hash function in each block of sender portion. Finally, this system produces the secure blockchain to the healthcare provider.

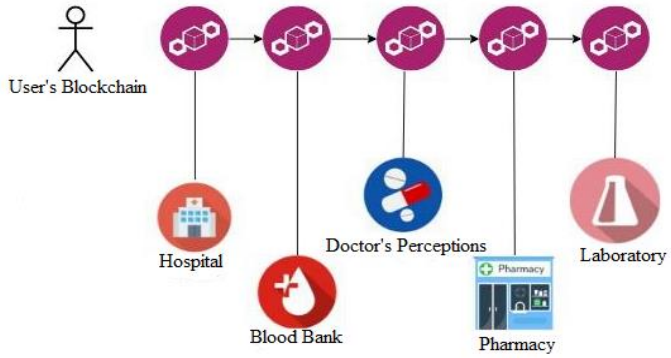

Fig. 2: Healthcare Blockchain [5]

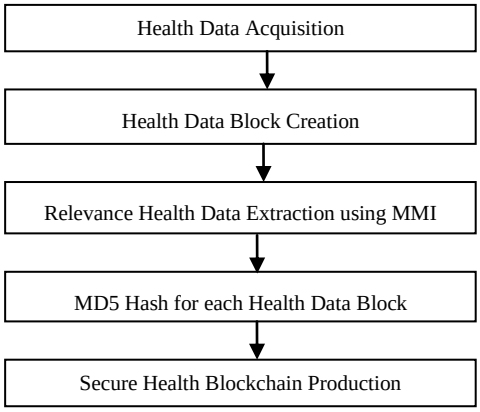

Fig. 3: Framework of the Proposed System

4.1. Mutual Information

Mutual information is a measure of statistical dependency that can determine complex relationships between features. This is a measure of the nonlinear and linear dependence between a set of features. Mutual information between two random features is a measure of the information one random variable provides about the other. If there is no dependence between the two variables, the mutual information method takes a minimum value of zero. If a strong dependence exists between the two variables, this mutual information method takes a positive method. Mutual information between two random features X and Y is as follows:

$$I(X;Y) = \sum_{x,y} p(x,y) \log \frac{p(x,y)}{p(x)p(y)} \quad (1)$$

where I(X;Y) is the mutual information between the two random features X and Y. The x and y represent realizations X and Y. The p(x, y) is their joint probability mass function. The p(x) and p(y) are the marginal probability mass functions.

4.2. Modified Mutual Information (MMI)

Modified mutual information (MMI) is based on identifying that the integrations of good features. Redundancy among features needs to be minimized because it is needed to maximize the joint dependency of top-ranking variables on the target features. According to mutual information, the purpose of causation-factor selection is to find a factor set S with m factors $\{x_i\}$, which have the highest mutual information value. MMI method searches the maximum relevance for satisfying factors, which approximates D(S, y) between factors x_i and class y. Maximum relevance is as follows:

$$\max D(s,y), D = \frac{1}{|s|}\sum_{x_{i\in S}} I(x_i, y) \tag{2}$$

Factors selected according to maximum relevance are likely to be highly redundant. When two factors depend highly on each other, the respective class-discriminative power would not change much if one of them were removed. To select mutually exclusive factors, MMI method adds the minimal redundancy that is as follows:

$$\min R(S), R = \frac{1}{|s|^2}\sum_{x_i, x_{i\in S}} I(x_i, x_j) \tag{3}$$

Operator Ø(D, R) combines D and R and considers the following simplest form to optimize D and R simultaneously. For features taking continuous values, which compute quantities such as the F statistic between features and the classification variable c as the score of maximum relevance that is as follows:

$$\max D(s,y), D = \frac{1}{|s|}\sum_{x_{i\in S}} F(x_i, y) \tag{4}$$

As the score of minimum redundancy, the average Pearson correlation coefficient of features is as follows:

$$\min R(S), R = \frac{1}{|s|^2}\sum_{x_i, x_{i\in S}} \left|c(x_i, x_j)\right| \tag{5}$$

MMI can also consider the distance function $d(x_i, x_j)$ for the minimum redundancy condition:

$$\min R(S), R = \frac{1}{|s|^2}\sum_{x_i, x_{i\in S}} d(x_i, x_j) \tag{6}$$

To find the causal factor relevance and redundancy, modified mutual information is taken as the basic criterion. MMI defines the relationship among different explanatory factors. MMI also finds a set of optimum casual factor that has the highest mutual information.

4.3. MD-5 Hash Function

MD-5 (Message Digest-5) processes a variable-length message into a fixed length output of 128 bits. Input message is broken up into 512 bit block. The message is padded because its length is divisible by 512. A single bit, 1, is appended to the end of the message. This is followed by many zeros to bring the length of the message up to 64 bits less than a multiple of 512. MD-5 operates on a 128 bit state, divided into four 32-bit words, denoted A, B, C and D. To modify the state, this algorithm uses each 512-bit message block. The processing of a message block consists of four stages, termed rounds. Each round is based on non-linear function F, modular addition and left rotation. These are four functions. These are as follows:

- F(B, C, D) = (B AND C) OR (NOT B AND D)
- G(B, C, D) = (B AND D) OR (C AND NOT D)
- H(B, C, D) = B XOR C XOR D
- I(B, C, D) = CXOR (B OR NOT D)

In the above four functions, a different one is used in each round.

5. Implementation of the System

The proposed secure healthcare system is implemented by using MATLAB programming language. In this system, there are two sides: the sender and receiver. This system transfers the patient healthcare data between sender and receiver. This system first loads the desired data. Then, this system splits the data into each block. From each block, this system reduces the redundant data using modified mutual information

(MMI) method. After reducing, this system encrypted this data by using MD-5 hash. Figure 4 and 5 shows the blockchain from the sender and receiver.

Fig. 4: Blockchain from the Sender

Fig. 5: Blockchain from the Receiver

6. Evaluation of the System

This system is tested different healthcare data about "Hypopharynx Carcinoma" and "Schwannoma" disease. To evaluate the performance of modified mutual information (MMI), this system uses the Univariate and Multivariate analysis methods. Mutual information rate is between "0" and "1". Table 1 shows each features about "Hypopharynx Carcinoma" and "Schwannoma" disease.

Table 1: Features about "Hypopharynx Carcinoma" and "Schwannoma" Disease

Features	Code	Diagnosis
History of present illness	HPI	Schwannoma
Lt sided weakness than Rt side	LTSide	Schwannoma
Lt eye blurred vision	LTEye	Schwannoma
Rt eye normal	RTEye	Schwannoma
Can't walk well	Cwalk	Schwannoma
Odynophegia 1.5 months	ODY	Hypopharynx Carcinoma
Cough +	COU	Hypopharynx Carcinoma
change of voice +	CV	Hypopharynx Carcinoma
Congestion of Pulmonary Disease	CPD	Hypopharynx Carcinoma
Healed, dry 4 cm diameter wound	HDW	Schwannoma

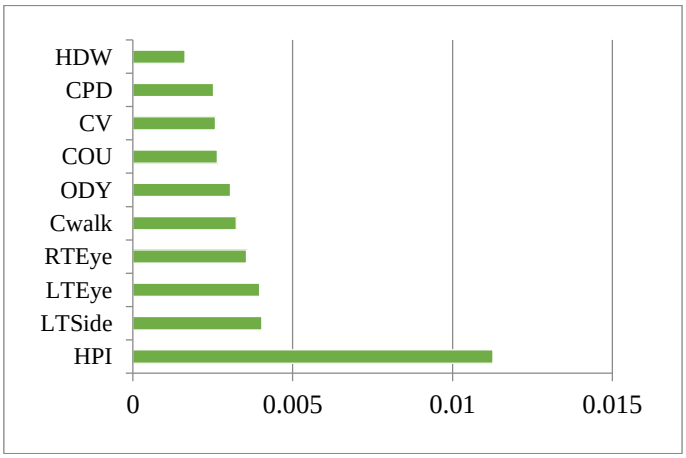

Fig. 6: Univariate Analysis based on MMI

Univariate analysis based on modified mutual information (MMI) is shown in Figure 6. Multivariate analysis with MMI for "Schwannoma" diagnosis and "Hypopharynx Carcinoma" diagnosis are shown in Figure 7 and 8.

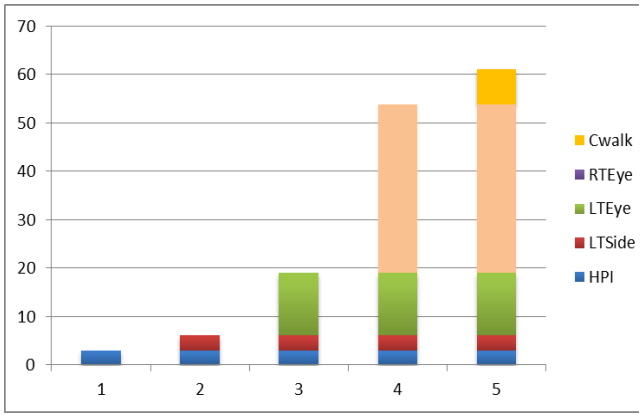

Fig. 7: Multivariate analysis with MMI for "Schwannoma" diagnosis

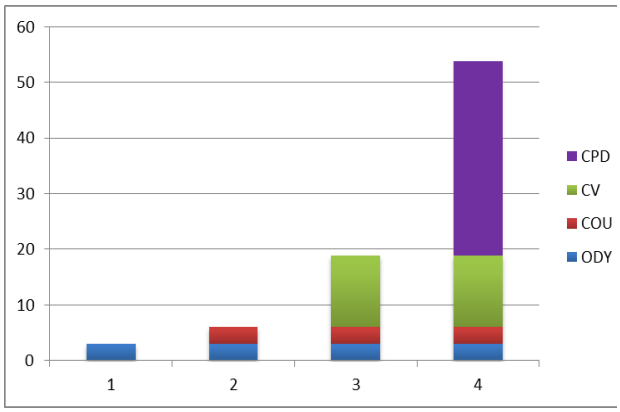

Fig. 8: Multivariate analysis with MMI for "Hypopharynx" diagnosis

7. Conclusion

In the patient-centric and traditional models, health data sharing faces the lack of trust and incentives to share. By using blockchain technology, the proposed system solved these problems. This system acts as a trust layer for sharing healthcare data. Moreover, blockchain that is produced from the system can be the bridge for the integration of medical device data and healthcare internet of things; the healthcare and lifestyle data collected by wearable devices can be critical for correct diagnosis since there is a lack of a proper way for a physician to access the patient-generated data.

8. References

[1] L. Xueping, Z. Juan and S. Sachin, "Integrating Blockchain for Data Sharing and Collaboration in Mobile Healthcare Application, IEEE, 2017.

[2] A. R. A. Mohammad, K. Yasar and M. C. E. Yagoub, "Fusing Identity Management, HL7 and Blockchain into a Global Healthcare Record Sharing Architecture", *International Journal of Advanced Computer Science and Applications*, vol. 10,no. 6, 2019, pp. 630-636.

[3] A. A. Lukman, A. James and A. A. Emmanuel, "Crypto Hash Algorithm-Based Blockchain Technology for Managing Decentralized Ledger Database in Oil and Gas Industry", *Multidisciplinary Scientific Journal*, vol. 2, 2019, pp. 300-325.

[4] G. Sylvester, *Blockchain*, Food and Agriculture Organization of the United Nations and the International Telecommunication Union, Bangkok, 2019.

[5] D. Rakic, "Blockchain Technology in Healthcare", *In Proceedings of the 4th International Conference on Information and Communication Technologies for Ageing Well and e-Health*, 2018, pp. 13-20.

[6] G. J. Katuwal, S. Pandey and M. Hennessey, " Applications of Blockchain in Healthcare: Current Landspace& Challenges", *arXiv*, 2018.

[7] S. Yaqoob, M. M. Khan and R. Talib, "Use of Blockchain in Healthcare: A systematic Literature Review", *International Journal of Advanced Computer Science and Applications*, vol. 10, no. 5, pp. 644-653, 2019.

[8] S. Sourabh, "Healthcare Blockchain Leads to Transform Healthcare Industry", *International Journal of Advance* Research, *Ideas and Innovations in Technology*, IJARIIT, 2018.