Researchers Journal of Science and Technology (REJOST)

https://rejost.com.ng

Enhancing Data Integrity in Telemedicine System Using Blockchain Approach

Effiong Nkereuwem, Godwin Ansa

Received: May 18, 2023 /Accepted: July 25, 2023

Abstract

The improvement that has come with tele-medicine has resulted in the availability of healthcare for all patients, especially those who reside in areas with a shortage of nearby medical professionals. This has also made it less expensive compared to in-person appointments. Records tampering by health workers and other forms of data breaches have come to affect the confidence of telemedicine systems. This research work aims to design a telemedicine system using the Algorand blockchain platform by incorporating the features of blockchain, to enhance data integrity by providing tamper-proof and unauthorized access and using Algorand Smart Contract (ASCIs) to enable, secure and provide verifiable management, allowing patients to control and provide explicit consent, this empowers patients with greater control over their data. Python programming language and PHP is used for the front end, and Algorand, which uses Python language for Algorand Smart Contracts (ASCIs), implemented using a stack-based language called Transaction Execution Approval Language (TEAL) for the backend. The methodology adopted is the Direct Science method, which applies process steps such as problem awareness, suggestion, development, evaluation, and conclusion. This eventually gives a robust system that is tamper-proof and provides a cost-effective and scalable platform compared to the existing work. This helps address concerns such as data breaches, unauthorized access, and data manipulation, which can compromise the safety and confidentiality of patients' sensitive medical information.

Keywords: Telemedicine; Blockchain; Algorand; Smart Contract; Cryptography; Electronic Health records (EHR).

✉ Effiong Nkereuwem: effiongnkereuwem@aksu.edu.ng

Department of Computer Science, Akwa Ibom State University, Ikot Akpaden

Introduction

Medical services delivered via telecommunications technology, such as teleconferencing, remote monitoring, and mobile health apps, are referred to as telemedicine. By eliminating the need for patients to physically visit a hospital or clinic, it allows them to consult with healthcare professionals remotely.

Telemedicine can be used for various purposes, such as remote consultations, diagnosis, treatment, and follow-up care. Additionally, it can be used to train and educate healthcare professionals in medicine. The patients who benefit the most from telemedicine are those who reside in rural or remote areas, have mobility issues, or need ongoing medical monitoring.

Using a cutting-edge database system called blockchain technology and its features as shown in Figure 1; open information exchange is possible within a network of businesses. In a blockchain database, data is stored in blocks that are linked together in a chain. The data is chronologically consistent, as nothing can be removed from or changed in the chain without network consensus, (2023, amazon - retrieved from https://aws.amazon.com/what-is/blockchain). Using blockchain technology, you can build an unchangeable or immutable ledger to keep track of orders, transactions, accounts, and payments. A shared view of these transactions is made consistent by the system's built-in mechanisms, which also stop unauthorized transaction entries. With the rise in telecommunication gadgets and their efficiency in connecting people even in remote areas through voice, video, text, etc., the use of technology to help in the administration of medical assistance to people is explored. The use of this technology does come with its problems, such as patient data leaks, data manipulation, and man in the middle, amongst various others.

According to Kali et al. (2018), data integrity is frequently cited as being seriously threatened by data manipulation. Data can be altered, and malicious actors might take advantage of this. By integrating blockchain technology into telemedicine systems and current telehealth, it is possible to create a wide range of new opportunities for secure healthcare digitization, including automating payment settlement, managing the identities of devices used for remote patient monitoring, establishing the source of clinical data, and ensuring the legitimacy of users requesting patient data. Figure 1 shows that transparency, auditability, immutability, and anonymity of people and data are all inherent aspects of blockchain technology. Blockchain technology has many potential applications. The most popular application for blockchains is as a distributed ledger for crypto-currencies. It has a lot of potential in a variety of business applications, including banking, government, insurance, finance, healthcare, media and entertainment, retail, and so on.

According to Salah and Jayaraman (2021), the decentralization feature enhances the general robustness of current healthcare systems by ensuring that patient Electronic Health Records (EHRs) is shielded from malicious attacks or unintentional data loss. Furthermore, by guaranteeing consensus regarding the blockchain ledger's state at the moment, consensus methods boost confidence among participants in telehealth and telemedicine. The in transputability of medical records is ensured via public-key cryptography, which requires each transaction to be digitally signed before being confirmed and recorded on the ledger.

Additionally, Salah and Jayaraman (2021) discuss how Blockchain technology can meet the unique requirements of the healthcare industry, including real - time EHR exchange and healthcare data management, Patient-centeredness, high performance, low cost, data security, availability, and privacy, as well as establishing transparency about the origin of medical records. In addition, the use of blockchain for interactive medical approaches such as "doctor in the loop" can increase security against potential database manipulation threats by making data available to the public.

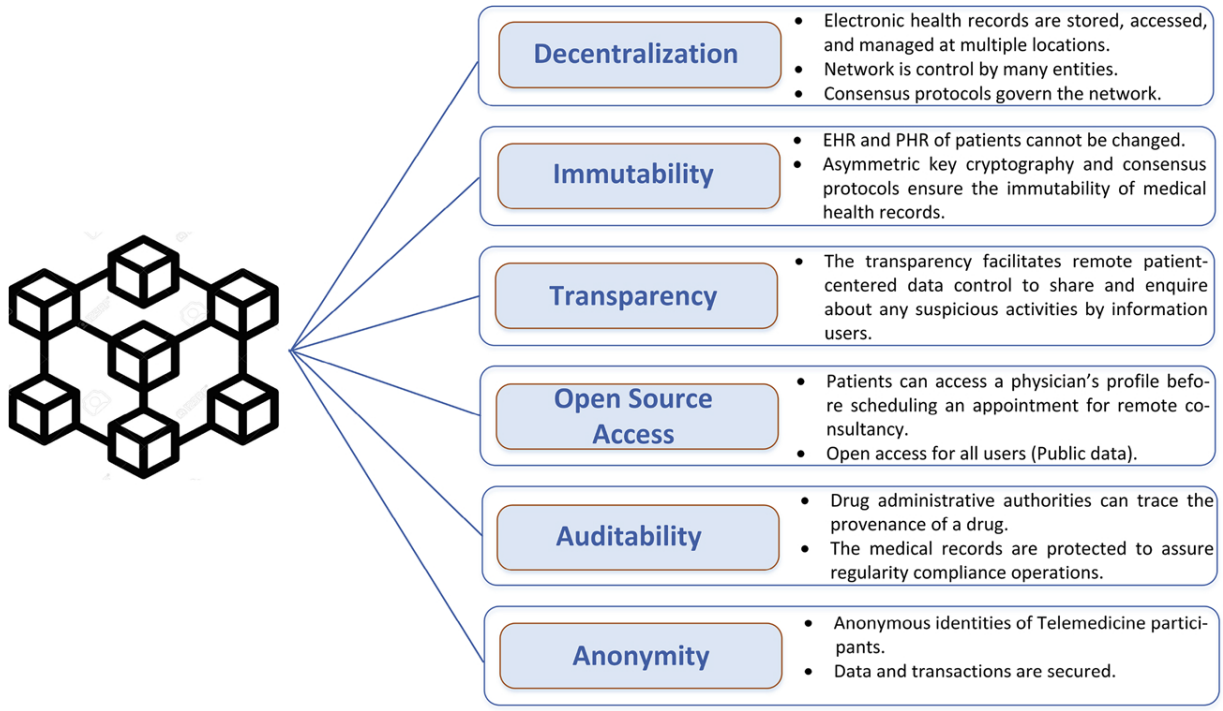

Fig. 1: Key Features of Blockchain Technology (Salah & Jayaraman, 2021)

With the problems of data theft and manipulation, this work uses the co-chain technology of Algorand blockchain, a private, permissioned blockchain that offers stringent restrictions that business and health care providers typically seek to design a telemedicine system that gives various levels of access and gives the patient the right to choose who could access their sensitive information. Layer 1 is accessible to everyone and can be used interactively, while Layer 2 is private.

The co-chain uses its own Algorand consensus protocol, is completely independent of the public chain, protects its transactions from prying eyes, chooses its validators, and is completely decentralized.

Related Literature

Using the Ethereum blockchain and its smart contract, Abugabah et al. (2017) created a telemedicine framework that is decentralized for a smart healthcare ecosystem. The focus of the solution was on creating a decentralized telemedicine framework, which included automated payment settlement claims by the medical insurers. The Ethereum blockchain relies on the proof-of-work consensus, which is

unstable in the event of a node failure. It also uses a lot of energy and processes transactions slowly.

In order to make the data gathered during the clinical trial process is unchanged, traceable, and potentially more reliable, Wong et al. (2019) proposed a blockchain-based system. The developed prototype demonstrated how a blockchain-based data structure and could be used to securely protect data in a clinical trial network and offer an unalterable and entirely traceable audit trail. Proof of concept work might necessitate a deviation from the original plan, and something new or imposed might change the suggested work.

In their study, Yaqoob et al. (2021) explained how to use blockchain technology for telehealth and telemedicine systems. They discussed how it can deliver telemedicine services in a secure, decentralized, traceable, and tamper-proof way.

So patients, doctors, researchers, medical institutes, hospitals, etc. can benefit from a patient's previously recorded medical history without violating their privacy and maintain availability, confidentiality and integrity while ensuring anonymity, Prabha et al. (2020) designed a health record-keeping system involving various actors; patients, doctors, insurance companies, pharmacies and more. To do this, he used a super-ledger structural block chain. To implement privacy and access control, a superfast ledger structure would require a different kind of resource, which would increase the cost of large, complex networks.

In their research, Wang et al. (2018) created a permissioned blockchain-based platform for sharing medical data. The blockchain-based platform can store a lot of medical data, and scientific research and medical institutions can easily access the data they need for various analyses. He put forth a permissioned blockchain-based platform for medical sharing that employs dual blockchain architecture, consensus on Concurrent Byzantine Fault Tolerance (CBFT), encryption technology and smart contract technology.

Methodology

Design Science Research (DSR) is the methodology used in this study. DSR, according to Gregor and Hevner (2013), is based on the need for something new or an improvement over what already exists. The new object is categorized using either a proposed system or an artifact. Examples of new artifacts or research-proposed systems include new software, algorithms, systems, or frameworks (Chatterjee et al., 2017). The steps that are taken to accomplish the goal of this research are depicted in Figure 2.

The telemedicine platform consists of the hospital interface where all the basic information concerning the patient and doctors and all hospital management such as name, date of birth, home address etc. are all stored and can be accessed by the hospital or any other as it does not contain vital information concerning the individual as shown in Figure 3. When the telemedicine is launched, it is being hosted on the blockchain and in this case the Algorand blockchain where all transactions are being done and stored in the blockchain through the use of smart contracts.

Smart Contract

Nick Saab, a computer scientist, first put forth the idea for a smart contract in 1994. It is a pre-programmed code to record and evaluate the information and data obtained and automatically trigger the system to execute the terms of the corresponding contract when the conditions stated in the program are satisfied.

Figure 4 illustrates how smart contracts, which include transaction preservation and state processing, operate on the blockchain. The transaction primarily consists of data sent, the characteristic of which is time. The smart contract's state will be updated once the transaction and event data has been passed into it. The state machine correctly and automatically chooses the contract action if the state satisfies the activation condition.

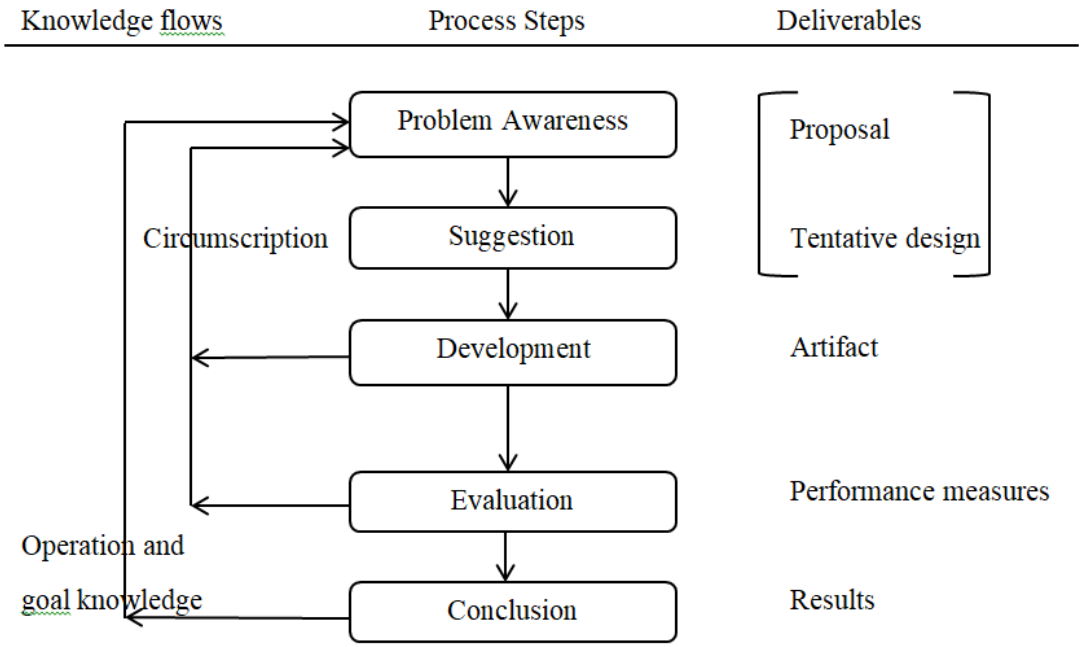

Fig. 2: Design Science Research general steps (Vaishnavi & Kuechler, 2004)

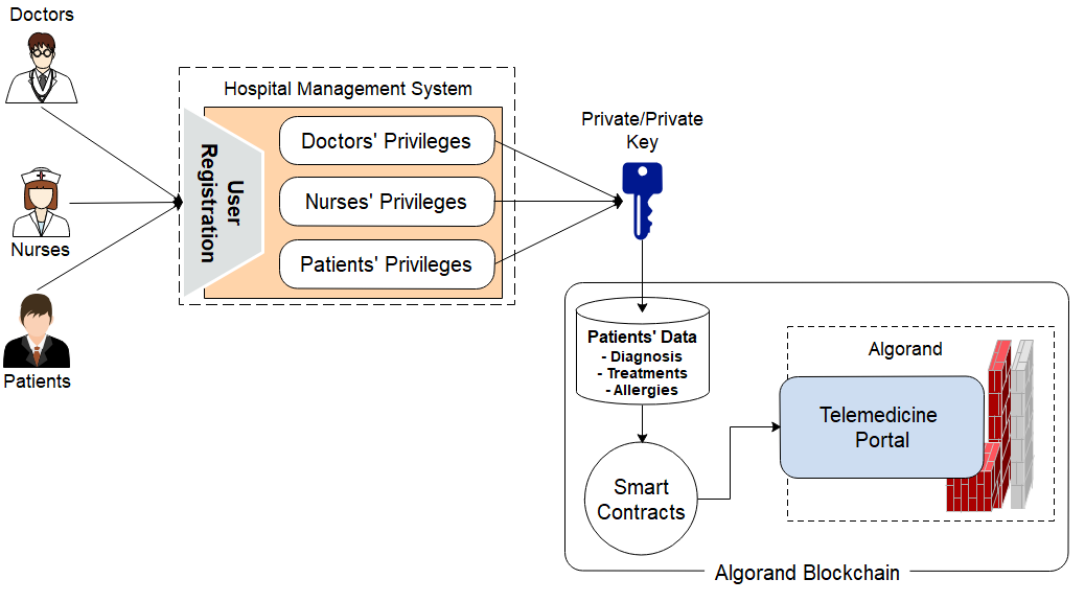

Fig. 3: System Architecture

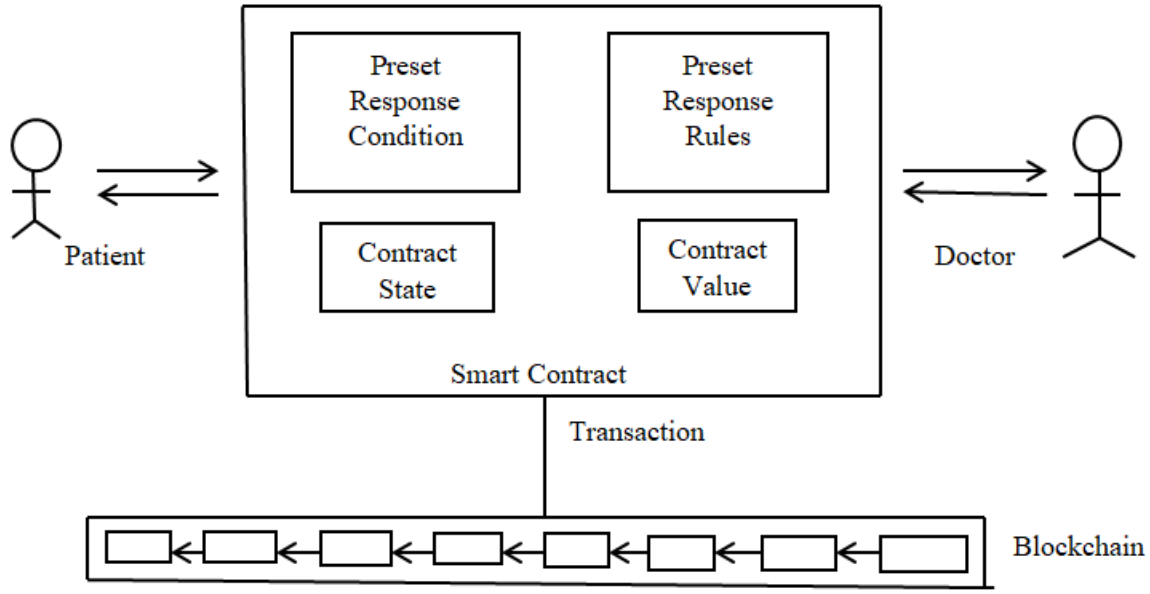

Fig. 4: Diagram of smart contract execution

Analysis of the proposed system

The proposed system is centered on the user of the telemedicine as shown in Figure 3. The approach adopted in our system is tailored to enhance the security of the users while also enhancing their privacy. The user is directly in charge of his data and can decide to grant or revoke permissions of the medical records accessibility. The analysis of the security and enhancement of the user data is presented in Figure 5 below.

In Figure 5, the backend of the telemedicine (labeled 1 in the figure) uses the Algorand consortium entities. The consortium is described in the consensus protocol. The telemedicine consortium uses the cryptographic sortition at each node at the beginning of each of the consensus protocol to determine if a node has a role to play in a particular step. It is a quick and easy operation that only requires the creation of one hash and a digital signature. A Verifiable Random Function is used to implement the sortition algorithm (VRF5). Users can create verifiable computations using VRF functions. By utilizing their private keys, the users create a proof that can be checked by other users using the user's public key.

Since Algorand is a public, decentralized, and permissionless blockchain, every block may be read, generated, and joined by anybody. However, a permissioned blockchain, known as co-chain, was also developed by the Algorand platform and is ideal for use in the development of telemedicine systems in this research as a public blockchain is not always the best option for handling sensitive information, such as electronic medical records of users. Co-chain is a private, authorized blockchain that offers the strict restrictions that businesses and health care providers normally seek out. As a layered system, it can still communicate with Algorand's public blockchain. Layer 1 is accessible to everyone and can be used interactively, while Layer 2 is private. The co-chain maintains complete autonomy from the public chain, hides the contents of its transactions from prying eyes, chooses its own validators, and uses its own Algorand consensus process.

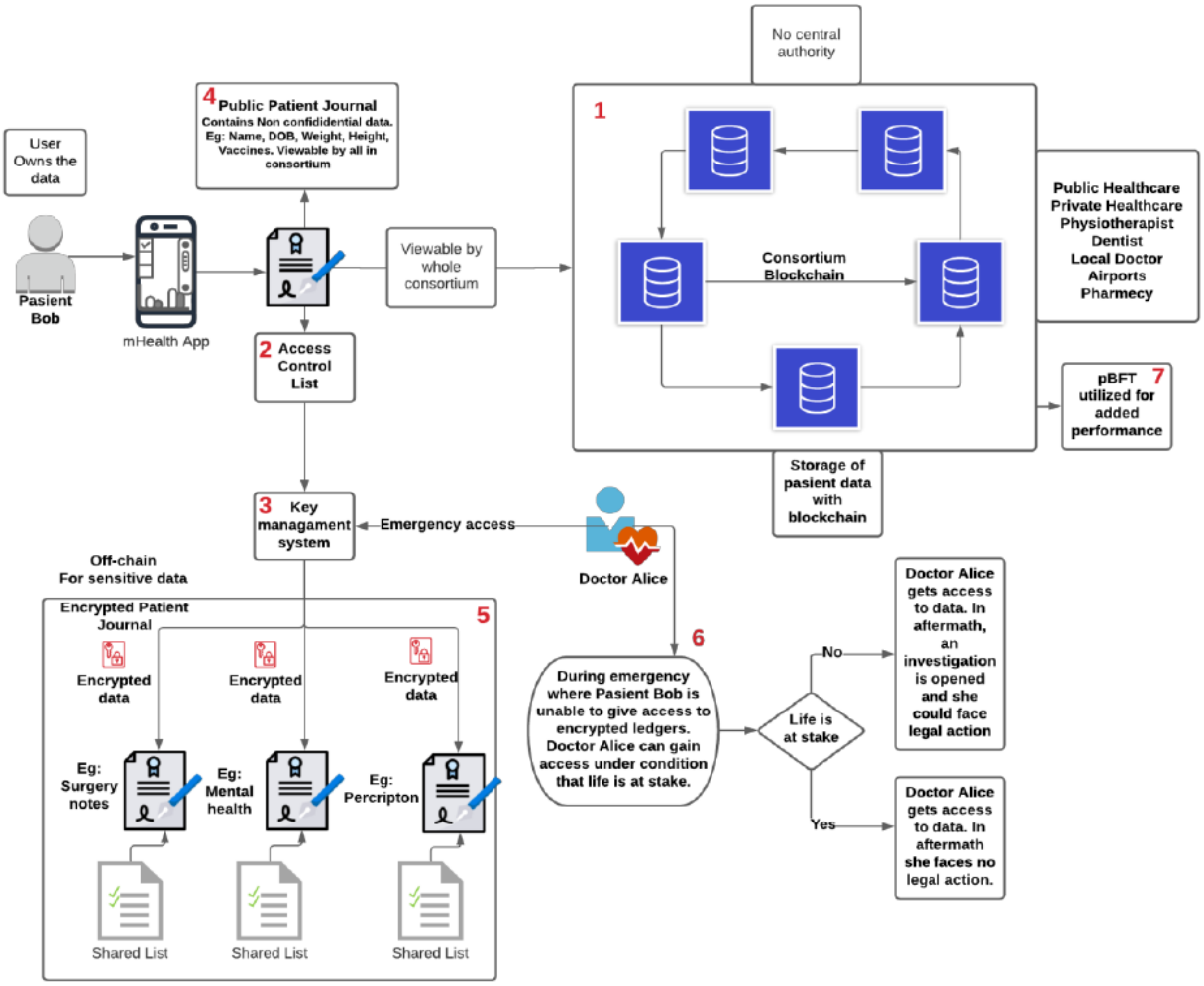

Fig. 5: Security and Privacy of Proposed System

Our proposed system is based on the Algorand permissioned blockchain (co-chain); therefore, the entities consist of government and private health care providers, general medical practitioners, physiotherapists, doctors, and dentists. These entities are represented in the system by a set of nodes, which are computers connected to the Algorithm Network. These organizations may have access to patient information that is not confidential. These details include the patient's name, date of birth, weight, and height, as shown in labeled (5) of Figure 5. To make it simpler for healthcare professionals to get essential information and give them a single location to look for it, this information is made available to everyone in the consortium. Each entity's information is saved in a database, increasing the attack surface because the data is dispersed. The user will also benefit from easy access to essential information because they will not need to join up elsewhere. The non-confidential patient's record available to all entities is sometime called the public patient journal, while private records are encrypted. Labeled (5) in Figure 6shows the type of information considered as patient's private journal. All sensitive data that a patient does not want to share, such as the type of surgery they had or the details of their procedure, is encrypted and kept privately on an off-chain blockchain. The off-chain blockchain, which is a separate blockchain used to store the private information

of individuals, is connected to the main blockchain, which is the foundation for telemedicine. Each patient's or individual's private data is stored separately and is protected through the generation of a set of encryption keys.

Secured Storage

Our proposed system utilizes a blockchain technology to implement a database search index tool. Unlike systems which use access control list method with a major drawback on scalability, the method in this system adds an extra layer of security a regular database which is used to mitigate issue of scalability. Instead of using a blockchain database, we store a pointer to the full encrypted electronic health records on the Blockchain as shown in Figure 6. In contrast to storing an entire database, the blockchain only stores a small amount of data. The security layer of the management of electronic health records is shown in section 4. Because the system limits the amount of information processed, it creates a much safer way to store access to data in the blockchain while maintaining performance. Having multiple entities access the database allows for decentralization.

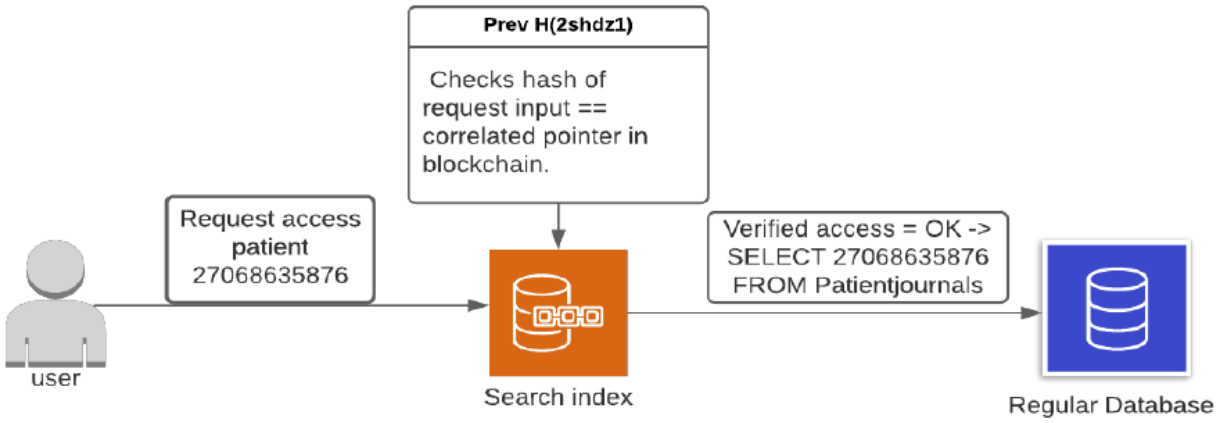

Fig. 6: Storage security layer of the proposed system

Access Control and Privacy Enhancement

An access (ACL) control list must be integrated in order to control who has access to the patient's private and confidential information. This updated list will contain information on who has access to view private data stored in the off-chain database. The patient must give permission for medical staff and doctors to access the private information. The patient can quickly make this choice in the user application. Figure 7 illustrates how the procedure causes the ACL to be updated. In this case, a crucial restriction is the need to update the key set. A generated private key pair and the ACL are related. Everyone on the ACL is then given access to the private key.

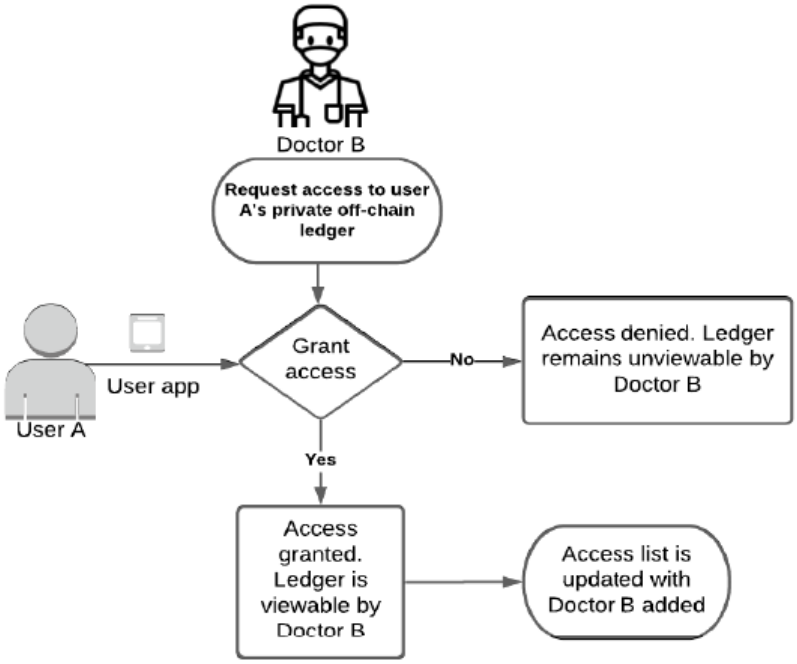

Fig. 7: Flowchart of access list to private data

The patient may also restrict access to their personal information. Additionally, using the user app makes this simple. New lists, including all IDs previously recorded for users with access revoked, then updated with ACLs. It is crucial to keep in mind that the person whose access was revoked now knows the previous keyset, which provided access to the private data. To work around this, a new key pair is generated and distributed for the IDs on the updated ACL.

Results and Discussion

Figure 8 shows the Algorand blockchain transaction template between the doctor and a patient; all the features that a blockchain possesses such as transaction ID, timestamp etc can be viewed. What sets Algorand apart is its speed and cutting edge capabilities. Algorand is fast, cheap, decentralized, carbon negative, and has advanced smart contract capabilities. Algorand can process thousands of transactions per second with instantaneous finality and transaction fees at a fraction of a cent. Other blockchains may be significantly more expensive, according to Kristin Boggiano, Co-Founder and President of Cross Tower and a member of the Blockchain and Crypto Assets Council (BACC).

The patient would have a session with the doctor complaining his/her problems and the doctor would therefore diagnose and probably prescribe drugs where applicable. This forms as the first transaction in the patient's chain.

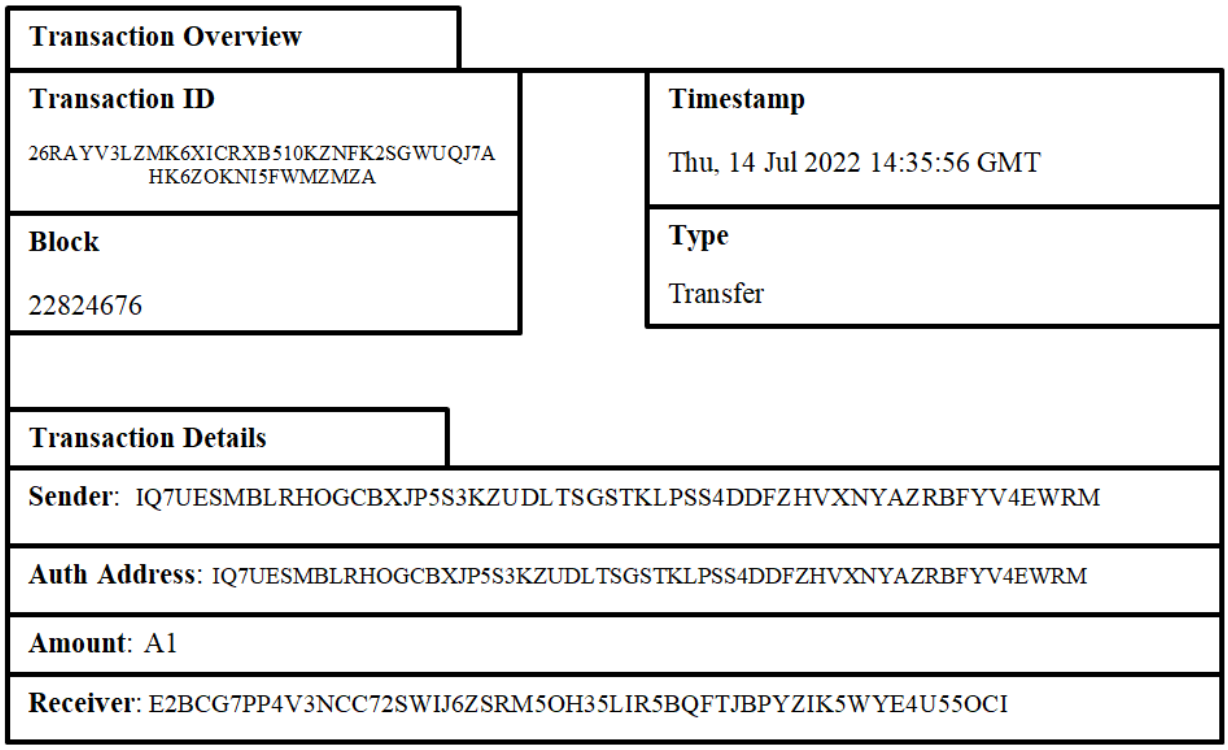

Fig. 8: Blockchain Transaction Overview between a Patient and a Doctor

This Algo transaction shows the transaction ID which is 26RAYV3LZMK6XICRXB510KZN-FK2SGWUQJ7AHK6ZOKNI5FWMZMZA and the Block number which is 22824676 with a time stamp of Thu, 14 Jul 2022 14:35:56 GMT, which is the time that this transaction was created.

The sender who is the patient has an Algo ID which is IQ7UESMBLRHOGCBXJP5S3KZU-DLTSGSTKLPSS4DDFZHVXNYAZRBFYV4E WRM and the receiver who is the doctor has an Algo ID which is E2BCG7PP4V3NCC72S-WIJ6ZSRM5OH35LIR5BQFTJBPYZIK5WYE4 U55OCI all have Identification and transaction identifications that are all in Cryptographic Hash format to ensure the information is not understood from unauthorized persons. This ensures that the data of the patient is secured and safe with the patient even if the hospital management may have the information, it would not be in a readable format.

Security Evaluation of Blockchain Platforms

Based on the six traditional definitions of security and dependability, the evaluation was done on the blockchain platform. The six attributes that are evaluated are:

1. Confidentiality: the potential to keep some transactions private; the lack of unauthorized sensitive data belonging to one or more nodes being leaked
2. Integrity: blockchain data not being improperly altered by unauthorized users
3. Availability: the system's capacity to deliver proper services without delays
4. Authorization: the system's capacity to define access privileges and rights to resources and to specify participant roles for approval
5. Accountability: the system's ability to track the actions and behaviors of a user's identity or a particular object

6. Client fairness: the system's willingness to democratically accept transactions from any customer regardless of choice.

Security Evaluation between Elliptic Curve Cryptography and RSA

An internet communication protocol known as Rivest Shamir Adleman (RSA) uses a public-key cryptographic algorithm (which our existing system used). Ron Rivest, Adi Shamir, and Leonard Adleman were responsible for its creation. Elliptic curve cryptography (which Algorand uses), a subset of public-key cryptography, uses the mathematics of elliptic curves to enable secure internet communication. Neal Koblitz and Victor S. Miller independently came up with the idea first.

They generate, encrypt and decrypt messages which help in data integrity. However RSA has several drawbacks as compared to ECC. These drawbacks make it convenient to use ECC in this work.

For public-key cryptosystems, ECC, in contrast to RSA, bases its design on the algebraic structure of elliptic curves over finite fields. ECC generates keys, which are therefore more difficult to decrypt mathematically. Therefore, ECC is considered a more secure implementation of public key cryptography than RSA and the next generation.

ECC generates keys and signatures faster with smaller cipher texts, keys, and signatures. It encrypts and decrypts data with mediocre speed. ECC uses a two-stage computation of signatures, which results in a lower overall latency than inverse. For authenticated key exchange, ECC has strong protocols, and the technology is well supported. Decryption and signing with RSA are both laborious processes that aren't always easy to implement securely.

Algorand by adopting ECC ensures high standards for both performance and security are upheld and never compromised. Websites work to simultaneously improve mobile optimization and online user data security, so ECC is used more frequently than RSA.

ECC has a big advantage over RSA as shown in Figure 9 when it comes to key size because a smaller key size can offer the same level of security as a bigger RSA key size. Because ECC uses smaller keys than RSA, it can offer the same level of security at a lower cost to computation and storage. This makes ECC relatively cheaper than RSA and has a good scalability for very large networks and users.

Figure 10 shows that when it comes to key generation, encryption, and decryption, ECC generally outperforms RSA. This is due to the fact that ECC processes data more quickly than RSA because it uses shorter key lengths and less complex mathematical operations. This makes ECC’s transaction time to be less and faster compared to RSA.

In transaction latency, compared to RSA, ECC has a sizable advantage in transaction latency as shown in Figure 11. This is so that data can be transferred at a faster rate thanks to ECC's smaller key sizes, which also lead to smaller data sizes. Lower latency is achieved by processing transactions more quickly thanks to faster data transfer rates.

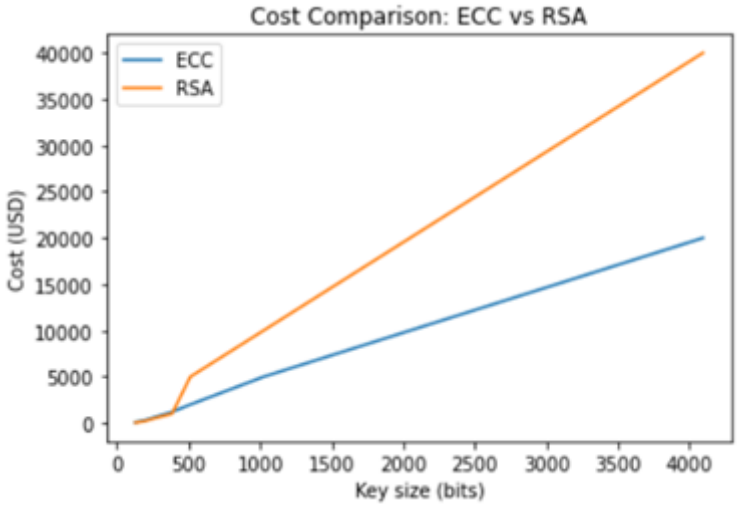

Fig. 9: Evaluation on Cost of Computation between ECC and RSA

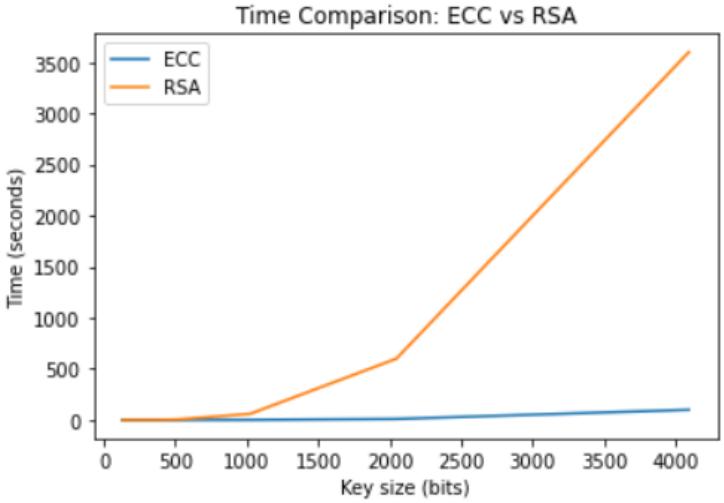

Fig. 10: Evaluation on Time in Execution between ECC and RSA

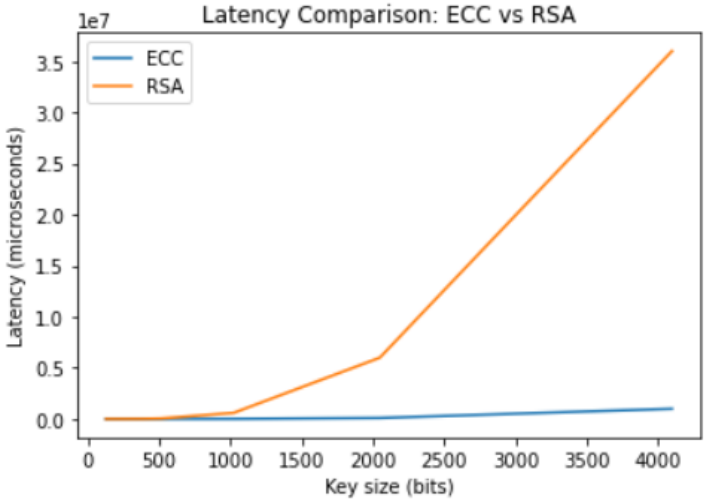

Fig. 11: Evaluation on Latency between ECC and RSA

Conclusion

By leveraging the secure and transparent nature of the Algorand blockchain, telemedicine providers can ensure large volumes of transactions can be handled securely and efficiently while ensuring the integrity, privacy, and availability of patient data. The Algorands blockchain's tamper-proof storage of encrypted medical records prevents unauthorized access or tampering, safeguarding sensitive patient information.

References

Abugabah, A., Nizamuddin, N., &Alzubi, A. A. (2020).Decentralized telemedicine framework for a smart healthcare ecosystem. IEEE Access, 8, 166575-166588.

Chatterjee, A., Shahaab, A., Gerdes, M. W., Martinez, S., &Khatiwada, P. (2021). Leveraging technology for healthcare and retaining access to personal health data to enhance personal health and well-being. In Recent trends in computational intelligence enabled research (pp. 367-376).

Gregor, S., &Hevner, A. R. (2013). Positioning and presenting design science research for maximum impact. MIS quarterly, 337-355.

Miller, V. S. (1985, August). Use of elliptic curves in cryptography.In Conference on the theory and application of cryptographic techniques (pp. 417-426). Berlin, Heidelberg: Springer Berlin Heidelberg.

Prabha, P., &Chatterjee, K. (2020, December).Securing Telecare Medical Information System with Blockchain Technology. In 2020 2nd International Conference on Advances in Computing, Communication Control and Networking (ICACCCN) (pp. 846- 851). IEEE.

Szabo, Nick. (1994). Smart contracts. Unpublished manuscript.

Vaishnavi, V. K., & Kuechler, W. (2015). Design science research methods and patterns: innovating information and communication technology. Crc Press.

Wang, X., Zha, X., Ni, W., Liu, R. P., Guo, Y. J., Niu, X., & Zheng, K. (2019). Survey on blockchain for Internet of Things. Computer Communications, 136, 10-29.

Wong, D. R., Bhattacharya, S., & Butte, A. J. (2019). Prototype of running clinical trials in an untrustworthy environment using blockchain.Nature communications, 10(1), 1-8.

Yaqoob, I., Salah, K., Jayaraman, R., & Al-Hammadi, Y. (2021). Blockchain for healthcare data management: opportunities, challenges, and future recommendations. Neural Computing and Applications, 1-16.

Koblitz, N. (1987). "Elliptic Curves Cryptosystems", Mathematics of Computation, vol. 48, pp. 203-209.