International Journal of Security and Its Applications
Vol. 12, No. 6 (2018), pp.47-56
http://dx.doi.org/10.14257/ijsia.2018.12.6.05

Improvising Security and Privacy Vulnerabilities in Smart Health

Muhammad Tahir[1]*, Rukaiya Javed[2] and Talat Altaf[3]

[1,2]Department of Computer Engineering
[3]Department of Electrical Engineering
Sir Syed University of Engineering and Technology
tahirfattani@gmail.com, rjavaidsh@gmail.com, drtaltaf@ssuet.edu.pk

Abstract

Internet of Things (IoT) is defined as the development of the internet with everyday objects. It is termed as a visionary transformation of objects that facilitate users and provide numerous services. IoT makes the device smarter and offers many benefits for patient monitoring by using the generated analytical data. However, adoption of these smart devices in daily life has given the birth to several security challenges and led to public security issues, including cybercrime threats, false usage of personal data and organized crimes. Breach of medical data means a patient at high risk. According to a survey in 2016, the total record of 554,454,942 offences has been reported by industry from education, financial, healthcare, technology and other domains [1]. There are several security vulnerabilities and threats that are not yet discovered, well-recognized, studied or spoken in detail. The purpose of this article is to give a broad overview of the field, highlights the security, privacy vulnerabilities and complexities that have already or are likely soon to rise. The paper is also introducing new-emerging security challenges with possible solutions and countermeasures against these threats and attacks that are not yet explained in detail with a logical explanation.

Keywords: *Data Breaches, Device Security, E-Health, Internet of Things (IoT), Smart Devices*

1. Introduction

Internet of Things (IoT) is a comprehensive framework for the information society. Various applications of IoT involve smart devices installed in different environments particularly in health, fitness and home automation [2][3]. These devices consist of objects such as sensing devices and computational components that may work on servers or cloud, and some additional features for smart and intelligent actions. It may also contain some data transferring features that may distinguish it from other systems such as Bluetooth, RFID (Radio Frequency Identification) tags and some barcodes NFC (Near Field Communication) tags etc. [4]. The development and adaptation of IoT are one of the remarkable achievements of the last decade. Worldwide a lot of organizations and multinational companies are giving priority to design and develop IoT based systems. IoT market has provided enormous possibilities for companies to do work more efficiently and create products that are beyond human imagination. According to research, by the year 2020, experts predict to awake 28 billion policy drive be joined the internet, a third of them are end devices such as personal computers, smartphones etc. The remaining two thirds are sensors, terminal, home appliance, thermostats, television, automobile, manufacture machines, city transportation and several extra things, which by tradition, not been internet enabled [5]. A software vendor named Marketo conducted research to look at newer

Received (August 23, 2018), Review Result (October 15, 2018), Accepted (October 22, 2018)

ISSN: 1738-9976 IJSIA

technologies and their effect on marketing. They provided a statistic that in 2017, 43.75% of international marketers are planning to include IoT in their marketing strategy [6].

Due to recent advancement in the biotechnology, signal processing, wireless communication and low power devices, health monitoring has become a lot easier as shown in figure 1 [7]. IoT based system is now able to monitor, store, analyse the personal health of a person and early detection of illnesses. Many smartphone applications are developed that assist in health care [8]. The smart pacemaker and ultrasound devices etc., are connected within a compact module and tracking a patient's health condition [9]. Many hospitals have started smart-bed, which automatically see the position of patient and spot-on it [10]. The smart medication dispensers automatically upload information to the cloud and alert doctors about their patient movement [11]. In fact, remote health monitoring systems are revolutionising the human life by providing real-time monitoring, swift stroke or event detection and data access.

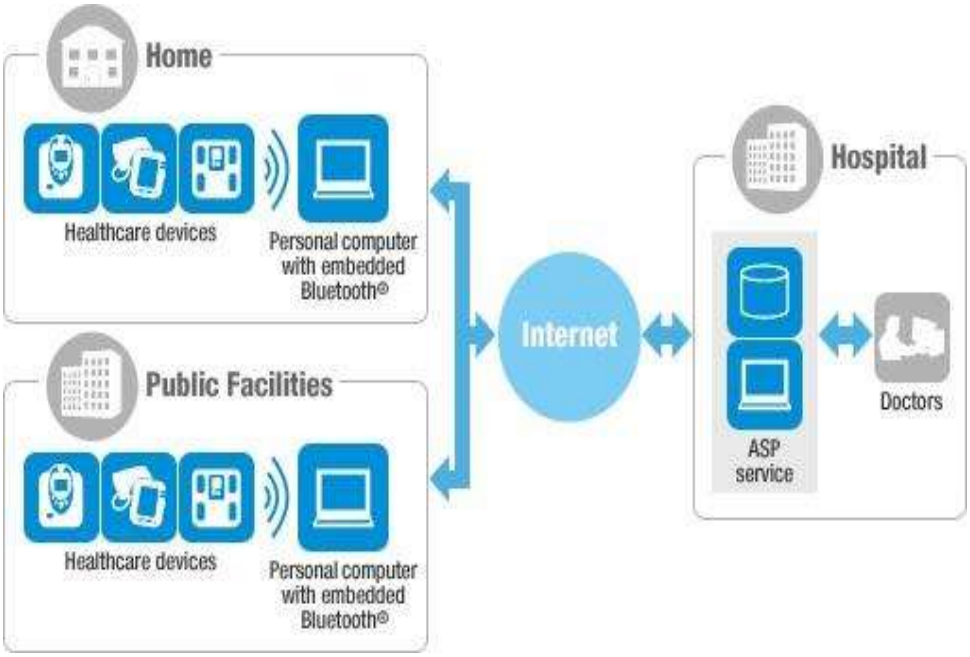

Figure 1. Remote Health Monitoring System

With IoT, smart devices are equipped with sensors to communicate via web and local networks. Connected devices with fewer security measures represent new efficient ways of attacking include the ease of surveillance practices, data breaches resulting in stealing and compromising of personal data. These data breaches can have extensive effects on consumer rights and the individual's perception related to the security of IoT.

Security issues arise because of insecure human-to-device and device-to-device interaction. According to a survey in the year 2016, many data breaches and leakages have been reported across the world. Panama Leaked set of 11.5 million confidential documents including identities of stakeholders and other sensitive information. Data Breach at the University of California at Berkley left 80,000 students, staff and vendors vulnerable to further attacks. North memorial health care in Minnesota had to pay up 1.55 million USD for failing to sign a business associate contract with a partner. Feinstein Institute in New York leaked the sensitive information of 13,000 patients and fined a monstrous 3.9 million USD. Europe had more than 200 incidents of theft in 2015 affecting 60 million records. The U.K. had the highest number of breaches, with more than 140 incidents affecting 20.7 million records. Germany came in second place with 11 offences [12]. Late last year, distinguished internet services such as Netix and Twitter were temporarily taken down an

immense distributed DDoS attack that involved hackers deploying malware to the ordinary webcams embedded in the devices. Authorities in U.S. and U.K. were investigating the Mirai malware, used in the offence to create a botnet (a group of devices commanded by hackers). However, this code still exists online, allowing to use little technical skills for intercepting services on a larger scale [13].

IoT gave an opportunity to business persons for developing user-friendly smart devices that make human life more comfortable. With this ease and development, several attacks affect the healthcare industry concerning financial loss, business disruption and their brand barred listed in Table 1.

Table 1. Threats and Attacks to Health Care Industry

Brand Repudiation	Business Disruption	Financial Loss
Operating license denial, Equipment damages	Supply chain and logistic Disruption, Contract repudiation	The market decline, uncertainty looming, Product boycott

In remote health monitoring, where patient's data has always been considered as sensitive and needs reliable protection against unauthorised data disclosure. Related to authorisation, there are different aspects of giving data access rights. The devices which are used to monitor health information often used with default access control settings. It can also depend on the wearer of an eHealth device that to whom he wants to give access. Some wearers wish to pre-configure individual access rights in the situation of an emergency or selectively allow persons or group of person's access to medical data. The user of an eHealth device also requires integrity and confidentiality of the data captured by that device. Security mechanisms could not provide opportunities for denial of service (DDoS) attacks on those devices.

In this paper, we highlighted the security and privacy vulnerabilities that can affect human life. We also discussed some key points that should be considered not to be modified, especially in the case of health care. The critical input of this study is to investigate the security risks and objectives of an e-health self-care system that includes health monitoring sensors, communication and storage solutions, data processing and representation, and the appropriate interfaces in between. Moreover, the study proposes initial heuristics for security metrics development via decomposition of security objectives. The proposed heuristics cover the main risk-driven security controls and strategies for the dissolution. In addition to the decomposition heuristics, initial measurement architecture development stages are also recommended. Availability objective decompositions include considerations for alarm management, monitoring of procedures rules, agreements, service mirroring etc.

The rest of the paper is aligned as mentioned. We presented a case study of a lady affected by data breach regarding her personal health information in section II. The ways to improve security and privacy from a different perspective is being discussed in section III. Section IV concludes the article.

2. Case Study

For further elaborating on the security and privacy issue in the health sector, we are considering the case study of a lady who was using a heart monitoring device. Unexpectedly, her insurance company refused to persist the contract on the ground of her heart problem. She found that it was happened due to the data breach. The lady tried to find the loopholes by going through the complex chain of actors, shown in Figure 2. She also

took help from different laws. The laws were related to the person that has been subjected to a data breach for notifying their customers and other parties regarding the violation and take further steps to prevent damages resulted from that breach. Such laws have been enacted most in the United States since 2002. These laws were ratified as the result of an increasing number of violations of consumer databases, containing personal, recognisable information.

Following is the complex chain of actors:

• Actor A: Retailer of the heart rate monitoring device;

• Actor B: Supplier of the heart rate monitoring device;

• Actor C: Advertising agency;

• Actor D: Producer/ Manufacturer of hardware;

• Actor E: Software engineers, developers of software;

• Actor F: Employer of actor E;

• Actor G: Developer of software code which actor E licensed to use it in its software;

• Actor H: Licensee, producer of software;

• Actor I: Data processor - an independent company;

• Actor J: Another company which supplied security measures;

• Actor K: Company responsible for software maintenance;

• Actor L: Hacker who breached the data;

• Actor M: Person/Company who made use of leaked data;

In all cases, with a complex supply chain, the allocation of responsibility and liability will be complexed, mainly when multiple jurisdictions may be involved. Thus, the European Commission's 2015 digital strategy notes that "Legal certainty to the allocation of liability is important for the roll-out of IoT" [14]. It is very challenging to determine which countries law applies to a particular situation.

To provide endless support and a large number of services, designers are encountering challenges mainly security-related researches. Several types of research and efforts are being made to determine potential threats and provide practical solutions for them [15][16]. Many frameworks have already been proposed. A designed is introduced which is based on the Architecture Reference Model (ARM) [17], derived from IoT. A European project to give a comprehensive view of IoT security and privacy needs. Two European projects scolotal and smartie have driven the ARM. The aim is to enable secure, and privacy preservation mechanisms to different IoT use cases and scenarios. Key challenges to cover the whole spectrum of security and privacy needs throughout the life cycle stages of smart devices. To succeed with the application of IoT security efficiently.

In real time the patient health condition is critical and crucial. A new concept that is using sensors and smart devices to collect real-time medical data from the remote environment [18]. Two fields are defined in the paper, e-health and m-health architecture to use the smart devices like phones, gadgets etc. The sensors sense and send the patient's data to the intelligent device. Secondly, the k-healthcare model is introduced which provides four layers; a sensor, network internet and service layer. These layers transfer the data more effectively and efficiently to end user or to a patient. The three-level intellectual framework is defined that can share and analyse a patient's data [19]. This system will give temporary advice and response towards any emergency condition that may happen at any place and time. IoT-based patient monitoring systems based on sensors network and internet [20]. The bridge is between both of these is called a gateway. There is a new concept of a smart e-Health Gateway UT-GATE where some significant characteristics have been implemented [21]. It is added the central idea of design which expresses an IoT based e-health system with higher overall system efficiency, performance, security and reliability.

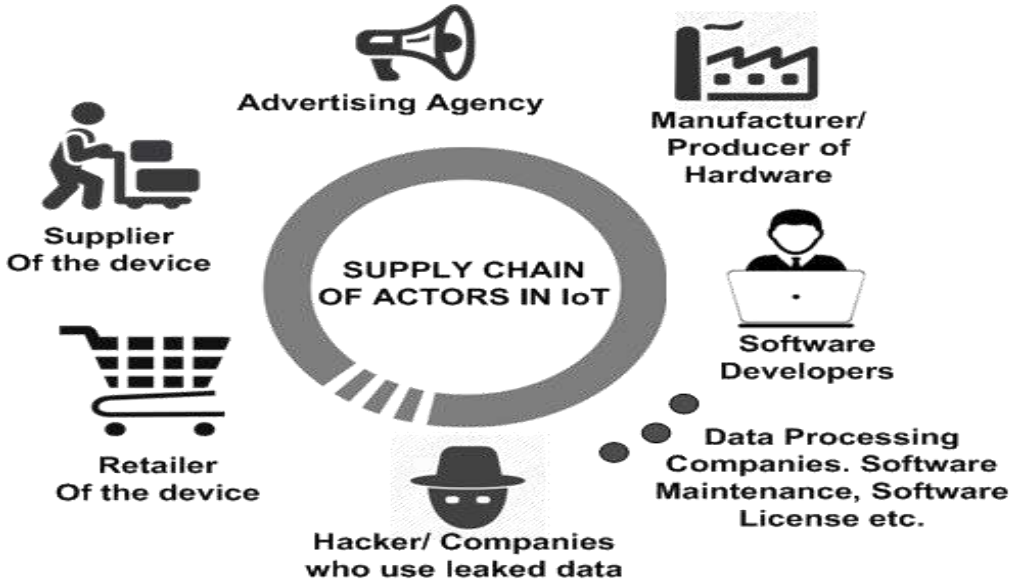

Figure 2. Complex Chain of Actors in IoT

Patient Monitoring System (PMS) has three segments: a body area network, hospitals, healthcare enterprises and communication networks [22]. Personal smart devices which are using within the enterprise have in growing problems. The protocol stack is developed for security in health and monitoring system [23]. During the testing of many systems, it is recommended that the low power system is best for e-health devices [24]. e-Health services can take advantage of the technological achievements in IoT. A cloud-based web server depends on home security. The web-based application is installed for interaction with cloud and mobile API [25]. A method to classify non-health devices with health data (Ex Micro oven, Coffee machine, smart TV) is also introduced. The following things need to be monitored which attacker usually uses such as operating frequency, modulation type, packet format, security of PIN devices and encryption of data during transmission.

We developed a little experiment to show that even some features of smart devices, the broadcasting of wireless networks SSID that it has been connected to, can be a potential privacy issue. We sniffed the wireless packets using a standard wireless adapter on a laptop. This data contains the SSIDs of the networks, searching for the geo-location of these SSIDs on services like wigle [26] can show an actual correlation between the data that the organisers of the summer school supplied us and our data as shown in Figure 3. This data

can also be narrowed down to a specific smartphone user (the source of the wireless packets), a scenario which can get pretty scary regarding the privacy of a smartphone user.

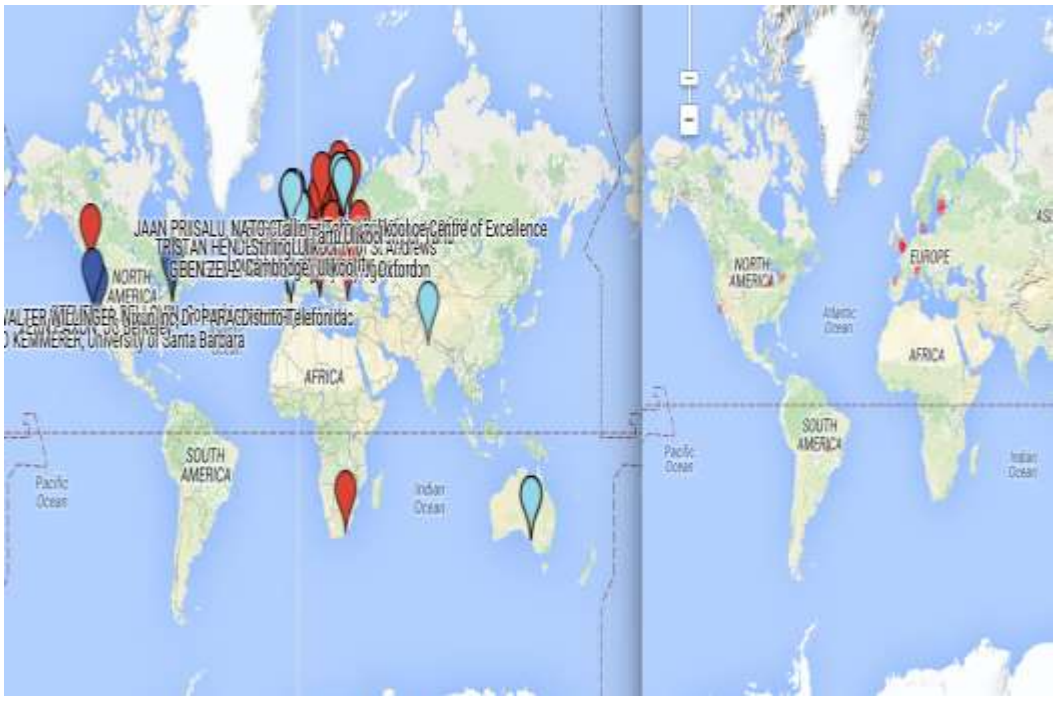

Figure 3. Comparison of Data Containing SSIDs

Since privacy is a critical asset for both end users and business that is by design and default should no longer be regarded as something peculiar. It should become a key selling point of innovative technologies confirmed by the Article 29 Working Group in its Working Paper 223 (Opinion 8/2014) regarding the Recent Developments on the Internet of Things, adopted in September 2014. Those principles have been introduced in Article 23 of the European Commissions draft proposal to a new Data Protection Regulation from 24th of January 2012 [27].

The Network Information Security (NIS) Directive mandates the EU members to implement national cybersecurity strategies, with particular attention to essential infrastructure. GDPR (General Data Protection Regulation) has objective to stream data protection and privacy laws throughout Europe. In the US, the Cybersecurity Information Sharing Act (CISA) incentivises private sector entities to engage in greater information sharing with one another as well as with the government, throughout liability protections. Health Information Portability and Accountability Act (HIPAA) compliances the issues related to the handling or disclosure of Protected Health Information (PHI) or Personal Health Records (PHR). With certain exceptions, a person or entity that creates, receives, maintains, or transmits PHI for a function or activity regulated by the HIPAA privacy rule for a covered entity is a business associate. The HITECH Act, a recent update made to overall HIPAA regulations, requires business associates to comply with HIPAA mandates regarding the handling and use of health information [28]. European and American countries have different legislation, directives and regulations related to various cyber-attacks that are abridged in Table 2.

Table 2. Legislations, Directives and Regulations related to Different Cyber-Attacks

Data breaches and Attacks	Europe	USA
Cyber-crime Hacking	Directives on attacks against information system (Article 82-89 TFEU)	Cybersecurity Act 2015 and multiple state laws under different Acts (Gramm-Leach-Billy Act, California Online Privacy Protection Act, Delaware Online Privacy and Protection Act)
Theft of Data / Identity	eDIAS Regulation	Federal Identity Theft and Assumption Deterrence Act 1988, the Federal Computer Fraud and Abuse Act
Business Associates	HIPAA	HIPAA
Privacy and Data Protection	NIS Directive, GDPR (Article 16(1) 7,8 and 11)	Cybersecurity Act 2015
Data Transfer (inside/outside)	Data breach regulation	CISA, 2015

Smart IoT in e-health with the dynamic environment can potentially solve security related problems. We have to consider which type of threats can harm the IoT, how to acquire knowledge and what is the potential harm in protecting the IoT in e-health against security threats. The impact that IoT may have in growing problems are insider threats somewhat within the enterprise. All the connected devices need to be secured, and user privacy must be considered. The devices connection must apply all parameters to achieve SSID, WEP, WPA. The route of data should be monitored. If it is adaptive routing then an adaptation of path must be checked, similarly, if it is the nonadoptive route, then there must be a random check on route security.

3. Ways for Improvising Security of IoT Based Systems

With the significant increase of IoT-based systems in our daily life, the IoT market has provided enormous possibilities for companies to do work more efficiently and create useful products. Here are some ways through which organisations can improve the security of the IoT-based system. As we have seen different aspects that are needed to consider when dealing with IoT devices and environments. The same consideration which right now is lacking, for lots of reasons ranging from the complexity of the issues to often shallow risk evaluation. Therefore, some effective measures should be taken in the future to ensure security, safety and privacy for users of IoT devices.

• Setup a Team of Security Specialists:

Product managers should work along with security specialists to take security as a critical consideration while designing core features and functionality of a product. A team will make sure that business and security concerns are well adjusted. This team will make sure any vulnerabilities can be identified early while developing the product.

• **Define Privacy Policies of IoT-based Product Usage:**

To protect customers from a data breach, IoT-based companies need to develop a privacy policy that mentions that "How the data is being collected from IoT Products", "How the data collected will be used" etc. Everyone is becoming very conscious about how their data is being collected, used or integrated into new systems. Therefore, the organisation should make explicit efforts to show their consumers that why the information is being obtained and where it will be used.

• **Incorporate best security practice while Product Development Process:**

The proactive risk management mechanism is nothing new, but it is an integral part of the production process. Business vendors need to identify and filter out any security issues or concerns during the development phases of the IoT-based product. They should study and understand the disruptive attack scenarios, and the financial or non-nancial impact on either the organisation or user. Once this is followed, leaders will know exactly how the security mechanism should be embedded throughout the product design process.

• **Educate Customers and Support Staff with Best Security Practice:** Planning and integrating high-quality security features into a product might take a long time. Therefore, organisations must educate and inform consumers to follow best security practices on a regular basis. For example, regularly changing passwords could protect you from being hacked by several vulnerabilities. Similarly, support staff must be well-trained in how to help customers to overcome these security issues or concerns. With this support, it will not only increase the reputation of the company but will also minimise the risk of security attacks.

• **Outbound traffic Analysis:**

The real-time analysis of outbound traffic on network pathways must be considered. Egress filtering restricts flow of unauthorised or malicious traffic outbound from a network to prevent internal compromise.

• **Multi-Tiered Integrated Supply Chain:**

Collaborative supply chain planning and real-time visibility across the supply chain must be considered.

• **Implement a Full Cybersecurity Plan in Case of Attack:**

Investigate extensively on the incident (a type of cyberattack, diagnosis of the affected equipment, the study of the entry points and vulnerabilities, alert and work closely with authorities), use the assistance of experts if needed and take appropriate disciplinary measures against noncompliant employees.

4. Conclusion

Internet of Things (IoT) is about an entirely new frontier of networked devices. IoT application in smart grid is needed to ensure data authentication, access rights, privacy and resilience to identified or unidentified attacks. From a technical perspective, the use of IoT requires the integration of different information and communication technologies concerning hardware and software. Energy level, identification, addressing, security and privacy of data are the key prospects in IoT. The current legal framework must take into account and establish by the country legislators. The contents of the legislation must give provision to an individual for protecting the data to be breached or acclaimed afterwards. Self-regulation measures have been applied but not sufficient to ensure data privacy and

security. Therefore, a framework or international legislator must be defined and implemented by regulatory authorities, globally. This will make the regulation public and monitored regularly. Different enforcement policies should be designed and applied to maintain security and data consistency. Many issues and challenges are yet to discover and not being addressed by the individual due to the unknown point of a data breach in the supply chain. Since, these measures are adding a significant impact on the business sector, especially making them focus on business model trials and adaptations to a new value chain configuration. All these challenges are opening up a new and inspiring way for the researchers and scientists to work on building the standards that may eradicate the security and privacy vulnerabilities.

References

[1] B. Sig. Medical & health. Bluetooth. [Online]. Available: http://www.bluetooth.com/Pages/Medical.aspx. June (2015).
[2] W. K. Hon, C. Millard, and J. Singh. Twenty legal considerations for clouds of things. (2016)
[3] Q. Zhou and J. Zhang. Research prospect of internet of things geography in Geo-informatics. Proceedings of the 19th International Conference on. IEEE, (2011).
[4] A. Banafa. Internet of things (IoT): More than smart things. Tech. Rep., April (2015).
[5] Marketo. The new technologies marketers intend to use in 2017. [Online]. Available: https://www.i-scoop.eu/ new-technologies-marketing-2017/.
[6] H. Vinutha, S. S. HV, and R. Narayan. The survey of internet of things. Imperial Journal of Interdisciplinary Research. 2, 12, (2016).
[7] J. P. Higgins. Smartphone applications for patients' health and fitness. The American journal of Medicine. 129, 11-19 (2016).
[8] U. Lindqvist and P. G. Neumann. The future of the internet of things. Communications of the ACM. 60, 2, 26– 30 (2017).
[9] A. Deshpande, A. Mathur, and S. Krishnamurthy. Application of internet of things in healthcare sector for bottom of pyramid in India. (2016)
[10] [Online]. Available: http://www.digilifeinc.com/
[11] Europe internet of things (IoT) security market growth, trends and forecasts (2015 - 2020). Information & Communications Technology, Tech. Rep. (2017).
[12] Wi. How to make 2017 the year of IoT security," Tech. Rep., February (2017).
[13] E. Commission. A digital single market strategy for Europe com 192 final. May (2015).
[14] J. Pacheco and S. Hariri. IoT security framework for smart cyber infrastructures. IEEE International Workshop of Foundations and Applications of Self Systems. IEEE. 242–247 (2016).
[15] F. Wortmann, K. Fl¨uchter. Internet of things. Business & Information Systems Engineering. 57, 221–224. (2015).
[16] E. F. R. P. IoT-A. Introduction to the architectural reference model for the internet of things. Tech. Rep.
[17] K. Ullah, M. A. Shah, and S. Zhang. Practical ways to use internet of things in the field of Medical and smart health care. Proceedings of International Conference on Intelligent Systems Engineering (ICISE). IEEE. 372– 379 (2016).
[18] A. Alahmadi and B. Soh. A smart approach towards a mobile e-health monitoring system Architecture. International Conference on Research and Innovation in Information Systems. IEEE. 1–5 (2011).
[19] A.-M. Rahmani, N. K. Thanigaivelan, T. N. Gia, J. Granados, B. Negash, P. Liljeberg, and H. Tenhunen. Smart e-health gateway: Bringing intelligence to internet-of-things based ubiquitous healthcare systems. 12th Annual IEEE Consumer Communications and Networking Conference (CCNC). IEEE. 826–834 (2015).
[20] Smart e-health gateway: Bringing intelligence to internet-of things based ubiquitous healthcare Systems. 12th Annual IEEE Consumer Communications and Networking Conference (CCNC). 826–834 (2015).
[21] J. Gomez, B. Oviedo, and E. Zhuma. Patient monitoring system based on internet of things. Procedia Computer Science. 83, 90–97 (2016).
[22] I. M. Ruiz, D. S. Cohen, and ´A. M. Marco. Iso/ieee11073 family of standards: Trends and Applications on e- health monitoring. Encyclopedia of E-Health and Telemedicine. IGI Global, pp. 646–660 (2016).
[23] H. Fotouhi, A. Causevic, K. Lundqvist, M. Bj. Communication and security in health Monitoring systems– a review. 40th Annual IEEE Conference on Computer Software and Applications (COMPSAC). 545–554 (2016).
[24] L. Pescosolido, R. Berta, L. Scalise, G. M. Revel, A. De Gloria, and G. Orlandi. An iot- inspired cloud-based web service architecture for e-health applications. IEEE International Conference on Smart Cities (ISC2). 1–4 (2016).
[25] Wigle net. Tech. Rep. [Online]. Available: https://wigle.net/.

[26] E. E. Commission. Proposal for a regulation of the European Parliament and of the council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (general data protection regulation). COM (2012) 11 final, 2012/0011 (COD), Brussels, January 25, (2012).
[27] [Online]. Available: http://www.lexology.com/library/detail.aspx?g= 769815b3-3087-4030-a469-e7c319970d8c.

Authors

Muhammad Tahir, is Associate Professor in the Department of Computer Engineering at Sir Syed University of Engineering & Technology. He completed his Bachelors in Computer Engineering from Sir Syed University of Engineering & Technology in 2005 and Masters Degree in Computer Systems in 2009 from NED University of Engineering & Technology. He completed his PhD from Università degli Studi di Roma "Tor Vergata", Italy. His research area is security and Privacy, Computer Networks and Computer Systems.

Rukaiya Javed, is Lecturer in the Department of Computer Engineering at Sir Syed University of Engineering & Technology (SSUET). She completed her Bachelors in Computer Engineering from Sir Syed University of Engineering & Technology in 2011 and got Master's Degree with specialisation in Computer Networks in 2015 from SSUET. She has her publications in national and international journals. Her research interest is in Computer Networks Computer Security and Wireless Sensor Networks (WSN)/ Multimedia WSN.

Prof Dr Talat Altaf, currently working as Chairman, Electrical Engineering Department and Acting Dean, Engineering at Sir Syed University of Engineering & Technology, Karachi. He has done BSc, Engg. (Hons), Electrical Engg; MSc Engg (Instrumentation) AMU, Aligarh and PhD (Electrical & Electronic Engg), University of Bradford, UK. He is Ex-Dean (Faculty of Electrical & Computer Engg., NED) & Meritorious Professor (retired). He is a Professional Electrical Engineer worked in Planning and Designing of Electrical Generation, Transmission System, Distribution Systems within Associated Technical Consultants from 1985 till 1998. Worked in Operation Section & Technical Services Section of Tarapur Atomic Power Station, India. He has got one-year Training based on Nuclear & Electrical Engineering at Bhasha Atomic Research Centre, Atomic Energy Commission, India. Planned and designed Electrical systems of different departments of Mehran University of Engineering & Technology, Jamshoro, Pakistan. Undergone three days training at SUPARCO Head Office, arachi. He was Senior Research Fellow at NED University and nvolved in PhD and MS Research Supervision. His Publications are about 41 in National & International Conferences/Journals. He is arded Best University Teacher, Award by the UGC (now HEC) for the year 2000.

