Security with Blockchain for Electronic Health Records Management System (Decoy- Cloud System)

Dr. K. Velmurugan[1], R. S. Iswarya[2], R. Jayaprithvi[3]
Head, Department of Computer Science and Engineering[1]
Students, Department of Computer Science and Engineering[2,3]
Anjalai Ammal Mahalingam Engineering College, Kovilvenni, Tiruvarur, Tamil Nadu, India

Abstract: *The global electronic health record (EHR) industry is predicted to develop at a rapid pace, reaching $39.7 billion by 2022. Access control is a critical tool for managing EHR data to ensure its security and privacy. This study offers a hybrid architecture that uses both blockchain and edge nodes to facilitate access control of EHR data. A blockchain-based controller controls identity and access control regulations and acts as a tamper-proof log of access events inside the architecture. In addition, in combination with the blockchain-based access control logs, off-chain edge nodes store EHR data and apply policies provided in the Abbreviated Language For Authorization (ALFA) to impose attribute-based access control on EHR data. We test the proposed hybrid architecture by measuring the performance of executing smart contracts and ACL policies in terms of transaction processing time and response time against unauthorized data retrieval using the Hyperledger Composer Fabric blockchain.*

Keywords: Attribute-based Access Control, Access Control List, Blockchain, Edge Computing, Hyperledger, Smart Contract.

I. INTRODUCTION

Data for patients' Electronic Health Records (EHRs) can be collected from a variety of sources in eHealth, including wearable devices, smart sensors, and medical imaging equipment. According to reports, the amount of EHR data will rise at a rate of 48 percent each year until it reaches 2,314 zettabytes by 2020 [1]. However, the US Department of Health and Human Services reports that between 2009 and 2017, there were more than 2,181 incidences of healthcare data breaches, resulting in the exposure of 176,709,305 medical records [2]. As a result, EHR data security has become a critical concern in eHealth. Although encryption addresses some of EHR's most fundamental security and privacy concerns, due to the extremely scattered and fragmented nature of EHR data and the complicated connection between data owners and data users, access control, in particular, is difficult to implement effectively. As a result, it's critical to provide a flexible and fine-grained access control solution for EHR data. Blockchain has recently been proposed as a possible method for EHR data management [3]. A blockchain-based infrastructure's intrinsic secure by-design feature has the potential to offer a tamper-proof ledger for all EHR access events. Before being uploaded to the blockchain, all access events can be validated and recorded using a consensus method. Traditional blockchain-based solutions, on the other hand, have two fundamental limitations in terms of EHR management.

First, while blockchain can maintain data integrity, it lacks sufficient access control methods to keep operations carried out by various parties contained. Second, the size of blocks in a blockchain is insufficient to hold EHR data that includes images and/or videos (e.g., X-ray, CT scan, and MRI) (e.g., ultrasound). To simplify attribute-based access control of EHR data, this article offers a hybrid architecture that uses both blockchain and edge nodes. The Hyperledger Composer Fabric [4] blockchain, in particular, implements smart contracts with Access Control Lists (ACLs) to impose identity-based access control of EHR data and report legitimate access events in blockchain for traceability and accountability. Edge nodes in cooperation hold EHR data and enforce attribute-based access control (ABAC)1 of EHR data using policies defined in the Abbreviated Language For Authorization (ALFA) [6].

ALFA is a compact representation that maps straight into extensible Access Control Markup Language (XACML). Furthermore, hash digest is utilized to preserve the integrity of EHR data stored in edge nodes, which aids in the detection of any EHR changes. Furthermore, smart contracts reference one-time self-destructing URLs [7], which include the

DOI: 10.48175/IJARSCT-4750

addresses of EHR data on edge nodes and will be delivered to healthcare providers if the ACL access policy is successfully executed. The URLs are then used by healthcare professionals to obtain EHR data from edge nodes.

As a result, only eligible users who pass the edge nodes' attribute-based access control can access the requested EHR data. We prototype the hybrid architecture utilizing the Hyperledger Composer Fabric platform to test our idea.

Furthermore, we undertake various experiments to validate both smart contracts and access control policies, demonstrating that the proposed system can keep track of EHR data management access events and transaction records. We test the system's transaction processing time and average response time against unauthorized EHR data requests in a variety of circumstances using numerous experiments.

1.1 Blockchain

Blockchain is a distributed, unchangeable database that makes recording transactions and managing assets in a corporate network much easier. A tangible asset (a house, car, cash, or land) can be intangible (intellectual property, patents, copyrights, branding). On a blockchain network, virtually anything of value can be recorded and traded, lowering risk and cutting costs for all parties involved. Information is the lifeblood of business. The faster and more accurate it is received, the better. Because it delivers immediate, shareable, and entirely transparent information kept on an immutable ledger that can only be viewed by permissioned network users, blockchain is excellent for delivering that information. Orders, payments, accounts, production, and much more may all be tracked using a blockchain network. You can see all facts of a transaction end to end since members share a single view of the truth, providing you more confidence as well as additional efficiencies and opportunities.

Key elements of a blockchain

- Distributed ledger technology
- Immutable records
- Smart contracts

1.2 Working of Blockchain

Each transaction is logged as a "block" of data as it occurs.

These transactions depict the movement of a tangible (a product) or intangible asset (intellectual). The data block can store any information you want, including who, what, when, where, how much, and even the state of a shipment, such as the temperature.

Each brick is linked to the ones that came before it and those that came after it. As an asset transfers from one location to another or ownership changes hands, these blocks form a data chain. The blocks validate the exact timing and sequence of transactions, and they are securely linked together to prevent any block from being changed or inserted between two other blocks.

In a blockchain, transactions are linked in an irreversible chain.

Each successive block enhances the prior block's verification, and hence the entire blockchain. The blockchain becomes tamper-evident as a result, giving the key strength of immutability. This eliminates the risk of tampering by a hostile actor, and creates a trusted record of transactions for you and other network users.

1.3 Attribute-Based Access Control (ABAC)

ABAC (attribute-based access control) is an authorization paradigm that determines access based on attributes (or characteristics) rather than roles. The goal of ABAC is to safeguard items like data, network devices, and IT resources from unauthorized users and actions—those that don't meet the requirements of an organization's security policies. ABAC, which evolved from simple access control lists and role-based access control, has become a popular kind of logical access control in the last decade (RBAC). The Federal Chief Information Officers Council supported ABAC in 2011 as part of an endeavour to help federal organisations enhance their access control infrastructures. They suggested that enterprises use the ABAC approach to safely share information. The main components of Attribute Based Access Control With ABAC, an organization’s access policies enforce access decisions based on the attributes of the subject, resource, action, and environment involved in an access event.

DOI: 10.48175/IJARSCT-4750

The qualities or values of a component involved in an access event are known as attributes. Attribute-based access control compares these components' attributes against rules. These rules specify which attribute combinations are permitted for the subject to conduct an action with the object successfully. Every ABAC solution may analyse attributes inside an environment and enforce rules and relationships based on how they interact in that environment. Policies take qualities into account when determining whether or not certain access conditions are permitted.

1.4 Access Control List (ACL)

An access control list (ACL) is a set of rules that determines which people or systems have access to which objects or system resources. Access control lists can also be found in routers and switches, where they serve as filters for determining which traffic is allowed access to the network. The access control list for each system resource is identified by a security property. Every user who has access to the system has an entry in the list.

The ability to read a file or all the files in a directory, write to the file or files, and execute the file if it is an executable file or programme are the most frequent privileges for a file system ACL. Network interfaces and operating systems (OSes), such as Linux and Windows, have ACLs. Access control lists are used on a computer network to prevent or allow particular types of traffic onto the network. They frequently censor traffic according on its origin and destination.

1.5 Edge Computing

Edge computing is a distributed computing platform that puts business applications closer to data sources like IoT devices and local edge servers. Faster insights, faster response times, and greater bandwidth availability are all possible business benefits of being close to data at its source.

The rapid growth of IoT devices, as well as their expanding computational capacity, has resulted in massive amounts of data. And as 5G networks expand the number of linked mobile devices, data volumes will continue to rise.

The promise of cloud and AI in the past was that they would automate and speed up innovation by generating actionable insight from data. However, network and infrastructure capacities have been overtaken by the extraordinary amount and complexity of data provided by connected devices. Sending all of the data to a centralised data centre or the cloud generates bandwidth and latency problems.

Edge computing is a more efficient option because data is processed and analysed closer to the point of origin. Latency is considerably decreased because data does not have to travel over a network to a cloud or data centre to be processed. Edge computing particularly on 5G networks provides faster and more thorough data processing, allowing for deeper insights, faster response times, and better consumer experiences.

1.6 HyperLedger

Hyperledger is an open source collaborative initiative aimed at advancing blockchain technologies across industries. The Linux Foundation is hosting a global partnership that includes leaders in finance, banking, the Internet of Things, supply chains, manufacturing, and technology. So there are a lot of promises – and Hyperledger is one of them. The Linux Foundation hopes to use it to establish an environment where software developers and enterprises can meet and collaborate to build blockchain frameworks.

In December 2015, the Linux Foundation established the platform. It announced the first founding members in February 2016, and 10 additional members joined in March 2016. Today, Hyperledger boasts a membership of over 100 people. The list includes a diverse group of well-known industry figures. It includes companies like Airbus and Daimler, as well as IT companies like IBM, Fujitsu, SAP, Huawei, Nokia, Intel, and Samsung, as well as financial institutions like Deutsche Börse, American Express, J.P. Morgan, BBVA, BNP Paribas, and Well Fargo, as well as Blockchain startups like Blockstream, Netki, Lykke, Factom, bloq, and Consensys. At Hyperledger, several of the world's largest IT and finance organisations meet with some of the hottest blockchain startups.

1.7 Smart Contract

Smart contracts are essentially programmes that run when certain criteria are satisfied and are maintained on a blockchain. They're usually used to automate the execution of an agreement so that all parties can be certain of the conclusion right away, without the need for any intermediaries or time waste. They can also automate a workflow, starting the following

DOI: 10.48175/IJARSCT-4750

step when certain circumstances are satisfied. Simple "if/when...then..." lines are written into code on a blockchain to make smart contracts work. When preset circumstances are satisfied and validated, the activities are carried out by a network of computers. These activities could include transferring payments to the proper parties, registering a vehicle, providing alerts, or issuing a ticket. When the transaction is complete, the blockchain is updated. That means the transaction can't be modified, and the results are only visible to those who have been granted access. There can be as many specifications as needed in a smart contract to convince the participants that the task will be executed correctly.

Participants must agree on how transactions and associated data are represented on the blockchain, agree on the "if/when...then..." rules that govern those transactions, investigate all conceivable exceptions, and design a framework for resolving disputes in order to set the terms. The smart contract can then be coded by a developer, though firms that use blockchain for business are increasingly providing templates, web interfaces, and other online tools to make smart contract construction easier.

II. LITERATURE REVIEW

The review looks into the field of Electronic Health Record (EHR) Management Systems, with a focus on the techniques and results of such systems during catastrophic events and following mass crises. Prior to the advent of smart contacts on the blockchain, much of the literature focused on \ frameworks and systems for sharing electronic health records (EHRs) across cloud infrastructures[39][41]. The implementation of a new method for expressing sophisticated logic on the web. Through the deployment of a Turing-complete language, blockchain ushered in a new era of research centred on distribution and peer-to-peer communication [52]. Indeed, following Ethereum, a new set of frameworks and systems based on the decentralized ideology has been researched and suggested by both academics and industry. [3][12][22] as well as the industry [32].

These frameworks use a variety of blockchain architectures, from Ethereum to later implementations (i.e., Hyperledger, Corda or Tendermint) It's important to understand the distinction between Electronic Medical Records (EMR) and Electronic Health Records (EHR) before diving into previous and current work (EHR). In fact, while the two names may appear to be synonymous and are sometimes used interchangeably, they refer to two distinct forms of digital recordings. The former can be thought of as a digital version of a patient's paper record that practitioners use. It includes the patient's medical history, including diagnoses and treatments administered by a specific physician. Instead, the latter is a more generic record that includes the whole patient medical history and is intended to be shared with other approved users from various healthcare providers [45]. [39] and [41] have presented some cloud solutions to the problem of EMR accessibility and sharing. [39] and [41] have presented some cloud solutions to the problem of EMR accessibility and sharing.

Patra et al. [39] investigated the impact of cloud computing on 25 26 be used to facilitate and improve healthcare services, particularly in remote regions. A variety of requirements must be met by the system, including availability, scalability, security, data transfer, storage, and collection methods. They suggest that storing patient data in the cloud can be done at a reasonable cost.

Doctors and medical professionals can then exchange and access this information. They do not, however, expand on the concept and limit the scope to a high-level design model with no implementation or tests. Yue et al. [54] described the architecture of a so-called data gateway application for healthcare data based on the blockchain, based on the notions in [39].They claim to be the first to propose a distributed ledger solution that addresses requirements such as EHR sharing and data management by patients. Although the architecture anticipates a private blockchain running in the cloud, it does not specify how it should be implemented or provide performance tests.

Azaria, Ekblaw, and colleagues [3] were the first to present a fully functional prototype of blockchain technology used to EHRs. They propose MedRec, a system that not only controls access and authenticates users, but also manages EMRs in a distributed manner, with the goal of addressing issues such as health data fragmentation, slow access, system interoperability, patient agency, and better data quality and quantity for medical research. They try to do this by describing a system with a modular design that can be easily integrated. In actuality, for scalability and adoption reasons, the actual medical record is kept off-chain on the hospital or provider's relational database rather than on the blockchain.

Metadata and references to the EHR's location are stored on the blockchain. A smart contract, more specifically, regulates the interaction between actors and data, as well as defining access restrictions and references to that data. The pointer is a tuple that includes a query string to run on the provider's database as well as the location (host port and credentials)

DOI: 10.48175/IJARSCT-4750

where the EHR can be accessed [3].The prototype is built on the Ethereum public blockchain, with access restriction based on the user's public keys, which are Ethereum addresses, and stakeholders participating as "miners" in the network (they run a node). Every party (including the patient) must have a blockchain node in order to engage with it. The fundamental disadvantage of this implementation is that each system actor must have a complete copy of the data.

Another issue is the consensus protocol's lack of scalability. Despite the fact that the authors do not mention it, the upper bound can be raised to 60 transactions per second[16]. Dubovitskaya, Xu, and others [12] take it a step further by presenting a framework and demonstrating various situations in which the usage of a shared ledger may assure privacy, security, availability, and fine-grained access control over EMR data. The authors present a prototype of an oncology-specific clinical system that allows patients' medical records to be shared for primary care. Their approach is intended to simplify permission management and data transfer between hospitals, as well as improve the management of long-term treatment and life-long monitoring for cancer patients. Patient data is encrypted and stored in a cloud repository off-chain, but access rights and EHR information are kept on-chain. The system is based on Hyperledger Fabric and uses the PBFT consensus algorithm. However, the prototype's scalability has yet to be proven in a real-world scenario.

The authors claim that PBFT consensus has good scalability qualities that have been tested up to tens of nodes, with block size playing just a minor effect. They designated performance analysis as future work.

Finally, Medicalchain [32] is an industry case study with similarities to the other concepts. The user takes ownership of their health record and has complete access to and control over the information it contains. It also assists to increase transparency among the various stakeholders engaged in a person's treatment, including hospitals, clinics, and health insurance companies. The whitepaper is essentially a business plan with a few technical details thrown in for good measure. Scalability qualities aren't mentioned. The method they use to ensure patient safety is worth mentioning: a backup access system for emergency scenarios. When the patient is unconscious and unable to give consent during a disaster, the backup could be especially useful. The system is comprised of an emergency bracelet that caregivers can scan to acquire vital information.

III. PROPOSED SYSTEM

We do tests to see how well the suggested hybrid access control system, which is based on the Hyperledger Composer Fabric architecture, performs. Depicts an example experiment with two doctors and five patients, each of whom is given a unique digital ID card to log into the blockchain network. The first three patients made appointments with Dr. #1, while the final two patients made appointments with Dr. #2. We put the access control method to the test by logging into the prototyped blockchain network with a Chrome browser, submitting transactions, and keeping track of the participants' access events and results. To test the performance of the proposed system, we compared the system reaction time of systems with varied numbers of patients. The tests were carried out on a machine with a default setup of a 2.9 GHz Intel i5 processor, 8GB of memory, and a 60 Mbps Ethernet connection.

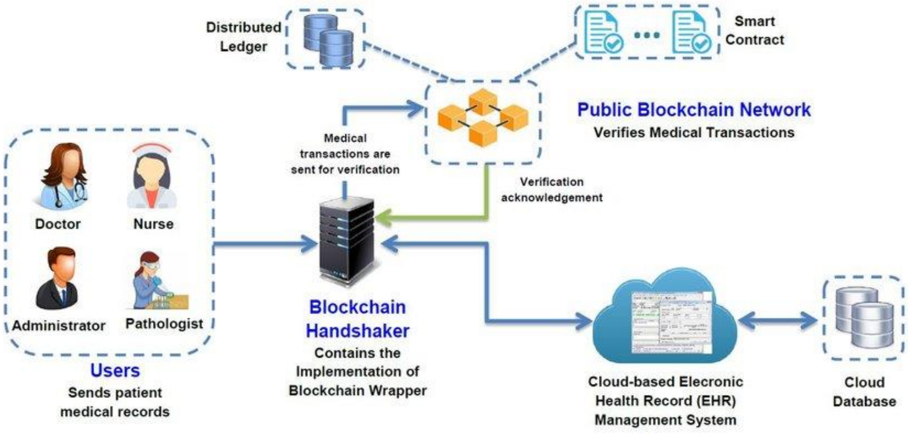
Distributed Ledger
Smart Contract
Public Blockchain Network
Verifies Medical Transactions
Medical transactions are sent for verification
Verification acknowledgement
Doctor
Nurse
Administrator
Pathologist
Users
Sends patient medical records
Blockchain Handshaker
Contains the Implementation of Blockchain Wrapper
Cloud-based Elecronic Health Record (EHR) Management System
Cloud Database

Fig 1 System Architecture of Proposed model

Test of Access Control on a Doctor: In the first experiment, we pretend to be a doctor and log into the blockchain network. A doctor has access to his or her patient list, which includes ID numbers, first and last names. If a clinician wants to get

EHR data for a specific patient, he or she must submit a transaction request with the patient's ID number. The system will return the URL address of the patient's EHR when you submit the request. Simultaneously, the blockchain network will record this retrieval action as a transaction event, complete with the event ID and timestamp. For analysis, any EHR retrieval record can be tracked back in real time.

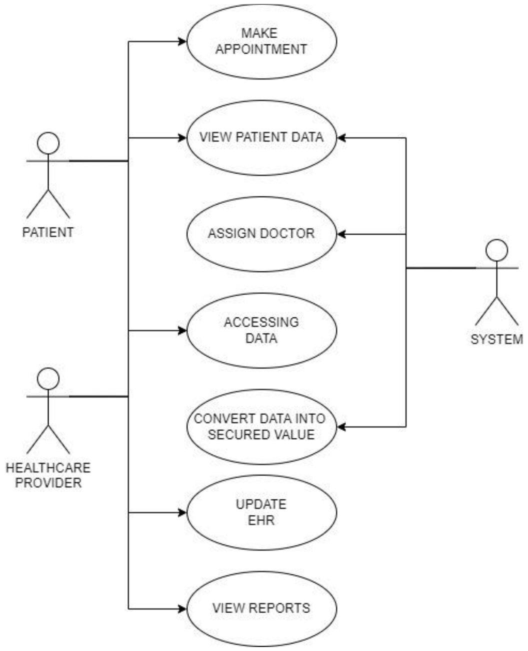

Fig 2 Use case diagram of the proposed system

A case diagram is a diagram that is used to describe how a system should work. The interaction of the actors with the system is depicted in a use case diagram. The system's Use-Case Diagram is shown in Figure 2. Administrators, patients, doctors, and physicians are all possible users of this system. This website employs a login system, which necessitates the creation of a username and password. The task of creating users falls to administrators. The administrator provides users with a username and password. Patients, in particular, must register with the doctor in advance of their appointment. A default username and password will be provided by the doctor, which the patient will update.

3.1 Module Description

1. The patient's smartphone app.
2. System for scheduling appointments that is intelligent.
3. EHR (Electronic Health Record) centralized

A. Patient's Smartphone App

Patient vital signs, patient data, text communication, and an integrated EHR are all available through the mobile EHR application.

Our healthcare providers can use the app to see how patients are doing both inside and outside of the hospital.

On a variety of Android and iOS devices, the software provides a consistent user experience.

A group of ten beta testers has utilised and maintained our copy of the software on a regular basis, indicating user acceptability.

B. Scheduling Appointments

Reduced wait times. Streamlined operations, queue segmentation, and optimized resources cut wait times significantly.

Improved customer experience

Increased staff productivity and efficiency.

Data-based insights for decision making.

DOI: 10.48175/IJARSCT-4750

C. EHR Centralized

An EHR system demonstrates how centralized data allows keeping a lot of information in one place. Then, if a patient moves between different health systems, all the providers who treat them can see the same, up-to-date information.

IV. CONCLUSION

In this research, we propose a hybrid architecture for imposing attribute-based access control to EHR data utilising both blockchain and edge nodes. The architecture makes use of blockchain to (1) execute smart contracts that enforce ACL policies and (2) record legitimate access events in the blockchain. Furthermore, EHR data is stored on edge nodes that follow ALFA's ABAC regulations. We evaluated the performance of access control by evaluating transaction processing time and response time against illegal retrieval attempts using the Hyperledger Composer Fabric blockchain, which was designed with smart contracts and ACL regulations. Our technology produces results in milliseconds, making it acceptable for use in real-time and secure EHR data access control frameworks, according to our tests. In order to improve performance, we want to research novel consensus protocol designs for the suggested mechanism in the future. We also intend to create a Hyperledger-based benchmark tool for a variety of performance assessments.

REFERENCES

[1]. Hao Guo, Wanxin Li, Mark Nejad, Chien-Chung Shen.” Access Control for Electronic Health Records with Hybrid Blockchain-Edge Architecture” in 2019 IEEE International Conference on Blockchain (Blockchain) Electronic ISBN:978-1-7281-4693-5 Print on Demand (PoD) ISBN:978-1-7281-4694-2 DOI: 10.1109/Blockchain.2019.00015

[2]. M. Aguilera and S. Toueg. “Failure Detection and Randomization: Hybrid Approach to Solve Consensus”. In: SIAM Journal on Computing 28.3 (Jan. 1998), pp. 890–903. ISSN: 0097-5397. DOI: 10.1137/S0097539796312915. URL: https://epubs.siam.org/doi/abs/10.1137/S0097539796312915(visited on 06/20/2018).

[3]. Elli Androulaki et al. “Hyperledger fabric: a distributed operating system for permissioned blockchains”. en. In: ACM Press, 2018, pp. 1–15. ISBN: 978-1-4503-5584-1. DOI: 10.1145/3190508.3190538. URL: http://dl.acm.org/citation.cfm?doid=3190508.3190538 (visited on 05/23/2018).

[4]. Asaph Azaria et al. “MedRec: Using Blockchain for Medical Data Access and Permission Management”. In: IEEE, Aug. 2016, pp. 2530. ISBN: 978-1-5090-4054-4. DOI: 10.1109/OBD.2016.11. URL:http://ieeexplore.ieee.org/document/7573685/ (visited on 05/23/2018).

[5]. Alysson Bessani, Joao Sousa, and Eduardo E.P. Alchieri. “State Machine Replication for the Masses with BFT-SMART”. In: IEEE, June 2014, pp. 355–362. ISBN: 978-1-4799-2233-8.DOI: 10.1109/DSN.2014.43. URL: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6903593 (visited on 05/31/2018).

[6]. Vitalik Buterin. Proof of Stake FAQ. 2016. URL: https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ(visited on 05/25/2018).

[7]. Christian Cachin and Marko Vukolic. “Blockchain Consensus Protocols in the Wild”. In: CoRR abs/1707.01873 (2017). arXiv: 1707.01873. URL: http://arxiv.org/abs/1707.01873.

[8]. Calliper: A blockchain benchmark framework to measure performance of multiple blockchain solutions. original-date: 2018-03-20T01:46:34Z. June 2018. URL: https://github.com/hyperledger/caliper (visited on 06/13/2018).

[9]. Miguel Castro and Barbara Liskov. “Practical byzantine fault tolerance and proactive recovery”. In: ACM Transactions on Computer Systems 20.4 (Nov. 2002), pp. 398–461. ISSN: 07342071. DOI: 10.1145/571637.571640. URL: http://portal.acm.org/citation.cfm?doid=571637.571640 (visited on 05/31/2018).

[10]. 111th Congress. “American Recovery and Reinvestment Act of 2009”. In: (2009). URL: https://www.gpo.gov/fdsys/pkg/PLAW111publ5/html/PLAW-111publ5.htm (visited on 03/20/2018).

[11]. George F Coulouris, Jean Dollimore, and Tim Kindberg. Distributed Systems - Concepts and Design (5th Edition). Pearson Eduction, May 2011. ISBN: 978-0132143011.

[12]. Centers for Disease Control, Prevention, et al. “HIPAA privacy rule and public health. Guidance from CDC and the US Department of Health and Human Services”. In: MMWR: Morbidity and mortality weekly report 52.Suppl. 1 (2003), pp. 1–17.

[13]. Alevtina Dubovitskaya et al. “Secure and Trustable Electronic Medical Records Sharing using Blockchain”. In: arXiv preprint arXiv:1709.06528 (2017).

[14]. European Commission. Overview of the national laws on electronic health records in the EU Member States and their interaction with the provision of cross-border eHealth services. Final report and recommendations. 2014. URL: https://ec.europa.eu/health/ehealth/projects/nationallaws_ electronichealthrecords_en (visited on 05/13/2018).

[15]. Ittay Eyal and Emin Gun Sirer. “Majority is not Enough: Bitcoin Mining is Vulnerable”. In: arXiv:1311.0243 [cs] (Nov. 2013). arXiv: 1311.0243. URL: http://arxiv.org/abs/1311.0243 (visited on 09/17/2018).

[16]. Juan Garay, Aggelos Kiayias, and Nikos Leonardos. “The Bitcoin Backbone Protocol: Analysis and Applications”. In: Advances in Cryptology - EUROCRYPT 2015. Ed. by Elisabeth Oswald and Marc Fischlin. Vol. 9057. Berlin, Heidelberg: Springer Berlin Heidelberg, 2015, pp. 281–310. ISBN: 978-3-662-46802-9 978-3-662-46803-6.

[17]. X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, “Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control,” Journal of Medical Systems, vol. 40, no. 10, p. 218 (8 pages), 2016.

[18]. A. Ekblaw, A. Azaria, J. D. Halamka, and A. Lippman, “A case study for blockchain in healthcare:medrec prototype for electronic health records and medical research data,” in Proceedings of IEEE Open & Big Data Conference, vol. 13, 2016, p.13.

[19]. R. Guo, H. Shi, Q. Zhao, and D. Zheng, “Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems,” IEEE Access, vol. 6, pp. 11 676–11 686, 2018.

[20]. 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.

[21]. G. Zyskind, O. Nathan, and A. Pentland, “Decentralizing privacy: Using blockchain to protect personal data,” in 2015 IEEE Security and Privacy Workshops. IEEE, 2015, pp. 180–184.

[22]. S. Wang, Y. Zhang, and Y. Zhang, “A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems,” IEEE Access, vol. 6, pp. 38 437–38 450, 2018.

[23]. H. Guo, E. Meamari, and C.-C. Shen, “Multi-authority attribute-based access control with smart contract,” In Proceedings of 2019 International Conference on Blockchain Technology (ICBCT 2019). ACM, 6 pages. https://doi.org/10.1145/3320154. 3320164.

[24]. A. Ouaddah, A. Abou Elkalam, and A. Ait Ouahman, “Fairaccess: a new blockchain-based access control framework for the internet of things,” Security and Communication Networks, vol. 9, no. 18, pp. 5943–5964, 2016.

[25]. D. D. F. Maesa, P. Mori, and L. Ricci, “Blockchain based access control,” in IFIP International Conference on Distributed Applications and Interoperable Systems. Springer, 2017, pp. 206–220.

DOI: 10.48175/IJARSCT-4750