A Custom Internet of Things Healthcare System

Mirjana Maksimović, Vladimir Vujović
Faculty of Electrical Engineering
University of East Sarajevo
East Sarajevo, Bosnia and Herzegovina
mirjana@etf.unssa.rs.ba, vladimir_vujovich@yahoo.com

Branko Perišić
Faculty of Technical Sciences
University of Novi Sad
Novi Sad, Serbia
perisic@uns.ac.rs

Abstract — **Health is the fundamental capability humans require to perceive, feel, and act effectively, and as such, it represents a primary element in the development of the individual, but also of the environment humans belongs to. That is why it is necessary to provide adequate ways and means to ensure the appropriate healthcare delivery based on parameters monitoring and direct providing of the medical assistance. The new technologies development and implementation, especially the Internet and Wireless Sensor Networks (WSNs) commonly known as the Internet of Things (IoT), enable global approach to the health care system infrastructure development. This leads to e-health system that, in real time manner, supplies a valuable set of information relevant to all of the stakeholders (patients, medical and paramedical stuff, and health insurance) regardless their current location. Commercial systems in this area usually do not meet the general patient needs, and those that do are usually economically unacceptable due to the high operational and development costs. In this paper, based on well-known low-cost technologies, there is a Do-It-Yourself (DIY) solution for a sustainable and adaptable patient oriented infrastructure development, presented.**

Keywords — Internet of Things; e-health; self-monitoring devices; Raspberry Pi;

I. INTRODUCTION

The ability of everyday devices to communicate with each other and/or with humans is becoming more prevalent and often is referred to as the Internet of Things (IoT). It is a highly dynamic and radically distributed networked system, composed of a very large number of smart objects [1]. Three main system-level characteristics of IoT [2] are:

- Anything communicates;
- Anything is identified; and
- Anything interacts.

The basic and most important smart object of IoT is a sensor node, or more precisely, Sensor Web (SW), which can be defined as a web of interconnected heterogeneous sensors that are interoperable, intelligent, dynamic, scalable and flexible. These smart objects are envisaged to provide smart metering, e-health logistics, building and home automation and many new uses not yet defined.

The human health today presents the primary focus of an increasing number of case studies and projects which goal is healthcare improvements and achieving the foundations for a global health system. Such systems should provide information to the patients and their doctors, regardless of the location where they are located [3]. This is known as e-health, and today is closely related to the Internet [4]. Including and applying IoT concepts to such defined global system, the possibility of its application for saving lives becomes unlimited [5].

Various e-health scenarios are enabled by rapid advancements in information and communications (IC) technologies and with the increasing number of smart things (portable devices and sensors). IoT powered e-health solutions provide a great wealth of information that can be used to make actionable decisions. By connecting information, people, devices, processes and context, IoT powered e-health creates a lot of opportunities to improve outcomes. Some of the most promising use cases of connected e-health include preventive health, proactive monitoring, follow-up care and chronic care disease management [4]. It can be stated that the IoT is a disruptive innovation, which bridges interoperability challenges to radically change the way in which healthcare will be delivered, driving better outcomes, increasing efficiency, and making healthcare affordable [6].

In order to track and record personal data it is necessary to use sensors or tools which are readily available to the general public. Such sensors are usually wearable devices and the tools are digitally available through mobile device applications. These self-monitoring devices are created for the purpose of allowing personal data to be instantly available to the individual to be analyzed. The biggest benefit of self-monitoring devices is the elimination of the necessity for third party hospitals to run tests, which are both expensive and lengthy. These devices are an important advancement in the field of personal health management.

Currently, self-monitoring healthcare devices exist in many forms. This paper presents the creation of such system which will include everything user would expect from a commercial system. In other words, by using inexpensive hardware and open source software, it is possible to create a DIY (Do-It-Yourself) system in such a way that own solution meets user's specific needs. Therefore, providing techniques to end-users and the possibility to shape products according to their needs is beneficial for both users and product developers.

II. THE IOT AND E-HEALTH

To improve human health and well-being is the ultimate goal of any economic, technological and social development. The concept of the IoT entails the use of electronic devices that capture or monitor data and are connected to a private or public cloud, enabling them to automatically trigger certain events. Nowhere does the IoT offer greater promise than in the

field of healthcare. McKinsey Global Institute in its report presents predictions and economic feasibility of IoT powered healthcare, which states that by 2025 the largest percentage of the IoT incomes will go to healthcare [7] (Fig. 1).

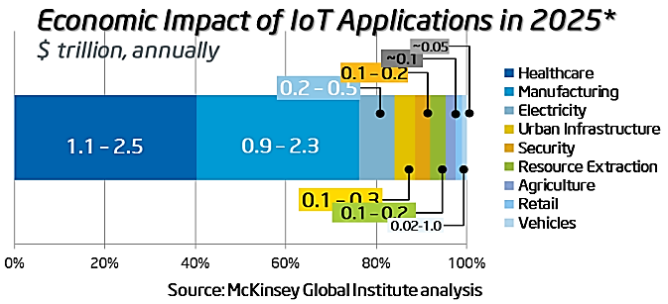

Fig. 1. Economic Impact of IoT Applications in 2025 provided by the McKinsey Global Insitute

Internet-connected devices, introduced to patients in various forms, enable tracking health information what is vital for some patients. This creates an opening for smarter devices to deliver more valuable data, lessening the need for direct patient-healthcare professional interaction. With faster, better insights, providers can improve patient care, chronic disease management, hospital administration and supply chain efficiencies, and provide medical services to more people at reduced costs [8]. The IoT has already brought in significant changes in many areas of healthcare. It is rapidly changing the healthcare scenario by focusing on the way people, devices and applications are connected and interact with each other (Fig. 2). Hence, it can be concluded that the emerging technology breakthrough of the IoT will offer promising solutions for healthcare, creating a more revolutionary archetype for healthcare industry developed on a privacy/security model [9].

Fig. 2. The confluence brought about by the IoT [6]

Typically, IoT powered e-health solution includes the following functions [10]:

- Tracking and monitoring (e.g. patient monitoring, chronic disease self-care, elderly persons monitoring or wellness and preventive care);
- Remote service;
- Information management;
- Cross-organization integration.

The requirements of IoT communication framework in e-health applications are [11]:

- Interoperability - is needed to enable different things to cooperate in order to provide the desired service.
- Bounded latency and reliability - are needed to be granted when dealing with emergency situations in order for the intervention to be effective.
- Authentication, privacy, and integrity - are mandatory when sensitive data are exchanged across the network (Fig. 3).

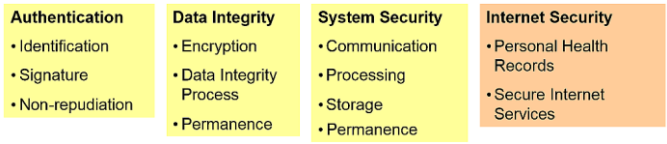

Fig. 3. Healthcare specific security standards [12]

A different technologies and architectures of IoT for healthcare can be found in various papers [4, 10, 13, 14], but next building elements are common for all of them [3]:

- Sensors that collect data (medical sensors attached with the patient to measure vital parameters, and the environmental sensors which monitor the surroundings of the patient);
- Microcontrollers that process, analyze and wirelessly communicate the data;
- Microprocessors that enable rich graphical user interfaces; and
- Healthcare-specific gateways through which sensor data is further analyzed and sent to the cloud.

In the next chapter a cheap solution for building IoT healthcare sensing devices will be presented.

III. DIY SELF-MONITORING DEVICE

The main application domain of body sensor network – BSN (a network of sensors attached to the human bodies) is continuous health monitoring and logging vital parameters of patients. In other words, these networked systems continuously monitor patients' physiological and physical conditions, and transmit sensed data in real time via either wired or wireless technology to a centralized location where the data can be monitored and processed by trained medical personnel.

Today's personal health monitoring systems and similar medical devices must use a variety of design techniques to protect the underlying design as well as protect the sensitive data stored within or transmitted to/from the device [15-22]. Many personal health monitoring devices must also be portable, so they need to be small, lightweight, and low-power [15].

In order to build own health monitoring device with aforementioned characteristics, this paper proposes a usage of ultra-cheap-yet-serviceable, small and powerful computer board - Raspberry Pi (RPi). A RPi has built in support for a large number of input and output peripherals and network communication, and it is the perfect platform for interfacing with many different devices and using in a wide range of applications (Fig. 4) [23].

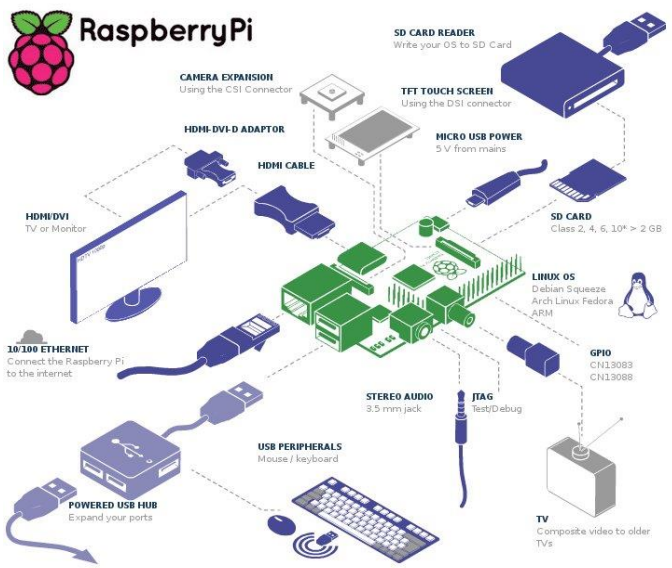

Fig. 4. Raspberry Pi components

Beside of that, enabling end-user programming on RPi, a complete open-source and low cost system based on IoT concepts can be created. There are two possible solutions for applying a RPi for building an IoT healthcare system:

- Using a third part RPi Sensor Shield for extending functionality; and
- Building solution from scratch using an analog/digital sensor elements and custom software programming.

A. *Sensor Shield*

Sensor Shield V2.0 (SSV2.0) (Fig. 5) performs biometric and medical applications where body parameters monitoring is performed by using 10 different sensors: pulse, oxygen in blood (SPO2), airflow (breathing), body temperature, electrocardiogram (ECG), glucometer, galvanic skin response (GSR - sweating), blood pressure (sphygmomanometer), patient position (accelerometer) and muscle/electromyography sensor (EMG) (Fig. 6) [24].

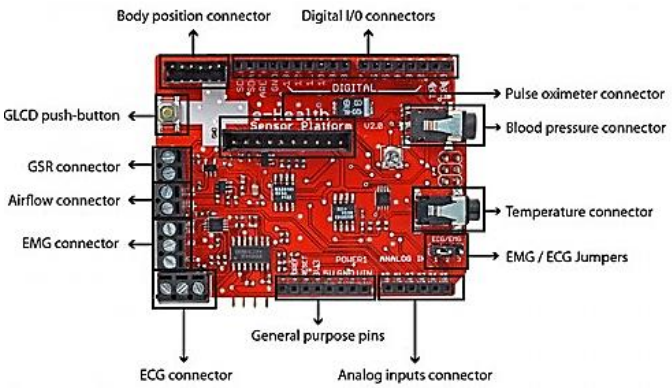

Fig. 5. e-health Sensor Shield V2.0

SSV2.0 enables real time monitoring the state of a patient or getting sensitive data in order to be subsequently analyzed for medical diagnosis. The biometric information gathered can be wirelessly sent using any of the six connectivity options available: Wi-Fi, 3G, GPRS, Bluetooth, 802.15.4 and ZigBee depending on the application [24].

Fig. 6. Monitoring in real time the state of a patient

Using a RPi's support for DSI (Display Serial Interface) and for CSI (Camera Serial Interface) solution easily can be expanded with display and camera, respectively. The price of the whole SSV2.0 kit without RPi is approximately 450 €.

B. *A custom solution*

The key elements for building a custom IoT healthcare solution is RPi's support for 26-pin GPIO (General Purpose Input and Output) port. Some of GPIO's pins can be used as digital inputs/outputs signals and can be programmed directly on RPi through high level programming languages. Some of GPIO's pins can be used as interfaces for embedded protocols for controlling a lot of electronic circuit (sensors, analog to digital converters (ADC), relay, status button, etc.). In other words, the GPIO port is the main way of connecting RPi with other electronic boards. Via GPIO port it is possible to communicate with other computing devices using a variety of different protocols including Serial Peripheral Interface (SPI) and Inter-Integrated Circuit (I²C). The main disadvantage of RPi is the absence of the ADC.

Using two components, a 10kNTC waterproof thermistor with range from -20 °C to 105 °C and PCF8591 8-bit I²C ADC, both chosen based on their price, availability and precision, a simple body temperature measurement system can be created (Fig. 7) [25].

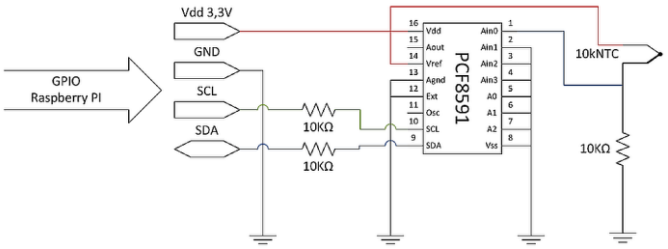

Fig. 7. Electronic circuit scheme of Raspberry Pi as a sensing unit

In similar way various sensors for measuring vital parameters can be connected. Based on chosen sensor types, an expert fuzzy system for decision making can be proposed as one of the solutions [25].

For delivering measurement information to user and comply with IoT ideology, a RPi must implement one of HTTP WEB Server (in our case, Apache Tomcat) which can provide a lightweight REST [26] services. In case of applying

a REST service to IoT solution, every action represents a resource and has a unique URI address via which is accessed to the sensor data. Thus, for the body temperature readings from sensors used in the example, a URI address is provided:

```
(server adress)/RPISensorWeb/sw/ntc10k
```

which generate a JSON (JavaScript Object Notation) response:

```
{"temp":"36.5"}
```

Since data from sensor node are obtained in JSON format, a different client application for visualization and processing can be created based on custom user's need. The price of this solution depends on quality of sensors (different manufacturer gives a different quality of hardware) and resolution of ADCs [27].

In both proposed cases, a sensed data can be relayed to the server or a base station in close proximity. In such way, the doctors and caregivers monitor the patient in real time through the data received through the server. The medical history of each patient, including medications and medical reports are stored in a central database in the cloud or visualized in real time for easy access and processing for logistics and prognosis of future complications. The data can be processed in two ways, on-board processing (allows immediate detection anomalies and care could be taken before the patient reaches healthcare institutes) and on server processing (uses the real time metadata received from the sensors to process them with respect to the data stored in the cloud itself). On server processing requires better resources in the form of memory, throughput and processing time and hence is more suitable [13].

In general, creating a connected product simple to use takes a mass effort. So, it's really important to consider early how humans will interact with the finished pattern and perhaps learn where the problems lie before investing a majority of expert study. Processes such as mocking-up the design and rapidly building early working prototypes can help greatly [28]. Therefore, the systems presented are aimed at developing a set of modules which can facilitate the diagnosis for the doctors through telemonitoring of patients.

Having in mind that IoT is an issue of scale and that scale affects everything, massive amounts of data, new devices and protocols, bursty traffic, a heavier reliance on the cloud and increased IPv6 deployment are five key impacts necessary to be considered in IoT vision [29]. In IoT there's a tension between effort, efficiency and time-to-market, and generally there's a trade-off between them: it is possible to have any two but not all three [28]. Connected devices, sensors, wearables, automobiles, and other non-human stuff will produce massive quantities of data. When viewed on a device-by-device basis, the bulk of data produced are not things of concern. Nevertheless, when submitted in aggregate, this data puts a substantial threat to specific networks and the systems that manage them. The solution is to consider a monitoring platform based on a distributed computing model. In other words, keeping performance data distributed across the network, it is easier to manage the challenge of massive data generated by the IoT [29]. Thus, it is of the essence to ensure data crosses safely from the physical to the digital world and be recorded electronically and stored in persistent, query-capable systems, where it can be processed and manipulated. The final step in developing custom solution demonstrates the path from the original sensor device through the engineering layers required for transmission of data, through the software services and human interaction, and finally back to the sensor, where the knowledge generated is utilized to make the sensing device more powerful and more precise [30].

IV. Security and Privacy Concerns of IoT Powered E-Health

The realization of the IoT generally requires dramatic changes in systems, architectures and communications which should be flexible, adaptive, secure, and pervasive without being intrusive [31]. The experts anticipate that the technologies of the IoT will bring forward critical developments in the areas of ethics, data protection, technical architecture, standards, identification of networked objects and governance [32]. In other words, as more intelligent devices are connected to the Internet, the potential privacy implications and general false sense of security associated with weak key management and data compromise become critical. Thus, security (protection of data and privacy) represents a critical component for enabling the widespread adoption of IoT technologies and applications (Fig. 8).

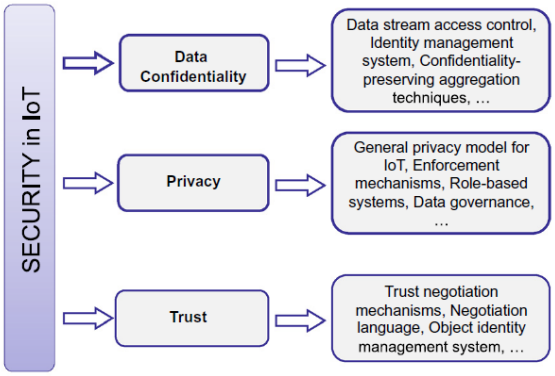

Fig. 8. Security challenges in IoT

The official breach reports from 2009 to mid-April 2013, presents the security risks for healthcare IT professionals (Fig. 9) [33].

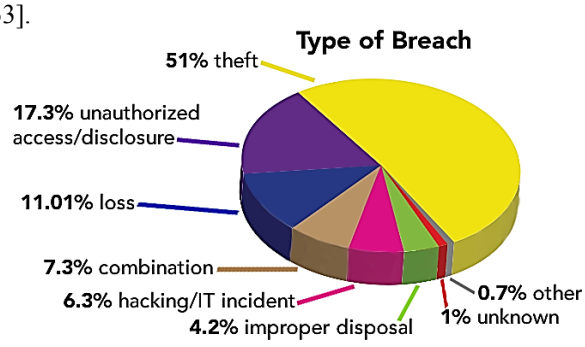

Fig. 9. Security risks for healthcare IT professionals

E-health systems store and process very sensitive data and should have a proper security and privacy framework and mechanisms. Fig. 10 shows the link between many important healthcare research problems and information security [18].

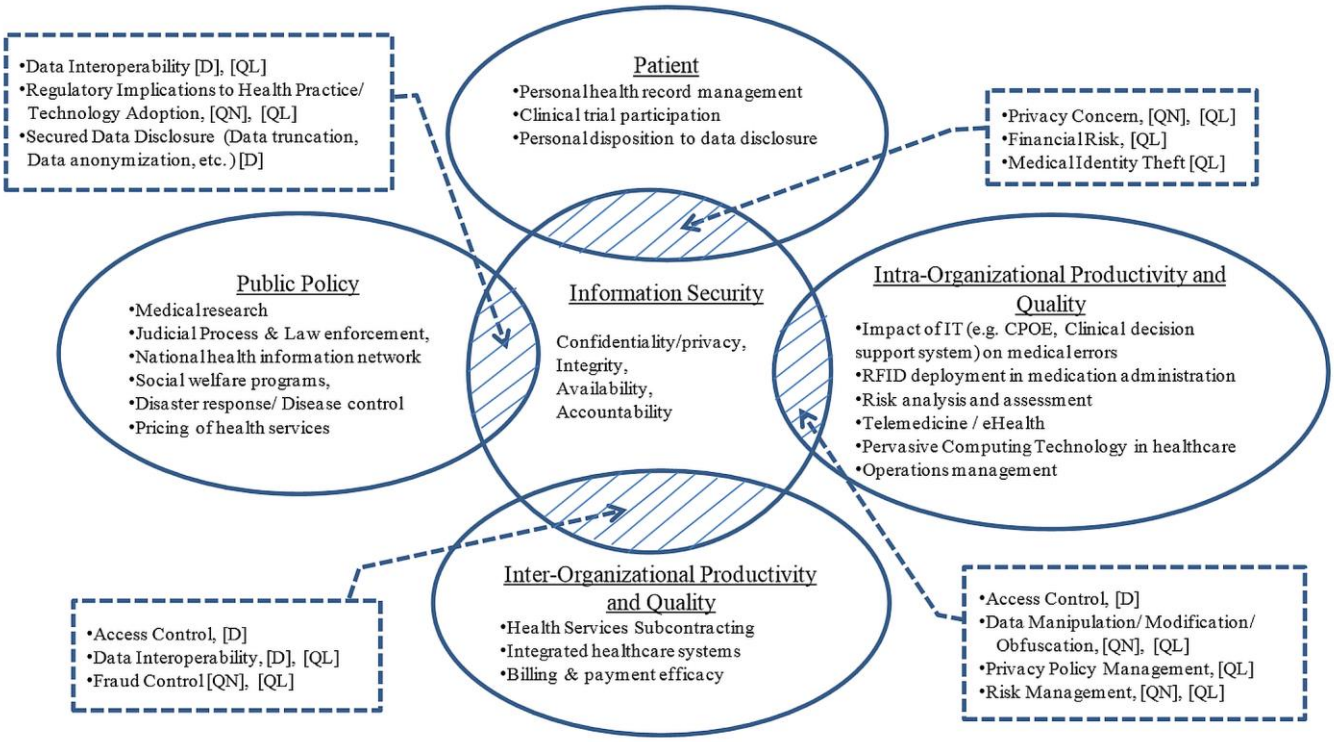

Fig. 10. Research Domains in the Healthcare Information Security [18]

As it is already mentioned, some of collected data may be private and patients don't want to share them with others, even clinic physicians. The disclosure of such private data could lead to unwanted privacy threats to the patients [34]. Thus, portable devices to record, store, and transmit patient data to a central server, need secure ways to transmit recorded data at high speed to ensure that personal records can't be compromised at any point. Protecting privacy must not be limited to technical solutions (encryption, ID management, privacy-enhancing technologies), but encompass regulatory (consumer consent, collection limitation, openness, accountability), market-based (self-regulation, privacy certification, consumer education) and socio-ethical considerations (consumer rights, public awareness, disclosure, consumer advocacy).

V. Conclusion

The rapid development of technology and the Internet leads to growing applications of new technological solutions at the global level. With the appearance of the Internet of Things concept, elements, such as sensors and sensor networks, are becoming available and applicable in all fields of human activity, thus providing conditions for the creation of expert systems that can operate anytime and anywhere. Following these trends, an indispensable application of it is in healthcare, where the application can be found in health monitoring, diagnostics and treatment more personalized, timely and convenient. All of this significantly improves health by increasing the availability and quality of care followed with radically reduced costs.

This paper discusses of economical, technological, security and application aspects of applying IoT in e-health. It also presents two solutions on the affordable prototyping platform for e-health based on RPi unit: one used existing Sensor Shield V2.0, and the second is based on principals for creating a custom solution – solution built from a scratch according to specific patient's needs. Using proposed solution is shown that applying technology based on IoT significantly can reduce a price of healthcare, but is also shown that there are elements (security and technology) for future improvement and consideration.

References

[1] Internet of Things, European Research Cluster on the Internet of Things, [Online]: http://www.internet-of-things-research.eu/about_iot.htm

[2] D. Miorandi, S. Sicarib, F. De Pellegrinia and I. Chlamtac, "Internet of Things: Vision, applications and research challenges", Ad Hoc Networks 10 (2012) 1497–1516

[3] D. Niewolny, "How the Internet of Things Is Revolutionizing Healthcare," Freescale, 2013, [Online]: http://www.freescale.com/healthcare

[4] D. Lake, R. Milito, M. Morrow and R. Vargheese, "Internet of Things: Architectural Framework for eHealth Security," Journal of ITC Standardization 01/2014; DOI: 10.13052/jicts2245-800X.133

[5] How the Internet of Things Can Save 50,000 Lives a Year, RTI White Paper, [Online]: http://www.rti.com/whitepapers/iot_can_save_lives.pdf

[6] P. Venkatramanan and I. Rathina, "HealthcareLeveraging Internet of Things to revolutionize Healthcare and Wellness", IT Services Business Solutions Consulting, © 2014 Tata Consultancy Services Limited

[7] The Internet of Things and Healthcare Policy Principles, Intel, [Online]: http://www.intel.eu/content/dam/www/public/emea/xe/en/documents/iot-healthcare-policy-principles-paper.pdf

[8] Transforming patient care with IoT, [Online]:

http://www.microsoft.com/en-us/server-cloud/solutions/internet-of-things-health.aspx

[9] Will the Internet of Things Analytics Revolutionize the Healthcare Industry?, A Saviance Technologies Whitepaper 2014

[10] Z. Pang, Technologies and Architectures of the Internet-of-Things (IoT) for Health and Well-being, PhD Thesis in Electronic and Computer Systems, KTH – Royal Institute of Technology, Stockholm, Sweden, January 2013

[11] N. Bui and M. Zorzi, "Health Care Applications: A Solution Based on The Internet of Things," Proceedings of the 4th International symposium on Applied Sciences in Biomedical and Communication Technologies – ISABEL 2011

[12] C. P. Waegemann, "Confidentiality and Security for e-Health," CEO, Medical Records Institute (MRI), [Online]: https://www.itu.int/itudoc/itu-t/workshop/e-health/s5-05.pdf

[13] S. Mukherjee, K. Dolui an S. K. Datta, "Patient Health Management System using e-Health Monitoring Architecture", IEEE International Advance Computing Conference (IACC), 2014, 400 - 405

[14] D. Salvi, E. Villalba Mora and M. T. Arredondo Waldmeyer, "An architecture for secure e-Health systems", [Online]: http://www.tsb.upv.es/eventos/workshophealthcare/documentos/C2-2.pdf

[15] Design of a Secure Personal Health Monitoring System, Application Example, © 2013 Microsemi Corporation.

[16] W. Wilkowska and M. Ziefle, "Privacy and data security in E-health: Requirements from the user's perspective," Health Informatics Journal 18(3) 191–201

[17] J. T. Kim, "Privacy and Security Issues for Healthcare System with Embedded RFID System on Internet of Things," Advanced Science and Technology Letters Vol.72 (Healthcare and Nursing 2014), pp.109-112

[18] A. Appari and M. Eric Johnson, "Information Security and Privacy in Healthcare: Current State of Research," August 2008, [Online]: http://www.ists.dartmouth.edu/library/416.pdf

[19] F. S. Tsai, "Security Issues in E-Healthcare," Journal of Medical and Biological Engineering, 30(4): 209-214

[20] S. Brands, "Privacy and Security in Electronic Health," Invited submission to the PricewaterhouseCoopers CCE Journal, 2003

[21] Information Security Policy, e-Health Ontario 2012, [Online]: http://www.ehealthontario.on.ca/images/uploads/pages/documents/InfoSecPolicy_EN.pdf

[22] H. Löhr, A.-R. Sadeghi and M. Winandy, "Securing the E-Health Cloud," in Proceedings of the 1st ACM International Health Informatics Symposium (IHI 2010).

[23] Raspberry Pi, [Online]: http://www.raspberrypi.org/

[24] e-Health Sensor Platform V2.0 for Arduino and Raspberry Pi [Biometric / Medical Applications], [Online]: http://www.cooking-hacks.com/documentation/tutorials/ehealth-biometric-sensor-platform-arduino-raspberry-pi-medical

[25] M. Maksimović, V. Vujović, B. Perišić and V. Milošević, "Developing a fuzzy logic based system for monitoring and early detection of residential fire based on thermistor sensors," Computer Science and Information Systems, Vol. 12, No. 1, pp. 63-89, 2015

[26] R. T. Fielding, Architectural Styles and the Design of Network-based Software Architectures, PhD Thesis in Information and Computer Sciences, University of California, Irvine, 2000

[27] V. Vujović and M. Maksimović, "Raspberry Pi as a Sensor Web node for home automation," Computers & Electrical Engineering, ISSN 0045-7906, DOI 10.1016/j.compeleceng.2015.01.019, 2015 (in press)

[28] Designing for Scale, [Online]: http://1248.io/whitepapers/1248_designing_for_scale.pdf

[29] How Will the Internet of Things Disrupt Your Performance Monitoring Strategy?, SevOne, [Online]: https://www.sevone.com/white-paper/how-will-internet-things-disrupt-your-performance-monitoring-strategy

[30] M.Roantree and M. Sallinen, "Introduction - The Sensor Web - Bridging the Physical-Digital Divide," [Online]: http://ercim-news.ercim.eu/en76/special/introduction-to-the-special-theme-the-sensor-web-bridging-the-physical-digital-divide

[31] L. Yan, Y. Zhang, L.T. Yang and H. Ning, "The Internet of things, From RFID to the Next-Generation Pervasive Networked Systems," Auerbach Publications, Taylor & Francis Group, 2008

[32] U. Meier-Hahn, European Commission publishes report on Internet of things, 2013, [Online]: http://policyreview.info/articles/news/european-commission-publishes-report-internet-things/114

[33] Top 5 HIPAA Security Risks As Providers Migrate to the Cloud, [Online]: http://cloudtweaks.com/2013/05/top-5-hipaa-security-risks-as-providers-migrate-to-tthe-cloud/

[34] F. Shih and M. Zhang, "Towards Supporting Contextual Privacy in Body Sensor Networks for Health Monitoring Service," [Online]: http://www.w3.org/2010/policy-ws/papers/09-Shih-Zhang-MIT.pdf