Journal of Engineering and Applied Sciences
MEDWELL PUBLICATIONS

Building a Blockchain Framework for Personal Health Records Based on the Analysis and Evaluation of Existing Solutions

[1]Alice Azar and [2]Kadan Aljoumaa
[1]*Higher Institute for Applied Science and Technology, Damascus, Syria*
[2]*Department of Computer Science, Higher Institute for Applied Science and Technology, Damascus, Syria*

Key words: Personal health records, blockchain, four views framework, hyperledger fabric

Corresponding Author:
Alice Azar
Higher Institute for Applied Science and Technology, Damascus, Syria

Page No.: 152-160
Volume: 16, Issue 4, 2021
ISSN: 1816-949x
Journal of Engineering and Applied Sciences
Copy Right: Medwell Publications

Abstract: Blockchain is one of the most important emerging technologies that have brought great changes in various fields due to its great impact on many commercial and industrial activities. After the blockchain's great success in the digital currency field, it has been used in other areas such as the Internet of Things, supply chain and healthcare. Emerging solutions adopting blockchain in the field of health records, provide directions for addressing some of its challenges. We aim to analyze current blockchain-based health records solutions by a reference study and a systematic comparison of the trends adopted by them, based on the "Four-Views Framework". We also aim to lay a systematic basis for our new approach that seeks building a comprehensive framework for health records. As a result, we proposed an architecture for a new framework that combines health data integration, management, exchange and access control management, taking into account privacy and security.

INTRODUCTION

In this study, we present a set of existing approaches that are concerned with developing solutions to the challenges that patients face when trying to access health care services: scattered health data, duplication of medical files and their in-ability to control, manage or share their data with healthcare providers, in a secure and reliable way.

By presenting the approaches, we aim to analyze and compare them using a method of comparison inspired by the four-views framework[1]. This framework provides a structural analysis of four views for the studied approach, so that, it is easy for us to compare the approaches and explain the characteristics of each approach as each view corresponds to a basic aspect of the studied approach.

In the following sections, we review the proposed systematic comparison framework in detail in terms ofdefining the four-views and their components, after which we apply the framework that we have built to the studied approaches.

The four-views framework: The four-views framework puts in our hands a scientific, intellectual and conceptual tool to analyze the studied approaches and highlight the main features that each approach has.

This framework has proven effective in improving our understanding of many engineering specialization such as requirements engineering[2], information systems engineering[3] and procedures engineering[4]. We will

Table 1: An example of the classifications of fields and their values[5]

Facet	Domain	Example of values
Facet 1	Single value	1
Facet 2	Set (value 1-3)	Value 1, Value 3
Facet 3	Enum {X value, Y value, Z value}	Value Z

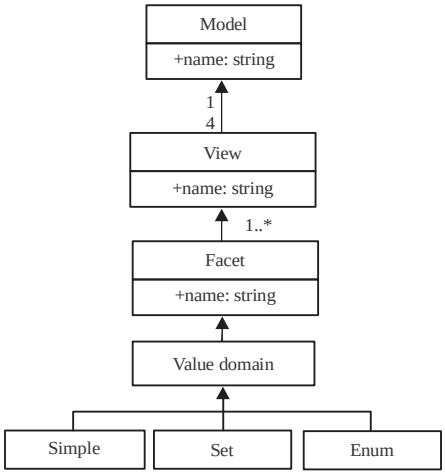

Fig. 1: Meta-model of the referenced framework[5]

therefore, use the comparison framework to help understand and compare current approaches to emerging health records solutions.

Meta-model: The initial framework of the four-views can be built by defining the aspects that make up the related view, in order to present the approach to be described. Each view has a name and is measured using a set of facets, each of which has specific values in the domain[5].

There are three classifications of domains, the simple, the enumerated and the set:

- Simple: corresponds to predefined types such as integer, boolean and strings
- Enumerated: the facet will have one of the specified de- fined list values {X value, Y value, Z value}
- Set: the facet can take one or more values from a predefined list[5]

Table 1 provides an example of each of the three classifications of domains (simple, enumerated and set) with an example of a value conforming to its type. Figure 1 shows the meta-model of the referenced framework.

MATERIALS AND METHODS

The main motivation of the proposed methodology consists of providing a systematic comparison framework and building a building a novel blockchain-based personal health records framework.

Building a systematic comparison framework: The referenced framework consists of four-views. Each view allows to analyze a specific aspect of the approach by posing four fundamental questions, namely "What?", "Why?", "How?" and "In What Way?" Just as each view is made up of a set of facets, each of the facets defines a single criterion for analysis and comparison. In the following sections, we will detail the aspects of each view and define the values that each aspect takes[1] (Fig. 2).

Subject view: It answers the question: what knowledge is included in the approach? It focuses on the primary purpose of the approach. In order to describe the "Subject" view, we suggest that the approaches should be studied in six aspects, namely:

Level of detail: Determines the degree of detail in the problem, objectives, contributions of the research, solution architecture and implementation of the proposed solution. It takes two possible values which are:

Black box: The level of detail is limited and is characterized by a superficial overview of the research topic, the solution architecture and the implementation methodology.

White box: Where the research has clarity and provide details of the research topic, the solution architecture and the methodology for its implementation.

Patient's record: According to Hasselgren *et al*.[6] patient's records are classified into:

EMR: It is a digital copy of the paper records found in the health provider's office. The information in EMRs doesn't travel easily out of the practice. In fact, the patient's record might even have to be printed out and delivered by mail to the care team[7].

EHR: It is a digital structure of patient health data that is preserved throughout their lives and stored in a data warehouse[8].

PHR: It represents health records related to patient care that are managed by the patient himself[9].

Implementation scope: The implementation scope takes one or more values from the set (patient, health facilities (hospitals, health centers), country, ...).

Implementation field: It takes one or more values from the set: (financial, health, medicinal, prescriptions, medical research, ...).

Health data type: Health data were classified according to their sources, into: data obtained by health care

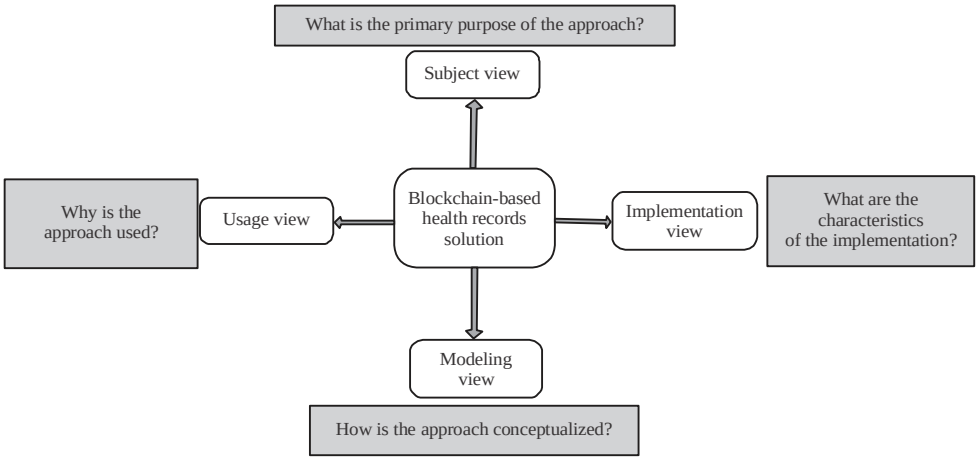

Fig. 2: The overall structure of the referenced framework

providers which is clinical data and data obtained by the patient which is personal health data, in addition to data obtained by the devices connected to the patient, namely the Internet of Things data[10].

Blockchain type: A distinction can be made between three main types of Blockchains which constitute the possible values for this facet: {public, permissionless, Blockchain Consortium (public, permissioned) and private permissioned}[11].

Usage view: It answers the question: "Why is the studied approach used?" It is concerned with the end state of the approach and the interim objectives. It focuses on the context of using approaches for building health record solutions using blockchain technology. This view can be expressed by the following facets:

Health records end goals: The intended goals of health records differ, depending on the main reason for building them. It is centered around one or more of the set's values: {Storing, management, sharing, security and privacy, interoperability, medical research, integration, access control management, patient sovereignty, scalability}.

Interim objectives: It represent a set of functions implemented by the approach in order to reach the end state. It takes one or more values from the following set: (add, edit, store, manage, exchange, query, display, ...).

Modeling view: It answers the following question: "How was the approach model conceived?" This view relates to the concepts, designs, technologies, formulas and symbols used. It is represented by the following facets:

Access mechanism and identity matching: Theaccess mechanism to health data through Blockchain were distributed as follows: Correspondence to the User ID.

Membership service provider: Using hyperledger fabric platform membership service to issue ECert Membership Certificate, TCert Transaction Certificate for access control.

Digital identity using public key: providing access to data by public keys through requesting and approving transactions.

FHIR URLs: Granting access by querying and retrieving data outside of the blockchain using FHIR URLs once located.

Blockchain model cost: The cost of a permissioned blockchain varies by the number of nodes and the amount of SaaS used in the application, i.e., the cost is fixed per month. As for permissionless blockchain, the monthly costs vary based on the transaction fees, as the cost of each transaction varies depending on the cost of the bitcoin or ether cryptocurrencies. As for hyperledger fabric blockchain, there are no transaction fees.

Model technologies: There are three technologies used in the studied approaches to build frameworks for health records:

Blockchain (BC): A distributed database that records a chronological list of records and transactions that are linked in a static manner through a series of blocks[12].

The Internet of Things (IoT): It is defined as "a model in which computing and networking capabilities are included in any kind of conceivable thing. These capabilities are used to inquire about the state of an object and change its state if possible"[13].

Cloud computing: "It refers to a service-oriented architecture that provides ubiquitous computing, greater flexibility and services on demand"[14].

Standards and regulations: Some methodologies discussed the use of several standards, including digital health standards and compliance with privacy and security regulations[15]. The most commonly used digital health standards are: older versions of HL7 standards[16] and Fast Healthcare Interoperability Resources Standard (HL7's FHIR)[17]. The most commonly used privacy and security regulations are: Health Insurance Portability and Accountability Act (HIPAA)[18] and the European General Data Protection Regulation (GDPR).

Consensus mechanism: It represent how consensus is reached in blockchain networks. There are many proposed and used consensus protocols and they're represented by the set: (Delegated Proof of Stake (DPoS), Proof of Work (PoW), Proof of Authority (PoA), Proof of Stake (PoS), Practical Byzantine Fault Tolerance (PBFT), Proof of Interoperability (PoI)[19], ...).

Consensus determination: This facet describes the determinators of the consensus mechanism. The number of nodes involved in the consensus mechanism relates to the type of the chosen blockchain. In public blockchains, all the nodes within the network participate in the consensus mechanism while in consortium blockchains, a selected set of nodes participate in the consensus mechanism. As for private blockchains, a selected set of nodes participate in the consensus mechanism or one organization only[6].

Encryption algorithms: Encryption algorithms can be classified according to the number or types of encryption keys used, into three categories approved by NIST[20]:

Symmetric encryption: It uses one encryption key for the purposes of encryption and decryption.

Asymmetric encryption: It uses two mathematically related keys, known as public and private keys, one for encrypting the data while the other is for decrypting it.

Hashing: It is used to transfer large sized random data into fixed small sized data, called hash value[20].

Smart contracts: Some blockchain infrastructures support smart contracts, for example the Ethereum platform[21] where smart contracts are defined as self-executing code in the blockchain network, facilitating negotiation, verification and execution of contracts digitally without a third party[22]. Other variants of smart contracts have emerged including the Hyperledger "chaincode"[23]. The bitcoin network does not use smart contracts or the equivalent because it limits its transactions by script size.

Mining rewards: It takes one or more of the set values: {tokens, access to data for medical research, mining share, none}.

Access control: Access control is usually defined by authorization models and access control policies to health data or records. Authorization models are categorized by level of detail into: Coarse-grained access control (CGA) and fine-grained access control (FGA)[24].

Model data: This aspect relates to the classification of data and their format in regards to input and output data.

Data classification (input and output): It takes one of the set values (structured, semi-structured, unstructured).

Data format (Input and output): Set of values (Text, XML, JSON, PDF, HL7 FHIR Resources, Any Format,...).

Storage methodology: There are three methodologies for data storage when using blockchain technology and they are[25]:

On-chain storage: Storing data in the form of secured transactions organized into sorted blocks and on the transaction log. Transaction validation, consensus protocols and decentralized execution of the program cause additional costs and time delays, in addition to the cost of mining and transaction fees.

Off-chain storage without anonymization: Aims to reduce the challenges of on-chain storage by transferring data and computing away from the blockchain to a data warehouse, server, or other third party[25].

Off-chain storage with anonymization: This methodology is based on data anonymization and then storing it outside the chain to maintain the security and privacy of patient's data.

Data stores: This facet is concerned with the repository for storing the system output of health data and it varies according to the type of data. We determined the values for this facet, according to the most frequently cited repositories in research papers on health records solutions:

Relational Databases (RDB): "It is a set of tables that contain data that have been synthesized into pre-defined categories".

Distributed Databases (DDB): It is a group of more than one interconnected database that is physically spread across different locations, that communicate over a network[26].

Cloud Storage (CS): It allows digital data to be stored and retrieved by multiple servers in often geographically different locations and managed by the hosting provider[27].

Cloud Data Lake (CDL): It is a central repository hosted on the cloud that stores all data of any scale. It can include structured data from relational databases, semi-structured data such as JSON, unstructured data such as documents and binary data such as images and video[28].

Blockchain (BC): It is an immutable transaction record that records data entries in a decentralized manner, grouped together into blocks of data and linked to previous and future blocks through hashing. It also enables entities to interact without a trusted centralized third party[29].

Implementation and validation view: It answers the question: What are the characteristics of the implementation and validation approach? It presents the technologies, algorithms and programming structures used to achieve the solution approach. We suggest describing this view with five facets, namely:

Model implementation: There are currently three approaches for building blockchain models:

- Using blockchain open-source frameworks or platforms
- Creating new native blockchain applications
- Building blockchain based on the implementation of a blockchain presented in previous work[6]

Blockchain frameworks/platforms: The literature review shows that most recent solutions use Ethereum[30] and hyperledger fabric[23]. Most solutions that used the bitcoin platform date back to 2016.

Ethereum[30]: Is an open-source blockchain platform that uses smart contracts and provides a decentralized virtual machine to work with nodes, create services, applications, or various contracts. its' cryptocurrency is called Ether[24].

Hyperledger fabric[23]: Is an open source blockchain platform, that supports Distributed Ledger Technology (DLT) by providing a modular framework that supports different components for different uses, including consensus mechanisms, storage models, identity services, access control and smart contracts (chaincode)[31].

Bitcoin: It was the first blockchain implementation which is a type of digital currency based on blockchain technology, used for e-commerce[31].

Django: It is a free, high-level, python-based web application framework[32].

MultiChain[33]: It is a Tribler-based proof of concept, secure and encrypted, BitTorrent peer-to-peer system that takes a different approach with multiple chains instead of one chain[33].

Programming languages: This facet focuses on the languages used to implement the solution model and it takes one or more set values: (JavaScript, Python, Solidity, GO, ...).

Performance metrics: They are methods of measuring and benchmarking the performance of models that differ according to the technologies and frameworks used. It takes one or more of the set values (Average Response Time (ART), Throughput or Transaction per second (TPS), Round Trip Time (RTT), Latency, Fairness, ...).

Implementation output: Represents the form of knowledge that resulted from implementing the proposed approach, taking one of the list values: {prototype, model architecture, decentralized application, functioning system, none}.

Related approaches (Previous solutions): There are many previous approaches concerned with health records and their challenges. We have chosen five previous state of the art solutions, namely MedRec[34], FHIRChain[35], Liang *et al*.[33], Peterson *et al*.[19] and BlocHIE[37], then, we have implemented our comparison framework to provide an analysis and evaluation to the solution.

RESULTS AND DISCUSSION

Analysis and evaluation based on the proposed framework: Based on the proposed framework and the definition of the concepts within it, we present an analysis of all the studied approaches according to the framework that we have built.

MedRec[34], FHIRChain[35] and BlocHIE[37] have similar approaches of blockchain implementation, they all use permissionless blockchain, so, they all face challenges of time consumption, scalability, confidentiality, 51% attack threat, transaction fees, mining process and high computing power implications. These approaches also require the participation of all nodes to reach consensus which greatly increases energy consumption and reduces efficiency. Moreover, in the MedRec model[34], although, the model assumes non-disclosure of Personally Identifiable Information (PII) and uses encryption of

Table 2: Comparison summary of the studied approaches

Face	BlocHIE[37]	Peterson *et al*.[19]	Liang *et al*.[36]	FHIRChain[35]	MedRec[34]
Subject					
Level of detail	Black box	Black box	Black box	Black box	White box
Patient's	EMR	EHR	-	-	EMR
Implementation scope	Patient health facilities	Patient health facilities	Patient	Health facilities	Health facilities
Implementation field	Health	Health, medical research	Health	Health	Health facilities research
Health data type	Clinical, PHD IoT	Clinical	PHD IoT	Clinical	Clinical
Blockchain type	Public, permission	Private, permission	Private, permission	Private, permission	Public, permission
Usage					
Health records end goal	Storing, sharing, integration	Mngmt, sharing interoperability, research	Integration, AC, patient sovereignty scalability	Sharing, interoperability, AC, scalability	Mngmt, sharing security, interoperability, research, Integration, AC, patient sovereignty
Interim objectives	Store, exchange query	exchange query	Mange, exchange query	Store, exchange query	Store, exchange query
Model					
Access mechanism	ID	FHIR URLs	MSP (ECert, TCert)	Digital identity (public key)	Digital identity (public key)
Blockchain model cost	-	-	Free	Paid (transaction rate, Ether)	Paid (transaction rate, Ether)
Model technologies	BC, IoT	BC	BC, IoT, cloud computing	BC	BC
Standards/Regulation:					
Standards	-	HL7's FHIR	-	HL7's FHIR	HL7, HL7's FHIR
Regulation	-	-	-	-	HIPAA
Consensus mechanism	PoW	Pol	PoS	PoS	PoW
Consensus determination	All Nodes	All Nodes	Selected set of nodes	One organization	All nodes
Encryption Algorithem:					
Symmetric	-	-	-	Sign then encrypt [38]	-
Asymmetric	-	-	-	PKA(-)	PKA(-)
Hashing	MD5	SHA-256	SHA-256	Keccak-256	Keccak-256
Smart contracts	Not utilized	MultiChain	Chaincode	Ethereum smart contract	Ethereum smart contract
Mining Reward	-	Mining share	None	Token	Token, access to data
Access Control	-	-	FGA	FGA	FGA
Modal Data:					
Classification action					
Input	Semi-structured	Semi-structured-Unstructured	Semi-structured-Unstructured	Semi-structured-Unstructured	Semi-structured-Unstructured
Output	Semi-structured-Unstructured	Structured	Semi-structured-Unstructured	Semi-structured	Semi-structured-Unstructured
Format:					
Input	-	Any format	-	-	Any format
Output	-	FHIR resources	-	-	Any format
Storage methodology	Off-chain, On-chain, storage without	On-chain, storage without anonymization	On-chain, Off-chain storage with	On-chain, storage without anonymization	On-chain, storage with anonymization
Data store	BC, DDB	-	BC, CS	RDB	RDB
Implementation					
Model execution	Open-source platform	Based on pervious implementation	Open-source platform	Open-source platform	Open-source platform
BC platform	Django	MultiChain	Hyperledger fabric	Ethereum	Ethereum
Programming language	Python	-	-	JavaScript, Solidity	Solidity, python
Performance metrics	TOS, Fairness	-	ART	-	-
Implementation output	Prototype	Model Architecture	Prototype	DApp	Functioning System

on-chain data, an unauthorized user could infer the occurrence of transactions by analyzing network communications.

Whereas, even without direct disclosure of the patient's name, a conclusion can be drawn about a particular patient from the metadata of one Ethereum address with several others. Not to mention that patient records are stored off-chain, where medical records are kept locally in separate relational databases for health care providers which poses a new challenge in terms of ensuring data security and patient sovereignty.

The authors also argue that a sustainable and secure peer-to-peer network can only be built by providing big data and incentivize researchers with access to data for medical research as a mining reward while engaging patients and service providers. However, the platform has not been validated for medical records and needs to be expanded in order to obtain health data that represent complex health system scenarios.

In the case of MedRec[34] and FHIRChain[35] and other Ethereum-based implementations[30], public keys are used as a form of digital identity. However, if the user loses their private key, it is impossible to authenticate that user. These systems also issue their own tokens to incentivize costly mining or to fuel the execution of smart contracts which increases computing power consumption and make interactions with other distributed systems more complicated. As for the BlocHIE approach[37], a model has been proposed for two loosely-coupled blockchains to handle different kinds of healthcare data while records are stored off-chain, personal health data is stored on-chain which leads to restricting data volumes and affects the system's performance, as it may lead to issues in assigning and matching data of the two blockchains.

As for the implementation of permissioned blockchain in healthcare, the approach of Liang *et al*.[36] uses the hyperledger fabric platform which implies that the model does not include transaction fees, nor does it issue tokens because it does not require participation in the mining process, therefore, there is no need to incentivize it. However, the data are stored on-chain which leads to data volumes restrictions and may violate the patient's right to delete his data or to revoke access to his data from a medical research or clinical trial.

While Peterson *et al*.[19] approach also uses permissioned blockchain, the data are stored off-chain without anonymization which poses a threat to data's security and privacy. Moreover, they did not provide any implementation details but rather settled for a conceptual solution explanation. In addition, the solution model is also limited in terms of smart contract functionality which is not fully supported by the implementation of the selected blockchain (MultiChain[33]). A projection of the five solutions approaches to the referenced four-views framework are presented in Table 2.

Table 3: MHMS Approach based on the referenced framework

View	Facet	Value
Subject	Level of detail	White box
	Patient's records	PHR
	Implementation Scope	Patient, Health facilities
	Implementation field	Health, medical research
	Health data type	Clinical, PHD, IoT
	Blockchain type	Private, Permissioned
Usages	Health records' end goals	Storing, mngmt, sharing security, interoperability, research, integration, AC, patient
	Interim objectives	Store, exchange, manage, query
	Access mechanism and identity matching blockchain model cost	MSP (ECert, TCert) free
Model	Model technologies	BC, IoT, cloud computing
	Standards/regulation:	
	Standards	HL7's FHIR
	Regulation	HIPAA, GDPR
	Consensus mechanism	PBFT
	Consensus determination	Selected set of nodes
	Encryption algorithms:	
	Symmetric	AES
	Asymmetric	RSA, ECDSA
	Hashing	SHA3-256
	Smart contracts	Chaincode
	Mining rewards	None
	Access control	FGA
	Model data	
	Classification:	
	Input	Structured, semi-structured, semi-structured,
	Output	Semi-structured, structured,
	Format:	
	Input	Any format
	Output	JSON, HL7 FHIR resources off-chain
	Storage methodology	storage with anonymization
	Data store	Cloud data lake
Implementation	Model Implementation BC Platforms	Open-source platform hyperledger fabric
	Programming languages	JavaScript, python
	Performance metrics implementation output	ART, TPS, RTT, latency prototype

Building a novel blockchain-based PHR framework: Based on our analysis and evaluation of the existing solution's approaches, we have paved the way to a new approach that takes into consideration, what went wrong with earlier approaches that adopted blockchain technology for health records.

We also made use of the strength characteristics of the aforementioned solutions benchmarking, to lay a systematic basis for our new approach, My Health My Story: a blockchain-based hyperledger framework for personal health records.

Our Approach is concerned with developing a framework aimed at collecting, integrating, managing and sharing of fragmented health records data in a secure and reliable manner, using blockchain. MHMS is a patient-centered framework that allows all patients enrolled in it to manage their personal health records across various healthcare providers. This framework will ensure protection of patient privacy and the security of their records, while observing health data management requirements including the patient-defined access control policy.

A projection of our proposed solution onto the referenced four-views framework presented in Table 3. Based on the above, we determined the added values for our approach which differs in orientation from previous work in the same field and it includes the following:

It supports Personal health records which gives the user complete control over his health data. It uses off-chain storage with anonymization methodology and it stores data in a cloud data lake. It addresses more challenges of health records as our approach seeks data integration, data storage, patient sovereignty, access control, data sharing, patient-centric interoperability, security and privacy.

It supports medical research, through a cloud data store that provides availability and quality of data for research purposes.

It uses public-key algorithms (RSA and ECDSA), symmetric encryption algorithm (AES) and hashing algorithms (SHA). It complies with HIPAA and GDPR regulations to ensure privacy and security.

It provides correctness and performance testing of the proposed system through several tools, namely: hyperledger composer and hyperledger caliper with performance metrics such as ART, TPS, RTT and latency.

The high-level architecture of My Health My Story: a blockchain-based framework for personal health record is presented in Fig. 3.

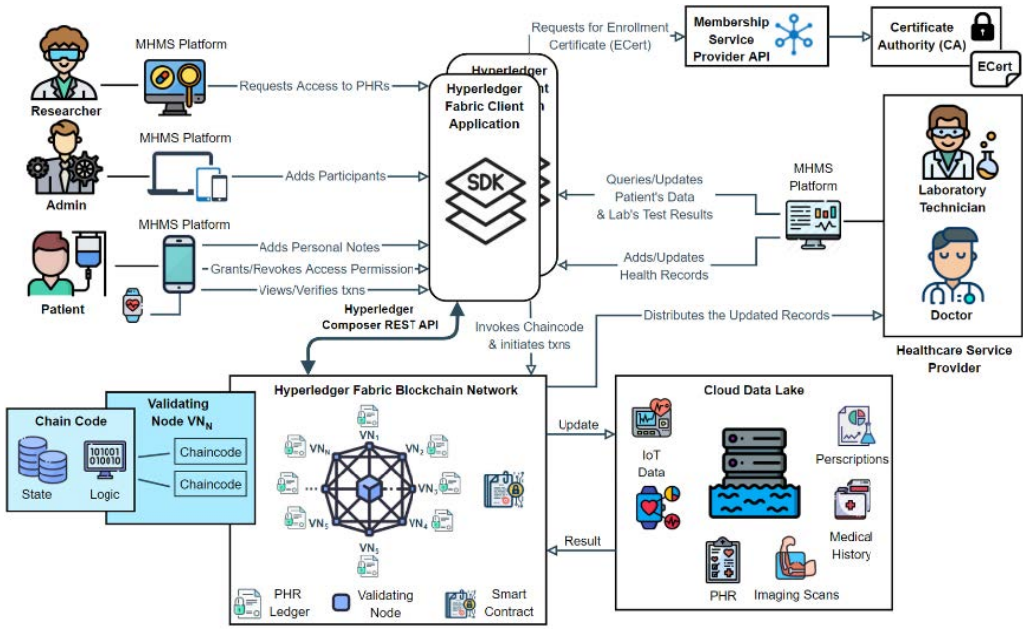

Fig. 3: MHMS high-level architecture

CONCLUSION

In this study, a systematic comparison framework was presented in detail and a set of blockchain-based health records solutions were presented, then they were projected onto the comparison framework and we finally, presented an analysis of these approaches in terms of their similarities and features. We also presented an architecture of our proposed framework for personal health records storage, management, interoperability and sharing. It ensures privacy, security, availability and fine-grained access control over highly sensitive patient's data.

As part of future work, we would like to implement a prototype of MHMS framework, test it with the data of the real patients, provide correctness and performance testing and a detailed security analysis. Our long-term goal is to validate the prototype for personal health records by obtaining health data that represent complex health system scenarios and apply those scenarios in practice to enhance the current healthcare data management.

ACKNOWLEDGMENTS

This research is supported by the Higher Institute for Applied Sciences and Technology, Damascus, Syria. The authors appreciate the valuable comments provided by the anonymous referees.

REFERENCES

01. Rolland, C., C.B. Achour, C. Cauvet, J. Ralyte and A. Sutcliffe *et al*., 1998. A proposal for a scenario classification framework. Requirements Eng., 3: 23-47.
02. Jarke, M., K. Pohl, S. Jacobs, J. Bubenko and P. Assenova *et al*., 1993. Requirements engineering: An integrated view of representation, process and domain. Proceedings of the 4th European Software Engineering Conference, September 13-17, 1993, Germany, pp: 100-104.
03. Jarke, M., J. Mylopoulos, J.W. Schmidt and Y. Vassiliou, 1992. DAIDA: An environment for evolving information systems. ACM Trans. Inform. Syst., 10: 1-50.
04. Rolland, C., 1997. A primer for method engineering. Proceedings of the Conference INFORSID (Informatique des Organisations et Systemes d'Information et de Decision), June 10-13, 1997, Toulouse, France, pp: 1-26.
05. Aljoumaa, K., 2011. [Intentional modeling and semantic annotation for the reuse of PASiS business services: Publishing and searching of intentional services]. Ph.D. Thesis, Pantheon-Sorbonne University, Paris, France. (In French)
06. Hasselgren, A., K. Kralevska, D. Gligoroski, S.A. Pedersen and A. Faxvaag, 2020. Blockchain in healthcare and health sciences-a scoping review. Int. J. Med. Inf., Vol. 134, 10.1016/j.ijmedinf.2019.104040
07. Garrett, P. and J. Seidman, 2011. EMR vs HER-what is the difference?. Health IT Buzz Inc, USA.

08. Gunter, T.D. and N.P. Terry, 2005. The emergence of national electronic health record architectures in the United States and Australia: Models, costs and questions. J. Med. Internet Res., Vol. 7, No. 1. 10.2196/jmir.7.1.e3
09. Tang, P.C., J.S. Ash, D.W. Bates, J.M. Overhage and D.Z. Sands, 2006. Personal health records: definitions, benefits and strategies for overcoming barriers to adoption. J. Am. Med. Inf. Assoc., 13: 121-126.
10. ISO., 2012. Health informatics-personal health records-definition, scope and context. International Organization for Standardization, Switzerland. Geneva, Switzerland.
11. Zheng, Z., S. Xie, H. Dai, X. Chen and H. Wang, 2017. An overview of blockchain technology: Architecture, consensus and future trends. Proceedings of the 2017 IEEE International Congress on Big Data (BigData Congress), June 25-30, 2017, IEEE, Honolulu, Hawaii, USA., ISBN:978-1-5386-1997-1, pp: 557-564.
12. Bahga, A. and V.K. Madisetti, 2016. Blockchain platform for industrial internet of things. J. Softw. Eng. Appl., 9: 533-546.
13. ITU, 2005. ITU internet reports 2005-the internet of things: Executive summary. ITU, Pages: 17.
14. Verma, J., 2014. Study of cloud computing and its issues: A review. Smart Comput. Rev., 4: 389-411.
15. Chukwu, E. and L. Garg, 2020. A systematic review of blockchain in healthcare: Frameworks, prototypes and implementations. IEEE. Access, 8: 21196-21214.
16. HLSI., 2007. January working group meeting. Health Level Seven International, Ann Arbor, Michigan.
17. HL7 FHIR, 2011. FHIR is a standard for health care data exchange. HL7 FHIR Foundation, USA.
18. HIPAA., 1996. Health insurance portability and accountability act of 1996. Public law, 104, 191, Health Insurance Portability and Accountability Act of 1996, USA.
19. Peterson, K., R. Deeduvanu, P. Kanjamala and K. Boles, 2016. A blockchain-based approach to health information exchange networks. Proc. NIST Workshop Blockchain Healthcare, 1: 1-10.
20. Mushtaq, M.F., S. Jamel, A.H. Disina, Z.A. Pindar, N.S.A. Shakir and M.M. Deris, 2017. A survey on the cryptographic encryption algorithms. Int. J. Adv. Comput. Sci. Appl., 8: 333-344.
21. Buterin, V., 2014. A next-generation smart contract and decentralized application platform. Ethereum White Paper, Ethereum Org., UK.
22. Buterin, V., 2013. A next generation smart contract and decentralized application platform. Ethereum, Ethereum White Paper, Ethereum Org., UK.
23. Anonymous, 2015. Advancing business blockchain adoption through global open source collaboration. Hyperledger Fabric, The Linux Foundation, San Francisco, California.
24. Yusuf, K., 2018. Granularity in authorization: Fine grained vs. coarse grained authorization. WordPress, USA.
25. Eberhardt, J. and S. Tai, 2017. On or off the blockchain? Insights on off-chaining computation and data. Proceedings of the European Conference on Service-Oriented and Cloud Computing, September 27-29, 2017, Springer, Oslo, Norway, pp: 3-15.
26. Tomar, P., 2014. An overview of distributed databases. Int. J. Inf. Comput. Technol., 4: 207-214.
27. Winburn, M. and A. Wheeler, 2015. Cloud Storage Security: A Practical Guide. Elsevier, Amsterdam, Netherlands,.
28. Anonymous, 2020. Cloud data lakes-from on-premise to the cloud. Dremio Corporation Software, Santa Clara, California.
29. Raikwar, M., D. Gligoroski and K. Kralevska, 2019. SoK of used cryptography in blockchain. IEEE Access, 7: 148550-148575.
30. Ethereum, 2015. Ethereum is a global, open-source platform for decentralized applications. Ethereum Org. UK.
31. Lin, I.C. and T.C. Liao, 2017. A survey of blockchain security issues and challenges. Int. J. Netw. Secur., 19: 653-659.
32. Django, 2020. Django makes it easier to build better web apps more quickly and with less code. Django Software Foundation, Amsterdam, Netherlands.
33. Norberhuis, S.D., 2015. MultiChain: A cybercurrency for cooperation. Master Thesis, Delft University of Technology, Delft, Netherlands.
34. Azaria, A., A. Ekblaw, T. Vieira and A. Lippman, 2016. Medrec: Using blockchain for medical data access and permission management. Proceedings of the 2016 2nd International Conference on Open and Big Data (OBD), August 22-24, 2016, IEEE, Vienna, Austria, pp: 25-30.
35. Zhang, P., J. White, D.C. Schmidt, G. Lenz and S.T. Rosenbloom, 2018. FHIRChain: Applying blockchain to securely and scalably share clinical data. Comput. Struct. Biotechnol. J., 16: 267-278.
36. Liang, X., J. Zhao, S. Shetty, J. Liu and D. Li, 2017. Integrating blockchain for data sharing and collaboration in mobile healthcare applications. Proceedings of the 2017 IEEE 28th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), October 8-13, 2017, IEEE, Montreal, Canada, pp: 1-5.
37. Jiang, S., J. Cao, H. Wu, Y. Yang, M. Ma and J. He, 2018. Blochie: A blockchain-based platform for healthcare information exchange. Proceedings of the 2018 IEEE International Conference on Smart Computing (SmartComp), June 18-20, 2018, IEEE, Taormina, Italy, pp: 49-56.