Blockchain-based model for authentication, authorization, and immutability of healthcare data in the referrals process

1st Goce Gavrilov
University American Colledge Skopje
School of Computer Science and Information Technology
Skopje, Macedonia
gavrilovgoce@yahoo.com

2nd Orce Simov
International Slavic University
"Gavrilo Romanovich Derzhavin"
Faculty of Computer Science
Sv. Nikole, Macedonia
osimov@yahoo.com

3rd Vladimir Trajkovik
University "Ss. Cyril and Methodus"
Faculty of Computer Science and Engineering
Skopje, Macedonia
trvlado@finki.ukim.mk

Abstract— The healthcare industry is continuously reforming and adopting innovative technologies that allow the digitalization of health information and automation of clinical processes. Some of the crucial requirements in these adaptations and implementations are interoperability across different departments and the security of a patient's sensitive data, mainly when data exchange.
The provisioning of confidentiality, integrity, consistency of data and data quality management is vital to ensure the best healthcare service delivery. The blockchain technology is a revolutionary invention, which ensures data integrity and confidentiality inside any system. The blockchain technology with application layers built on it, promise a mechanism that provides data integrity and privacy, most privacy, and security in healthcare services. In this paper, we propose an e-referrals model with the main focus on supporting authentication and authorization of entities in the process of issuing referrals to provide data integrity and confidentiality. The proposed model offers a framework for managing patients' referral data between doctors on the primary, secondary, and tertiary levels of healthcare.

Keywords— blockchain, authentication, authorization, e-referral, healthcare

I. INTRODUCTION

Today, citizens' health care is of prime importance in most world countries, as the number of patients and diseases continues to increase. Maintaining health records for every patient is a necessity for managing future health needs for citizens. Computer-aided medical support terms, such as e-Health, e-health record, e-referrals, e-scheduling, and e-prescription have appeared as a result of the evolution of information and communication technologies (ICT).
The existence of diverse health devices and apps with a combinations of the Internet of Things (IoT) have contributed to transfer of a large amount of medical data daily. Access and sharing patient's data before, during and after the treatment process are every day needs of doctors and other healthcare staff [1]. This extensive connected but distributes database of citizens' health information creates significant privacy, security, and availability issues.
Electronic availability of these data online makes it easier for hackers and other malicious attackers to access this confidential information. Also, the openness of patient's data via the internet, exposes this information to more hostile attacks compared to the paper-based records [2].

Referrals represent the link and interface between healthcare providers in primary and secondary healthcare [3]. According to [4], [5], [6], the referral process is defined as transferring (including data sharing) of responsibility of patient healthcare from referral provider to another physician or provider. This transfer of patient healthcare should be reversed back in an appropriate time. Consequently, linking healthcare service levels is essential.
Paper-based referrals sending by fax, still the standard process in many practices, creates referral delays due to incomplete or missing information such as patient data, clinical laboratories, etc [7]. Paper-based referral processes can lead to inadequate information exchange, lost or misplaced paper records, as well as medication errors resulting from illegible handwriting with limited standardization [8].

E-referral is an electronically transmitted message such as XML documents or PDF documents that can be received and viewed by the reviewer [9], [10]. According to that, e-referrals represent a new mechanism for the integration of the different levels of health care [11]. E-referrals allude to the automation of the referral process in which appointments and other information regarding the consultation and review are transferred between two or more healthcare providers. E-referral systems have been designed to improve wait times and efficiency by electronically standardizing information and communication within the referral process.

Healthcare data are highly sensitive data, and the process of their sharing or transferring them from one institution to another (from primary healthcare to secondary, secondary to tertiary or horizontally between clinics on the same level of healthcare) has always had privacy and confidentiality concerns [12]. According to EU legislation, [13] a patient has to provide consent when someone wants to access his/her data. The law enforcement and other specific public agencies may legally access health information, according to the Health Insurance Portability and Accountability Act [14]. Medical referrals are transmitted between primary and secondary, secondary, and tertiary healthcare institutions or horizontally between clinics on the same level of healthcare daily. Medical referrals are subject to potential attacks from unauthorized persons.

The referrals are prone to attack by intruders and may be intercepted, modified, or fabricated. Even if data are safely shared between different doctors the integrity of health records [15] remains a significant issue. Data privacy [16] is also under threat, and health and medical data are prone to safety crises. Due to the sensitivity of the information contained in the referrals, especially the medical findings and doctors' opinion, the possibility of intercepting this information is a risk that should not be ignored.

Because of heavy regulation and bureaucratic inefficiency, the e-referral system's innovation is not on a high-speed line. At the same time, many healthcare facilities have a critical need for such new innovation, especially in the area of data privacy and security [17]. According to findings presented in [17], the patient's data contains data that is highly valued to cybercriminals. Healthcare facilities must introduce new security measures to address these threats or be subject to the all-out of failure to do so. Blockchain technology represents a useful mechanism for securing and protecting vulnerable patient data. The application of blockchain in the healthcare area represents an important challenge for solving privacy and security concerns [18]. Blockchain technology has the potential to address the interoperability challenges [19] in healthcare information systems and to be the technical standard that enables healthcare entities to share electronic health data securely.

The main goal of this paper is to propose a framework model for e-referrals that can be used by doctors, patients and different entities involved in e- referral processes. Our solution solves privacy, security, availability, data integrity and confidentiality problems, and access control over e-referral data. The remainder of the paper is organizing as follows. Section 2 highlights the literature review and work related to the blockchain and healthcare system. Section 3 presents the model for the e-referral blockchain system. We discuss the proposed system model and future plans in section 4 and conclude the paper in section 5.

II. LITERATURE REVIEW - BLOCKCHAIN IN HEALTHCARE

When we are trying to research and review available literature concerning blockchain in an e-referrals information system or general in healthcare, it is crucial to understand the context of blockchain technology and the proposition her usage as a means for providing patient's data security mechanism. To do this, first, we need to give a brief description of blockchain technology and then analyze the previous work in an academic environment in a relationship with the use of blockchain to address privacy and security concerns in healthcare.

The blockchain is one of the most often used phrases of the last couple of years, so that Gartner has suggested that blockchain would reach the peak of inflated expectations very soon [20]. The idea of utilization of blockchain in healthcare comes out of the need for security and interoperability in healthcare. The existence of diverse health devices and apps with a combinations of the Internet of Things (IoT) have contributed to a transfer of a large amount of medical data daily. This data traffic and exchange need management regarding privacy and security. Blockchain technology can offer a solution that not only helps to securely store and sharing of medical and healthcare data but also to assure the confidentiality of each patient's data by giving the patients, as well as their medical and health data ownership [17]. Blockchain technology can redefined the data modeling and governance deployed in many healthcare applications. This is mainly due to its adaptability and ability to segment, secure, and exchange medical data and services in an unprecedented way. Many current development projects in healthcare have blockchain technology in the center of their development [21].

With the progress in electronic health and medical-related data, data store in healthcare cloud, the promotion of regulations for patient data privacy protection, new opportunities are appearing for health data management, as well as patients' convenience to access and share their health's data [22].

The blockchain is a distributed ledger technology based on the principles of a peer-to-peer network and cryptographic notions (such as hash, asymmetric encryption, and digital signature). Blockchain, as a concept of a distributed database, was for the first time described by Nakamoto in 2008 [23]. This technology provides a transparent, decentralized, authenticated platform that applies a consensus-driven approach to facilitate the interactions of multiple entities in the network through the use of a shared ledger.

The blockchain technology consists of blocks, with each block representing a set of transactions. Like a structure of data [24], a blockchain has several significant properties described below. First, blocks are provably immutable - this means each block contains a hash, or numeric digest of its content, that verifies the integrity of the containing transactions. The hash of the next block in the blockchain network is dependent on the hash of the current block, the hash of the current block is dependent on the hash of the previous block. This effectively makes the entire blockchain history immutable, as changing the hash of any block "n – i" would also change the hash of block n [25]. The functioning blockchain does not depend on a central, trusted authority, rather than, the responsibility of functioning is distributed to all nodes which participate in the network. Because is missing central authority that will verify the validity of the blockchain, a mechanism for reaching network consensus must be employed [26]. The concept of decentralized trusted authority comes as an opposite solution to almost every system that was built using the client-server architecture. Removing the central trusted authority outside of the system means there is no longer a mediator processing the actions and the data.

Several techniques used to ensure network consensus are Proof of Work function in Bitcoin [23], Proof of Stake [27], and Proof of Activity [28]. Firstly, Blockchain technology was originally designed for the financial sector, and it has the potential to change the healthcare system for the better. By providing a mechanism for the controlled exchange of sensitive data for healthcare professionals, blockchain technology can improve the transparency and data sharing between clinical and research data systems [29].

Current identity tools and mechanisms do not support this modern approach to authentication and authorization. Instead of checking on physical identity documents, the processes, and methods that are required expensive and tedious counter visits, they must change to the direction on simplifying the checks but, at the same time, maintaining the level of security with using new technology like the blockchain.

There are a lot of different approaches in the literature for supporting healthcare authentication. Trust management is tied to authentication mechanisms as the means to identify the trustee. Recent work from Zyskind et al. [30] shows the interest of blockchain technology as a personal data management platform focused on privacy. According to Zyskind et al. [30], the blockchain helps to leverage user control over data in the context of social networks and big

data. Blockchain technology may offer a way to bypass the problem of the central government body of identity control by delivering a secure solution without the need for a trusted, central authority. Blockchain-based identity authentication is particularly salient in the last few years of internet penetration.

III. SYSTEM DESIGN FOR E-REFERRAL

For the implementation of blockchain technology in the healthcare system, especially in the e-referrals process, we have first to understand how blockchain ledger works under the hood. Blockchain technology owns a built-in identity mechanism, a cryptographically secure key pair. So each participant with a specific activity on the network is assigned these keys. All participants knew each other by these keys because the original identities of participants in the network are not visible [31].

The smart contract plays a vital role in performing the agreement among various stakeholders involved in the system when implementing the blockchain in the e-referrals system. By developing the codes can be created a smart contract and these codes define the agreement signed by the various stakeholders such as a patient, doctor, or physician. A smart contract is an integral and inseparable part of the blockchain-based applications. A smart contract represents a computer protocol that follows specific rules, codes and constraints agreed by all participants in the network. It is an agreement made among various involved stakeholders in the defined system. The referrals data can be encrypted and shared with the whole ledger available within the respective network.

To implement the e-referral system in our case, we propose decentralized identity management built on top of an Ethereum (or multi-block) consortium network. Our proposed identity management system is using the decentralized smart-contract standard that defines the method for ownership and transferability of the referrals. With these features are enabled:

- Eliminate the possibility of the existence of counterfeit referrals
- Enable regulatory insight into the number of issued and realized references for every citizen
- Enable regulatory insight into the number of unfulfilled referrals for every citizen
- Enable regulatory insight into the number of specialist reports, findings, assessments and opinions
- Create an immutable record for issued referrals, specialist reports, findings, assessments, and opinions

The patient referral process workflow starts when a patient is registered to receive health services, and medical personnel determines the diagnosis of the patient. Referral form has to complete with the name of the referred healthcare facility and other required information when the patient needs to be referred to. There are two types of referrals which be issued, an emergency referral and an outpatient referral. Depending on the referral type, the patient will be served in the designated healthcare facility by either emergency or outpatient measures. If a referral is returned, then the referred healthcare facilities have to fill in the referral form. After that, the referral's institution receives referral data.

Figure 1 represents a logical architecture of the proposed e-referral management system model. Application layer, a Database, and an authentication and authorization server are the main components of the proposed model. Authentication and authorization of the users, system make by validating transactions in the blockchain network. The user (the patient, doctor, physician) communicates with the system through the e-referral application. This e-referral application can be web, mobile, or a standalone application that interacts with the application server via integration services to perform the desired functions. For delivering a requested medical and health data, the application server needs to communicate with the database and the authentication server. To accomplish these activities, users must be authenticated and authorized.

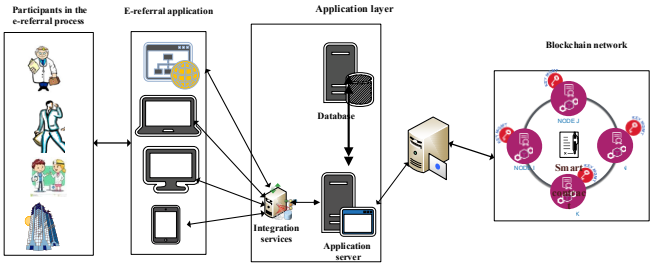

Fig. 1: Logical architecture of the e-referral system model

The application server assigns work to the authentication server to check the authenticity of the user and to authorize access to the database. A standalone or cloud-based database may be used [32], and it is used in the system to limit the amount of data in the blockchain as much as possible. After receiving a permission validation from the authentication server, access to the database from the application server is allowed. The authentication server has an intermediary role between the application server and the blockchain network. It authenticates and authorizes the user and able to interact with the blockchain network. The blockchain network records data operations and various data access requests for immutability and integrity protection. The nodes in the blockchain network keep the network in running state and maintain the ledger. Nodes follow the rules in the smart contract, validate and broadcast transactions and run the consensus protocol.

The patient first must registers in the trusted services offices by providing personal details (such as ID, Biometrics, and PIN), together with the public key of the patient. Also, to enable a referral needs the public key of the doctor. Since the registration process is a one-time process, patients provide their details using their mobile devices or web application.

The public key(s) of the doctor(s) responsible for referrals are added to the information file of the patient. The doctors together with their public keys, must be already registered in the trusted services. After the patient's registration process, the constructed information file about the patient will be sent to the blockchain. Next, the patient goes to the doctor to gets the needed referral. By using the mobile application on a mobile device, the patient generates ID and a secret key pair (private/public key pair) to authenticate him/herself. After that, if the doctor wants to issue referral/s, he/she will send a request to the blockchain network using his/her key material. Upon receiving the referral request by the blockchain network, it will check the validity of the doctor and whether the patient has granted the update permission to that

particular doctor. If the check is successful, it performs the referral issuing operation. When filling the data for specialist reports, findings, assessments and opinions, similar kind of steps are taken.

Figure 2 shows the steps of healthcare data management workflow in blockchain.

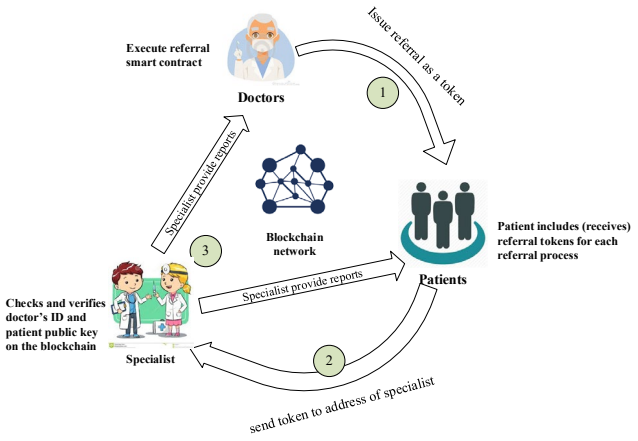

Fig. 2: E-referral process with blockchain

Three leading roles of participants are mainly existing in our proposed system:

1. Primary healthcare doctor - Issues referrals by executing a smart contract that tokenizes a valid prescription. During the process of issuing referrals are used metadata such as doctor's ID, patient's ID, quantity, healthcare institution where the patient is referred, the type of review to be performed, physician (see Figure 2).
2. Patient - Receives a token representing a valid referral prescribed by a doctor. The patient receives the necessary health service at an authorized healthcare facility by sending token to the facility's public wallet (responsible for storing the users' private and public cryptographic keys).
3. Specialist (doctor on the next level of healthcare) - After receiving a token from a patient, the doctor makes the necessary examinations and filled the specialist reports, findings, assessments and opinions, prescribe medication, etc. After these actions specialist sends information to the doctor and patient. Specialist checks and verifies a valid referral by checking the permission blockchain for a signature between the patient and doctor.

Healthcare authorities with read-only access to the ledger may be considered to be a "fourth role".

IV. DISCUSSION AND FUTURE WORK

The rapid developments in Information Communication Technology (ICT) causes increased digitalization in the healthcare sector. One of the top priorities in the healthcare sector is to provide safer manners of accessing the patients' health and medical information throughout the whole process of referrals process. Blockchain technology assumed to be among one of the suitable ways of authentication, authorization, and sharing the health and medical information. The potential of blockchain in the e-referrals process is being realized by many involved stakeholders (patients, doctors, physicians, healthcare management staff) and its immense impact on improving the healthcare interoperability and collaboration and enhanced healthcare economy and revenues.

One of the vital on-going obstacles in the current e-referrals systems is the lack of a mechanism for authentication and authorization, and blockchain offers the possibility to handle this issue. The blockchain's future in healthcare sector seems to be quite pronounced and visionary. However, the practicality of the healthcare applications and especially application for e-referral using blockchain is mostly untested yet. From these reasons, the future development includes implementation a functional prototype of the proposed architecture, shown in Section 3. A proposed system model is based on an open-source community blockchain framework called Hyperledger Fabric. It is also permitted instead of using Hyperledger Fabric, to use other cloud-based blockchain services. Future work includes implementation and testing of the proposed system in a closed environment, development of most of the components of the system, connection with some outsourced components, demonstration of the up-scaling of the system and goes to real implementation.

V. CONCLUSION

Blockchain technology in healthcare information systems has brought immense opportunities in terms of not only providing secure and efficient data storage but also sharing and control access to the data. System model for identity and access management in the e-referrals process using blockchain technology are prposed in our paper. The core focus in the paper is pointed to the theoretical design of a secure and efficient data access mechanism for current referrals systems using the blockchain technology. We have also proposed the potential smart contract agreement considering this e-referrals scenario.

Blockchain implementation in the e-referrals system and in general in healthcare systems is a significant challenge in a rapidly evolving era of privacy and security concerns. With the progress in electronic health and interoperability, healthcare data store in the cloud and patient data privacy protection regulations, new opportunities are appearing for health data management, as well as patients' convenience to access and share their health data.

REFERENCES

[1] S. Alla, L. Soltanisehat, U. Tatar, and O. Keskin, "Blockchain Technology in Electronic Healthcare System", Proceedings of the 2018 IISE Annual Conference, In K. Barker, D. Berry, C. Rainwater, eds. ISBN: 978-1-5108-6935-6, 2018 May 19-22, pp.754-760.

[2] G. Gavrilov, O. Simov, and S. Manasov, "Blockchain technology for authentication, authorization and immutability of healthcare data in process of recipes prescriptions", **Scientific Journal «INTERNATIONAL DIALOGUE: EAST-WEST»** (ISSN print:1857-9299, ISSN online: 1857-9302), pp. 319-326, 2019

[3] A. Mehrotra, C.B. Forrest, and C.Y. Lin, "Dropping the baton: specialty referrals in the United States", Milbank Quarterly, vol. 89(1), pp.39-68, 2011.

[4] J. Warren, S. White, K.J Day, Y. Gu Y, and M. Pollock, "Introduction of electronic referral from community associated with more timely review by secondary services", Applied Clinical Informatics, vol. 2(4): pp. 546-564, 2011.

[5] A. Esquivel, "Characterizing, Assessing and Improving Healthcare Referral Communication", PhD Thesis, The University of Texas School of Health Information Sciences at Houston, 2008.

[6] T.M. Akande, "Referral system in Nigeria: study of a tertiary health facility", Annals of African Medicine, vol. 3, No. 3, pp. 130 – 133, 2004.

[7] C. Hughes, P. Allen, M. Bentley, “e-Referrals: why we are still faxing”, Aust Fam Physician, vol. 47(1–2), pp. 50–57, 2018.
[8] F.K. Thiong’o, “Framework for the Implementation of a Patient Electronic Referral System: Case Study of Nairobi Province”, MSc Thesis, University of Nairobi, School of Computing and Informatics Scientific 2011.
[9] L. Tian, “Improving knowledge management between primary and secondary healthcare: an e-referral project”, Health Care Inform Rev Online, vol. 15, pp. 31-37, 2011
[10] A. Coleman, “Developing an e-health framework through electronic healthcare readiness assessment”, PhD Thesis, Nelson Mandela Metropolitan University, 2010.
[11] A.H. Chen, E.J. Murphy, and H.F Jr Yee, “eReferral - A New Model for Integrated Care”, The New England Journal of Medicine, vol. 368(26), pp. 2450-2453, 2013 Jun 27.
[13] G. Gavrilov, E. Vlahu-Gjorgievska, and V. Trajkovik, “Healthcare data warehouse system supporting cross-border interoperability”, Health Informatics Journal, pp. 1-12, https://doi.org/10.1177/1460458219876793, 2019.
[13] GDPR, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
[14] M.L. Johns, “HIPAA privacy and security: A practical course of action”, Topics in Health Information Management, vol. 22(4), pp. 40-48, 2002.
[15] M. Herlihy, M. Moir, “Enhancing accountability and trust in distributed ledgers. arXiv preprint arXiv:1606.07490, 2016.
[16] J. Zou, Y. Wang, M.A Orgun, “A dispute arbitration protocol based on a peer-to-peer service contract management scheme”, In: 2016 IEEE international conference on web services (ICWS). IEEE, June 2016, pp. 41–48.
[17] K. Peterson, R. Deeduvanu, P. Kanjamala, and K. Boles, “A Blockchain-Based Approach to Health Information Exchange Networks”, Available at: https://www.healthit.gov/sites/default/files/12-55-blockchain-based-approach-final.pdf [Accessed January 25, 2020].
[18] K.J. Smith, G. Dhilon, “Blockchain for Digital Crime Prevention: The Case of Health Informatics”, Blockchain for Digital Crime Prevention: Health Informatics, *Twenty-third Americas Conference on Information Systems, Boston, 2017.*
[19] N. Mountford, K. Threase, M. Quinlan, R. Maher, R. Smolders, P. Van Royen, I. Todorovic et al. “Connected Health in Europe: Where are we today?”, University College Dublin, 2016.
[20] Gartner (2016). “Hype Cycle for Emerging Technologies”, Stamford, CT, USA: The Gartner Group. Available at: http://www.gartner.com/newsroom/id/3412017. [Accessed January 2, 2020].
[21] S. Khezr, M. D. Moniruzzaman, A. Yassine, and R. Benlamri. “Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research”, *Appl. Sci.,* vol. *9*, pp. 1736-1764, 2019, https://doi.org/10.3390/app9091736.
[22] D. V. Dimitrov, “Blockchain Applications for Healthcare Data Management”, Healthc. Inform. Res., vol. 25, pp. 51–56, 2019.
[23] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system”, Available from: https://bitcoin.org/bitcoin.pdf. [Accessed January 12, 2020].
[24] B. Singhal, G. Dhameja, and P. S. Panda, “Beginning Blockchain: A Beginner’s Guide to Building Blockchain Solutions”, ISBN-13 (pbk): 978-1-4842-3443-3. ISBN-13 (electronic): 978-1-4842-3444-0. https://doi.org/10.1007/978-1-4842-3444-0, Apress.
[25] E. Karafiloski, “Blockchain Solutions for Big Data Challenges- A literature review”, IEEE EUROCON 2017, 6–8 JULY 2017, OHRID, R. MACEDONIA, 978-1-5090-3843-5/17/$31.00 ©2017 IEEE.
[26] G. Zyskind, O. Nathan, A.S. Pentland, “Decentralizing Privacy: Using Blockchain to Protect Personal Data”, 2015 IEEE CS Security and Privacy Workshops. DOI 10.1109/SPW, 2015, pp. 180-185.
[27] S. King and S. Nadal, “PPCoin: Peer-to-peer crypto-currency with proof-of-stake”, Self-Published Paper, August, 19, 2012.
[28] I. Bentov, C. Lee, A. Mizrahi and M. Rosenfeld, “Proof of activity: Extending bitcoin's proof of work via proof of stake”, ACM SIGMETRICS Performance Evaluation Review, vol. 42(3), pp. 34-37, 2014.
[29] A.C. Marek, “Blockchain as a Foundation for Sharing Healthcare Data”, *Blockchain in Healthcare Today*™ ISSN 2573-8240 online https://doi.org/10.30953/bhty.v1.13. [Accessed February 12, 2020].
[30] G. Zyskind, O. Nathan, and A.S. Pentland, “Decentralizing privacy: Using blockchain to protect personal data”, Proceedings - 2015 IEEE Security and Privacy Workshops, SPW 2015, pp. 180–184.
[31] Blockchain in Healthcare. Available: https://www.hyperledger.org/wpcontent/uploads/2016/10/ey-blockchain-in-health.pdf. [Accessed January 10 2010].
[32] A. Dimitrievski, E. Zdravevski, P. Lameski, and V. Trajkovik, “Addressing Privacy and Security in Connected Health with Fog Computing”, In Proceedings of the 5th EAI International Conference on Smart Objects and Technologies for Social Good (GoodTechs '19). Association for Computing Machinery, New York, NY, USA, pp. 255–260. DOI: https://doi.org/10.1145/3342428.3342654