IMPLEMENTATION OF FOG COMPUTING IN IOT-BASED HEALTHCARE SYSTEM

Mirjana Maksimović

Faculty of Electrical Engineering, University of East Sarajevo, BH, mirjana@etf.unssa.rs.ba

A general survay

DOI: **10.7251/JIT1702100M**

UDC: **004.78:004.35**

Abstract: INowhere do the technology advancements bring improvements than in the healthcare sector, constantly creating new healthcare applications and systems which completely revolutionize the healthcare domain. The appearance of Internet of Things (IoT) based healthcare systems has immensely improved quality and delivery of care, and significantly reduced the costs. At the same time, these systems generate the enormous amount of health-associated data which has to be properly gathered, analyzed and shared. The smart devices, as the components of IoT-driven healthcare systems, are not able to deal with IoT-produced data, neither data posting to the Cloud is the appropriate solution. To overcome smart devices' and Cloud's limitations the new paradigm, known as Fog computing, has appeared, where an additional layer processes the data and sends the results to the Cloud. Despite numerous benefits Fog computing brings into IoT-based environments, the privacy and security issues remain the main challenge for its implementation. The reasons for integrating the IoT-based healthcare system and Fog computing, benefits and challenges, as well as the proposition of simple low-cost system are presented in this paper.

Keywords: Fog computing, Cloud computing, healthcare, Raspberry Pi.

INTRODUCTION

The explosion of advances in Information and Communication Technologies (ICTs) has completely revolutionized the healthcare sector. The evolution of the Internet of Things (IoT) defined as an ecosystem of smart devices in which applications and services are driven by sensed, collected and exchanged information between devices, as well as with the environment, with or without human intervention, makes it highly prominent in the healthcare sector. The incorporation of the IoT into healthcare sector contributes to immense improvements in healthcare by radically changing the way of healthcare delivery, driving better outcomes, increasing efficiency, and making healthcare affordable, acceptable, and available to anyone and anywhere at any time [31].

The IoT-based healthcare system appears as an adequate approach to ensure the appropriate (effective and proactive) healthcare delivery based on parameters monitoring and useful medical knowledge obtained on the gathered and analyzed health-related data [9, 19]. Its omnipresence in peoples' lives has resulted in the increasing number of diverse, smart medical devices and sensors, which more than ever before generate and transmit data. On a daily basis, these devices and sensors generate a prodigious amount of health-related data. There are estimates that healthcare data produced by IoT-based systems will be 25000 petabytes in 2020 [14]. Managing this data, collecting, analyzing, interpreting, and sharing is quite challenging.

Putting escalating volumes of rapidly growing, and mostly unstructured health-associated data to the Cloud and transmitting response data back requires a larger bandwidth, a considerable amount of time and can suffer from latency issues. This is not

tolerable in time-sensitive and emergency response applications, such as healthcare. Scientific efforts to deal with these challenges have resulted in the realization of Fog computing vision. Fog computing creates an additional layer of computing power between the devices and the Cloud. Fog infrastructure enables splitting big data to sub data, and managing smaller and time-sensitive data at miniature data analysis centers. In this way, decentralized and intelligent processing closer to where the data originates, without the need to send every piece of information to the Cloud, is realized, what frees up time and storage space in the Cloud [7]. This approach is far better when dealing with the requirements of IoT communication framework in healthcare applications.

This paper represents a study of the importance, opportunities, benefits and challenges of Fog computing and the IoT-based healthcare system integration. The rest of the paper is structured as follows: the fundamentals of IoT-based healthcare systems are discussed in the second section, while the third section emphasizes the main principles of Fog computing as well as the justification of its implementation in an IoT-driven healthcare system. The way of creating a simple IoT-powered, low-cost healthcare system based on Fog computing principles is proposed in the fourth section, while section five discusses privacy and security issues in Fog computing paradigm. The last section contains concluding remarks.

The IoT-based healthcare system

The proliferation and widespread adoption of new technologies, particularly IoT and smart devices, have created new ways of healthcare delivery, thus improving human health and well-being. The powering healthcare systems with the IoT vision lead to numerous advantages, such as the availability and accessibility, an ability to provide a more "personalized" system, and high-quality cost-effective healthcare [21]. Hence, IoT is considered as promising solutions for the healthcare sector, since it places the patient in the center of the treatment process, enables self-managing their own disease, gives health professionals faster and secure access to all information they need to care for the patient, enables remote care and assistance through associated networked-monitoring equipment [2].

To realize the IoT-based healthcare system, following elements are essential: a variety of sensors (consumer-based, wearable devices, internally embedded devices and stationary devices), microcontrollers, microprocessors, healthcare-specific gateways and the Cloud [25]. In other words, there is a three-layer architecture of IoT-powered healthcare system that consists of:

- Sensing/perception layer which main functions are sensing and collecting data as well as some communications and controlling actions.
- Network layer which is responsible for communication, connectivity, routing, etc.
- Application layer made of functional modules for application systems and users. At this level the sensed and collected data is being used for analysis, computations, visualizations, etc.

In other words, the IoT-driven e-health solution enables [21]:

- Sensing and collecting patient health-related data from a diversity of sensors in remote, secure, and safe manners.
- The appliance of a variety of data mining techniques and algorithms in order to discover hidden patterns and detect any anomalies, and based on obtained valuable knowledge make predictions and actionable decisions.
- Sharing the data through wireless connectivity with those who can make adequate and timely feedback.

An increasing number of smart medical devices and sensors used in IoT-driven healthcare vision implies the fast generation of large amounts of diverse data. In order to successfully deal with growing amounts of great variety of data and high speed of data generation and processing it is necessary to deal with technical and security issues [16]. From the technical perspective, the sensor and smart devices used in IoT-driven healthcare system for monitoring patients' current healthcare status have limited computation and storage capabilities, and hence they are not able to deal with the large amount of fast generated diverse medical data [2]. Posting these data to the Cloud for processing and storage and transmitting response data back also is not the right solutions, because it requires a larger bandwidth, a considerable amount of time and can suf-

fer from latency issues. Regarding privacy and security issues, all data related to a patient's health and medical history are especially sensitive and need to be protected in the appropriate way [21]. Having in mind the estimations regarding an astonishing number of IoT smart devices that will be in operation in the following period and expected data traffic [8], as well as security and privacy requirements, it is obvious that Cloud is not capable of dealing with these challenges. The solution for faster computing and connectivity is seen in the realization of an additional layer, which will be placed between end devices and Cloud (Fig. 1). This layer refers to Fog computing and based on its advantages has a potential to revolutionize various domains, especially time sensitive such as healthcare.

However, Fog infrastructure will show its full potential only by successfully overcoming numerous challenges for its implementation [11].

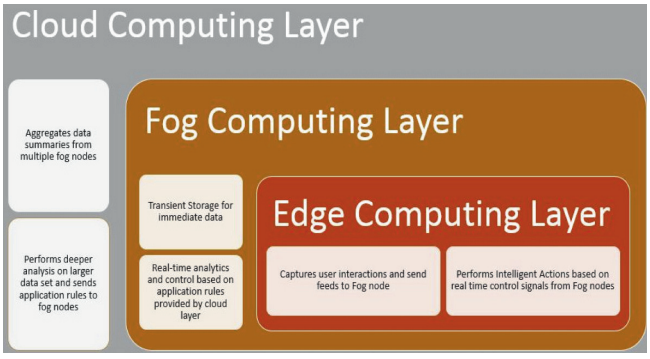

Figure 1. *The role of computing layers in an IoT system [12]*

FOG COMPUTING IN IOT-BASED HEALTHCARE SYSTEM

Fog computing is a novel trend in computing established by Cisco [5] that extends the Cloud computing paradigm at the edge of the network, processing data near data source (Fig. 1). Enabling data analytics and knowledge generation to occur at the data source, Fog computing significantly decreases the data volume that must be moved between end devices and Cloud [22].

While in Cloud computing, data and applications are processed in Cloud, which is a time-consuming task for voluminous data, Fog computing operating on the edge of network consume considerably less time. Furthermore, sending the large quantities of high-velocity and high-variety of IoT-generated data to the Cloud creates problems regarding bandwidth issues. High latency and scalability problems caused by servers' remote locations are additional drawbacks of Cloud computing [4]. The main differences between Fog and Cloud computing are presented in Table 1.

However, it is necessary to keep in mind that Fog computing is not a replacement for Cloud computing. Instead, Fog computing is the solution to Cloud's limitations. Reducing amounts of data and its movement across the network, and performing processing at the edge of the network, Fog infrastructure reduces congestion, eliminates bottlenecks, and enhances security [27].

These benefits make the Fog computing far more beneficial for many applications as compared to the Cloud, especially for [6, 17, 23]:

- Applications that require very low and predictable latency like health-monitoring and various emergency response applications;
- Geographically distributed sensor/actuator networks - applications in which thousands or millions of things across a large geographic area are generating data (e.g. smart cities, environmental monitoring);
- Fast mobile applications such as smart connected vehicle or connected rail; and
- Large-scale distributed control systems (e.g. smart grid).

The IoT applications which generate large volumes of data, produced by diverse IoT devices and generated at high speed, especially benefit from Fog computing. In IoT-powered healthcare applications, real-time processing and event response are crucial. Fog computing enables real-time and online analytic even when connectivity is poor or lost with the Cloud, and implies less congestion and faster real-time interaction and optimizations for IoT devices what makes it perfect for utilization in IoT-based healthcare systems. With supported heterogeneity, improved interoperability, and enhanced privacy issues, IoT-based healthcare system using Fog computing has potential to become reliable, simpler, scalable, and exceptionally high performance than ever before.

Table 1. *Fog computing vs. Cloud computing [4, 15]*

Requirement	Fog computing	Cloud computing
Hardware	Limited storage/ compute resources	Scalable storage/ compute resources
Data storage	Temporary	Permanent
Latency	Low	High
Delay jitter	Very Low	High
Bandwidth	Low	High
Response time	Seconds to minute	Minutes, days or weeks
Location of server nodes	At the edge of local network	Within the Internet
Distance between client and server	One hop	Multiple hops
Security	Can be defined	Undefined
Attack on data *enroute*	Very low probability	High probability
Location awareness	Yes	No
Geo-distribution	Distributed	Centralized
Number of server nodes	Very large	Few
Support for Mobility	Supported	Limited
Flexibility	High	Limited
Agility	High	Limited
Type of last mile connectivity	Wireless	Leased line

The major benefits of IoT-powered healthcare system where Fog computing principles are implemented can be summarized as follows:

- Enhanced quality of care based on accurate and on-time diagnoses and treatments, and decreased incidence of medical mistakes.
- Convenient, efficient, patient-tailored, and cost-effective healthcare delivery accompanied with more satisfied patients' and healthcare providers' experience.
- Improved preventive care and monitoring and treatments of rural residents' health conditions through online healthcare services.
- Saving time and reducing costs together with improved efficiency and coordination.

The development of a simple, low-cost IoT-based healthcare system using Fog computing

The success of Fog computing is based on the implemented Fog devices that must be capable to perform successful processing at the very early stage. In other words, Fog devices must be able to deal successfully with fast generated voluminous data, and to filter and transmit the important data to the Cloud. There is a variety of Fog nodes, with various hardware and software capabilities. In order to present the creation of a simple, low-cost IoT-based healthcare system that uses Fog computing (Fig. 2), the Raspberry Pi (RPi) is chosen as a key building element based on its performances: small, cheap, powerful, and fully customizable. RPi is a programmable small computer board, which has built-in support for a large number of input and output peripherals and network communication [19]. Some of its 26-pins GPIO (General Purpose Input and Output) port can be used as digital input/output signals and can be programmed directly on RPi through high-level programming languages (e.g. C++, Python, and Java.), while others can be used as interfaces for embedded protocols for controlling a set of electronic circuit (sensors, analog to digital converters (ADC), relay, status button, etc.). Hence, the GPIO port represents the main way of connecting RPi with other electronic boards as well as the communication link with other computing devices using a variety of different protocols, including Serial Peripheral Interface (SPI) and Inter-Integrated Circuit (I^2C) [19, 20]. To measure the patient's vital parameters, three sensors were chosen in the realization of custom IoT-based healthcare solution [20]:

- Temperature sensor (TTC05) – detection of body temperature and its changes;
- Heart rate sensor (Pulse sensor module) – detection of body's heart rate or pulse; and
- Blood pressure sensor (US9111) – used to detect blood pressure.

Electronic circuit scheme of Raspberry Pi as a sensing unit for measuring vital parameters and details about delivering measurement information complying IoT ideology is presented in previous works [19, 20].

However, compared to previous manners of realization, instead of sending all raw data to the Cloud, RPi can be used as a sink node (Fog node). Collected medical data (temperature, heart rate, and blood pressure) from the RPi (Fog node) are sent to the gateway (Fog server) for processing and storage. In other words, embedding some of the data mining techniques, fuzzy logic approaches or some other

type of artificial intelligence into the Fog server (e.g. laptop or PC), raw data can be processed intelligently and in real-time without sending it to the Cloud (Fig. 2). It is important to note that, based on its performances, RPi can also serve as a gateway.

In this way, computations are performed only where the data originates, instantly alerting health-care providers in a case of detected abnormal values and enabling faster real-time reaction. By implementing Fog infrastructure, there is no need to post large amounts of measured values of vital parameters to the Cloud because the most of the data processing is done at Fog layer. The aggregated results, in the sense of some kind of analysis over some period (e.g. historic and predictive analysis, machine learning, and virtualized data) can be sent to the Cloud for further processing, knowledge discovering, advanced decision making, and storage, whenever it is permitted by the network conditions. When the data is uploaded to the Cloud, the Fog storage is being released. Hence, Cloud computing layer aggregates data summaries from multiple Fog nodes/servers, performs deeper analysis and based on achieved insights performs rule and pattern updates at the Fog level.

SECURITY AND PRIVACY ISSUES IN FOG COMPUTING

The rapid development of IoT-based health-care systems is followed with the privacy and security risks. Since private data regarding health are especially sensitive, they must be protected in appropriate manners. The necessity of generation, processing, and sharing health-related data with the appropriate level of security and privacy is an important goal that must be accomplished. Therefore, the security and privacy issues of IoT-driven health-care systems must be threatened on many levels, with security and privacy framework and mechanisms built into the whole health-care ecosystem, from the device, to the network, to the data center, in order to fulfill following aspects of privacy and security [21, 24]:

- Confidentiality – the data is only available to authorized users,
- Data integrity – the data cannot be modified without detection,
- Accountability – the identification of the creator of an event or data is enabled,
- Availability of services, and
- Access control - the functionality and data are only available to authorized users.

Since Fog can be looked as an extension of the cloud, evidently some of the existing security and privacy challenges remain. However, because of Fog computing distinct characteristic (mobility support, location awareness, and low latency), it introduces novel security and privacy challenges, what may influence the Fog computing implementation into the IoT system. From the other side, the Fog computing could offer an ideal platform to deal successfully with many security and privacy issues in the IoT [32]. Fog computing potential to address security and privacy issues in IoT applications is as follows:

- Privacy – Fog nodes at the edge of network usually gather sensitive data generated by sensors and end devices, in health-care applications particularly. Fog computing enables the analyzing and processing data at the edge, and thus minimize the transmission of sensitive data to the Cloud, what contributes to the privacy preservation. Storing data in the Fog layer contributes to better protection of data. In order to protect data privacy, sensitive data

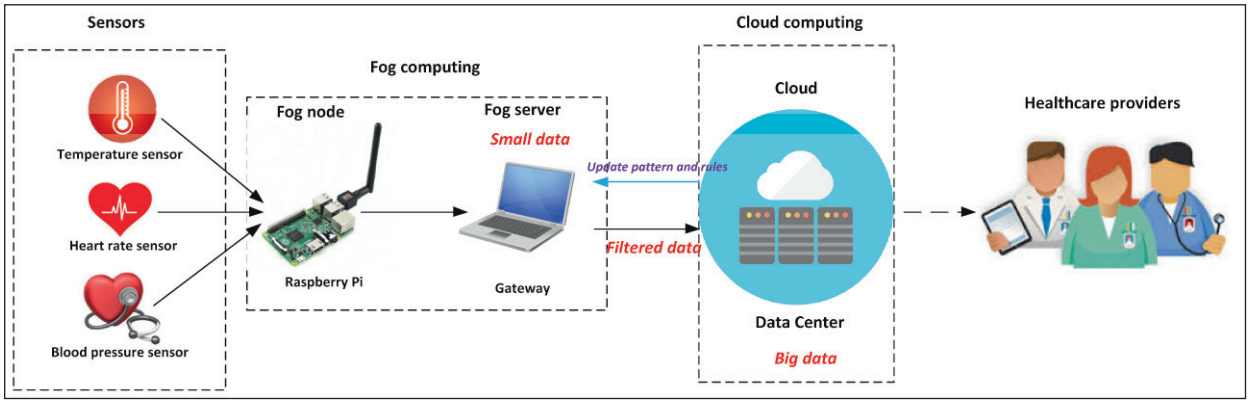

Figure 2. *Prototype of Fog-assisted and IoT-based health-care system architecture*

from end users have to be encrypted before outsourcing it to the Fog node [32]. There are various privacy-preserving techniques (e.g., differential privacy, homomorphic encryption) that can be applied between the Fog and the Cloud to preserve data privacy [1]. Among data privacy, usage privacy, and location privacy are also important challenges that must be considered and accomplished.

- Authentication – The Fog level holds the potential to enable authentication in IoT devices or appliance of light-weight encryption algorithms between Fog nodes and IoT devices to improve the authentication [1]. The authentication at different levels of Fog nodes is discussed in [29].
- Networking security – Fog nodes, deployed at the edge of network, bring numerous challenges regarding the network management. The solution for overcoming challenges related to the implementation and management, alongside increased network scalability and decreased costs can be found in the employment of SDN (Software Defined Networks). Authors of [32] discuss new challenges and opportunities connected to network security during appliance of SDN techniques in Fog computing: network monitoring and intrusion detection system, traffic isolation and prioritization, network resource access control, and network sharing. However, the Fog vision contributes to necessary security updates of IoT devices [1].
- Attack detection – Fog computing enables the improved detection of unusual behavior or malicious attacks, on both the IoT device and the Cloud sides [1]. Attack detection on the Fog node side can be performed by monitoring and analyzing log file, access control policies and user login data. In this way, Fog nodes are able to identify threats or attacks faster and mitigate them before they are passed through to the system [26]. At the Fog network side, malicious attacks such as denial-of-service (DoS), port scanning, etc. can be detected. Even Fog level holds the potential to monitor the security status of distributed systems in a scalable and trustworthy manner, it is very challenging to implement attack detection in geo-distributed, large-scale, high-mobility Fog computing environment and at the same time fulfill the low-latency requirement [32].
- Access control – Fog level facilitates the adoption of many standard access control models and creates an opportunity for designing new access control models [24]. A policy-based resource access control in Fog computing, to support secure collaboration and interoperability between heterogeneous resources is presented in [11]. However, the access control design spanning end user-Fog-Cloud, satisfying designing goals and resource constraints is challenging [32].

Despite the numerous benefits of Fog computing implementation in IoT systems, there are numerous challenges that must be considered. Even there are works that discuss privacy and security issues in Fog computing [1, 3, 11, 13, 18, 26, 28-30, 32], these aspects still can be considered as understudied. The development of novel security and privacy mechanism according to the Fog computing paradigm and their implementation will enable Fog computing vision to show its full potential in IoT systems.

Concluding remarks

The current IoT solutions, powered by an army of smart devices, cause dramatic changes in every aspect of our lives. Health-care sector did not remain immune to technology advancements. In contrary, the health-care field is seen as the domain where the IoT is able to show its full potential. IoT-driven health-care systems and applications lead to enhanced availability, accessibility, quality, and cost-effective health-care delivery. However, these systems pose numerous challenges regarding data exchange, interoperability, and availability of resources, security and privacy. In order to deal with these challenges, integration of Fog computing and IoT-based health-care systems, appears as the appropriate solution. Fog computing, as the result of a constant need for better, faster and more secure computing, with its features (low latency, low bandwidth, heterogeneity, interoperability, scalability, increased level of security and privacy, real-time processing and actions) is perfect for implementing into IoT-based health-care approaches. The Fog comput-

ing principles are demonstrated in proposed simple, low-cost IoT-based health-care system, where data receiving, sending, and manipulating is done in the localized environment. Applying technology based on IoT and Fog computing in proposed solution makes possible handling and overcoming existing challenges and constraints and significantly contributes to decreasing costs of health-care delivery.

Authorship statement

Author(s) confirms that the above named article is an original work, did not previously published or is currently under consideration for any other publication.

Conflicts of interest

We declare that we have no conflicts of interest

REFERENCES

[1] Alrawais A, Alhothaily A, Hu C and Cheng X (2017) Fog Computing for the Internet of Things: Security and Privacy Issues, IEEE Internet Computing, pp. 34-42.

[2] Andriopoulou F, Dagiuklas T and Orphanoudakis T (2017) Integrating IoT and Fog Computing for Healthcare Service Delivery, In: Keramidas, G., Voros, N., Hübner, M. (eds.) Components and Services for IoT Platforms, Springer International Publishing Switzerland

[3] Archana Lisbon A and Kavitha R (2017) A Study on Cloud and Fog Computing Security Issues and Solutions, International Journal of Innovative Research in Advanced Engineering (IJIRAE), Issue 03, Vol. 4, pp. 17-22.

[4] Augur H (2016) Is Fog computing the future of the Cloud?, Dataconomy, Available at: http://dataconomy.com/2016/03/fog-computing-future-cloud/. Accessed on September 1, 2017

[5] Bonomi F, Milito R., Zhu J and Addepalli S (2012) Fog computing and its role in the internet of things, in Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing (ACM, New York), pp. 13-16.

[6] Bonomi F, Milito R, Natarajan P and Zhu J (2014) Fog Computing: A Platform for Internet of Things and Analytics, Bessis, N., Dobre, C. (eds.), Big Data and Internet of Things: A Roadmap for Smart Environments, Studies in Computational Intelligence, Springer International Publishing Switzerland

[7] Bresnick J (n.d) How Fog Computing May Power the Healthcare Internet of Things, Healthanalytics. Available at: http://healthitanalytics.com/features/how-fog-computing-may-power-the-healthcare-internet-of-things. Accessed on May 16, 2017

[8] Cisco Visual Networking Index: Global mobile data traffic forecast update, 2016-2021 (2017). Available at: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html. Accessed on May 8, 2017

[9] Craciunescu R, Mihovska A, Mihaylov M, Kyriazakos S, Prasad R, and Halunga S (2015) Implementation of Fog Computing for Reliable EHealth Applications, 49th Asilomar Conference on Signals, Systems and Computers, pp. 459-463.

[10] Dastjerdi AV and Buyya R (2016) Fog Computing: Helping the Internet of Things Realize its Potential, Computer, pp.40-44.

[11] Dsouza C, Ahn GJ and Taguinod M (2014) Policy-driven security management for Fog computing: Preliminary framework and a case study. In: IRI. IEEE.

[12] Encash (2016) How Fog computing helps businesses fully encash IoT benefits, Available at: http://www.encash.org/2016/08/fog-computing.html. Accessed on August 14, 2017

[13] Fakeeh KA (2016) Privacy and Security Problems in Fog Computing, Communications on Applied Electronics (CAE), Vol. 4, No. 6, Foundation of Computer Science FCS, New York, USA.

[14] Feldman B, Martin EM, Skotnes T (2012) Big Data in Healthcare, Hype and Hope, Dr. Bonnie 360?,

[15] Firdhous M, Ghazali O and Hassan S (2014) Fog computing: will it be the future of cloud computing? in Proceedings of the 3rd International Conference on Informatics & Applications, Kuala Terengganu, pp. 8-15.

[16] Goyen M (2016) Big Data and Analytics in Healthcare, Vol. 16, Issue 1, Available at: https://healthmanagement.org/c/healthmanagement/issuearticle/big-data-and-analytics-in-healthcare. Accessed on May 26, 2017

[17] Joshi N (2016) Why is fog computing beneficial for IoT?, Available at: https://www.linkedin.com/pulse/why-fog-computing-beneficial-iot-naveen-joshi?articleId=8166335329880272527#comments-8166335329880272527&trk=sushi_topic_posts_guest. Accessed on June 8, 2017

[18] Lee K, Kim D, Ha D, Rajput, U. and Oh H (2015) On Security and Privacy Issues of Fog Computing supported Internet of Things Environment, 6th International Conference on the Network of the Future (NOF)

[19] Maksimovic M, Vujovic V and Perisic B (2015) A custom Internet of Things healthcare system, 10th Iberian Conference on Information Systems and Technologies (CISTI), pp. 653-658.

[20] Maksimovic M, Vujovic V and Perisic B (2016) Do It Yourself solution of Internet of Things Healthcare System: Measuring body parameters and environmental parameters affecting health, Journal of Information Systems Engineering &

Management, 1:1, pp. 25-39, Lectito BV, Netherlands.

[21] Maksimovic M and Vujovic V (2017) Internet of Things based e-health systems: ideas, expectations and concerns, In: Khan, S., Zomaya, A., Abbas, A. (eds.) Handbook of Large-Scale Distributed Computing in Smart Healthcare, Scalable Computing and Communications. Springer, Cham

[22] Munir A, Kansakar P and Khan SU (2017) IFCIoT: Integrated Fog Cloud IoT Architectural Paradigm for Future Internet of Things, IEEE Consumer Electronics Magazine

[23] Naranjo PGV, Shojafar M, Vaca-Cardenas L, Canali C, Lancellotti R and Baccarelli E (2016) Big Data Over SmartGrid - A Fog Computing Perspective, SOFTCOM 2016 Workshop, pp. 1-6.

[24] Neuhaus C, Polze A and Chowdhuryy MMR (2011) Survey on Healthcare IT Systems: Standards, Regulations and Security, Hasso-Plattner-Instituts für Softwaresystemtechnik an der Universität Potsdam.

[25] Niewolny D (2013) How the Internet of Things Is Revolutionizing Healthcare, Whitepaper, Freescale.

[26] OpenFog (2016) Top 5 ways Fog computing can make IoT more secure, 2016. Available at: https://www.openfogconsortium.org/top-5-ways-fog-computing-can-make-iot-more-secure/. Accessed on June 4, 2017

[27] Sabu N (2015) Fog computing technology, Available at: https://www.slideshare.net/NikhilSabu/fog-computing-technology. Accessed on April 28, 2017

[28] Stojmenovic I (2014) Fog computing: A cloud to the ground support for smart things and machine-to-machine networks, Australasian Telecommunication Networks and Applications Conference (ATNAC).

[29] Stojmenovic I and Wen S (2014) The fog computing paradigm: Scenarios and security issues. In: Federated Conference on Computer Science and Information Systems (FedCSIS), pp.1-8-

[30] Stojmenovic I, Wen S, Huang X and Luan H (2016) An overview of Fog computing and its security issues, Concurrency Computat.: Pract. Exper. 28:2991–3005.

[31] Venkatramanan P and Rathina I. (2014) Healthcare Leveraging Internet of Things to revolutionize Healthcare and Wellness, IT Services Business Solutions Consulting, Tata Consultancy Services Limited

[32] Yi S, Qin Z and Li Q (2015) Security and Privacy Issues of Fog Computing: A Survey, WASA.

Submitted: September 15, 2017.
Accepted: November 17, 2017.

About the Author

Mirjana Maksimovic is an assistant professor at Faculty of Electrical Engineering, University of East Sarajevo, Bosnia and Herzegovina. Her current research and teaching interests extend to a range of topics in Telecommunications, Computer Science, Automation and Electronics. She has published more than 70 papers in national and international journals and conferences.