EasyChair Preprint

№ 5555

PR Wallet Based Blockchain Access Protocol to Secure EHRs

Mehul Gupta

May 19, 2021

PR wallet based blockchain access protocol to secure EHRs

Mehul Gupta, School of Information Technology and Engineering, Vellore Institute of Technology, Vellore, India
mehul.guptavit@gmail.com

Abstract- With the increase in the amount of data generated, especially in the healthcare sectors, one demands a revolution in the way data and records are being handled in this sector. The patients demand to gain instant access to their health data whenever the need calls. Many applications have promised their clients for such instant access. But the centralized systems driving the healthcare industry which comes handy to these instant access data, pose yet another concern for privacy and security of these patients' health records. This extremely sensitive health data risks being compromised by malicious intents and hence further attract cybercrimes. Legacy systems concerned with all the record-keeping and tracking of the patient's data are centralized and often need some third-party access to the data. These systems are also confined to an institution or an authority governing them and hence it becomes difficult to share this sensitive information with some external concerned legal authorities, even in case of any emergency. Blockchain, simply defined as a distributed ledger, has the characteristics to provide a decentralized, privacy-preserving environment in which records can be searched and shared easily with the concerned authorities. Although many institutions are contributing to developing blockchain as a means to secure EHRs, there have been discussions on its usability, especially like how elderly people or people with certain illnesses will be able to authorize institutions. Hence, in this paper, to address this issue, we introduce a Patient Record (PR) wallet and a new protocol to access the hybrid blockchain. We shall further introduce a similar application that addresses some of the common issues in this modal.

Keywords: Electronic Health Records, Ethereum blockchain, Digital wallet, Smart contracts

1. Introduction:

The Healthcare industry all around the world is emerging as one of the largest sectors, both in terms of the workforce involved and its contribution to the GDPs (Gross Domestic Product) of leading developing nations, according to the World Health Organization. With such tremendous growth, a massive amount of data is also generated in the form of patient's health

records, clinical information, doctor's analysis, or data generated in the form of IoT (smartwatches, or any health-monitoring applications). Hence there arises an ever-growing concern for the security of this data [22][23], which is highly sensitive to any patient. Since this huge data is normally centralized in nature, risks associated with its compromise may put the lives of many people at stake. Cyber-attacks on these EHRs are also common [24], with millions of records being compromised due to a small back door in the security of these systems. Studies estimated an amount of whopping $380 per medical record that was being compromised [1]. Blockchain, the technology which gained worldwide attention from developers after the launch of Bitcoin, has effectively addressed the issues related to data centralization, searching and sharing medical records across institutions, and helping the patient to control his/her medical records.

1.1 What is Blockchain?

Blockchain, put simply can be described as a technology which can be used to store transactions and its metadata on nodes or blocks, which are decentralized in nature. Depending on the configuration, a block can hold several transaction data. The blocks can contain the data about the transaction, details of participating parties, and most importantly a unique hash of the previous block in the series. The first block, however, is an exception called the Genesis block. The hash of a block is generated by algorithms like SHA-256, which changes even on slight modifications to block contents. Hence, each block is linked to the previous block, using this hash unique to each block. This characteristic makes the blockchain resistant to modification, and hence its immutability property.

Nodes are the building blocks of this decentralized ledger. A node can be any storage space that contains a copy of blockchain. In Ethereum, Geth is used to control any such node. As each node stores a copy of the blockchain, there is no single point of failure in the system as opposed to central servers. Blockchain, which was introduced as the underlying technology beneath bitcoin, has revolutionized many sectors, including finance, automotive, and healthcare.

1.2 Blockchain and its expansion in EHRs

Blockchain can be explained simply, as a chain of blocks tied together with the means of hash codes. As stated, each block in a blockchain apart from the genesis block, consists of the hash

of the previous block, and hence even a slight modification to data shall render the complete chain invalid. Although blockchain has the potential to serve in many different applications in healthcare and medicine, its use is increasing at a limited pace due to some practical demerits. Patients, especially the old-age persons, or be it people suffering from chronic illness are prone to forget their secret keys and are unable to manage their medical records. Such persons need to be specially assisted in their health and medicines.

1.3 Digitalizing medical records with blockchain

The existing state of the art technologies is sweeping well into the healthcare sector to digitalize patient records into EHRs with Machine learning algorithms used to identify the contamination from medical images to NLP which can help assist patient for common symptoms or develop medical notes using speech recognition. These technologies could perform much efficiently if these records can be digitalized. Now let us imagine a coronavirus patient going to the clinic with his physical copy of medical records. This contaminated physical copy of his record is often circulated through all the medical staff, including the physician, and the chemist, which can further escalate the contamination numbers.

If this same medical record had been accessed through a digital medium, the detection, tracking, and the observation of that patient would have been much easier. Blockchain shall help in not only digitalizing these records but also provide a safer decentralized medium for these accesses.

2. Existing Research:

There have been many previous works on the use of blockchain in healthcare to secure EHRs. One such work is MedRec, a 2016 MIT Media Lab initiative to create a blockchain-based record management system of patient's EHRs [2]. Developed on Ethereum blockchain, MedRec not only allows patients to control how their medical data is shared but also allows them to keep their transactional history all at one place.

A similar EHR management system, namely, MedChain [10] was developed to improve the existing healthcare technologies. Developed on the Ethereum blockchain, the system uses that only the nodes with permissions shall access the personal blockchain. Several approaches and initiatives related to securing EHRs with blockchain are also being made, for instance, MedBlock [13], MIStore [14], Healthchain [11], and Ancile [12].

A number of researchers argued that using blockchain for securing the EHRs could pose several disadvantages especially for elderly people, or persons with some chronic illness due to which the patient is unable to interact or grant necessary permissions to the concerned institution [4][5]. Cichosz et al. [3] presented a NEM blockchain solution for this problem, by introducing a multi-signature account for the patient. In case of emergency, the records can be accessed by authorizing permissions to the healthcare provider through a trusted party.

Hardware wallets have been a key asset in managing private keys in blockchain, but its integration in securing EHRs can add a new layer of security to it. D Ivan [6] mentioned a similar use of security tokens in preserving patient medical records on blockchain. Md. Ashraf Uddin et al. [7] deals with patient monitoring with the help of the data generated through various wearable devices, smart sensors, or other IoT devices [25][26]. It proposes a Patient centric agent that would manage the data streams and blockchain on which the distributed data be kept on.

Ms. R. Poorni et al. [8] discussed a digital certificate blockchain-based design to provide a more secure user authentication. It makes use of the immutability property of the blockchain, and hence the serial numbers of the certificates are stored in the blockchain instead of the actual certificate. To avoid further forgery, the design incorporates the alpha-blending of unique imprints.

Leila Ismail et al. [9] proposed a lightweight blockchain which reduces the network overhead and the computational complexity as compared to the Bitcoin network. This architecture can be effective in healthcare as the medical records can invite high traffic simultaneously.

3. Proposed System

The authorization system proposed is built over the Ethereum public blockchain. Ethereum enables dApps to run through a browser, without even the users have to mine a complete node of the blockchain. Smart contracts are an important feature of Ethereum, which while eliminating the need of a third-party also ensures that the contracts are deployed with ease.

To address the issue of mishandling of crypto keys, we introduce a Patient record wallet (or a PR wallet). A PR wallet, is particularly a password protected peripheral device which can be used to secure secret keys, and can be used for signing, authorization, etc. for transactions involved in managing EHRs. PR wallet shall contain the secret keys of the owner and can be used wherever authorization with private key is necessary.

This PR wallet can be password protected, or can even be biometric protected, using fingerprint scanner, or face unlock. Biometric enabled protection shall also guarantee access to medical data even when the patient is suffering from acute illness, or from chronic diseases like Alzheimer's disease, where he is not able to share his credentials [5]. This shall eventually allow emergency access of essential services to the patient.

Since this PR wallet acts as a cold storage, the risk associated with its compromise as compared to other hot wallets is also very less. Moreover, if the device gets misplaced, the patient can just be issued another one, without him being punished as the loss of his medical records. This PR wallet can not only act as an authorization system to the blockchain DApp, but it can also be used to establish a role-based access control over the records. Using this, a similar multi-party authorization system can also be incorporated in case of medical emergencies [15] to access patient's records.

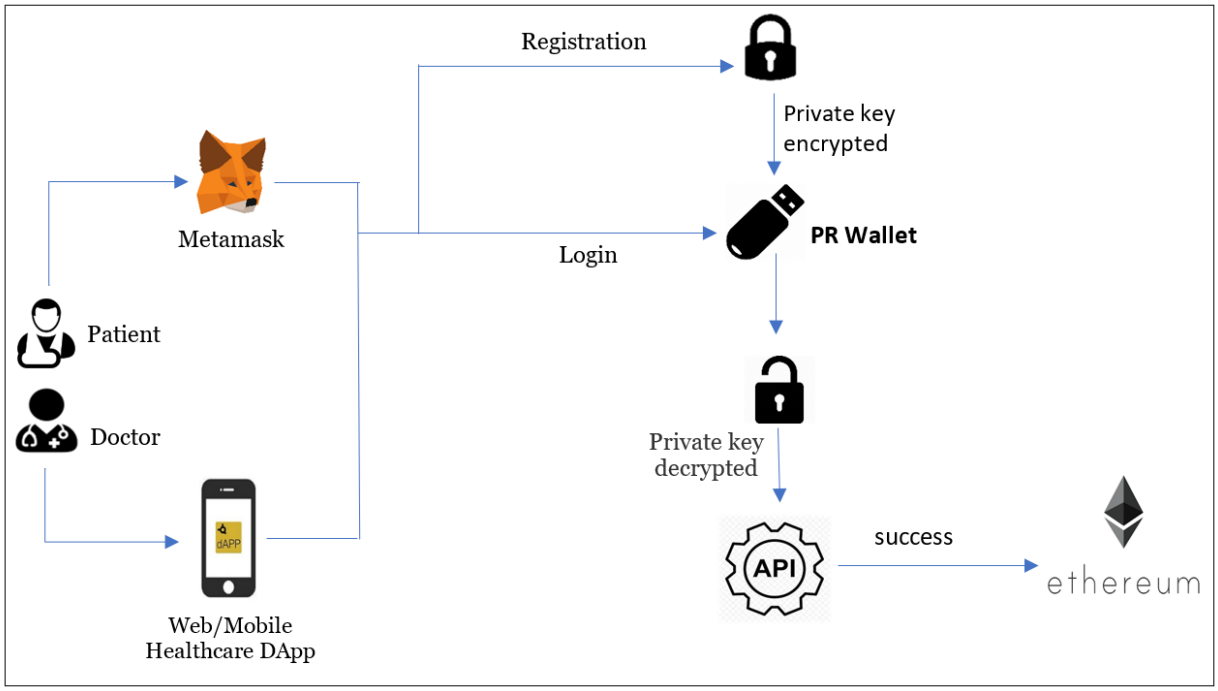

Fig 1 Protocol design of the proposed system

Fig 1. explains the architecture of the application whenever the patient wishes to access his clinical records, through Metamask or either by any healthcare web/mobile DApp. The user is automatically logged in by fetching the private key from the wallet. The wallet can be used similarly for signing any record, or in case of any authentication requirement. We shall further

see the uses of this wallet for multi-party patient authentication as well. Fig 2. shows the feature provided by Metamask to connect a hardware wallet to it similar to PR wallet.

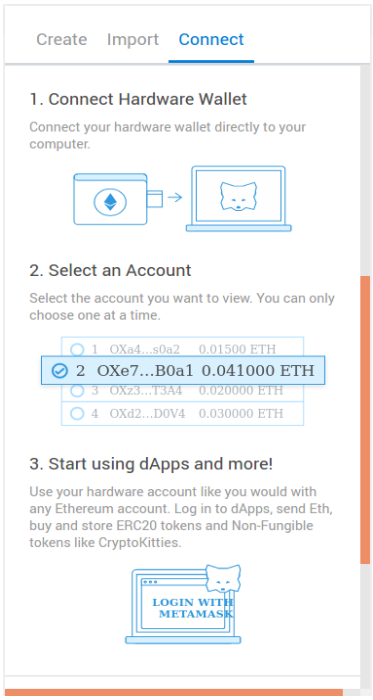

Fig 2 Connecting wallet through Metamask

4. Experimental Setup and Results Discussion

The application is developed using truffle and Ganache, which are an easy alternative to develop local Ethereum blockchains. The app uses Nodejs to handle server-side Ajax calls. Fig. 3 shows the patient registration module, which authenticates the user through Metamask after connecting the wallet to the blockchain. The application makes use of the smart contract to automate certain transactions, which gets deployed on the blockchain. The application provides facilities of easy management and sharing of EHRs, which are encrypted using AES-256 algorithm and stored in a separate address space.

Fig. 3 depicts the scenario when the user tries to connect to the healthcare application for the first time. For the process, a smart contract is deployed on the blockchain after the patient enters his public Ethereum address, which is assigned to map a particular user. Public Ethereum address also restricts the use of legitimate user details, such as name, place, DOB, etc. thus maintaining the user's privacy as well. Apart from deploying the smart contract, the user also requires to pay some processing fees, in the form of Gas. The gas amount is paid in the form

of Ethers, which is ultimately paid as a transaction processing fee to the miners. The regulating authorities, in this case, can determine the gas required for each transaction. The user also has the option to trade with another currency of his choice, in case he is not able or willing to transact with Ethers. The application automatically informs the patient, in the event of any errors, like insufficient funds, gas prices, or in deployment.

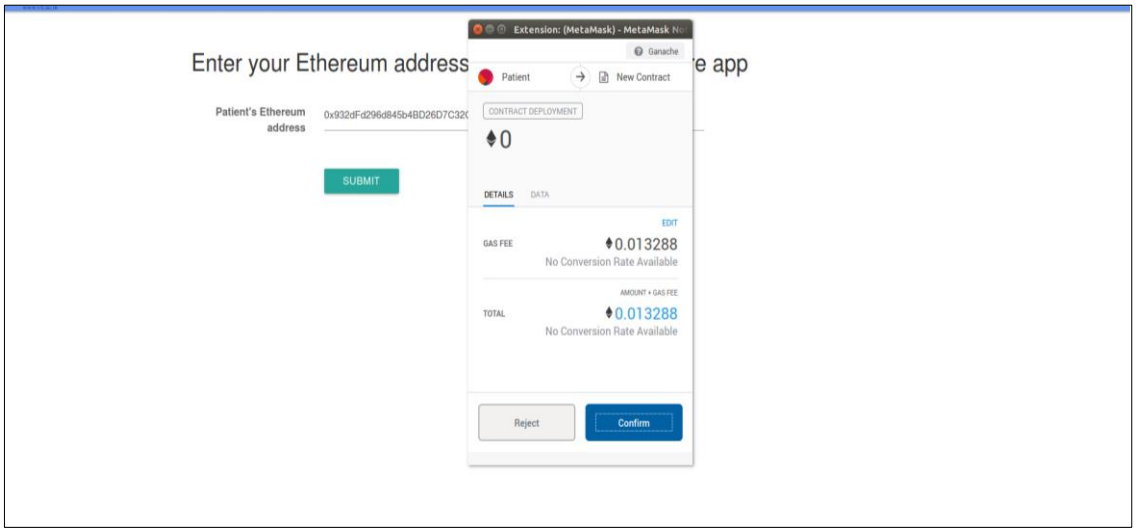

Fig 3. Patient registration on the DApp through smart contract

Ethereum, the blockchain technology on which the app is built, disables any possibility of an external party that can control the blockchain and hence the data. This means that the app is evidently resistant to data leaks as opposed to other applications, probably based on central servers and the everyday glitches in their code. Moreover, the distributed architecture of Ethereum makes it protected from many cyber-attacks, like DoS, DDoS, SQL injection, which targets SQL databases explicitly. The authorized authorities are required to validate any transaction before being mined on the blockchain, which further eliminates any type of network fraud or corruption of any type.

An additional security feature has been incorporated in the application where the smart contract deployed can also function as multi-signature functionality. This means that the smart contract will be deployed only if some amount of permissioned authorities agrees to sign the contract. The feature can be used to eliminate certain corrupt members who are trying to validate fraudulent data. This can also be useful especially when a patient using a multi-party auth feature cannot provide required permissions to the authority. In that case, other trusted parties

can proceed with the process on behalf of the patient. Further, the use of PR wallet acts as an alternative to grant access permissions and easy handling of the susceptible private key.

The application also deals with the issue of scalability, which can affect the transactions occurring per unit time on the blockchain, and can thus reduce its computational capacity. The application consists of a storage pool, which contains the actual records encrypted through AES-256 algorithm using a randomly generated symmetric key, whereas the hybrid blockchain consists of the address of the storage, decryption key, hash of the previous block and other metadata about the transaction, including the signature of the concerned authorities. The signature is required primarily for authentication and integrity, and at the same time, to avoid any replay attacks using nonce. When a record is accessed, the corresponding decryption key (symmetric key in this case) is fetched from the blockchain, the record is decrypted using this key, and the signature is matched and presented to the viewer.

For the purpose of testing and deploying the application, we have used Ganache. Ganache provides us with some virtual accounts with 100Eth for testing and local development. When deployed on the Ethereum Mainnet, it provides a similar functionality, as exhibited by Ganache. Fig. 4 shows some of the dummy transactions performed on the application by virtual accounts, with the transaction hashes and the contract address to which it was deployed. A column also displays the amount of gas required to deploy each transaction.

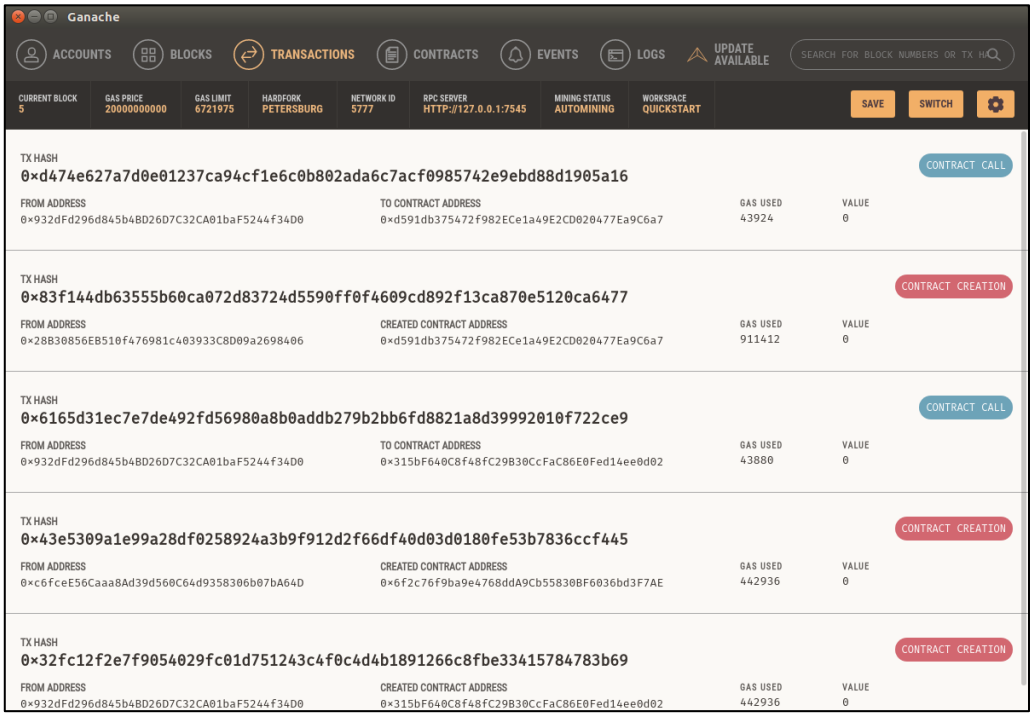

Fig 4. Transaction log of contracts deployed on blockchain

Reports estimated that around 41 million patient records were compromised in the US in 2019, which amounts to about triple the numbers breached in 2018. This demonstrates how bad even a single attack can be, when we have not started calculating the cost of such breaches. Most of the breaches occurred as a result of systems being siloed and running on outdated technologies. The application solves the problem of traditional attacks on central servers and protects the secret key being compromised for malicious intents. The medical status of the patient is signed duly before pushing its encrypted copy onto the storage space. Fig. 5 shows how the application makes use of the smart contract to request the concerned authorities to sign the patient's medical note.

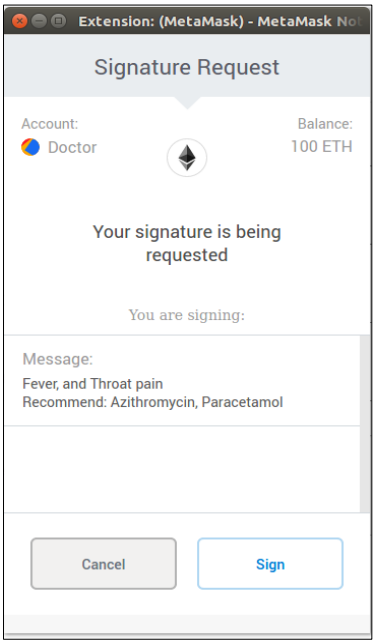

Fig 5. Signature requested to authorities by Metamask

Blockchain has the characteristics to deal with common issues such as single node failure, data integrity, inter-communication in a distributed environment, and various system vulnerabilities, pertaining to many central servers and cloud-based applications. However, the Bitcoin technology is not capable of delivering high transaction throughput, and promised scalability and privacy, and undergoes energy loss in the form of miner's efforts who could not make it to the main chain. There have been many approaches to design the healthcare support system using blockchain, big-data analytics with cloud computing, or using smart sensors and IOT integration. We present a tabulated and summarized result of this application's functionalities with some similar applications in this domain.

Table 1. Comparison of different applications for healthcare management [27]

	[16]	[17]	[18]	Our proposed system
Blockchain-based	Y	Y	Y	Y
Smart contracts	N	Y	Y	Y
Scalability	Y	Y	N	Y
Integrity	Y	Y	Y	Y
Access Control	N	Y	Y	Y
Multi-party authentication	N	N	N	Y
Integrated IOT support	N	N	N	N

5. Limitations of the system

The application is designed in such a way to address even the smallest issues pointed out by many researchers, including the question of security, scalability and private key authorization by critical patients. However, there still remain some challenges which we need to address collectively. The health data in the EU is governed by the GDPR (General Data Protection Regulation), which allows the monitoring of all Personal Identifiable Information (PII) [19]. According to GDPR guidelines, patients must govern the data added to the blockchain and hence, they have the right to update or modify this data. Also, they must have a right to wipe out this data. These two guidelines seem to conflict with the fundamental principles of blockchain. However, researchers have come up with some solutions as using Modifiable blockchains [20]. The project is also capable of dealing with this cause to some extent as it uses a hybrid blockchain as mentioned earlier. Also, there are some uncertainties on the technology as it new and hence not widely accepted. People are still not very reluctant to accept this, security and privacy being some of the major concerns.

Another prime concern is the extent to which the existing healthcare technologies are compatible with the modal. These technologies may find it difficult to interoperate with this decentralized web, which further questions its usefulness apart from the cost involved in its

installment. Scalability still remain a paramount concern as the system shall be dealing with enormous volumes of data per second, as the Bitcoin network supports an upper bound of 7 transactions per second. Although, as proposed in other research works [21], this application also attempts to fix this issue by implementing a separate storage space for the actual records, this issue can still be a bottleneck for the underlying technology.

6. Conclusion

With the tremendous data healthcare industry is generating, we must start thinking on ways to continually improve our data management techniques, but at the same time not compromising on the security and privacy of this data at any cost relating to the sensitivity associated with it. The healthcare system thrives to move from a central authority-based system to a patient-driven modal. This shift comes with a series of challenges that are being addressed and blockchain effectively solves the underlying problems associated with this shift.

The proposed PR (Patient Record) wallet acts as a medium to provide safe and simple access to the blockchain with hassle-free management of secret keys. It can also act as a medium for patients who hesitate going digital with their records to move to EHRs. The device shall provide security and reliability with its cryptographical encryption algorithms, which are not easier and feasible to break. The device shall prove successful in solving the patient's griefs of handling these keys and allows painless sharing and transfer of these records in case of acute illness.

The application provides ways by which the patient can grant and revoke any record specific permission to the authorities just with one tap. The use of Ethereum and smart contracts have made this automation very easier to implement. The latency in encryption and decryption of EHRs also affects the overall performance. For this purpose, we have used Cryptr, a Node.js module to encrypt strings via AES-256 algorithm in a quick and simple way. The application is also aimed at resolving the problems caused by direct transmissions of diseases in clinics, especially through hard copies of patients’ medical records and the increased risk associated with further contaminations of chains of people, for a disease like Covid19.

7. References

[1] Harshini, V. M., Danai, S., Usha, H. R., & Kounte, M. R. (2019, April). Health Record Management through Blockchain Technology. In 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI) (pp. 1411-1415). IEEE.

[2] Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016, August). Medrec: Using blockchain for medical data access and permission management. In 2016 2nd International Conference on Open and Big Data (OBD) (pp. 25-30). IEEE.

[3] Cichosz, S. L., Stausholm, M. N., Kronborg, T., Vestergaard, P., & Hejlesen, O. (2019). How to use blockchain for diabetes health care data and access management: an operational concept. Journal of diabetes science and technology, 13(2), 248-253.

[4] Agbo, C. C., Mahmoud, Q. H., & Eklund, J. M. (2019, June). Blockchain technology in healthcare: a systematic review. In Healthcare (Vol. 7, No. 2, p. 56). Multidisciplinary Digital Publishing Institute.

[5] Kassab, Mohamad, et al. "Blockchain: a panacea for electronic health records?." 2019 IEEE/ACM 1st International Workshop on Software Engineering for Healthcare (SEH). IEEE, 2019.

[6] Ivan, D. (2016, August). Moving toward a blockchain-based method for the secure storage of patient records. In ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST (pp. 1-11).

[7] Uddin, M. A., Stranieri, A., Gondal, I., & Balasubramanian, V. (2018). Continuous patient monitoring with a patient centric agent: A block architecture. IEEE Access, 6, 32700-32726.

[8] Poorni, R., Lakshmanan, M., & Bhuvaneswari, S. (2019, July). DIGICERT: A Secured Digital Certificate Application using Blockchain through Smart Contracts. In 2019 International Conference on Communication and Electronics Systems (ICCES) (pp. 215-219). IEEE.

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

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

[11] Ahram, T.; Sargolzaei, A.; Sargolzaei, S.; Daniels, J.; Amaba, B. Blockchain Technology Innovations. In Proceedings of the 2017 IEEE Technology & Engineering Management Conference (TEMSCON), Santa Clara, CA, USA, 8–10 June 2017; pp. 137–141.

[12] Dagher, G.G.; Mohler, J.; Milojkovic, M.; Marella, P.B.; Marella, B. Ancile: Privacy-Preserving Framework for Access Control and Interoperability of Electronic Health Records Using Blockchain Technology. Sustain. Cities Soc. 2018, 39, 283–297.

[13] Fan, K.; Wang, S.; Ren, Y.; Li, H.; Yang, Y. MedBlock: Efficient and Secure Medical Data Sharing Via Blockchain. J. Med Syst. 2018, 42, 136.

[14] Zhou, L.; Wang, L.; Sun, Y. MIStore: A Blockchain-Based Medical Insurance Storage System. J. Med. Syst. 2018, 42, 149.

[15] Radhakrishnan, B. L., A. Sam Joseph, and S. Sudhakar. "Securing Blockchain based Electronic Health Record using Multilevel Authentication." 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS). IEEE, 2019.

[16] Sahoo, Manuj Subhankar, and Pallav Kumar Baruah. "HBasechainDB–A Scalable Blockchain Framework on Hadoop Ecosystem." Asian Conference on Supercomputing Frontiers. Springer, Cham, 2018.

[17] Zhang, Peng, et al. "FHIRChain: applying blockchain to securely and scalably share clinical data." Computational and structural biotechnology journal 16 (2018): 267-278.

[18] Kim, Min Gyu, et al. "Sharing medical questionnaries based on blockchain." 2018 IEEE International Conference on Bioinformatics and Biomedicine (BIBM). IEEE, 2018.

[19] Akarca, D., et al. "Blockchain Secured Electronic Health Records: Patient Rights, Privacy and Cybersecurity." 2019 10th International Conference on Dependable Systems, Services and Technologies (DESSERT). IEEE, 2019.

[20] Lee, Nam-Yong, et al. "Modifiable public blockchains using truncated hashing and sidechains." IEEE Access 7 (2019): 173571-173582.

[21] Cichosz, Simon Lebech, et al. "How to use blockchain for diabetes health care data and access management: an operational concept." Journal of diabetes science and technology 13.2 (2019): 248-253.

[22] Reddy, G. T., Sudheer, K., Rajesh, K., & Lakshmanna, K. (2014). Employing data mining on highly secured private clouds for implementing a security-asa-service framework. J. Theor. Appl. Inf. Technol, 59(2), 317-326.

[23] Iwendi, C., Jalil, Z., Javed, A. R., Reddy, T., Kaluri, R., Srivastava, G., & Jo, O. (2020). KeySplitWatermark: Zero Watermarking Algorithm for Software Protection Against Cyber-Attacks. IEEE Access, 8, 72650-72660.

[24] Numan, M., Subhan, F., Khan, W. Z., Hakak, S., Haider, S., Reddy, G. T., ... & Alazab, M. (2020). A systematic review on clone node detection in static wireless sensor networks. IEEE Access, 8, 65450-65461.

[25] RM, S. P., Maddikunta, P. K. R., Parimala, M., Koppu, S., Reddy, T., Chowdhary, C. L., & Alazab, M. (2020). An effective feature engineering for DNN using hybrid PCA-GWO for intrusion detection in IoMT architecture. Computer Communications.

[26] Bhattacharya, S., Kaluri, R., Singh, S., Alazab, M., & Tariq, U. (2020). A Novel PCA-Firefly based XGBoost classification model for Intrusion Detection in Networks using GPU. Electronics, 9(2), 219.

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