# Towards a Break-Glass Model to access EMR in case of emergency based on Blockchain and ABAC

Mohammad Ali Saberi
*Department of Computer Science and Mathematics*
*University of Quebec at Chicoutimi*
Chicoutimi, Canada
mohammad-ali.saberi1@uqac.ca

Mehdi Adda
*Department of Computer Science and Mathematics*
*University of Quebec at Rimouski*
Rimouski, Canada
Mehdi_adda@uqac.ca

Hamid Mcheick
*Department of Computer Science and Mathematics*
*University of Quebec at Chicoutimi*
Chicoutimi, Canada
Hamid_mcheick@uqac.ca

***Abstract*— Blockchain technology is a fast-evolving sector that has proposed value in different domains. A distributed healthcare system for managing electronic medical records has various significant advantages in comparison to centralized healthcare systems. In a distributed system without a central authority, many threats such as data leakage by human mistake or a single point of failure are no longer feasible. A small number of recent research have proposed healthcare systems that have used IPFS and Blockchain as part of their security and storage components. Both have a transparent process and clear logic as a distributed system. In emergency care, access to medical records is an indisputable need to make efficient decisions fast. Current regulatory and bureaucratic processes make it near impossible to serve the data in a timely manner. This research designs a model of a break-glass mechanism for EMR management systems to provide access to healthcare professionals just in case of emergency. This conceptual model provides access to patients' records with regard to patient privacy and data security, which they set previously by themselves.**

***Keywords—ABAC, Break-glass, Blockchain, EMR, IPFS, Distributed healthcare system, EMR management system***

## I. INTRODUCTION

**Background:** Several healthcare systems have used Blockchain technology to improve data accessibility between multiple healthcare providers and hospitals [1]. Blockchain ledger provides an immutable and transparent view of all transactions in chronological order. Blockchain technology has enabled data accessibility by removing intermediaries to omit centralized dependency. A break-glass access control system is a mechanism for providing access to encrypted medical records in case of emergencies. It usually bypasses the access policy to provide timely access for health professionals [2].

**Problem:** Patients' health records accessibility for healthcare professionals is effective in patients' treatment processes, especially in case of emergency [3]. Patient health records are stored in different online and offline data sources such as different hospitals, which are not connected nor available in a timely manner even in case of emergency for other health providers. The patients' health records should be accessible to healthcare professionals regardless of business matters to save human lives. These matters motivate us to propose a solution for this problem. Privacy is a matter in medical records storing and transmitting; besides medical records need to be protected from unauthorized access but be available timely during emergencies [4]. The question of our research is how can healthcare professionals access electronic medical records in case of emergency in a timely and secure manner?

**Objective:** The authors of the paper aim to develop a conceptual model for a break-glass mechanism to access patients' EMRs in case of emergency for healthcare professionals in Blockchain-based healthcare systems by regarding patient privacy. This research aims at a critically important problem in the recently proposed healthcare system, which is increasing the saving patient lives by delivering the EMRs timely. Applying Blockchain technology as one of their design pillars to deliver transparency in data accessibility.

**Contribution:** We reviewed the notable proposed blockchain-based healthcare systems in the domain of the problem. We summarized their value proposition to understand the strengths and weaknesses of such systems and draw a clear picture of the suitability feature in the aspect of the discussed problem. Proposing an ABAC break-glass mechanism for a Blockchain-based healthcare system as a conceptual model is the main contribution in this paper. It is a novel concept that has been developed along with other research in this domain. It is not similar nor comparable to any proposed model in this domain. Although some researchers have proposed Blockchain-based healthcare systems, we are the first researchers to propose a break-glass mechanism for a Blockchain-based healthcare system. Being related but differentiated in the research domain besides developing the related concept based on significant research in this domain is the authors' contribution. It helped us to develop a related but distinguished conceptual model to devise a unique value in this domain.

## II. STATE OF THE ART

In this section, we have reviewed notable research in this domain to present the main argument of our design logic. We draw relatedness between our research and the body of knowledge in Blockchain technology, IPFS, ABAC in the context of healthcare systems.

Implementation of access control based on Blockchain has been mentioned in some research projects such as [5,6,7]. They

provide security for their system through a Decentralized Application (DApp). They proposed a decentralized ABAC model against other research projects that are commonly proposed to centralize ABAC. They propose decentralization to purge some sort of problems in scaled scenarios such as the supply chain in synchronization and trust between the parties [5]. They used smart contracts to solve current centralized systems' issues by implementing a DApp. One major problem with Blockchain is its storage cost [6]. The InterPlanetary File System (IPFS) proposed an enforced cryptographic authorization and access control scheme to deliver a secure service for storing personal health records. Pournaghi et al. [8] raised keeping medical records in different data sources as a problem that engaged current context healthcare systems. Medical records in databases of separate hospitals have added a new controlling layer to medical records, which is an obstacle to accessing medical records fast enough, even for patients. Concerns about the security, privacy, and accessibility of medical records are essential in addition to the patient's authority on the belonging medical records. The combination of attribute-based encryption (ABE) and identity-based encryption (IBE) to encrypt medical data is not new, which is proposed in [9,10]. This combination supports fine-grained access control to facilitate access management in the system. Blockchain technology has a high potential to integrate health records from different sources [10]. Shi et al. [10] survey blockchain-based healthcare systems in the aspect of security and privacy and have found that Blockchain has a high potential to apply security, integrity, and privacy into healthcare systems. Blockchain characteristics such as immutability, transparency and decentralized distributed data storing present a range of applications in healthcare systems that meet some challenges in accessing the patient's medical records.

Blockchain technology has met a number of significant requirements of a healthcare system such as security, privacy, anonymity, integrity, authentication, controllability, auditability [10] but it has a high rate of redundancy in data storing which systematically inefficient for storing large files as a cost-effective data warehouse. Blockchain technology presents strong support for a high number of transactions and traffic that shows great potential in combination with other technologies to be used. Certain alternatives for data storing that could be used alongside blockchain to perform cost effectiveness are Cloud, P2P, and DFS. Distributed systems are more desirable for performance in scaled traffic besides volume. Distributed file systems (DFS) are welcomed, such as Inter-Planetary File System (IPFS) and Swarm, as the representative DFSs for system designers [11]. 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. IPFS, a distributed hash table (DHT), is a key component that maps keys to values in the distributed system. It is like a large table that presents what data is stored, where and who has what data [14]. 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. Our proposed conceptual model has been raised and shaped by our understanding, which has come through the studied papers that are all presented in the state of the art. It has been shaped based on the advantages and suitability are discussed in the reviewed paper.

## III. Conceptual Model

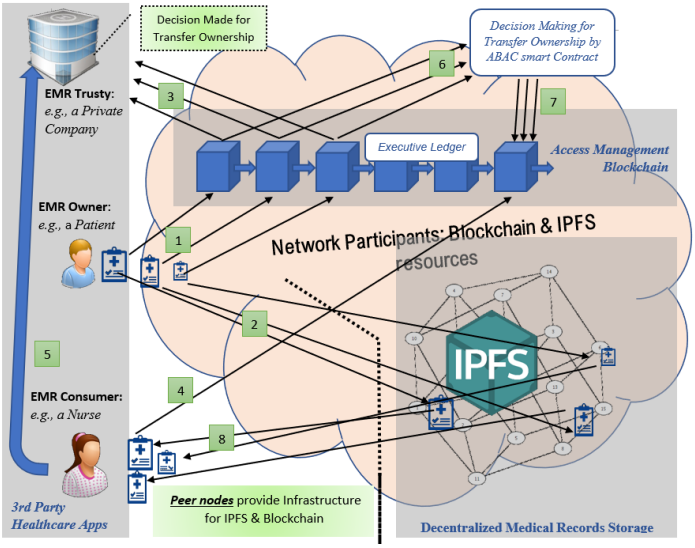


*Figure 1- Blockchain-based ABAC Break-glass*

The components of the conceptual model have been proposed in three domains. These three components have been illustrated as three gray rectangles in Figure 1 to distinguish the area of each element in comparison to the others. The structural design has been shaped as follows:

- **Access management Blockchain:** ABAC system and access ownership logs are stored in Blockchain to manage access rights, granting, or revoking the ownership of related medical records. It works based on the public / private key to identify rightful users.
- **Decentralized medical records storage**: IPFS has chosen to be used to store encrypted EMRs as distributed storage to secure EMRs from flaws such as the single point of failure, private data leakage, and unauthorized access to EMRs. It has chosen to store EMRs and protect them from flaws such as the single point of failure, private data leakage, and unauthorized access.
- **3rd party healthcare apps**: Our model is just the individual data layer of a healthcare system. Third-party software developers can use the system as EMR storage to transparent their system processes with Blockchain. This potential could be an incentive for collaboration and contribution to other companies and software developers to use our model in their software.

As described in the preliminary, Blockchain is made by linking the block. Each block started by the hash value of the previous block and hashing of the whole block with that value guaranteed the uniqueness of the previous block of the Blockchain, and all the nodes are accepted the new block by consensus algorithms. The security of our ABAC break-glass mechanism is provided by such a mechanism that works with

public/ private keys. The user sends an insert request for its encrypted medical records, and it determines the owners of the EMR. If the request has the correct format of the blockchain standard, which is defined in the consensus algorithm, the node creates necessitated records in the response and broadcasts to the network. Each insert creates various records based on the number of EMR owners. Each record has an access information part for retrieving the data through IPFS, 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. In the information part, owners can set the public key of the EMR trustees, which are the third party to the application. They can investigate the attributes of the consumer and permit or reject them in the response to requests. This means the transfer is exclusively dependent on the EMR owner's public/private key.

## IV. Limits & Discussion

We propose a combination of Blockchain and IPFS as our novel ideas. Blockchain is used as a secure integrated infrastructure for ABAC break-glass mechanisms, and IPFS provides a distributed file storage system to store large EMR files. Cloud technology is one alternative to IPFS data storing, but it is not discussed in this paper. Other researchers can extend the proposed break-glass mechanism to cloud storage, but swarms and private blockchain are too similar to our design. Consensus mechanism could be related domain to the extended area of this research, which is not discussed in this paper because it does not have effective directly on Break-glass mechanism. Implementation and performance have not been considered, and it could be towards extending the current research.

## V. Conclusion

This research is in progress and 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 have numerous potentials to transform the conventional healthcare system. We propose the main idea of the conceptual model for an ABAC break-glass mechanism for EMRs in a Blockchain-based healthcare system. We use Blockchain and IPFS to deliver greater accountability and accessibility to the healthcare system. State-of-the-art has discussed security, privacy, and integrity as its embedded qualitative features in Blockchain-based healthcare systems. Our model meets these qualitative features, which are required such as privacy by ABAC structure as well as guaranteeing the accessibility of EMR in case of emergency by Break-glass mechanism. There remain several challenges for those who want to implement the system. This is a work in progress research that needs to be discussed in more detail to adapt to the current Health System routines for implementation. We extend the domain area to further insight for developing the research.

## References


[1] A. Dubovitskaya et al., "ACTION-EHR: Patient-Centric Blockchain-Based Electronic Health Record Data Management for Cancer Care," J Med Internet Res, vol. 22, no. 8, p. e13598, Aug. 2020, doi: 10.2196/13598.

[2] Y. Yang, X. Liu, and R. H. Deng, "Lightweight Break-Glass Access Control System for Healthcare Internet-of-Things," IEEE Trans. Ind. Inf., vol. 14, no. 8, pp. 3610–3617, Aug. 2018, doi: 10.1109/TII.2017.2751640.

[3] M. T. de Oliveira et al., "A break-glass protocol based on ciphertext-policy attribute-based encryption to access medical records in the cloud," Ann. Telecommun., vol. 75, no. 3–4, pp. 103–119, Apr. 2020, doi: 10.1007/s12243-020-00759-2.

[4] V. Aski, V. S. Dhaka, and A. Parashar, "An Attribute-Based Break-Glass Access Control Framework for Medical Emergencies," in Innovations in Computational Intelligence and Computer Vision, Singapore, 2021, pp. 587–595, doi: 10.1007/978-981-15-6067-5_66.f

[5] Figueroa, Añorga, and Arrizabalaga, 'An Attribute-Based Access Control Model in RFID Systems Based on Blockchain Decentralized Applications for Healthcare Environments', *Computers*, vol. 8, no. 3, p. 57, Jul. 2019, doi: 10.3390/computers8030057.

[6] H. M. Hussien, S. M. Yasin, N. I. Udzir, and M. I. H. Ninggal, 'Blockchain-Based Access Control Scheme for Secure Shared Personal Health Records over Decentralised Storage', *Sensors*, vol. 21, no. 7, p. 2462, Apr. 2021, doi: 10.3390/s21072462.

[7] S. Tanwar, K. Parekh, and R. Evans, "Blockchain-based electronic healthcare record system for healthcare 4.0 applications," Journal of Information Security and Applications, vol. 50, p. 102407, Feb. 2020, doi: 10.1016/j.jisa.2019.102407.

[8] S. M. Pournaghi, M. Bayat, and Y. Farjami, 'MedSBA: a novel and secure scheme to share medical data based on blockchain technology and attribute-based encryption', J Ambient Intell Human Comput, vol. 11, no. 11, pp. 4613–4641, Nov. 2020, doi: 10.1007/s12652-020-01710-y.

[9] H. Wang and Y. Song, 'Secure Cloud-Based EHR System Using Attribute-Based Cryptosystem and Blockchain', J Med Syst, vol. 42, no. 8, p. 152, Aug. 2018, doi: 10.1007/s10916-018-0994-6.

[10] S. Shi, D. He, L. Li, N. Kumar, M. K. Khan, and K.-K. R. Choo, 'Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey', *Computers & Security*, vol. 97, p. 101966, Oct. 2020, doi: 10.1016/j.cose.2020.101966.

[11] Y. Kurt Peker, X. Rodriguez, J. Ericsson, S. J. Lee, and A. J. Perez, 'A Cost Analysis of Internet of Things Sensor Data Storage on Blockchain via Smart Contracts', *Electronics*, vol. 9, no. 2, p. 244, Feb. 2020, doi: 10.3390/electronics9020244.

[12] 'Distributed Hash Tables (DHTs)'. https://docs.ipfs.io/concepts/dht/ (accessed Jun. 20, 2021).