Secure and Efficient Data Accessibility in Blockchain based Healthcare Systems

Vidhya Ramani[1], Tanesh Kumar[1], An Braeken[2], Madhusanka Liyanage[1], Mika Ylianttila[1]
[1] Centre for Wireless Communications (CWC), University of Oulu, Finland
[2] Industrial Engineering INDI, Vrije Universiteit Brussel VUB, Brussels, Belgium
Email: [1][firstname.lastname]@oulu.fi, [2]an.braeken@vub.ac.be

***Abstract*—The healthcare industry is constantly reforming and adopting new shapes with respect to the technological evolutions and transitions. One of the crucial requirements in the current smart healthcare systems is the protection of patients sensitive data against the potential adversaries. Therefore, it is vital to have secure data access mechanisms that can ensure only authorized entities can access the patients medical information. Hence, this paper considers blockchain technology as a distributed approach protect the data in healthcare systems. This research proposes a blockchain based secure and efficient data accessibility mechanism for the patient and the doctor in a given healthcare system. Proposed system able to protect the privacy of the patients as well. The security analysis of our scheme shows that it can resist to well-known attacks along with maintaining the integrity of the system. Moreover, an Ethereum based implementation has used to verify the feasibility of our proposed system.**

***Index Terms*—Blockchain; Smart Healthcare; Data Accessibility; Security; Privacy; Ethereum; Smart Contracts**

I. Introduction

The concept of blockchain is being well-known for its use in bitcoin and cryptocurrencies. It has got widespread attention from various stakeholders due to its immense business potential and utilization in various applications such as banking, healthcare and supply chain management [1]–[3]. Medical and healthcare services are one of the prominent and crucial services which need to be delivered on the required time and through secure and safer means. Blockchain as a decentralized and distributed technology can play a key role in providing such healthcare services. Blockchain technology promises to provide immense opportunities in the healthcare sector such as secure data storing and sharing among various stakeholders, nationwide data interoperability and flexible and quick billing/payment modes [4].

With the recent advancements in the Internet technologies, the world is facing a digital transformation in terms of acquiring improved and better quality of daily life services. Technologies such as Internet of Things (IoTs), sensing technologies and 5G among others are providing numerous useful contributions in various aspects of the healthcare services [5]. The current healthcare systems are mostly based on centralized servers where multiple entities within the network require permission to access the medical information. This can cause delay in offering the medical services and also potential leakage of the information. In such kind of healthcare systems, patients are mostly unaware regarding which entities are storing and using their medical data without their consent. One of the challenges with the current healthcare systems is the secure accessibility of the medical data by various entities within the system/network. Blockchain can be utilized in such cases to achieve the secure accessibility and integrity of the healthcare data. Therefore, the main focus of this research is to propose a secure and efficient mechanism for data accessibility.

Motivation:

The current online healthcare services such as Electronic Health/Medical Record (EHR/EMR) play a key role for storing, sharing and maintaining personal medical records of the patients. However, there are a number of shortcomings which may lead to leakage of the patients sensitive medical information. For example, using the current approaches of managing healthcare systems, it becomes challenging for the patients to keep track of which entity is actually accessing the healthcare data and for what kind of purpose. Blockchain technology can be vital in such cases because it provides data ledger based features which is distributed to all entities within the network. A patient can monitor which entity is actually accessing the data and can grant the accessibility permission to only the authorized entities accordingly. Therefore, the core motivation behind this work is to utilize blockchains for healthcare systems and to address the potential shortcomings in the current healthcare systems.

Our Contributions and Organization of Paper

Considering the recent security requirements of the healthcare systems, there is a clear need of the secure and efficient blockchain based healthcare system that can not only provide secure and easy data access to the patients but also to other key entities involved in the system such as doctor can also retrieve and append the data with the patient's consent. And at the same time, the system must follow the key security features such as confidentiality, integrity and authentication. Thus, the goal of this paper is to propose the blockchain based healthcare system in which append or retrieval of patients medical data can be done securely by the authorized doctor and with the approval of the particular patient. Moreover, our proposed system can also offer the scalability feature which is a key requirement in the current healthcare systems.

The remainder of the paper is organized as follows. Section II highlights the literature work related to blockchain based healthcare schemes. Section III defines the preliminaries considered in this paper. Section IV presents the system model for the defined problem statement. We evaluate the security strength in Section V and implementation results in Section VI. Performance Evaluation of the proposed system is mentioned in Section VIII. Finally we conclude the paper in Section VIII.

II. Related Work

Healthcare data is considered as highly sensitive and requires secure and safer means to protect it. Thus, the storage, sharing and managing medical data should be done in secure ways [6], [7]. There are various mechanisms already proposed to address such issues, for example, numerous authentication schemes are presented in [8], [9], [10] in order to fulfill the need of secure and efficient medical data accessibility, manageability and other key security requirements. These solutions were helpful at some extent in offering various security requirements under desired healthcare scenarios. However, with the current advancement in healthcare technology, these approaches are not just sufficient because the patient has been exploited by various stakeholders through different means and without their consent [11], [12]. In this context, researchers are keen to find various secure solutions based on blockchain based healthcare approaches [13].

There have been various research studies related to potential utilization of blockchain in healthcare, presented by various researchers in the literature [14], [4]. Electronic medical treatment processes for manual and remote access of the patients data and protecting the privacy of the healthcare data are the most prior fields of application where Blockchain technology can create value [15]. The work in [16] has proposed MedRec in which a decentralized way of using blockchain technology is adopted to manage the EHR/EMR. The authors also provided a potential case study of blockchain usage in healthcare, which provides a prototype for EHR/EMR. Moreover, the work in [17] presents MedShare that provides the trustless way of sharing the healthcare data among various service providers using blockchain. Henceforth, research community are defining different mechanisms for the secure data accessibility of blockchain based healthcare system. This work provides a contribution towards an efficient and improved data accessibility mechanism by using private/permissioned blockchain for the secure and faster healthcare data access. Thus, this paper proposes a methodology that is completely based on the patient's access control for processing and accessing the data by other stakeholders. The medical data is stored in the database located at peer to peer networks whose address is stored in the blockchain. The degree of access is for function of the data which patient are permitted to access whereas doctor needs access control from the patient.

Ethereum is a public blockchain platform [18], with possibility to create smart contracts and focuses on the Blockchain technology development. A Smart Contract is a computer based protocol, consisting of rules, agreed by the stakeholders according to their requirements and also it has a Turing complete architecture for securing the patient's data and the rules that can also be modified by the legal person whose signature is in the agreement [19]. A Smart Contract is also used to interact with the blockchain and healthcare providers according to their need and also manages the patient's healthcare information by managing the access control given by the stakeholder and secured administration of the healthcare record [20].

The healthcare systems presented in the above literature are capable to ensure the secure data sharing of the patient records, for example, secure sharing of the patient's EHR/EMR with the other entities. However, none of the system in the literature addresses the whole append/retrieval process from patients and doctors. For example, a general healthcare scenario must include the append/retrieve operations from patients as well doctor because doctor also require to retrieve the patient's data to check the previous medical history and can append the data in the form of medical prescription or any other medical report. Therefore, our proposed system is particularly addressing such healthcare scenario where append and retrieve operations can be performed by the both patients and doctors.

III. Preliminaries

A. Problem Setting

In this work, we have taken a potential healthcare scenario, where the patients healthcare record can be managed more securely by the hospital. For this purpose, we have used the blockchain technology to ensure integrity and security of the medical data. We have assumed that the actual medical data is stored in the medical server and the address of that record is saved in the blockchain. The patient and doctor can retrieve the actual medical data through the address, which is stored in the blockchain. The healthcare data may include all kinds of medical records such as doctors prescriptions, medical history, laboratory reports and billing information. In this usecase, we consider that only patient and doctor are the authorized entities for accessing the patients healthcare information and with the patients permission. Therefore, the main focus of this work is to propose a secure mechanism of adding and retrieving the medical data by ensuring the integrity of the blockchain.

B. Network Setting

We distinguish five different entities in the system, being the Patient (P), the Doctor (D), the Registration Center (RC) as a trusted party, the Mobile Device (MD), and the Blockchain (BC). The patient first registers with the RC in person by providing personal details (such as ID, Biometrics and PIN), together with the public key of the patient and the doctor.

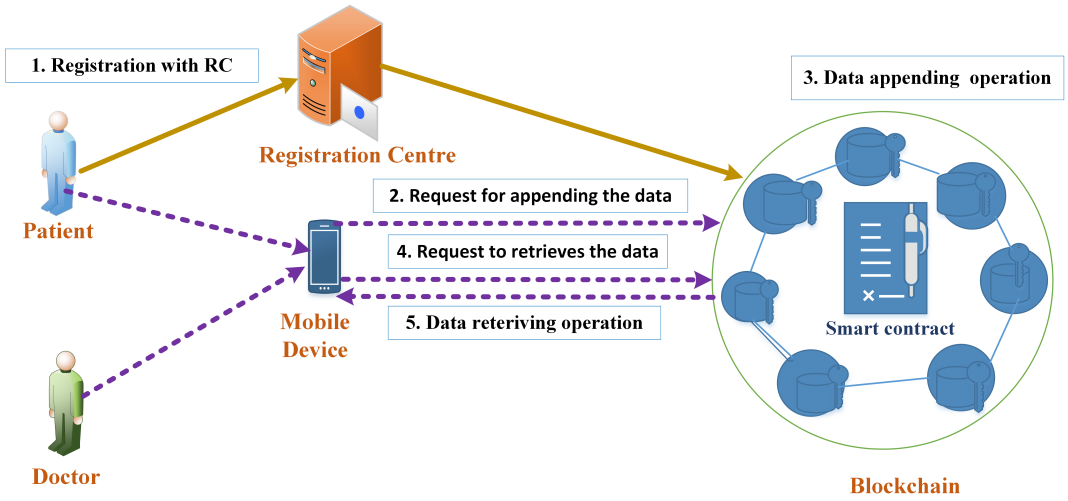

Fig. 1: System model of the proposed healthcare scenario

The public key(s) of the doctor(s) responsible for the treatment of the patient are added to the information file of the patient. Note that the doctors, together with the information on their public key, are already registered with the RC. After the registration process by the patient, the constructed information file about the patient will be sent to the Blockchain, which is shown in Figure 1.

Next, the patient goes to the doctor for the required treatment. The patient generates ID and a secret key pair (private/public key pair) using the installed app on the mobile device to authenticate him/herself. Next, if the doctor wants to update the data, he/she will send a request to the BC using his/her key material. Upon receiving the update request by the BC, it will check the validity of the doctor and whether the patient has granted the update permission to that particular doctor. If the check is successful, it performs the update operation. A similar kind of steps are also taken into account in the case of retrieving the patients data by the doctor.

C. Cryptographic Operations

The public key related operations in our proposed scheme rely on Elliptic Curve Cryptography (ECC), offering more lightweight public key cryptographic operations than the classical discrete logarithms or RSA based systems. Let us denote the elliptic curve (EC)$E_{p(a,b)}$ to be used in our scheme by $y^2 = x^3 + ax + b$ with a and b two constants in F_p and $D = 4a^3 + 27b^2 \neq 0$, together with the base point generator P of the curve of prime order q. All points on $E_{p(a,b)}$, together with the infinite point form an additive group. There are two elementary operations related to ECC resulting in another point of the EC, the EC multiplication $R = rP$ with $r \epsilon F_q$ and the EC addition $R1 + R2$. ECC relies on two computational hard problems.

- The Elliptic Curve Discrete Logarithm Problem (ECDLP). This problem states that given two EC points R and Q of $E_{p(a,b)}$, it is computationally hard for any polynomial-time bounded algorithm to determine a parameter $x \epsilon F_q$, such that $Q = xR$.
- The Elliptic Curve Diffie Hellman Problem (ECDHP). Given two EC points $R = xP$,$Q = yP$ with two unknown parameters $x, y \epsilon F_q$, it is computationally hard for any polynomial-time bounded algorithm to determine the EC point xyP.

Furthermore, we denote the operation H as the one-way cryptographic hash function (eg. SHA2 or SHA3) that results in a number of F_q. The encryption and decryption of a message M and corresponding ciphertext C using a symmetric key k is denoted by $C = E_k(M)$ and $M = D_k((C)$ respectively. As encryption algorithm AES or even a lightweight crypto algorithm can be used. The concatenation of two messages M_1 and M_2 is denoted by $M_1 \| M_2$.

D. Notations

The most frequently used notations in our scheme are mentioned in Table 1.

IV. The System Model

Figure 1 presents the different phases in the scheme: the registration (1), the request for data appending/adding (2), the data appending/adding operations (3), the request for data retrieving (4) and the data retrieving operations (5). We now discuss each of them into more detail.

A. Registration Phase

If a new patients arrives to the hospital for treatment, the patient must first register with the RC before going to the doctor. Since, it is a one time registration, they need to provide their details using their mobile device, such as their identity id_p , their public key pk_p and the public key of the doctor(s) pk_d treating them. For the ease in notation, we consider exactly one doctor. Note

TABLE I: Notation for proposed scheme

Notation	Description
P	Patient
D	Doctor
id_p	Identity of patient
MD	Medical device
id_d	Identity of doctor
RC	Registration center
$H(.)$	Hash function
$E_k(.)/D_k(.)$	Symmetric encryption/decryption with key k
pk_p	Patients public key
sk_p	Patients private key
$\|$	Concatenation operator
$\oplus$	XOR operator
T	Time stamp
k	Key
BC	Blockchain
pk_d	Doctors public key
sk_d	Doctors private key
M	Patient's record

that also relatives can be involved in the scheme, at the same way as doctors but with only reading rights.

Next, the RC sends (id_p, pk_p, pk_d) to the BC signed by the patient and by the RC. Note that (id_p, pk_d) has been already sent to the BC. Furthermore, then the BC verifies the signatures of the patient and RC and keeps (id_p, pk_p, pk_d) on the BC.

B. Request for Data Appending/Adding

In this phase, the doctor wants to update/add data M into the BC, with the approval of the patient. We here suppose, both doctor and patient possess their own MD on which the health application is running. Therefore, the doctor first encrypts the data with a common key, derivable by the patient. Next, the patient checks the validity of the encryption and if positive it performs its signature on the encrypted value. Finally, the doctor approves the signature of the patient and transmits the information to the BC. To be more concrete, this results in the following steps:

- Denote the current timestamp with T. The doctor determines $r = H(sk_d, T)$, and computes $R = rP$. Next, the doctor derives the symmetric key $k = rpk_p$ and the corresponding ciphertext $C_1 = E_k(M, T)$. This value C_1 together with T,R is transmitted to the patient.
- The patient is able to also compute $k = sk_pR$, which can be used to decrypt C_1. The resulting message is checked with the current data shown (presented in real) by the doctor to the patient and the timestamp.
- If the check is positive, the patient generates a signature by computing $C_2 = sk_PH(pk_p\|pk_d\|C1\|R\|T) \oplus kH(id_p\|R\|C_1\|T)$. It also computes $K = kP$, which is used for the signature verification. Finally the patient sends the output in the form of tuple $C_{SR} = (id_p, pk_d, T, R, K, C_1, C_2)$ to the doctor.
- The doctor now checks if C_1, T, R, id_p, pk_d are unchanged and if $K = kP$. If this is the case, it sends $(id_p, pk_d, T, R, K, C_1, C_2)$ to the BC. Note that it does not need to check the validity of the signature as this will be performed by the miners in the scheme.

C. Data Appending/Adding Operation

Next, upon receiving the tuple, the BC performs the following actions:

- First, the BC checks the timestamp T and looks up the public key of the patient and its corresponding registration contract.
- Then, it verifies the validity of the signature and thus the request by checking the equality $C_2P = pk_PH(pk_p\|pk_d\|C_1\|R\|T) \oplus KH(id_p\|R\|C_1\|T)$. This check ensures that the data is coming from patient id_p and that the doctor with public key pk_p is involved.
- Step 3: If this is positive, the tuple C_{SR} is stored on the BC.

D. Request for Data Retrieving

If the doctor wants to retrieve the data of a patient in a certain time interval T_p, then the doctor will send (id_p, id_d, T_p), signed by the doctor to the BC.

E. Data Retrieving Operation

After receiving this message, the BC will perform the following steps:

- The BC now checks the freshness of T_p, the validity of the signature and if the doctor is granted the permission by the patient to access the data (as stored on the BC).
- If so, it retrieves all data corresponding with that period. The data has the form $C_{SR'} = (pk_p, T, R, C_1, C_2)$. Note that id_p is replaced by pk_p and pk_d is removed from the stored tuple as it is already known by the doctor. As the BC already checked for the integrity, it is sufficient for the doctor to compute the key $k = H(sk_d, T)pk_p$ and the corresponding decryption of C_1.

V. Security Analysis

We now explain why our proposed scheme is able to offer the required security features.

A. Confidentiality

This feature includes that only the patient at any time and the doctor at a predefined period, specified into the RC contract, should be able to derive the patients data. The data stored on the BC is of the format $(id_p, pk_d, T, R, K, C_1, C_2)$. First of all, this data is constructed in such a way, due to the ECDHP and ECDLP, that only the doctor and patient are able to derive the clear text. In this case, the doctors secret key equals to $H(sk_d, T)pk_p$ and the patients key equals to sk_pR. Note that $H(sk_d, T)$ should be used instead of a random value r, because the doctor is not able to store all the different random values of all communications

of the different patients. Secondly, only the doctor that satisfies the conditions of the predefined contract stored on the BC is able to construct such a message.

Due to the integration of the timestamp into the ciphertext, the signature request to the patient cannot be replayed at a later moment by the doctor.

B. Integrity

This feature defines that nobody is able to change the patients data without notification of the patient. As the patient provides its signature onto the encrypted message, assurance is obtained on the integrity of it. The BC checks the validity of the signature, before being stored. In fact, everybody with knowledge of the public key of the patient is able to check the validity of the signature, which is a feature also called public verifiability. The proposed mechanism for the signature is based on the Schnorr signature scheme [21], [22].

C. Authentication

A scheme offers authentication if the entity claiming to send the message is correct. In this case, due to the usage of a signature, which is based on the famous Schnorr signature scheme, this feature is inherently included. Consequently, no other person is able to do a man-in-the-middle attack or impersonation attack.

VI. Implementation

For implementing the healthcare blockchain, the smart contract plays the vital role for executing or performing the agreement among various stakeholders involved in the system. A smart contract can be created by developing the codes and these codes define the agreement signed by the various stakeholders/parties such as a patient or a doctor. The healthcare data can be encrypted and shared to the whole ledger available within the respective network.The smart contract cannot access the other smart contract without having the permission. Hence the system is a permit trusted, transparent and traceable transaction. The smart contract can be developed by using smart contract development tools, written through a programming language such as Solidity.

In our healthcare usecase, we mainly focus on the two operations, retrieve and append/adding the medical data through blockchain. We consider that the patient and doctor both can retrieve the data. And for appending the medical data, the doctor can only modify/update the data along with the patients permission. For retrieving and appending the data, the person must be authorized and approved by the concerned person, being the patient, as indicated in the registration contract. Also, the patient can only have the access rights to change or add the doctor's details and also they can only add some other person to see the patient's record. After, all these steps then the encrypted data is sent to the requested person (who sends the request for the data) with their address and the required steps are mentioned in the following algorithm.

Algorithm 1 Algorithm for the proposed system

if ¡function(checkprivilege)==true¿ **then**
$check \quad timestamp \leftarrow for\ both\ patient\ and\ doctor$
$function(retrieveaddress) \leftarrow retrieve\ address(record)$
else¡Abort the session¿
end if
Retrieve data:
if ¡function(agreement)==true¿ **then**
$retrieve\ data \leftarrow from\ the\ address(record)$
$return(patientdata) \leftarrow to\ the\ particular\ requestID(patient\ or\ doctor)$
end if
Append data:
if ¡function(agreement)==true¿ **then**
$append \quad data \leftarrow to\ the\ particular\ patient\ record$
$return(success) \leftarrow to\ the\ doctor$
end if
change privilege:
function ¡CHANGE PRIVILEGE¿(¡msg.sender==patient¿) ¡ Only patient can change the doctor's details or add some other person¿
end function

Before appending/retrieving the data, the smart contract first verifies the registration contract, to make sure that the doctor has access rights to the patient's data. If the doctor doesn't have the access control then the system sends false statement and aborts the session. Therefore, it verifies the patient's address and doctor's address with the existing details in the blockchain.

VII. Performance Evalution

Scalability: Since, it is a private blockchain, the time taken for the whole process is lesser than the main network. It is measured as the response time per transaction. The results shows as the average time for generation of a new block is around 13 secs that is also same for the smart contract transaction. For confirmation it takes 36 secs but it also depends on the gas price before confirming it generates the next few blocks, takes around 90-120 seconds. For retrieving the data, it takes 54 secs and for appending the data, it takes 1-2 mins depends on the data.

Access control: Access control decisions are made by the patient defined in the smart contract. If the third parties/unknown entity want to access the system, the smart contract will deny the request and aborts the system.

Integrity: Integrity plays a major role between patient and the smart contract. Since the patient already signed with the smart contract, so no other person can change/modify the signed agreement. In our scenario, the doctor/ third parties cannot have a rights to change or alter the agreement in the smart contract

TABLE II contains the features comparison of our proposed system with other existing blochain based

healthcare systems. In the comparison, we have set two options for evaluations, i.e. Y-yes (It is reliable and available) and N-No (It doesn't have the feature).

TABLE II: Comparison of various features of proposed system with the existing systems

Feature	[14]	[16]	[17]	[23]	[24]	Our System
Access Control	Y	Y	Y	Y	Y	Y
Confidentiality	N	Y	Y	N	Y	Y
Integrity	N	Y	Y	N	Y	Y
Patient/Doctor Authentication	N	N	Y	Y	Y	Y
Scalability	Y	N	Y	Y	N	Y

VIII. Conclusion

Blockchain in healthcare systems has brought immense opportunities in terms of not only providing secure and efficient data storing, sharing and access but also generates a potential scope in the healthcare business for various stakeholders. In this paper, the core focus is to design a secure and efficient data accessibility mechanism for current healthcare systems using the blockchain technology. Furthermore, we analyzed that our proposed scheme can fulfill the requirements of confidentiality, integrity and authentication. We have also proposed the potential smart contract agreement considering this healthcare scenario.

Acknowledgment

This work has been performed under the framework of the SECUREConnect (Secure Connectivity of Future Cyber-Physical Systems), 6Genesis Flagship (grant 318927) and Towards Digital Paradise projects. This research is funded by Academy of Finland and TEKES, Finland. The authors would also like to acknowledge the contribution of the COST Action CA15127 (RECODIS) and CA16226 (SHELD-ON).

References

[1] R. Beck, "Beyond bitcoin: The rise of blockchain world," *Computer*, vol. 51, no. 2, pp. 54–58, February 2018.

[2] T. Aste, P. Tasca, and T. D. Matteo, "Blockchain technologies: The foreseeable impact on society and industry," *Computer*, vol. 50, no. 9, pp. 18–28, 2017.

[3] A. Manzoor, Y. Hu, M. Liyanage, P. Ekparinya, K. Thilakarathna, G. Jourjon, A. Seneviratne, S. Kanhere, and M. E. Ylianttila, "Demo: A Delay-Tolerant Payment Scheme on the Ethereum Blockchain," in *19th IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM 2018)*, 2018.

[4] M. Mettler, "Blockchain technology in healthcare: The revolution starts here," in *2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom)*, Sept 2016, pp. 1–3.

[5] S. B. Baker, W. Xiang, and I. Atkinson, "Internet of things for smart healthcare: Technologies, challenges, and opportunities," *IEEE Access*, vol. 5, pp. 26 521–26 544, 2017.

[6] M. Puppala, T. He, X. Yu, S. Chen, R. Ogunti, and S. T. C. Wong, "Data security and privacy management in healthcare applications and clinical data warehouse environment," in *2016 IEEE-EMBS International Conference on Biomedical and Health Informatics (BHI)*, Feb 2016, pp. 5–8.

[7] K. Abouelmehdi, A. Beni-Hssane, H. Khaloufi, and M. Saadi, "Big data security and privacy in healthcare: A review," *Procedia Computer Science*, vol. 113, pp. 73 – 80, 2017, the 8th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN 2017) / The 7th International Conference on Current and Future Trends of Information and Communication Technologies in Healthcare (ICTH-2017) / Affiliated Workshops.

[8] N. Kahani, K. Elgazzar, and J. R. Cordy, "Authentication and access control in e-health systems in the cloud," in *2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS)*, April 2016, pp. 13–23.

[9] A. A. Azeta, D. O. A. Iboroma, V. I. Azeta, E. O. Igbekele, D. O. Fatinikun, and E. Ekpunobi, "Implementing a medical record system with biometrics authentication in e-health," in *2017 IEEE AFRICON*, Sept 2017, pp. 979–983.

[10] T. Kumar, A. Braeken, M. Liyanage, and M. Ylianttila, "Identity privacy preserving biometric based authentication scheme for naked healthcare environment," in *2017 IEEE International Conference on Communications (ICC)*, May 2017, pp. 1–7.

[11] B. Yksel, A. Kp, and znur zkasap, "Research issues for privacy and security of electronic health services," *Future Generation Computer Systems*, vol. 68, pp. 1 – 13, 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X16302667

[12] F. Jabeen, Z. Hamid, A. Akhunzada, W. Abdul, and S. Ghouzali, "Trust and reputation management in healthcare systems: Taxonomy, requirements and open issues," *IEEE Access*, vol. 6, pp. 17 246–17 263, 2018.

[13] C. Esposito, A. D. Santis, G. Tortora, H. Chang, and K. K. R. Choo, "Blockchain: A panacea for healthcare cloud-based data security and privacy?" *IEEE Cloud Computing*, vol. 5, no. 1, pp. 31–37, Jan 2018.

[14] P. Zhang, M. A. Walker, J. White, D. C. Schmidt, and G. Lenz, "Metrics for assessing blockchain-based healthcare decentralized apps," in *2017 IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom)*, Oct 2017, pp. 1–4.

[15] W. Liu, S. Zhu, T. Mundie, and U. Krieger, "Advanced blockchain architecture for e-health systems," in *e-Health Networking, Applications and Services (Healthcom), 2017 IEEE 19th International Conference on*. IEEE, 2017, pp. 1–6.

[16] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "Medrec: Using blockchain for medical data access and permission management," in *2016 2nd International Conference on Open and Big Data (OBD)*, Aug 2016, pp. 25–30.

[17] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, "Medshare: Trust-less medical data sharing among cloud service providers via blockchain," *IEEE Access*, vol. 5, pp. 14 757–14 767, 2017.

[18] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum Project Yellow Paper*, vol. 151, pp. 1–32, 2014.

[19] M. Wohrer and U. Zdun, "Smart contracts: security patterns in the ethereum ecosystem and solidity," in *Blockchain Oriented Software Engineering (IWBOSE), 2018 International Workshop on*. IEEE, 2018, pp. 2–8.

[20] P. Zhang, J. White, D. C. Schmidt, and G. Lenz, "Applying software patterns to address interoperability in blockchain-based healthcare apps," *arXiv preprint arXiv:1706.03700*, 2017.

[21] L. Savu, "Signcryption scheme based on schnorr digital signature," *arXiv preprint arXiv:1202.1663*, 2012.

[22] H. Morita, J. C. Schuldt, T. Matsuda, G. Hanaoka, and T. Iwata, "On the security of the schnorr signature scheme and dsa against related-key attacks," in *International Conference on Information Security and Cryptology*. Springer, 2015, pp. 20–35.

[23] Q. Xia, E. B. Sifah, A. Smahi, S. Amofa, and X. Zhang, "Bbds: Blockchain-based data sharing for electronic medical records in cloud environments," *Information*, vol. 8, no. 2, p. 44, 2017.

[24] H. Yang and B. Yang, "A blockchain-based approach to the secure sharing of healthcare data."