Framework for Next Generation of Digital Healthcare Systems

Jovan Karamachoski(✉) and Liljana Gavrilovska

FEIT, University Ss. Cyril and Methodius in Skopje,
Skopje, Republic of Macedonia
jovankaramac@yahoo.com, liljana@feit.ukim.edu.mk

Abstract. The healthcare system is one of the most important segments of the modern society. The support of cost effective and reliable digital solutions, can enhance the health of the patients and improve the healthcare system as a whole. The evolution of the eHealth systems shows immense benefits from implementation of modern technologies (e.g. smartphones, 3G and 4G networks, IoT sensor networks) improving quality of life and increasing comfort. One of the last technological breakthrough, the Blockchain technology, is promising even better improvements in eHealth systems by enhancing the privacy and security protection, easing the usability of the IoT devices, predicting potential hazardous illnesses and leveraging the comfort of living. This paper proposes a generic framework for a novel eHealth system based on the Blockchain technology that complements the development of the future 5G services.

Keywords: eHealth · Blockchain · Framework for healthcare systems

1 Introduction

The healthcare system, together with the healthcare regulations can create significant impact on the comfort of the patients' life. It can also affect the health condition of the community as a whole. Modern healthcare system relays on digital technologies for gathering and storing patients' data, remotely diagnosing illnesses and monitoring vital signs. The digital technologies used to deliver medical care or monitor patients' health condition are known as telemedicine, telehealth or eHealth. The terms are used interchangeably. However, the last one points to the most modern Internet-based solutions. All of them exchange medical data through different telecommunication systems.

The development of the electronic healthcare systems for delivering medical care on a distance can be divided into pre-Internet and Internet-based electronic healthcare systems. The pre-Internet electronic healthcare systems are also referred as telemedicine systems. They focus on enabling the medical care on a remote sites, and/or on digitalization of the medical records.

The development of the Internet-based healthcare systems, known as eHealth systems, also passed through several generations. Each generation introduces a new subsystem or a feature, (e.g. cloud-based solutions, integration of 4G services, IoT devices, Blockchain, integration of 5G services). There are three existing Internet-based generations of eHealth systems developed until today.

© ICST Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2019
Published by Springer Nature Switzerland AG 2019. All Rights Reserved
V. Poulkov (Ed.): FABULOUS 2019, LNICST 283, pp. 12–24, 2019.
https://doi.org/10.1007/978-3-030-23976-3_2

In this paper we propose a novel generic framework for the next generation of eHealth systems, the fourth generation, with strong accent to the privacy, security, persistence and usability of data. It implements the most modern technologies, like Blockchain and Machine Learning, and provides enhanced comfort and users' mobility.

The paper is organized as follows. Section 2 presents the related work and Sect. 3 gives our definition of eHealth system generations and their characteristics. In Sect. 4 we are proposing the generic layered approach for building the next (fourth) generation of eHealth systems. Section 5 gives the direction for the future work and Sect. 6 concludes the paper.

2 Related Work

There are already some ongoing activities, both in academia and in companies, focusing on implementation of the Blockchain technology integrated with the IoT networks, for design of enhanced healthcare systems [1]. They try to deliver competitive solutions, despite the limitations of the current Blockchain technology. The main hook for this fusion is the privacy-by-design provided by the Blockchain technology. It might solve the most important privacy issues for the healthcare systems.

The Blockchain technology provides the access management capabilities for the patients. The authors in [2–5] propose access management protocols for medical data records, based on the Blockchain technology. The self-executable Smart contracts deployed on the Blockchain, can check credentials of the users, compare the authorization roles and privileges, change the scope of control based on patients' needs and execute any restrictive code to change a user privileges. The Blockchain ledger can record all input parameters, roles and privileges and can act as an arbiter for access management. Particular solutions for access management based on Blockchain technology can be adapted from other scenarios, such as IoT network access control mechanisms, presented in [6–8]. These solutions can provide enhanced automation in machine-to-machine type communication scenarios.

Another important aspect of the healthcare system design is the storage of medical data. As described in [1], the scalability issue regarding the storage capacity is immense in a large-scale scenarios. Current baseline Blockchains have poor storage capacity and are inappropriate for the healthcare system solutions. The academia offers several solutions, targeting the storage capacity. The authors in [9] propose general guide for architecture design and storage location. They stress the importance of the extensively distributed architecture for Blockchain based scenarios, in order to benefit from the decentralization of the procedures. Particular solutions can be found in [10–12]. The papers propose scalable data storage solutions, where the Blockchain acts as a ledger of data addresses, pointing out the location of the particular data.

The implementation of the Smart contracts in automatic or semi-automatic manner, will improve the machine-to-machine communications. Moreover, the implementation of the Artificial Intelligence (AI) agents capable to execute Machine Learning algorithms in the Blockchain networks can conduct predictive analysis. In practical healthcare systems these AI agents (Doctor-bots) can determine personalized diagnoses

or predict illnesses or epidemics. The importance of the Internet of Robotic Things for the Ambient Assisted Living (AAL) in correlation with future Blockchain-based solutions can be found in [13]. The AAL is extremely important for the patients with dementia or Alzheimer's disease. Also the AAL solutions are tightly linked with smart home solutions. This enables many Blockchain-based smart home and smart city solutions to be implemented in the future eHealth systems [14–16].

3 Healthcare System Generations

The healthcare practice on a distance is present for centuries, but the development of the telemedicine, date back in the second half of the 20th century, after the initial development of the telemedicine system for health condition monitoring of the astronauts. Recent history of the telemedicine developments can be found in [17]. The first telemedicine projects were television and telephone based two-way communication systems that enabled consultation practices. Mainly bulky, pricey and very complex, these projects were not successful telemedicine solutions. After the initial phase, by the end of 20th century, the telemedicine systems started to be based on computers, servers and local network, basically used to digitalize the patients' data. Generally, these are the systems collocated in hospitals, built with intention to enhance the internal workflow and inter-sector communication. They are mainly offline (Internet-less) systems. The main concern are the security of the communication and privacy of the patients' data. The lack of Internet access in these types of electronic healthcare systems decreases the privacy related concerns mainly because the systems are not spread among large number of institutions and the access to the data is physically protected. Also, the potential awareness of the patients' privacy was low.

At the end of the 20th century, with the development and deployment of the Internet, new type of telemedicine systems emerged [18], today known as eHealth systems. The eHealth systems are online Internet-based systems, where the entities from different healthcare institutions are connected and are able to share information, collaborate in real-time or access patients' information on a distance. The deployment of the Internet and the cost-effectiveness of the modern systems, spread the medical point-of-presence in every hospital, every office and even in each mobile device. The omnipresence of the eHealth systems and services, rises the awareness for privacy issues requiring further enhancements. There are several generations (phases) in development of the eHealth systems.

3.1 First Generation eHealth Systems

The first generation of eHealth systems is built from independent and isolated corporate networks, with data centers collocated in the hospitals, as presented in Fig. 1. These systems are dimensioned to store sufficient amount of medical records, with easily extensible capacity due to server modularity. They are following general client-server architecture focusing on the enhanced network protection. The supplied Internet access exposes the systems to potential attacks and rises privacy concerns. The maintenance of the corporate network is huge burden for the hospitals, since it requires skilled

engineers and expensive equipment to maintain reliable network with strong security and privacy. The privacy management is guaranteed by the hospitals and patients don't have any control over their personal data or collected health related data.

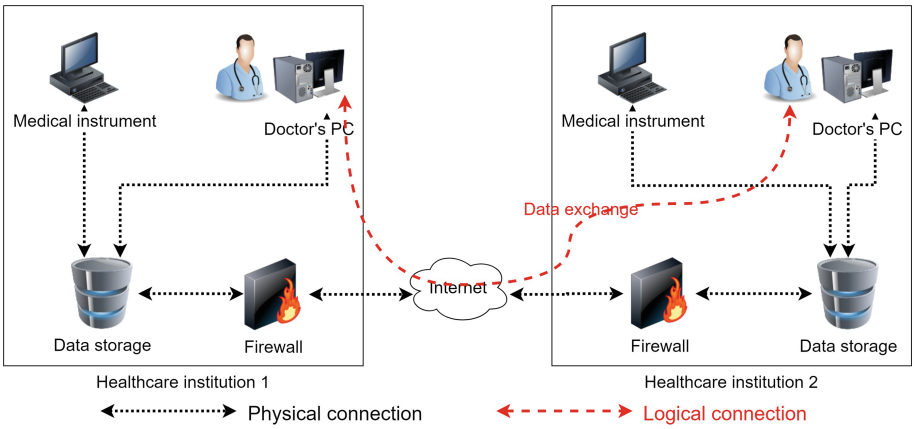

Fig. 1. Simplified communication procedure in first generation of eHealth systems

3.2 Second Generation eHealth Systems

The second generation of eHealth systems is characterized by introduction of cloud-based and IoT services (see Fig. 2). With the development of the cloud-based services, the eHealth systems were transformed from the hospital-centric to cloud-centric. The centralization of the system solutions, rises concerns for the privacy and security of the patients' data. This may decrease the expenditures of the hospitals for maintenance of the corporate network. However, the single point of access for this type of systems is potential bottleneck and makes it prone to attacks. Consequently it requires higher level of security, authentication and authorization measures are taken into account. Beside the concerns there are benefits from this type of systems. Mainly the cost effectiveness is the biggest benefit, but also the Government institutions can have greater insight in the patients' health status and the possibility to analyze the financial aspect of the healthcare system.

The introduction of the IoT nodes in the second generation of eHealth systems, provide the patients and the healthcare practitioners with better tool for monitoring of the patients' health status with higher precision and better comfort [19, 20]. The placement of the wireless health monitoring sensors on the patients' body for constant monitoring, supplies the healthcare practitioners with real-time data of the patients' health condition. The 3G data network access offers enhanced mobility in real-time monitoring protocols for any measured patient's parameter independently of the patients' location. The widespread high speed Internet access also offers more advanced services, such as remote surgery services on-the-go, home assistance for elder people, remote diagnostics, etc.

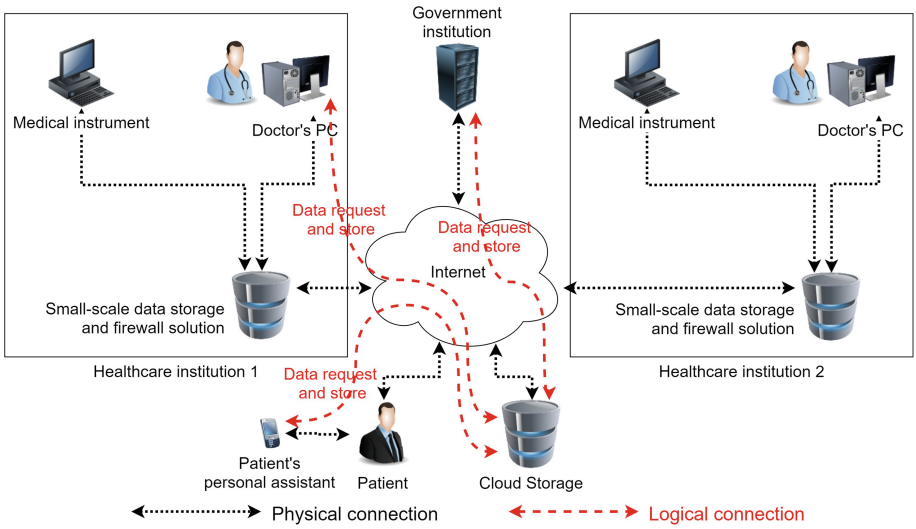

Fig. 2. Simplified communication procedure in second generation of eHealth systems

3.3 Third Generation eHealth Systems

The third generation of eHealth systems try to fix the growing privacy concerns, by introduction of the Blockchain technology in the system (see Fig. 3). The new environment witness continuous growth in number of mobile devices and application. With widespread high-speed Internet access, through Wi-Fi and 4G networks, the eHealth services can be delivered on a mobile device. These types of eHealth services are known as mHealth services. With the introduction of the Blockchain technology the patients can have full control of the auditability of the data. The patients can give temporal or permanent access to the healthcare practitioner by authorization through mobile application connected to the Blockchain. Other entities and governmental institutions can access the data if they are granted. The Blockchain acts as a ledger or third-party node to manage the access rights, as a complementary technology to the centralized cloud-based architecture. Several solutions are currently elaborated in [4, 21–23]. The main advantage of this generation of eHealth system over the previous ones is the user-centric approach for privacy management over the personal health related data. The implementation of the Blockchain technology solves the end-point privacy, but still have problem with privacy protection in the cloud. Moreover, there is a possibility of security attacks of stealing credentials or data from the end-user devices.

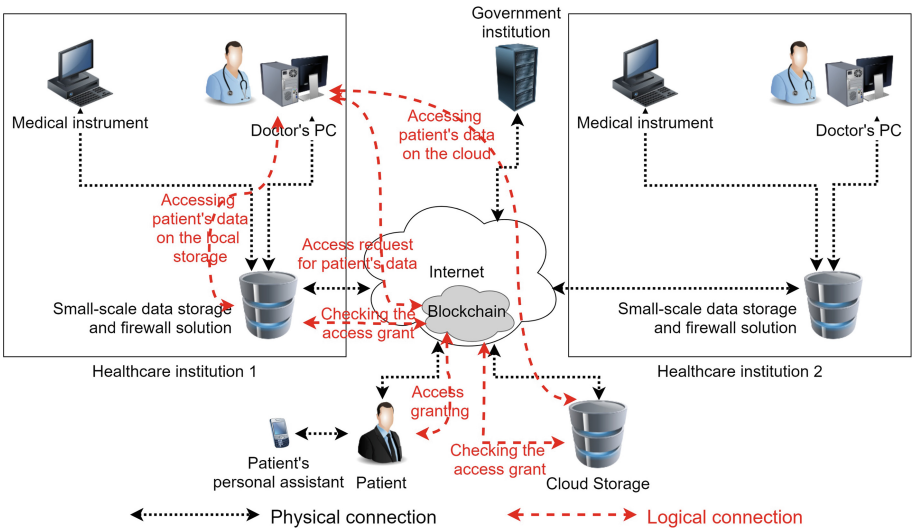

Fig. 3. Simplified communication procedure in third generation of eHealth systems

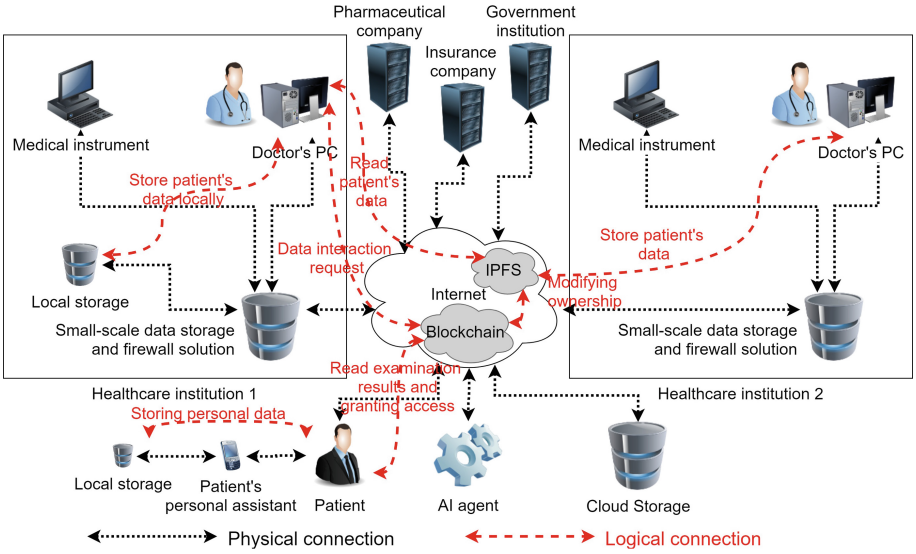

Fig. 4. Simplified communication procedures for basic use case scenario in fourth generation of eHealth systems

3.4 Fourth Generation eHealth Systems

The goal in this paper is to propose a generic framework for the next generation of eHealth systems. The fourth generation will have further improvements regarding the privacy, storage management, service availability, broader range of monitored health-related parameters, new business models, predictive analysis and even new architecture

design, as presented on Fig. 4. Beside the introduction of 5G networks as the main backbone for Internet access, this generation of eHealth systems will decentralize the data storage by implementation of the Blockchain sharding and will introduce Artificial Intelligence (AI) agents. The AI agents allow monitoring the patient's condition or population health condition and predicting any illness or epidemics. The enhanced and miniaturized IoT devices will offer constant health monitoring of elder people and tracking potential hazardous and health threatening conditions at work or/and at home. Many government institutions, pharmaceutical companies, insurance companies and other independent bodies can be interested in further analysis of the patients' data. The simplified communication procedures, are presented in Fig. 5.

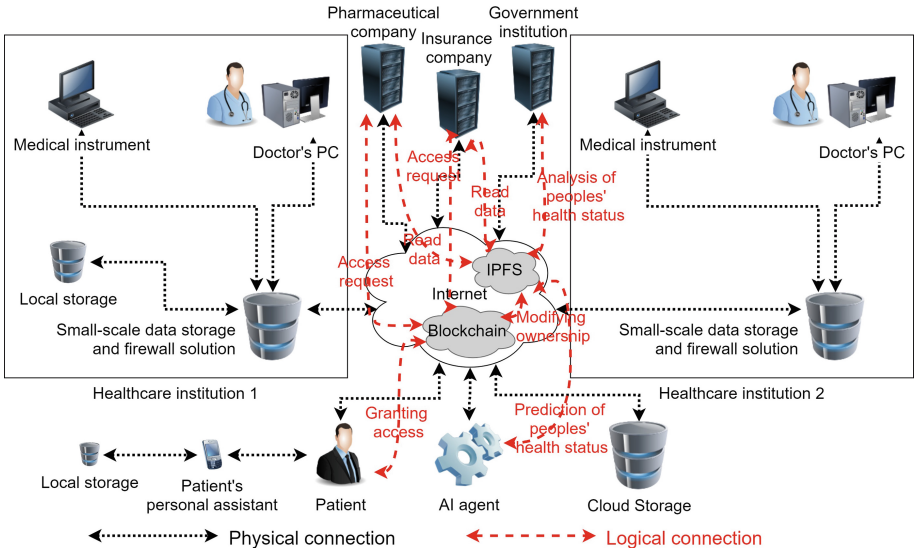

Fig. 5. Simplified communication procedures for other use case scenarios in fourth generation of eHealth systems

The implementation of the proposed generic framework for fourth generation eHealth system will provide advancement over the previous storage solutions, by implementing multimodal storage solution, without essential need of cloud-based databases. Also the new framework will offer more commodities for the patients and elder people by simplification of the usability and enhancing the Quality of Experience (QoE). The most important outcome will be the enhanced general population health. Contrary, the main disadvantage is the high complexity of the system for initial deployment due to small acceptance rate and the lack of understanding of the Blockchain technologies. After the initial deployment the system will be self-orchestrated due to deployed Smart contracts. The Smart contracts also provide the government's law framework to be implemented by a delegated entity.

4 Fourth Generation's Specifics

The generic framework for the future eHealth systems offers many advantages but also faces many problems towards the implementation phase. The specifics of the fourth generations of eHealth systems reflect on the overall layered eHealth system architecture, its entities and functionalities.

Layered Architecture. The proposed Layered structure of the next generation of eHealth systems is presented in Fig. 6. Based on the most recent technologies, the new system will offer enhanced privacy, data security, data persistence, user-centric data access management, predictive health analysis, new business models, etc.

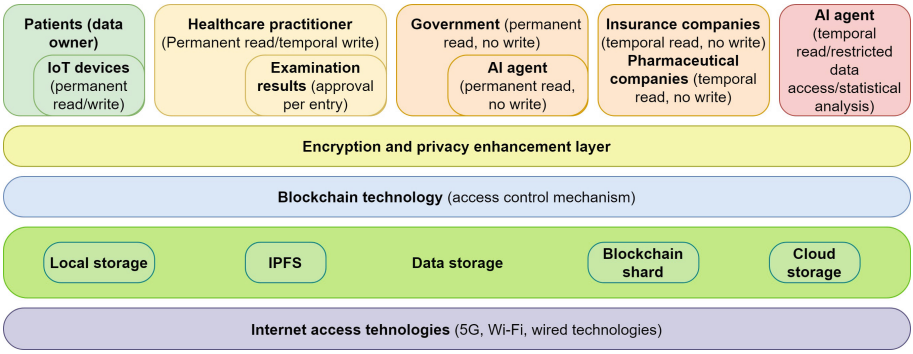

Fig. 6. Layered structure of the next generation eHealth system

The most important part of the architecture is the patient, or the data owner in the system. The Wallet address or more precisely the Blockchain public address presents the identity of the patient in this electronic system. The patient will have full control of its personal health data by use of mobile application. A Smart contracts, deployed on the Blockchain, will conduct the access restrictions set by the patients. The patient will be able to grant or revoke access rights on-the-go. By default, every data collected for the patient will be secured. Depending on the scenario, the patient can open selected data set and publically share it with relevant entities. Taking into account that any personal IoT device connected to the patient will collect large amount of data, it is convenient to give permanent data read and write permission to any IoT device attached on the patient body. The permission can be retracted in any time after the device is removed or there is no need for further data collection.

The healthcare practitioner will be another entity in the framework with main role to conduct medical protocols for the patient. The patient can choose to grant permanent or temporal data access to the doctor. The most convenient approach is the patient to choose a family doctor and grant him permanent data access, but he can also grant temporal access to any other doctor/specialist/emergency room doctor. In order to deter the doctor from entering data without patient's awareness, every entry of data by the doctor should be acknowledged by the patient.

New Use Cases and Business Models. The increased privacy will offer several new use cases and potential business cases. As a main advantage is the ability of the system to give the Governmental institutions a tool for monitoring of the health status of the nation. The openness of the data to the Government can increase the effectiveness of the healthcare system as a whole. By attaching AI agents to the eHealth system, the Governmental institutions can do predictive analysis for the expenditures of the healthcare system. Also, the AI agent can do predictive analysis per patient or per group of people, can suggest further treatment and predict illness or epidemics. The patient will give permanent data access to the Governmental institutions for full or restricted set of data, depending on the legislation.

The private sector, mainly the insurance companies, will be able to introduce new business cases like personalized insurance plan or adaptive insurance plans. Depending on the mutual agreement, the patient can grant the insurance company access to a limited set of data. This will enable the insurance company to track the health status or past health related issues of the patients and accordingly make personalized offer to the patient. For this reason the patient can grant temporal data access to insurance company, valid for the whole period of the agreement validity.

The pharmaceutical industry will also have benefit. The double-blinded studies conducted by the researchers, are of great importance for the pharmaceutical companies. This system will enable the pharmaceutical companies to have even bigger set of examined patients without revealing the patient identity. This will give the pharmaceutical companies better understanding of the medication effectiveness. The patients' habits and health condition can be used as input data for further analysis for the medication success rate. To incentivize the patients to participate in any future research, the pharmaceutical industry can pay for the data shared by the patients. This way the patients can monetize the collected data.

Introduced Intelligence - Smart Solutions. An independent public AI agents implemented in a form of Smart contract, can leverage the capabilities of the healthcare system. The AI agent will enable the system to predict possible pandemics or epidemics, but also can track patient's health and patient's habits and predict personalized health conditions. These AI agents can analyze the health condition of patients, without exposing the private data. The data set exposed to the AI agent can be negotiated or selected by the user. The access can be granted temporarily to a verified public AI agents. To incentivize the patient to share the personal data, the AI agent will pay the patient for the shared data. In order to be self-sustainable, an AI agent can sell the output data to independent researchers, can mint digital currency and can buy patients' data.

Enhanced Security. The entities involved in the communication will exchange data through the encryption and privacy enhancement layer. The anonymization introduced by the Blockchain is not sufficient to protect the patients' identity. This layer considers implementation of strong encryption in any information transaction and enhanced privacy protection tools, like TOR [24].

New Blockchain Types. The coordination of the procedures and execution of Smart contracts will be orchestrated by the Blockchain layer. Further analysis is required to

determine which type of Blockchain will suite the eHealth system the most. The eHealth system based on a permissionless Blockchain will build trust from the openness of the code and procedures in the system. Also this will encourage the community to develop the whole system even further by fixing the issues, building applications and support the system. Contrary to the permissionless Blockchain, the permissioned Blockchain is relatively limiting solution that can still rise concerns regarding the privacy of the system. The perfect solution will be a combination of the advantages of both types of Blockchains. Generally speaking, the interfacing between the two distinct types of Blockchains will be great starting position.

Scalability and Storage Solutions. For future-proof next generation healthcare digital system, we are looking forward for a Blockchain solution that will solve the major scalability issue related to the data storage capacity of the whole system. As potential data storage solutions for the eHealth system we are proposing the use of local storage, IPFS (Inter-Planetary File System), Blockchain sharding and Cloud data storage.

Due to heavy data load of images and videos in the healthcare systems, but also the huge amount of IoT devices that are collecting patients' data, an offload from the Blockchain must take place. The local storage will be used by the patients and healthcare practitioners, as a fast access data storage. The data storage limitations of IoT device will be solved by periodical data offload to a dedicated local storage of the patient. The current version of IPFS offers slow but reliable data access, therefore the IPFS will be used to obtain redundancy of the data. The local storage and IPFS storage is not sufficient to withhold the traffic that is transiting through the eHealth system. Because of that, Blockchain sharding will split the data streams and offload the main Blockchain from the intensive data exchange. Further, the eHealth system will have optional cloud storage used as a cold storage for the patient data or will be used for compatibility reasons with the current system designs.

New Internet Access. The bottom of the layered structure is referring to the 5G, Wi-Fi and other wired broadband technologies as a main network solutions to provide Internet access to the users. The current deployment of 5G network will offer high speed mobile Internet access for the patient and more significant is that this technology will enable the healthcare practitioners to have continuous real-time monitoring of the patient parameters, by the deployed IoT devices. The Wi-Fi networks and other wired broadband network technologies will enable not only the healthcare practitioners but also the family members with tool for constant monitoring and assisted living for elder people.

5 Future Work

The development of Blockchain pave the path for future communication solutions with high level of security and privacy for the end users. Beside the existing healthcare solutions that are complemented with Blockchain technology to provide better privacy protection, this paper offers framework for broader use of Blockchain as a main technology for orchestration the future eHealth systems. The main future task would be the definition of the protocols for interaction between the entities in the eHealth system

(patients, healthcare practitioners, governmental institutions, insurance companies, pharmaceutical companies and AI agents).

The most promising are the existing technologies, such as Ethereum (as permissionless technology) and Hyperledger (as permissioned technology). The performances analysis of the permissionless and the permissioned technologies, concerning the eHealth systems, will determine the platform for building the final solution. It must consider the existing IoT related Blockchain solutions as a starting point in definition of the interaction between the autonomous IoT devices in the eHealth system.

Future system solutions may focus on fragmented implementation of the proposed layered architecture. The first step will be to upgrade our current general purpose Smart contract on Ethereum platform and build an adapted Smart contract for an eHealth testbed. The current general purpose Smart contract offers write access management over the data, and it needs to be upgraded by procedures for read access management by implementation of encryption layer and plug-and-play functionalities for the IoT devices.

As a long-term imperative will be the implementation of the proposed forth generation eHealth system solution on a new Blockchain technology that will implement multi-dimensionality of the future Blockchains that natively solves the scalability issues, and provides high level of end-to-end security and privacy protection. The multi-dimensionality can be provided by sharding, clustering or offloading the data from the main Blockchain.

6 Conclusion

This paper proposes generic framework for the novel generation of eHealth systems based on the Blockchain technology. The reliability of the Blockchain technology is proven by the large amount of products that are already present on the market. The inherent liveness of the collected data and the persistence of the ledger-like Blockchain technology, makes it suitable for the eHealth systems. Foremost, the integration of the Blockchain technology in the eHealth systems will leverage the privacy of the patients while the implementation of the advanced cryptographic mechanisms will secure the overall communication and the data storage. We are foreseeing huge improvement in the usability and data management in the future eHealth systems. This will allow the immense health improvement of the population. The future work will be toward the definition of the system level functionalities and protocols, and building the future-proof eHealth system bottom up.

References

1. Karamachoski, J., Gavrilovska, L., Sefidanoski, A.: The fusion between Blockchain and IoT for healthcare systems. In: ETAI Conference, pp. 1–6 (2018)
2. Linn, L., Koo, M.: Blockchain for health data and its potential use in health IT and health care related research. In: ONC/NIST Use of Blockchain for Healthcare and Research Workshop, Gaithersburg, Maryland: USA. ONC/NIST (2016)

3. Schwerin, S., et al.: Medixain: Robust Blockchain Optimization Enabling Individual Medical Wallet Architecture (2017)
4. Ekblaw, A.C.: MedRec: blockchain for medical data access, permission management and trend analysis (2017)
5. Jesus, E.F., Chicarino, V.R., de Albuquerque, C.V., Rocha, A.A. de A.: A survey of how to use blockchain to secure internet of Things and the stalker attack. Secur. Commun. Netw. **2018** (2018). https://doi.org/10.1155/2018/9675050
6. Ouaddah, A., Abou Elkalam, A., Ait Ouahman, A.: FairAccess: a new Blockchain-based access control framework for the Internet of Things. Secur. Commun. Netw. **9**(18), 5943–5964 (2016). https://doi.org/10.1002/sec.1748
7. Bagchi, R.: Using blockchain technology and smart contracts for access management in IoT devices. Thesis, University of Helsinki (2017)
8. Dukkipati, C., Zhang, Y., Cheng, L.C.: Decentralized, blockchain based access control framework for the heterogeneous Internet of Things. In: Proceedings of the Third ACM Workshop on Attribute-Based Access Control, pp. 61–69 (2018). https://doi.org/10.1145/3180457.3180458
9. Liao, C.-F., Bao, S.-W., Cheng, C.-J., Chen, K.: On design issues and architectural styles for blockchain-driven IoT services. In: 2017 IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW), pp. 351–352 (2017). https://doi.org/10.1109/icce-china.2017.7991140
10. McConaghy, T., et al.: BigchainDB: a scalable blockchain database. White paper, BigChainDB (2016)
11. Yu, X.L., Xu, X., Liu, B.: EthDrive: a peer-to-peer data storage with provenance. CAiSE-Forum-DC, Germany (2017)
12. Shafagh, H., Burkhalter, L., Hithnawi, A., Duquennoy, S.: Towards blockchain-based auditable storage and sharing of IoT data. In: Proceedings of the 2017 on Cloud Computing Security Workshop, pp. 45–50 (2017). https://doi.org/10.1145/3140649.3140656
13. Vermesan, O., et al.: Internet of robotic things: converging sensing/actuating, hypoconnectivity, artificial intelligence and IoT Platforms (2017)
14. Dorri, A., Kanhere, S.S., Jurdak, R.: Towards an optimized blockchain for IoT. In: Proceedings of the Second International Conference on Internet-of-Things Design and Implementation, pp. 173–178 (2017). https://doi.org/10.1145/3054977.3055003
15. Sharma, P.K., Park, J.H.: Blockchain based hybrid network architecture for the smart city. Future Gener. Comput. Sys. **86**, 650–655 (2018). https://doi.org/10.1016/j.future.2018.04.060
16. Dustdar, S., Nastic, S., Scekic, O.: A novel vision of cyber-human smart city. In: 2016 Fourth IEEE Workshop on Hot Topics in Web Systems and Technologies (HotWeb), pp. 42–47 (2016). https://doi.org/10.1109/hotweb.2016.16
17. Zundel, K.M.: Telemedicine: history, applications, and impact on librarianship. Bull. Med. Libr. Assoc. **84**, 71 (1996)
18. Shirzadfar, H., Lotfi, F.: The evolution and transformation of telemedicine. Int. J. Biosens. Bioelectron. **3**(4), 303–306 (2017). https://doi.org/10.15406/ijbsbe.2017.03.00070
19. Chatterjee, P., Armentano, R.L.: Internet of Things for a smart and ubiquitous ehealth system. In: 2015 International Conference on Computational Intelligence and Communication Networks (CICN), pp. 903–907 (2015). https://doi.org/10.1109/cicn.2015.178
20. Ida, I.B., Jemai, A., Loukil, A.: A survey on security of IoT in the context of eHealth and clouds. In: 2016 11th International International Design and Test Symposium (IDT), pp. 25–30 (2016). https://doi.org/10.1109/idt.2016.7843009
21. Medicalchain Whitepaper 2.1. https://medicalchain.com/Medicalchain-Whitepaper-EN.pdf

22. Da Conceição, A.F., da Silva, F.S.C., Rocha, V., Locoro, A., Barguil, J.M.: Eletronic Health records using blockchain technology. arXiv preprint, arXiv:1804.10078 (2018)
23. McFarlane, C., Beer, M., Brown, J., Prendergast, N.: Patientory: A Healthcare Peer-to-Peer EMR Storage Network v1 (2017)
24. Syverson, P., Dingledine, R., Mathewson, N.: Tor: the second generation onion router. Usenix Security (2004)