JOIV : Int. J. Inform. Visualization, 6(4) - December 2022 890-896

INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION

journal homepage : www.joiv.org/index.php/joiv

Decentralized Children's Immunization Record Management System for Private Healthcare in Malaysia Using IPFS and Blockchain

Faiqah Hafidzah Halim [a], Nor Aimuni Md Rashid [a,*], Nur Farahin Mohd Johari [a], Muhammad Amirul Hazim Abdul Rahman [a]

[a] *Faculty of Computer and Mathematical Science, UiTM Cawangan Melaka (Kampus Jasin), 77300 Merlimau, Melaka, Malaysia*

Corresponding author: [*]aimuni5294@uitm.edu.my

***Abstract*—In Malaysia, private healthcare providers keep computerized records of vaccination data, including personal information, diagnostic results, and vaccine prescriptions. However, such sensitive information is commonly stored using a centralized storage paradigm which subsequently brings about the issue of maintaining user privacy. Concerning this, unauthorized access to crucial information such as identity details and ailments that a patient is suffering from, as well as the misuse of patients' data and medical reports, are common threats to user's (patient) privacy. To overcome this problem, the researchers suggest leveraging IPFS (Interplanetary File System) and blockchain technology to create a decentralized children's immunization record management system. While respecting patient privacy, the proposed system also allows authorized entities, such as healthcare professionals, and provides easy access to medical data (e.g., doctors and nurses). The proposed decentralized system integrates IPFS, blockchain, and AES cryptography to ensure consistency, integrity, and accessibility. A permission Ethereum blockchain allows hospitals and patients within private healthcare providers to connect. We utilized a combination of symmetric and asymmetric key encryption to provide secure storage and selective records access. The proposed system was analyzed using Wireshark to evaluate the overall system's performance in terms of integrity and accessibility while sharing patient records. This project aims to provide automated system keeper using autonomous agents collaboratively with the role of blockchain for further enhancement.**

***Keywords*—Blockchain; immunization; IPFS; patient privacy; decentralized system.**

Manuscript received 14 Jan. 2022; revised 19 Mar. 2022; accepted 27 Apr. 2022. Date of publication 31 Dec. 2022.

I. INTRODUCTION

In the 1950s, Malaysia initiated the National Immunization Program (NIP), and it was integrated into the Maternal and Child Health Program designed based on the World Health Organisation's (WHO) Expanded Programme on Immunisation (EPI). The EPI recommends that all countries immunize themselves against six childhood diseases [1]. However, the NIP has expanded protection against 13 major childhood diseases. This expanded program was introduced to help reduce the burden of illness and disability from vaccine-preventable diseases, and it is also one of the most cost-effective strategies for reducing child mortality.

Every country's NIP is in charge of providing immunization services, with private sector contributions varying. In low and middle-income countries, vaccines have traditionally been included in a package of basic health care given and funded by the government, with international donors often supplementing the package. A country's economic, governance, and administrative capacities directly impact the ability to provide these services[2]. However, the common and major problem while handling immunization records is the decentralized data system among the private sector health facilities.

In order to manage the decentralized immunization record, we proposed the use of blockchain. Blockchain is a decentralized, peer-to-peer (henceforth, P2P) ledger in which transactions are digitally stored into blocks. The blockchain network's nodes (miners) are responsible for connecting the blocks in chronological order[3]. Blockchain nodes maintain their network active by storing a copy of the stored data[4]. As a result, blockchain records the complete history or provenance of data. A blockchain digital ledger can be used to maintain sample test results, patient data, discharge summaries, and immunization statuses. Clinical laboratories, patients, hospitals, and government-funded healthcare institutions will be able to manage healthcare information in

a decentralized manner utilizing self-executing contracts known as "smart contracts"[5].

The newest and most promising technology in the modern economy is blockchain. Blockchain is a decentralized, immutable digital database of economic activity that may be used to record nearly any exchange of value, not just money. This technology can assist in resolving a variety of industry issues, including trust, transparency, security, and the dependability of data processing. To ensure availability, immutability, and security, many crucial applications are built on distributed structures employing blockchain technology[6].

This study uses the Bitcoin blockchain as an example for optimizing blockchain data storage and considers the transaction data to be kept in IPFS (InterPlanetary File System). Only the IPFS hash of the transaction is included in the block to reduce the load on the blockchain's data storage. In the current Bitcoin network, most nodes maintain the same ledger data. A content-addressed file system is IPFS, and the hash for identical transaction data in IPFS is identical. As a result, the data in each node is consistent since the IPFS hash of the transactions recorded by each node in the blocks is the same. At the same time, this approach gets rid of the network's reliance on the quantity of fully functional nodes, allows any form of transaction, and maintains all transaction data, maintaining the traceability of the blockchain [7], [8].

The distributed file storage technology offered by IPFS makes connections to P2P networks easier. A file's unique hash is calculated by IPFS and made available to all network peers. Each time a file is updated, the hash is altered. With its P2P decentralized file storage system and content-addressable method of accessing the stored files, IPFS is regarded as the foundation of Web 3.0 [9].

A study by Patnaik et al. [10] proposed an application used to share files across networked environments or in a distributed system. The authors present a framework that applies IPFS and Ethereum blockchain to guarantee secure, reliable, and tamper-proof activities. They outlined five objectives in their study, which include: 1) Any shared file cannot be downloaded to ensure any facsimile; 2) Any operations and changes performed to files can be tracked and recorded to the blockchain network in real time; 3) Data history will be collected and published to the blockchain network; 4) Users can retrieve any information about the files and the provenance data such as the owner of the files, number of views and edit process to the documents; 5) The blockchain network publishes the provenance record globally and certifies by the blockchain nodes. This application only allows end users to access digital files while using the application and not allowing them to store the digital content on their own devices. The Ethereum Testnet/Ropsten blockchain is used to store user information and audit logs securely, while IPFS is used since it gets free hosting forever in a decentralized platform. This study achieved its objectives from the validation and analysis conducted.

With an enormous amount of digital data being generated day by day, security and capacity have been a big challenge. Many studies have proposed blockchain and IPFS to keep digital data safe and efficient. In a study by Ye and Park [11], an evaluation to demonstrate the superior performance of their system is provided, namely DApp. They combined blockchain and IPFS to assure secure data storage, higher bandwidth processing, and lower costs. This system administers user information, file list information uploaded by the user, and file data information. Several experiments were conducted to measure the performance of the proposed system.

Their experiment involved 100 vehicles' On-Board Diagnostics (OBD) data in testing and analyzing the data rate of transferring data, which DApp processes to the smart contract and the one not processed by the proposed system. The time taken to upload the data through the system was 1451 ms. On the contrary, it took 1854 ms to upload the data without using DApp, which is slower. They also examined the upload speed by using ten times the data size from their previous experiment, and the results showed that the speed increased significantly even when the data size was increased.

They also experimented with using numerous sizes of data to confirm system efficiency. As a result, this system was proven as a safe and efficient way to store vehicle data using the Ethereum blockchain and IPFS. A digital signature method was used to guarantee the security and durability of vehicle data, regardless of its size. The authors also claimed that users could take control of their data which can be shared with others using public key encryption methods to assure data safety.

Medical data such as a patient's private details, medical reports, and other information are very confidential and sensitive. The current system uses a centralized storage model, which has security issues. [12] We proposed a distributed off-chain storage using IPFS and blockchain technology to address this problem. Their study used the consortium blockchain framework to store medical information to ensure data security. The consortium blockchain increases access security since it only allows legal peers to join or access the network. Their main objective was to guarantee patient reports' privacy. They divided the framework into three modules: data upload, mining process, and finally, data storage. Generally, the healthcare provider needs to upload the patient information using a Web User Interface (Web UI), and a mining procedure will take place to validate the process. A hash data storage will be used at the end to secure the patient report. This proposed framework is implemented and tested in Python flask, while the blockchain module is used to store the hash, and IPFS is used as a data storage layer. The testing analysis shows that using their proposed framework successfully achieves the main objective of secure and safe data sharing among healthcare providers.

Kumar et al. [13] and Dasaklis et al. [14] proposed a blockchain system to address the problem of healthcare data fragmentation. Blockchain helps healthcare providers to share data by maintaining existing decentralized databases and providing immutability of medical information. The authors employed smart contracts to preserve network consensus during the transmission of medical records. On the other hand, the model uses cloud-based storage (world state). It is possible that entrusting sensitive medical data to a third party will result in it being easily hacked. Wang et al. [15] and Jin et al. [16] describe a parallel healthcare system that artificial intelligence to work with virtual patients and doctors. The virtual or fake doctor receives the patient's report and confirms the patient's disease before issuing a report. The

expert then double-checks the produced report (doctor). The blockchain network is used to distribute the report. On the other hand, the process of disseminating the reports takes a lengthy time.

Meanwhile, Bhuiyan et al. [17] described a blockchain-based storage mechanism for patient healthcare data. The concept allows medical centers, hospitals, and insurance companies to share data. The model, however, does not provide for data privacy. In order to secure medical data, Zhao et al. [18] proposed a key management strategy. The AES algorithm implements key management, and a secret key is used to exchange data among peers.

On the other hand, the model just utilizes one key for data communication. As a result, if the attacker knows the key, data can be compromised or altered. Uddin et al. [19] used blockchain technology to deploy the Patient-Centric Agent (PCA) in a patient monitoring system to provide data confidentiality and privacy during peer-to-peer communication. They have also discussed the importance of medical data interoperability in a healthcare system. On the other hand, the approach keeps the data in a cloud structure, which restricts it owing to third-party reliance.

The use of Electronic Health Records (EHR) is spreading rapidly throughout the world. On the other hand, the current EHR systems have their own unique set of privacy and security challenges to deal with. Reen et al. [20] suggested a mechanism that addresses most of the issues with these issues. Hospitals and patients from all over the world can connect using Ethereum's permission blockchain. Using both symmetric and asymmetric key encryption, Reen et al. [20] provided secure storage and limited access to records. It gives patients total control over their medical records and allows them to approve or reject a hospital's access to them. To store records, their project used IPFS) which has the advantage of being dispersed and ensuring record immutability. The proposed methodology also keeps track of disease statistics without invading any patient's privacy. The work in this study was prompted by the following findings from the current literature. The study's contributions can be summarized as follows:

- We suggest a decentralized paradigm in which we only maintain the content-addressed hash of vaccination records rather than the entire record in the blockchain network, hence lowering the network's size. The IPFS, distributed file storage system, is used to store immunization records.
- Hash representation on blockchain storage protects the anonymity of patient immunization records.

This proposed model will concentrate on the local network, and two servers would join the IPFS as members of the local IPFS network. The IPFS uses a peer-to-peer hypermedia protocol to make this web faster and safer. This protocol allows permanent and decentralized storage and sharing. When a file is posted to IPFS, it is separated into many fragments. Each item has a hash value that solely saves content. The file's value has been created and can be downloaded from any node. Asymmetric encryption is used to encrypt the hash of the generated IPFS hash key. Because it is not hosted on a single server, decentralized storage is more accessible.

II. Materials and Method

This section proposes a model for blockchain-based immunization record storage applications using IPFS. The primary objective of this framework is to provide a centralized immunization record with the privacy of the vaccine recipient's personal data. This project will concentrate on the local network. Two servers will join the IPFS as members of the local IPFS network. The IPFS uses a peer-to-peer hypermedia protocol to make this web faster and safer. This protocol allows permanent and decentralized storage and sharing. When a file is posted to IPFS, it is separated into many fragments. Each item has a hash value that solely saves content. The file's value has been created and can be downloaded from any node. Asymmetric encryption is used to encrypt the hash of the generated IPFS hash key. Because it is not hosted on a single server, decentralized storage is more accessible.

Fig. 1 shows the overall system architecture for the proposed blockchain-based immunization record management using IPFS. The medical officer who's responsible for the immunization process communicates with the IPFS and consortium blockchain through the developed immunization application (ImRecApp). Users can subscribe to store and manage data, and the data is saved in an Ethereum smart contract that runs automatically when certain conditions in ImRecApp are met. The mining process is used to verify immunization records. ImRecApp is a centralized platform that stores or accesses user information and immunization records and uploads some of the data to IPFS to store the returned hash value in the smart contract of the consortium blockchain network.

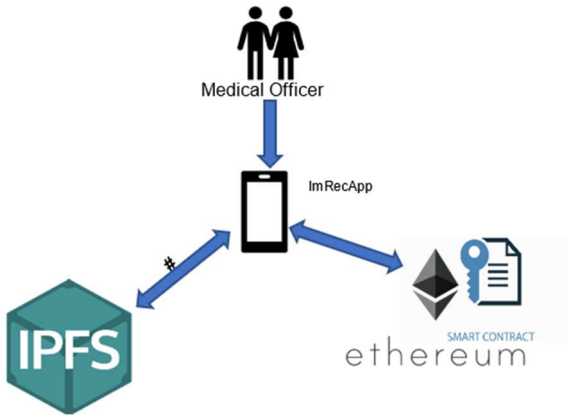

Fig. 1 Proposed system architecture

The operation of the proposed model can be summarized as follows:

- In order to receive the Proof-of-Identity, the medical officer or healthcare provider must be registered with the consortium blockchain network.
- The medical officer may use the ImRecApp as the user interface to upload the immunization records of the attended patients.
- The miners are responsible for validating the provided immunization record. These approaches are used to ensure that the blockchain network remains consistent.
- The miners distribute the immunization record to the legitimate peers in the consortium blockchain network

to verify the transaction by seeing their local copy and generate and add a new block to the consortium blockchain network.

- The immunization record is then put in the IPFS after it has been confirmed. Furthermore, IPFS creates a hash (content-addressed) that is saved in the on-chain storage (blockchain network). The hash of the generated IPFS hash key is then encrypted using asymmetric encryption to increase data privacy. The list of transactions is only accessible to peers who have signed onto the network. A peer (medical officer) must register with the consortium network to become a member.

A. Hash Key Generation Process

Fig. 2 shows the process of hash key generation after the immunization record has been uploaded to the ImRecApp. The user chooses the file to be uploaded from their device. The system then checks if there is any duplication of the file. If there is none, the system would then store the data on the IPFS network, and the IPFS will create the file hash key. If the error occurs, the system will prompt the error message.

Once the user chooses the file to be checked, the system compares the current value of md5 and sha1 of the file with the original value from the database. The server will prompt the user with a verified message if the value is the same. If the value is changed, the server would prompt the user with a message that data has been changed, as shown in Fig 3.

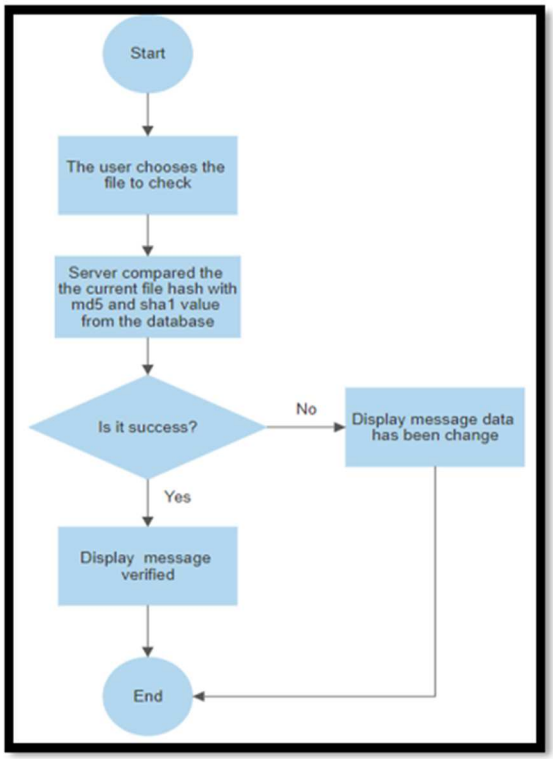

Fig. 2 Hash key generation

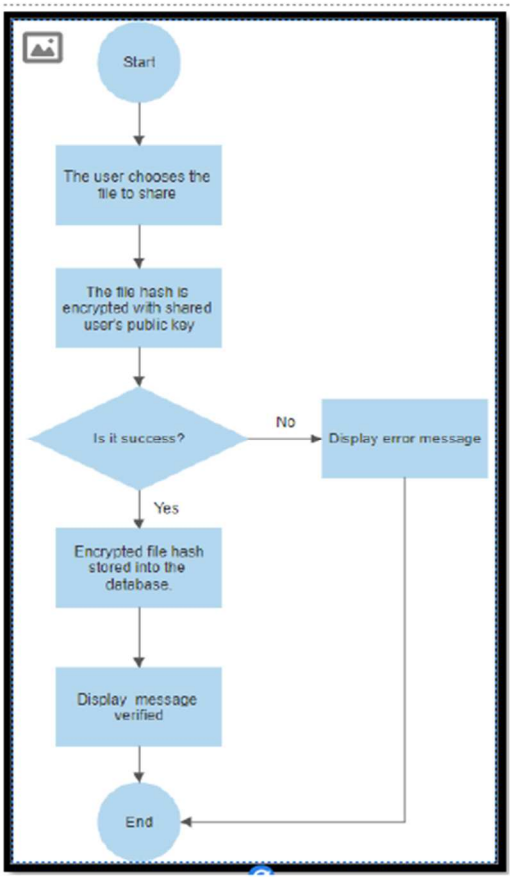

Fig. 3 Hash key verification

For the user to share the immunization files in the distributed network, the user selects the file to share from their system's file list. The system then checks to see if the file has been duplicated. The data would be stored in the shared user table if there is none. However, if an issue happens, the system will display a notification. The flow of the file-sharing process is shown in Fig. 4.

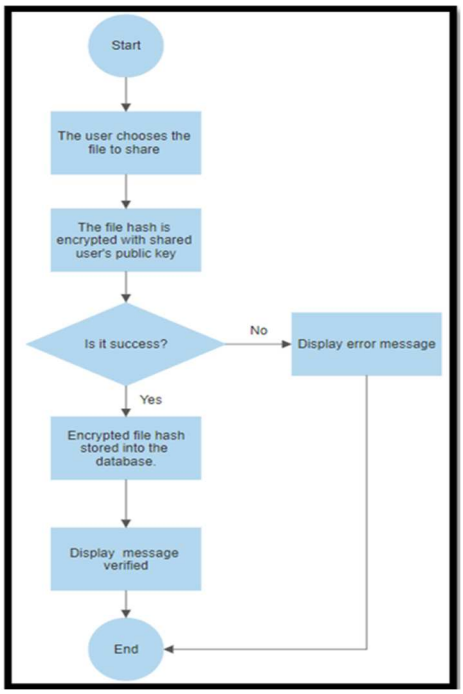

Fig. 4 File sharing process flow

B. *ImReacApp Interface Design*

Fig. 5 depicts ImrecApp's UI design. Users can choose from four different navigation icons. The main page also shows user information and files saved in the system storage. By pressing the upload button, the user can send their file to the system, requesting it from the local machine. Users must choose the file and enter the file's description in the description textbox to make it easier to sort and identify it. Aside from that, users can transmit their files to other users who want to share them. The file will be encrypted with the receiver's public key, allowing only that person to open it. Users must select the file id button to proceed to the next page.

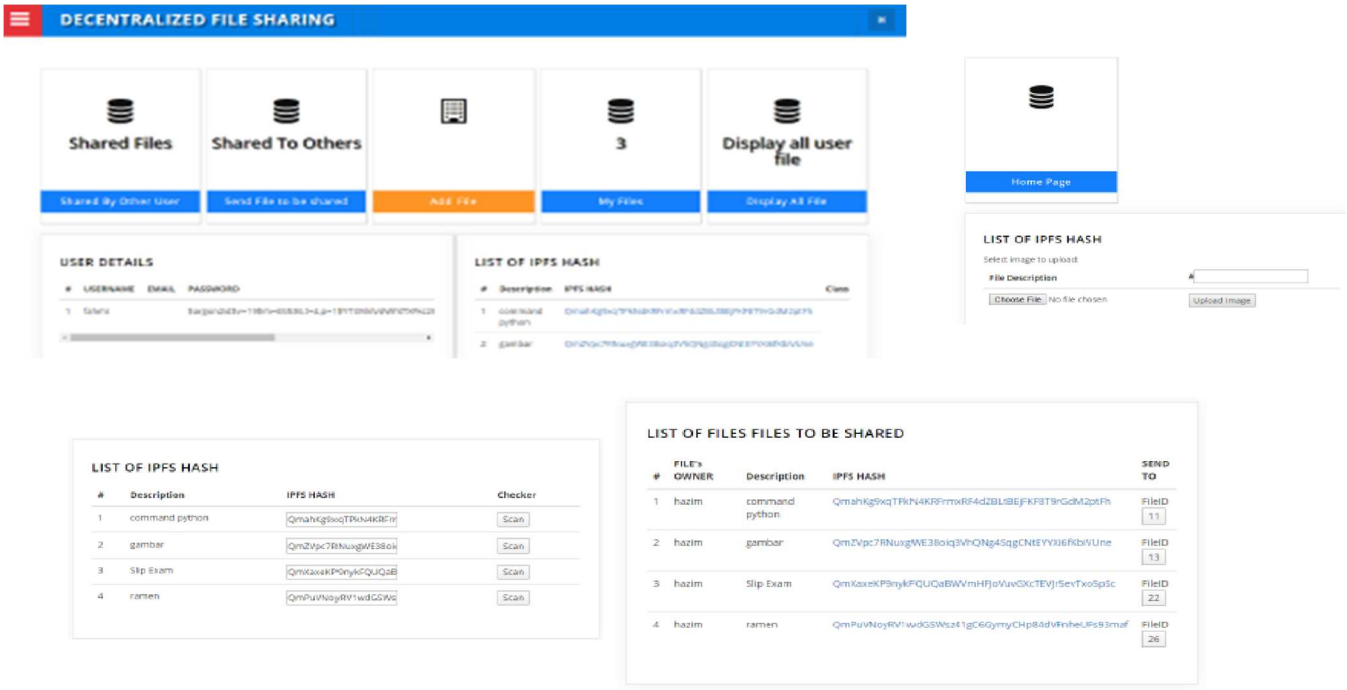

Fig. 5 ImREc App UI

Following the user's selection of the file to be shared. On this page, the user must select the individual with whom he or she wishes to share. To finish the process, click the submit button. The pop-out notice would say "*The File Already Shared*" if the file has already been shared with that user. The success message will appear if the file was successfully shared. All files shared among users are visible to the user. The user can access the file hash on this page, which is encrypted. The recipient's public key is used to encrypt the file. As a result, only the recipient has access to the file. If the user has access to the file, the IPFS hash value on the right of the page shows "*Verified*" whereas if the user does not have it, it will show "*Unverified*"

C. *Distributed Storage*

An IPFS network, which consists of two connected nodes, supports distributed storage technology. The file is duplicated on each node. Apart from implementing the private and public keys in this project, asymmetric encryption was included due to increased security concerns. Because all nodes linked to the network save a copy of the data, this distributed storage technique can help to duplicate and safeguard the integrity of the data from being altered or erased.

The file previously executed in distributed storage technology is shown in Fig. 6. The user who does not have the private key for the owner's file is not authorized to read the file when it arrives. The private key function was employed in this project. The database then added the users to the authorized table once valid. Only authorized users can access the file that is saved in the database since it is encrypted using the receiver's public key. Users can see all shared transactions, but they can only access them if they have the correct key.

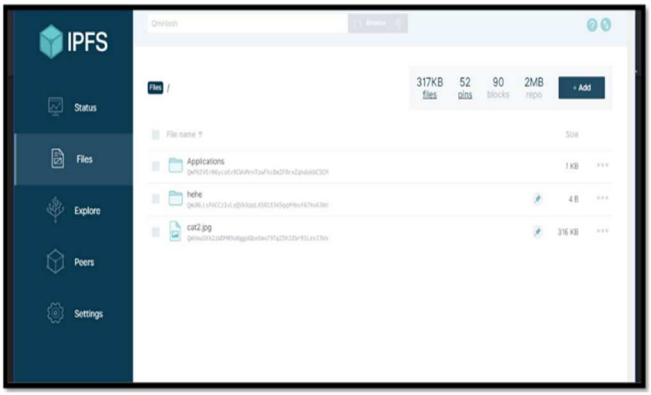

Fig. 6 Distributed Storage

III. Results and Discussion

This proposed model was tested based on the performance and integrity test. First, to test the network performance file sharing between the server and client. Secondly, by monitoring the security of the file-sharing web system using a Wireshark.

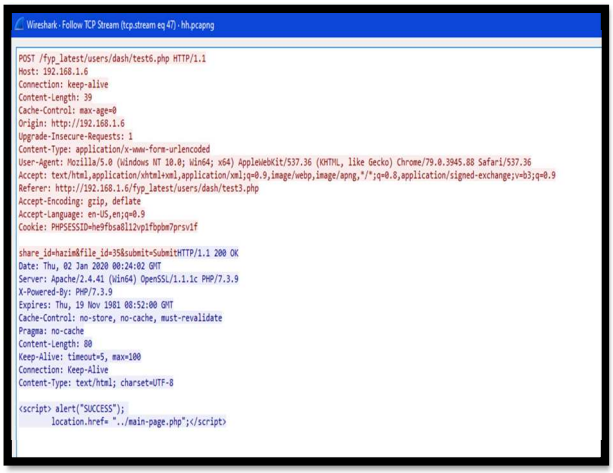

Fig. 7 Network Analysis

Fig. 7 displays the network analysis between the server and client when the client posted file hashing to another user. The data transfer did not include the file hash key, but only the ID and one of the files were used. This was done in order to ensure the key was hidden. Thus, it could not be sniffed. For the network performance analysis, the initial performance of the system was measured to the performance of the file-sharing system after the experiments were executed.

TABLE I
NETWORK PERFORMANCE TESTING

Test	Transfer (MB)	Bandwidth (MB)
1	1.25	1.279
2	1.38	1.407
3	1.50	1.537
4	1.38	1.407
Total	5.51	5.630
Average	1.38	1.4075

Table 1 shows the result between the client to the server. The test was done four times to calculate the average bandwidth usage on the network between the server and client. The first test was tested by transferring a 1.25 Mb packet to the server from the client, and the bandwidth usage was 1.2799 Mb. The second test was tested by transferring a 1.38 Mb packet and showed 1.407 bandwidth usage. The test was tested with a packet of 1.50 Mb, resulting in bandwidth usage of 1.537 Mb. The last test was tested using the same amount of packet, 1.38 Mb, and the result was the same as the previous.

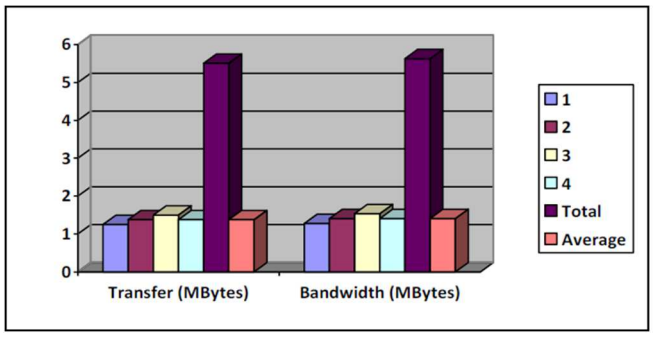

Fig. 8 Network Performance Result Bar Chart

Fig. 8 shows the overall result in the chart bar graphic. Based on the result of the testing, it shows that the usage of the bandwidth is still on average and almost the same as the packet transferring value. The network bandwidth might change due to several factors, such as the number of users, internet speed connection, and packet size.

IV. CONCLUSION

The concept and implementation of blockchain and IPFS for keeping patient immunization records were detailed in this study. For scalability, only hashes of reports were maintained in the blockchain. Unlike the currently available centralized storage system for patient immunization records among Malaysian healthcare providers, the suggested model is decentralized to cater to the issues of a distributed network system. Furthermore, unlike cloud-based systems, the concept does not rely on a third party and offers fair service to approved peers.

ACKNOWLEDGMENT

The researchers thank UiTM Cawangan Melaka for funding this study through the TEJA Internal Grant number GDT2021/2-10. Also, we are grateful to everyone who was part of this work, whether directly or indirectly.

REFERENCES

[1] L. P. Wong, P. F. Wong, and S. AbuBakar, "Vaccine hesitancy and the resurgence of vaccine preventable diseases: the way forward for Malaysia, a Southeast Asian country," *Hum Vaccin Immunother*, vol. 16, no. 7, pp. 1511–1520, Jul. 2020, doi: 10.1080/21645515.2019.1706935.

[2] A. Levin and M. Kaddar, "Role of the private sector in the provision of immunization services in low- and middle-income countries," *Health Policy Plan*, vol. 26, no. Suppl. 1, pp. i4–i12, Jul. 2011, doi: 10.1093/heapol/czr037.

[3] M. Y. Jabarulla and H.-N. Lee, "A Blockchain and Artificial Intelligence-Based, Patient-Centric Healthcare System for Combating the COVID-19 Pandemic: Opportunities and Applications," *Healthcare*, vol. 9, no. 8, p. 1019, Aug. 2021, doi: 10.3390/healthcare9081019.

[4] A. A. Monrat, O. Schelen, and K. Andersson, "A Survey of Blockchain From the Perspectives of Applications, Challenges, and Opportunities," *IEEE Access*, vol. 7, pp. 117134–117151, 2019, doi: 10.1109/ACCESS.2019.2936094.

[5] M. Hölbl, M. Kompara, A. Kamišalić, and L. Nemec Zlatolas, "A Systematic Review of the Use of Blockchain in Healthcare," *Symmetry (Basel)*, vol. 10, no. 10, p. 470, Oct. 2018, doi: 10.3390/sym10100470.

[6] J. Golosova and A. Romanovs, "The Advantages and Disadvantages of the Blockchain Technology," in *2018 IEEE 6th Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE)*, Nov. 2018, pp. 1–6. doi: 10.1109/AIEEE.2018.8592253.

[7] Q. Zheng, Y. Li, P. Chen, and X. Dong, "An Innovative IPFS-Based Storage Model for Blockchain," in *2018 IEEE/WIC/ACM International Conference on Web Intelligence (WI)*, Dec. 2018, pp. 704–708. doi: 10.1109/WI.2018.000-8.

[8] X. Wu, Y. Han, M. Zhang, and S. Zhu, "Secure Personal Health Records Sharing Based on Blockchain and IPFS," 2020, pp. 340–354. doi: 10.1007/978-981-15-3418-8_22.

[9] R. Kumar and R. Tripathi, "Implementation of Distributed File Storage and Access Framework using IPFS and Blockchain," in *2019 Fifth International Conference on Image Information Processing (ICIIP)*, Nov. 2019, pp. 246–251. doi: 10.1109/ICIIP47207.2019.8985677.

[10] S. Patnaik, X.-S. Yang, and I. K. Sethi, *Advances in Machine Learning and Computational Intelligence*. Singapore: Springer Singapore, 2021. doi: 10.1007/978-981-15-5243-4.

[11] H. Ye and S. Park, "Reliable Vehicle Data Storage Using Blockchain and IPFS," *Electronics (Basel)*, vol. 10, no. 10, p. 1130, May 2021, doi: 10.3390/electronics10101130.

[12] R. Kumar, N. Marchang, and R. Tripathi, "Distributed Off-Chain Storage of Patient Diagnostic Reports in Healthcare System Using IPFS and Blockchain," in *2020 International Conference on*

COMmunication Systems & NETworkS (COMSNETS), Jan. 2020, pp. 1–5. doi: 10.1109/COMSNETS48256.2020.9027313.

[13] T. Kumar, V. Ramani, I. Ahmad, A. Braeken, E. Harjula, and M. Ylianttila, "Blockchain Utilization in Healthcare: Key Requirements and Challenges," in *2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom)*, Sep. 2018, pp. 1–7. doi: 10.1109/HealthCom.2018.8531136.

[14] T. K. Dasaklis, F. Casino, and C. Patsakis, "Blockchain Meets Smart Health: Towards Next Generation Healthcare Services," in *2018 9th International Conference on Information, Intelligence, Systems and Applications (IISA)*, Jul. 2018, pp. 1–8. doi: 10.1109/IISA.2018.8633601.

[15] S. Wang et al., "Blockchain-Powered Parallel Healthcare Systems Based on the ACP Approach," *IEEE Trans Comput Soc Syst*, vol. 5, no. 4, pp. 942–950, Dec. 2018, doi: 10.1109/TCSS.2018.2865526.

[16] H. Jin, Y. Luo, P. Li, and J. Mathew, "A Review of Secure and Privacy-Preserving Medical Data Sharing," *IEEE Access*, vol. 7, pp. 61656–61669, 2019, doi: 10.1109/ACCESS.2019.2916503.

[17] M. Z. A. Bhuiyan, A. Zaman, T. Wang, G. Wang, H. Tao, and M. M. Hassan, "Blockchain and Big Data to Transform the Healthcare," in *Proceedings of the International Conference on Data Processing and Applications - ICDPA 2018*, 2018, pp. 62–68. doi: 10.1145/3224207.3224220.

[18] H. Zhao, P. Bai, Y. Peng, and R. Xu, "Efficient key management scheme for health blockchain," *CAAI Trans Intell Technol*, vol. 3, no. 2, pp. 114–118, Jun. 2018, doi: 10.1049/trit.2018.0014.

[19] Md. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, "Continuous Patient Monitoring With a Patient Centric Agent: A Block Architecture," *IEEE Access*, vol. 6, pp. 32700–32726, 2018, doi: 10.1109/ACCESS.2018.2846779.

[20] G. S. Reen, M. Mohandas, and S. Venkatesan, "Decentralized Patient Centric e- Health Record Management System using Blockchain and IPFS," in *2019 IEEE Conference on Information and Communication Technology*, Dec. 2019, pp. 1–7. doi: 10.1109/CICT48419.2019.9066212.