Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 198 (2022) 185–192

Procedia Computer Science

www.elsevier.com/locate/procedia

The 11th International Conference on Current and Future Trends of Information and Communication Technologies in Healthcare (ICTH 2021)
November 1-4, 2021, Leuven, Belgium

Break-Glass Conceptual Model for Distributed EHR management system based on Blockchain, IPFS and ABAC

Mohammad Ali Saberi [a]*, Mehdi Adda [b], Hamid Mcheick [a]

[a]*Department of Computer Science and Mathematics University of Quebec at Chicoutimi, Chicoutimi, G7H 2B1, Canada*
[b]*Department. of Computer Science and Mathematics University of Quebec at Rimouski, Rimouski, G5L 3A1, Canada*

Abstract

The recently proposed Blockchain-based healthcare system proposes an interesting vision for the level of data integrity and security. This research aims to propose a conceptual model of a break-glass conceptual for Blockchain-based healthcare systems. In case of emergency, it provides access to the whole patient's medical records for healthcare professionals as quickly as possible regarding patients' privacy and data security. The proposed conceptual model was designed based on blockchain technology, IPFS (InterPlanetary File System), and ABAC (Attribute-Based Access control) as a novel design in this domain. In current healthcare systems, regulatory and non-integrated offline data sources make it near impossible for timely access to patients' EHRs and EMRs, even in case of emergencies for healthcare professionals. Our conceptual model could be a satisfactory alternative not only for patients but also for governing organizations to handle this situation clearly by regarding patients' privacy. Additionally, it can work in an untrusted environment, and it doesn't require bypassing the access control system to make the patients' data available. In case of emergencies, healthcare professionals receive medical records access near just in time with regard to all the rights of security and privacy based on the attribute which were set by the patients in the past. This novel conceptual model has been designed by coupling Blockchain technology with IPFS, and the attribute base control system (ABAC).

Keywords: Blockchain; EHR; Break-glass; ABAC; Healthcare system; Access Control

* Corresponding author. Tel.: +1-581-560-9020
E-mail address: mohammad-ali.saberi1@uqac.ca

10.1016/j.procs.2021.12.227

1. Introduction

1.1. Background

Blockchain technology is a fast-evolving sector that becomes more popular with researchers, and innovative projects are presented every day. The number of research projects in the healthcare system domain that is conducted with blockchain technology has exhibited a disruptive technology that has a high potential to be used in healthcare systems. The various types of innovation propose new advantages to other sectors which are similar but centralized. Dubovitskaya et al. 2020[1] had used this technology to improve data accessibility between multiple healthcare providers and hospitals. The peer-to-peer distributed ledger technology in Blockchain provides an immutable and transparent understanding of all the transactions that happen. Data is stored in the form of transactions in the chain ledger, and it is signed digitally into blocks in chronological order. Shared and immutable data storing in the blockchain technology make it a popular option for removing intermediaries, and it is a possible option to omit the centralized dependency [1]. The complexity and cost of a modern healthcare system are high in many cases, and the data flows are different based on each design, but it could be more effective in health record management and cost by applying blockchain technology [2]. Blockchain emerged to provide a distributed financial records exchange and storing infrastructure that has enabled data accessibility in a securely distributed manner. It can be a disruptive technology to increase the interoperability of healthcare providers in access to patient health records and increase the data integrity level [1].

In emergency care, access to medical records is an indisputable need to make efficient decisions as fast as possible. Electronic Medical Records (EMR) and Electronic Health Records (EHR) need to be available for healthcare professionals to access a patient's data promptly to facilitate the decision-making process [3]. A break-glass access control system is a mechanism for accessing encrypted medical records in case of emergencies for healthcare professionals to care for patients properly. It bypasses the access policy of the medical records to provide timely access to the EMRs for health professionals [4]. Attribute-based access control (ABAC) supports dynamic attributes to permit or reject the access request based on the object, subject, action, and context (environmental attributes) therefore, it decides to permit or reject the user access request [5].

1.2. Problem

Advancement in IoT-enabled medical services has caused new demand for creating connected environments and developing integrated patient's health records for effective treatment in healthcare services. In the current context, patient health records are stored in various data sources such as different hospitals and clinics which are not connected nor available timely even in case of emergency. The patients' health records should be accessible to healthcare professionals for efficient decisions on patient treatment processes, especially in case of emergency regardless of business matters such as routines or bureaucratic processes to save human lives. These matters motivate us to research this domain and develop a solution for this problem. Privacy is a matter in medical and health records storing and transmitting, and it needs to be protected from unauthorized access, but it should be available timely during emergencies for healthcare workers to make a vital decision on patients' treatment fast and effectively [6]. The question of the research is how to provide all of the health records of a patient in case of emergency for healthcare professionals in a timely and secure manner?

1.3. Objective

This paper aims to develop a conceptual break-glass model to provide access to EMRs and EHRs in case of emergency for healthcare professionals in a Blockchain-based healthcare system by regarding patient privacy. This matter is critical to saving patient lives by delivering EMRs and EHRs in a timely manner which is our main motivation in this research besides regarding patients' privacy rights. Several significant proposed blockchain-based healthcare systems have been reviewed and summarized in the domain of Blockchain-based healthcare systems to design the proposed conceptual model. We study their value proposition to understand the strengths and weaknesses

of such systems to draw a clear picture of the suitability feature in the aspect of the discussed problem. Developing a conceptual model for break-glass mechanisms in such healthcare systems is the objective of our research.

1.4. Contribution

Designing a novel break-glass conceptual model for healthcare systems using a combination of Blockchain Technology, IPFS, and ABAC is our main contribution. Our novel conceptual model has been developed along with other research projects in this domain. It is not similar nor comparable to any proposed model in this domain. Although several researchers have proposed Blockchain-based healthcare systems, we are the first research paper that proposes a break-glass mechanism for a Blockchain-based healthcare system that does not bypass the access control system to make the records available for healthcare professionals. Our proposed model is related to the body of knowledge by reviewing the related significant research in this domain and combining their results in a novel design is the authors' contribution. It helps us to develop a related but distinguished conceptual model to propose a unique value in this domain and extend the body of knowledge.

2. State of the art

In this section, we have reviewed notable research in this domain to create a comprehensive understanding of the domain. We present the main argument of each research to draw a relationship between our research and the body of knowledge. We have discussed Blockchain technology, IPFS, ABAC in the context of healthcare systems in the following review.

Dubovitskaya et al. [1] have focused on high levels of patient mobility by making the EMR access manageable through Blockchain. They proposed a prototype to share EHR access through Blockchain and the encrypted EMRs to store in the public cloud. Patients can manage their health records. In their prototype, they implemented an independent pluggable module regarding the FHIR standard to facilitate the adoption of their system. They had mentioned they use HL7 in their prototype for better interoperability too. Blockchain can improve the verification and integrity of health data and impact cost and data quality in healthcare systems. It eliminates the 'middleman' for healthcare systems and removes the required multiple levels of authentication. Blockchain increases transparency in data access for everyone who is part of the blockchain architecture to solve the various challenges faced by the healthcare industry today [2].

In [7,8] they implement their access policies based on Blockchain technology, the same as much other research such as [1,2] they provide security by a Decentralized Application (DApp). ABAC models are mostly centralized, which is a feature that might be the cause of a problem in scaled scenarios such as supply chain in synchronization and trust between the parties. They had stated smart contracts and blockchain technology solves current centralized systems issues to be a flexible infrastructure that represents the relationship of trust and support essential in the ABAC model [7]. One of the major problems with Blockchain is its storage capacity. In Hussien et al. [8] they discussed an existing gap between PHRs and Blockchain, and they stated it is fillable by encrypting medical data and outsourcing an InterPlanetary File System (IPFS) storage. They called it "smart contract-based attribute-based searchable encryption (SC-ABSE)" and it has been made by combining ciphertext-policy attribute-based encryption (CP-ABE), searchable symmetric encryption (SSE), smart contract, and IPFS storage [8].Pournaghi et al. [9] raised keeping medical records in different data sources as a problem. Medical entities have added a controlling layer on medical records which is an obstacle to accessing medical records fast enough, even for patients. Kumar and Tripathi [10] aim to solve scalability issues in the blockchain network. The cause of the issue is due to duplication in the peer. They propose a solution by integrating smart contracts and the Bell Lapadula security policy Model. Diverse permission management and verifiable transparent access control are the potency of Blockchain which is declared by Zhu et al in their research [11]. They propose Transaction-based Access Control (TBAC) platform to integrate the ABAC model and the Blockchain system.

As discussed in the above research, Blockchain has a high potential to integrate health records from different sources. Additionally, the above researchers have specified a high level of security and privacy as features of their proposed systems. Therefore, Blockchain has a high potential to apply security, integrity, privacy into healthcare systems. Blockchain characteristics such as immutability, transparency and decentralized distributed data storing

present a range of applications in healthcare systems. There are some challenges in accessing the patient's medical records. Healthcare providers and regulatory has different processes to grant access to a single medical record.

Most of the reviewed architectures in this paper are blockchain-based healthcare systems that use a distributed ledger database on a peer-to-peer (P2P) network that comprises a list of ordered blocks chronologically. These are decentralized distributed systems without any dependency on third parties for regulation but themselves. Because of decentralization, a Blockchain-based system has no limits such as a single point of failure, and data is stored in the ledger that is accessible by all the nodes in the blockchain. Shi et al. [12] do a survey in this domain in 2020 that shows not only that the mentioned features are the benefits of using Blockchain but also show anonymity and controllability as strong as the others. All momentous research projects in the domain agreed upon, Blockchain technology has created an opportunity to transform the design of current EHR management systems by proposing new architecture, frameworks, and models based on Blockchain. They demonstrated EHR management system transformation in the aspect of some quality features. Shi et al. [12] classified them into security, privacy, anonymity integrity, authentication, controllability, accountability, and auditability.

All the reviewed EHR management systems in this research and Shi et al. [12] review paper used blockchain as storage for access control management. In rare research, blockchain is used as storage for medical records. The high rate of redundancy has made blockchain expensive for storing data in volume. There is a range of solutions for data storing in volume, but distributed systems are more popular for great performance in traffic besides volume. Instability, lack of auditing, and incentive mechanisms in Peer-to-Peer (P2P) distributed file systems raise a need for alternative technology. Distributed file systems (DFS) are welcomed in this context to develop new technologies such as Inter-Planetary File System (IPFS) and Swarm. Blockchain-based DFSs successfully provide a solution to cover disadvantages of blockchain in data warehousing and using Blockchain strength such as scalability and privacy [13].

Kurt Peker et al. [14] address some quality features in their research such as integrity, authenticity, availability, and fault tolerance which all exist in Blockchain by their declaration, and they continue Blockchain is suited for some scenarios in IoT too because of its distributed architecture which does not have a single point of failure. In Kumar and Tripathi [15], they propose an IPFS based blockchain storage model to solve the storage problem just for transactions. In their storage model, miners store transactions on IPFS and get the returned IPFS hash value of transactions into the distributed hash table. Francesco Maesa et al. [16] proposed a blockchain-based access control system to track the change ownership of the data. The right to transfer access from one user to other users through a proposed access control system. They recommend to those who plan to extend their research to study how to better embed an access control system in blockchain technology.

As discussed earlier, the opportunity for Blockchain to apply towards EHR systems is to increase security and privacy in addition to integration, accountability, and accessibility, which has been discussed in this section. Our models have been shaped based on some quality features which have suitability and advantage for use. These advantages and suitability are discussed in the reviewed paper and mentioned in the state of the arts. In the result section, we propose our model, and in the discussion section, we fully discussed our design in the aspect of 'Why' and 'How'.

3. Results

In this section, we propose a break-glass mechanism that applies to the Blockchain-based Healthcare system to grant access to a particular patient’s medical records. In case of an emergency, healthcare professionals can request to access the patient’s EMRs, and this mechanism will be activated to provide EMRs to healthcare professionals. Additionally, we discuss why we choose such a structure and how it relates to other research and body of knowledge. But at first, we present a summary of the state of the art to explain our point of view and drill down into the question of this research to draw a picture of how the state of the art is related to it. We have some assumptions which are not discussed in this paper such as how the Blockchain-based healthcare system works in detail but to create a comprehensive understanding of our results some related topics have been discussed. The rules and designs of the Blockchain have been shaped by the body just to serve as the main data which is stated as the purpose of Blockchain. In this paper, the purpose of using Blockchain is:

1) Logging the access requests to medical records of patients.
2) Grant and revoke access to medical records by patients to individuals.

to meet the requirements such as security, privacy, integrity, and accountability which are fully discussed in the state-of-the-art section. Medical records of each patient are used privately by only authorized individuals. The body of the block contains the hash value of the Merkle tree root for transactions. The Merkle tree stores transactions in every leaf, and the hash value stores into the non-leaf nodes and both nodes concatenated in child nodes to support the efficiency for verification and integrity [12]. The consensus algorithm is not subjective in this paper because we assume all the consensus algorithm alternatives are not relevant to the performance of the break-glass mechanism, and the focus of this research is just on the break-glass mechanism. As we know, about Blockchain, each block contains a set of immutable records in chronological order. Immutability is a quality feature that is implemented by storing the hash value of the previous block in the current block. Each block has two hash values, one is the hash value of the previous block, and the other is the hash value of itself. In this procedure, any manipulation on the records will change the input of the hash function and consequently generate a new hash value that is different from the current. Therefore, the described block will be systematically unchained to the Blockchain due to a falsified root hash. IPFS is a distributed file system that provides a high-throughput content-addressed block storage model, with content-addressed hyperlinks that connect all computing devices with the same file system. In IPFS, a distributed hash table (DHT) is a key component which maps keys to values in the distributed system. IPFS is used for content routing systems and acts as an orchestrator between a catalogue and a navigation system. It likes a large table that presents what data is stored where and who has what data [18]. DHT has no single point of failure, and nodes do not need to trust each other. In comparison with cloud storage, IPFS has no central server, and the data is stored distributed in some ways, that is delivered infrastructure as a service for those who are not interested in doing all their requirements by themselves. The IPFS design delivers a secure mechanism, however, nodes do not obligate to trust each other for file storing [17].

As we explained before, this is a conceptual model which has several alternatives to implement each part of it and we do not discuss in detail that is out of the focus of this research. We proposed a Blockchain-based ABAC break-glass mechanism for EMR and we focused on lighting up the proof of concept in our conceptual model. The conceptual model is illustrated in figure1:

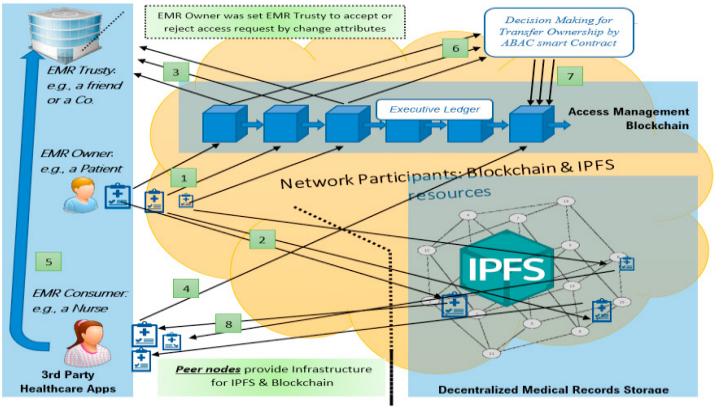

Fig. 1. ABAC Break-glass Conceptual Model based on Blockchain & IPFS.

The conceptual model has been described by three types of description. The structural design describes the conceptual structure in general, the user's role defines various types of roles, and the key elements present the domain of each element in detail. The structural design has been shaped as follows:

- Executive ledger: It is a blockchain ledger with the ability to execute smart contracts. There are many open-source non-proprietary alternatives for this element of our model, it could be a fabric ledger or a fork of Ethereum, etc. The logic of the model is embedded into the ledger, eventually, the chain of blocks is created by

this logic. Record structure, block encryption, new block creation, linking blocks, and all components except medical records storage are placed into the ledger as has shown in figure1. In the short description, the system management is implemented by the executive ledger indirectly.

- Network Participants: The who participates in the blockchain ledger and IPFS storage to provide system resources such as processors and storage. Each participant of the peer-to-peer network by providing resources such as processors and storage does tasks such as persists records, executes smart contracts, and obeys the logic of the Blockchain system to keep it alive. ABAC and EMR storage systems require infrastructure resources that are used for IPFS and Blockchain processing. These resources have been provided by peer nodes.
- Break-glass mechanism: The mechanism which every EMR owner can enroll in for giving reading permission of their medical record to healthcare professionals in case of emergencies that has presented as a flow in the figure1. the Break-glass mechanism, some participants propose trusting services to EMR owners to set attributes in case of emergency as a trusted party which is available in case of emergency. These trusted parties use the authorization of healthcare professionals to set attributes in the executive chain. The main task of this mechanism would be delivering access to electronic medical records of an individual patient as fast as possible and regarding privacy and security of those set by patients themselves.
- Consensus mechanism: An agreement on how to data persistence mechanism into the blockchain which writes the records of each block and creates new blocks to continue the chain of the blocks by connecting each block to the next one. There are some reference algorithms to implement this mechanism, such as POW and PBFT, which are explained in [12] and most of them could be used by this conceptual model.
- Users: All individuals who use the networks are users. Patients, nurses, 3rd party applications, researchers, etc. Users use the network through the application services which has been presented as a gray rectangle in figure1.

Based on our design and the characteristics of blockchain which we had discussed in the preceding, the key goal of our design is a secure break-glass mechanism in the blockchain-based EHR systems. In our proposed conceptual model, we have various types of network users called which have been called roles. An individual user could have one or more roles. The model consists of the following roles:

- EMR Owner: the patients or their trusted party that represent the EMR & EHR ownership
- EMR trusty: authorized by Owner to made decision for setting new attributes on EMRs & EHRs In emergencies
- EMR Consumer: Who has limited right based on the attributes defined by EMR owner or EMR trusty.

In the preceding part, we have discussed structural design and roles in our conceptual model. Structural design and the role of users are logical elements of our broken glass conceptual model to deliver EMRs, but an understanding of the software structural elements is also required. These three elements have been illustrated as three gray rectangles in figure1 to distinguish the area of the element in comparison to the others. the proposed model builds on some key elements which are explained below:

- Access management Blockchain: Access Control List (ACL), ABAC system, and access ownership log stored in Blockchain. Access Management Blockchain is a structure for storing access rights, granting, or revoking the ownership of medical records. It works based on the public / private key to identify which user has the right to change the ownership of each access. The identification key of each user such as healthcare professional, research institute, hospital, patient, etc. is their public key. Granting or revoking permission to a user is a process that has been done based on a public/ private key. The security of this method is proven and that is a very convenient practice that is used by many systems. Hence, this method systematically does the authorization, and all EMRs are protected from unauthorized access.
- Decentralized medical records storage: IPFS has chosen to be used to store encrypted EMRs as distributed storage to secure EMRs from flaws such as a single point of failure, private data leakage, and unauthorized access to EMRs. It has been chosen for storing as distributed storage to secure EMRs from flaws such as a single point of failure, private data leakage, and unauthorized access to EMRs. The first advantage of using the IPFS is the ability to store encrypted files as separate chunks which are placed in different servers. The capability of storing and retrieving encrypted data from IPFS is proof of privacy of the system and it creates the ability to work

in untrusted environments which are fully protected from unauthorized access. A single point failure flaw is not valid for the proposed model due to the nature of distributed storage.

- 3rd party healthcare Apps: Our Conceptual model is just the data layer of a healthcare system. 3rd party software developers can use the system as EMR storage. Due to the transparent nature of Blockchain, there is high potency for collaboration and contribution from other companies and software developers to use our model in their software. Third party contributions are a key advantage for the model, and we recommend making the Blockchain public to deliver the availability of development to other software developers.

Users, after encrypting their medical records, send an insert request to one of the blockchain nodes. If the request has the correct format of the blockchain standard defined in the consensus algorithm, it creates necessitated records in the response. The user should send the file size, hash of the file, its public key, and the public keys of all other EMR owners in the insert request. Blockchain node process request and based on consensus algorithms communicate with the network and the request creates records in the blockchain. Each insert request is based on the number of EMR owners and creates various records. Each record has an access information part which is encrypted by the owner's public key. In the access information part, the IPFS storage URL and public keys of the node for secured communication have been embedded. All public keys are available in the blockchain, and it determines which information is readable for whom. Users communicate with IPFS based on blockchain records through a secure encrypted connection created by the exchange of their public key that had been registered in blockchain records. In this method, each user can transfer ownership of their medical records which are registered into the Blockchain ledger. As explained, of inserting records into Blockchain, it has an information part that is encrypted by the owner's public key. In the information part, owners can set the public key of the EMR trustees. EMR trustees are the 3rd party to the application. They can investigate the attributes of the consumer and permit or reject them in the response to requests.

The above explanation has presented our proposed conceptual model, but the next question is what the workflow is in case of an emergency to make EMRs accessible for healthcare professionals. Under our ABAC break-glass mechanism, EMR trustees have permission to transfer ownership and access attributes. The EMR Owner has set attributes in the information part of the records and transferred the ownership to the EMR trustees who received the master authority to check the contextual attributes to reject or permit break-glass access. In this method, in case of emergency, all EMRs of the patient are traceable on the blockchain by its public key, and all its EMR trustees are determined by the transaction log of the Blockchain. EMR trustees can be every individual, such as an organization or a friend. Using encrypted data protects the privacy and security of all patients with respect to all rights of patients. All rights must be transferred to another party by the EMR owner or EMR trustees selected by the owner. This means the transfer is exclusively dependent on the EMR owner's public/private key.

4. Limits & Discussion

This paper aims to facilitate the accessibility of patient data for healthcare professionals as fast as secure in case of an emergency. Blockchain and IPFS show great potential in transforming the conventional healthcare system in which we present operational usage by a conceptual model for an ABAC break-glass mechanism. This is a great opportunity to deliver more accountability and accessibility to a blockchain-based healthcare system, however, discussed in the state-of-the-art has security, privacy, and integrity as its embedded qualitative features. Our conceptual model meets the requirements of the healthcare system such as privacy and security by its ABAC as well as guaranteeing the accessibility of EMR in case of emergency for healthcare professionals by Break-glass mechanism. Additionally, it serves accountability based on the immutability nature of the Blockchain in information persistence. Nevertheless, there remain several challenges for those who want to implement the system to adapt to the current operating system and current Health System routines.

5. Conclusion

This paper aims at facilitating the accessibility of EMR for healthcare professionals as fast as they can secure in case of an emergency. Blockchain technology and distributed file systems show great potential in transforming the

conventional healthcare system in which we present operational usage by proposing a conceptual model for an ABAC break-glass mechanism for EMRs in a healthcare system that it used Blockchain and IPFS in its design. This is a great opportunity to deliver more accountability and accessibility to a blockchain-based healthcare system, however, discussed in the state-of-the-art has security, privacy, and integrity as its embedded qualitative features. Our conceptual model meets the requirements of the healthcare system such as privacy and security by its ABAC as well as guaranteeing the accessibility of EMR in case of emergency for healthcare professionals by Break-glass mechanism. Additionally, it serves accountability based on the immutability nature of the Blockchain in information persistence. Nevertheless, there remain several challenges for those who want to implement the system such as adapting to the current routines with the proposed system. Also, we have discussed extending domain areas for further insight into this research.

References

[1] Dubovitskaya, A., Baig, F., Xu, Z., Shukla, R., Zambani, P.S., Swaminathan, A., Jahangir, M.M., Chowdhry, K., Lachhani, R., Idnani, N.,Schumacher, M., Aberer, K., Stoller, S.D., Ryu, S., Wang, F., 2020. ACTION-EHR: Patient-Centric Blockchain-Based Electronic HealthRecord Data Management for Cancer Care. Journal of Medical Internet Research 22, e13598.

[2] Tanwar, S., Parekh, K., Evans, R., 2020. Blockchain-based electronic healthcare record system for healthcare 4.0 applications. Journal of Information Security and Applications 50, 102407.

[3] T. de Oliveira, M., Bakas, A., Frimpong, E., Groot, A.E.D., Marquering, H.A., Michalas, A., Olabarriaga, S.D., 2020. A break-glass protocol based on ciphertext-policy attribute-based encryption to access medical records in the cloud. Ann. Telecommun. 75, 103–119.

[4] Yang, Y., Liu, X., Deng, R.H., 2018. Lightweight Break-Glass Access Control System for Healthcare Internet-of-Things. IEEE Trans. Ind. Inf. 14, 3610–3617.

[5] Kashmar, N., Adda, M., Atieh, M., Ibrahim, H., 2021. A Review of Access Control Metamodels. Procedia Computer Science 184, 445–452.

[6] Aski, V., Dhaka, V.S., Parashar, A., 2021. An Attribute-Based Break-Glass Access Control Framework for Medical Emergencies. In: Sharma, M.K., Dhaka, V.S., Perumal, T., Dey, N., Tavares, J.M.R.S. (Eds.), Innovations in Computational Intelligence and Computer Vision, Advances in Intelligent Systems and Computing. Springer, Singapore, pp. 587–595.

[7] Figueroa, Añorga, Arrizabalaga, 2019. An Attribute-Based Access Control Model in RFID Systems Based on Blockchain Decentralized Applications for Healthcare Environments. Computers 8, 57.

[8] Hussien, H.M., Yasin, S.M., Udzir, N.I., Ninggal, M.I.H., 2021. Blockchain-Based Access Control Scheme for Secure Shared Personal Health Records over Decentralised Storage. Sensors 21, 2462.

[9] Pournaghi, S.M., Bayat, M., Farjami, Y., 2020. MedSBA: a novel and secure scheme to share medical data based on blockchain technology and attribute-based encryption. J Ambient Intell Human Comput 11, 4613–4641.

[10] Kumar, R., Tripathi, R., 2021. Scalable and secure access control policy for healthcare system using blockchain and enhanced Bell–LaPadula model. J Ambient Intell Human Comput 12, 2321–2338.

[11] Zhu, Y., Qin, Y., Gan, G., Shuai, Y., Chu, W.C.-C., 2018. TBAC: Transaction-Based Access Control on Blockchain for Resource Sharing with Cryptographically Decentralized Authorization. In: 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC). Presented at the 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC), IEEE, Tokyo, Japan, pp. 535–544..

[12] Shi, S., He, D., Li, L., Kumar, N., Khan, M.K., Choo, K.-K.R., 2020. Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey. Computers & Security 97, 101966.

[13] Huang, H., Lin, J., Zheng, B., Zheng, Z., Bian, J., 2020. When Blockchain Meets Distributed File Systems: An Overview, Challenges, and Open Issues. IEEE Access 8, 50574–50586.

[14] Kurt Peker, Y., Rodriguez, X., Ericsson, J., Lee, S.J., Perez, A.J., 2020. A Cost Analysis of Internet of Things Sensor Data Storage on Blockchain via Smart Contracts. Electronics 9, 244.

[15] Kumar, R., Tripathi, R., 2019. Implementation of Distributed File Storage and Access Framework using IPFS and Blockchain. In: 2019 Fifth International Conference on Image Information Processing (ICIIP). Presented at the 2019 Fifth International Conference on Image Information Processing (ICIIP), IEEE, Shimla, India, pp. 246–251.

[16] Maesa, D.D.F., Mori, P., Ricci, L., 2017. Blockchain Based Access Control. In: Chen, L.Y., Reiser, H.P. (Eds.), Distributed Applications and Interoperable Systems, Lecture Notes in Computer Science. Springer International Publishing, Cham, pp. 206–220.

[17] Wang, S., Zhang, Yinglong, Zhang, Yaling, 2018. A Blockchain-Based Framework for Data Sharing With Fine-Grained Access Control in Decentralized Storage Systems. IEEE Access 6, 38437–38450.

[18] Distributed Hash Tables (DHTs) [WWW Document], n.d. URL https://docs.ipfs.io/concepts/dht/ (accessed 6.20.21).