ADAPTIVE SOLUTION FOR KEY CHALLENGES IN INTERNET OF MEDICAL THINGS

RMPHK Rathnayake[1] and MS Karunarathne
Department of Computing & Information Systems, Faculty of Applied Sciences,
Sabaragamuwa University of Sri Lanka, P.O. BOX 02, Belihuloya
[1]*rathnayakepiumi19@gmail.com*

Abstract- Internet of medical things refers to the worldwide network of interconnected medical devices based on a standard communication protocol. Moreover, it is about interconnected medical devices via the internet at any time, with anyone, at any place, to any service, from any network. With the rapid advancements of technology connected through the internet, the healthcare field also affected immensely. This study is an attempt to investigate the most useful technologies and key challenges regarding the Internet of Medical Things (IoMTs) nowadays. This paper proposes an adaptive model to address the identified challenges. The main contribution of this study is an entrusted framework for IoMTs which satisfies major challenges of security, privacy and the data integrity of the sensor data. Furthermore, the proposed cloud-based health management system will increase data availability, storage needs and processing power. In the cloud-mobile architecture, the security is entrusted with three methods: Advanced Data Encryption, Attribute-Based Encryption and Proven Data Possession. The proposed model shows how these 3 methods along with cloud technology address the identified challenges: Security, Privacy, Data Integrity, Processing Power and Storage Issues in medical applications. Local databases are the most common use of the data storage. In this model, it is giving the cloud-based solution along with the algorithm which helps to increase the security level of the sensor data. The used encryption and data provable methods are most recognized and strong algorithms in today world.

Keywords- Internet of Medical Things, Advanced Data Encryption, Attribute-Based Encryption, Proven Data Possession, cloud technology

I. INTRODUCTION

In the healthcare field, there are significant applications of the internet of things (IoT), such as medical equipment and medical medication control, medical information management, telemedicine, mobile medical care and personal healthcare management systems. These technologies are helping to make hospital intelligent treatment by collecting, handling, storing, transmitting and sharing digital data such as medical information, personal information, medication information, and equipment information within the hospitals.

In this paper, some of the major technologies of the internet of medical things are being evaluated.

A. Wi-Fi

Wi-Fi is a facility which allows devices to connect with another, though the internet especially without wired connections, in a particular area. Hospitals may have existing Wi-Fi infrastructure that allowing long communication range which is reducing initial costs. Wi-Fi can use in combination with other technologies. Wi-Fi may have higher power consumption too. (Jin, 1--2)

Wi-Fi networks are more vulnerable to attack by unauthorized users because they are more difficult to secure than a wired network. It also has installation difficulties as it is so commonly used. Consumers may find another Wi-Fi setup in the medical building interference with the wireless signal and it has law transmission speed

(Wells, 2009). Newly founded multi-Gbps communication is the evaluation of Wi-Fi technology which is to enable high-speed device synchronization (Cordeiro, 2010). Nowadays, there is much Wi-Fi enabled blood, telemetry systems, mobile x-ray machines, IV pumps and glucose meters in the hospitals.

B. Zigbee

Zigbee is IEEE 802.15.4 based technology used to create personal area networks. It is a low power, short-range, low data rate, low cost, low maintenance wireless ad-hoc network (Li, 2010). It has the potential for use in wireless medical monitoring. There are also drawbacks such as taking time to send set of data by up to four times compared to other low power technologies, lack of communication directly with existing cellular and internet infrastructure, low data rate, neediness of specialized skills to operate ZigBee compliant devices, security issues, high replacement cost, time consuming to adapt fast to the environment (Kanwar, 2012).

Zigbee technology is widely used in chronic disease monitoring, personal wellness monitoring, and personal fitness monitoring applications. Also, it can be used in devices that already exist including the pulse oximeter,

blood pressure monitor, pulse monitor, weight scale and glucose meter (Ahamed, 2009).

1) Zigbee System Architecture

operations also control by this layer. All the link setup, authentication, link configuration and other protocols carry by link manager protocol. Host controller interface allows command line access to the base-band layer and

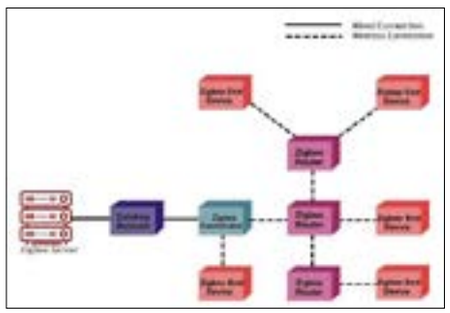

Figure 1. Architecture of Zigbee System

ZigBee system structure includes three different types of devices: ZigBee coordinator (ZC), Router(ZR), and End Device(ZED). Every ZigBee network should contain at least one ZigBee coordinator who acts as a root and links to the network. The coordinator is mainly responsible for handling and storing the information while performing the receiving and passing data operations. Zigbee routers act as middleware devices that enable data to pass to one to another device. End devices have limited functionality to communicate with the parent nodes (Alliance., 2006). The number of routers, coordinators and end devices depends on the type of networks such as the tree, star, mesh networks and so on (Horowitz, 2007).

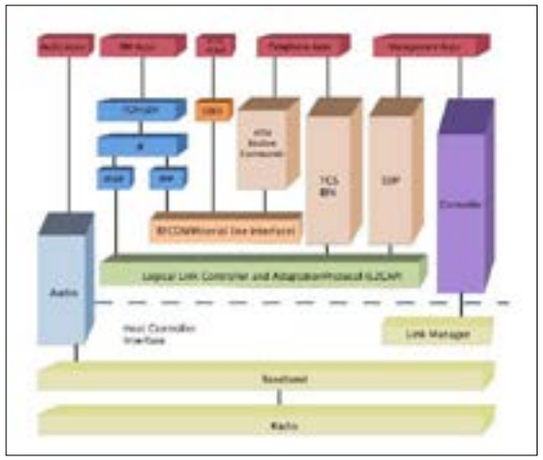

Figure 2. Architecture of Bluetooth

link manager for receiving status information. Protocol types are initially identified in logical link control and adaptation protocol (L2CAP). It provides connection-oriented and connectionless data services to host protocols above the L2CAP. Radio frequency communication protocol (RFCOMM) let upper layer protocols to communicate over a wired interface. So that applications do not need to know anything about Bluetooth. Service discovery protocol (SDP) uses to detect available services (Haartsen, 1998).

C. Bluetooth

Bluetooth is a wireless system that uses radio waves to communicate. It is a standard for the short-range wireless interconnection of devices such as mobile phones, computers, and electronic devices. The range of Bluetooth is 1 to 24Mbps (depends on version). The range of area is 30m. Bluetooth requires high power consumption. This is unsuitable for continuous medical monitoring applications (Bhagwat, 2001). Bluetooth is specially used in medical products such as Blood Glucose (BG) meters, Pulse oximeters, heart rate monitors and asthma inhalers.

1) Architecture of Bluetooth
When considering the architecture of the Bluetooth, it consists 2 layers: radio layer and base-band layer and 4 protocols: link manager protocol, logical link control and adaptation protocol, radio frequency communication protocol and service discovery protocol. These layers and protocols are connected via a host controller interface. All these functions run over the radio layer. Base-band layers work with the link manager to carry out the processes like creating link connections with the devices. Power saving

2) Bluetooth Law Energy (BLE)
Bluetooth Low Energy (BLE) is a feature which comes along with the Bluetooth version 4.0. The purpose of using BLE in healthcare systems is transmitting very small packets of data at a time while consuming less power. It is enabling Bluetooth smart devices to operate for months or even years. Because Bluetooth cannot use for continuous monitoring systems. BLE can be used for wireless devices to monitor and send medical information from biomedical sensors to smart-phones.

This technology has reduced the power and cost than Bluetooth. The range of the BLE is 15 to 30m. Bandwidth is 1Mbps (four times than ZigBee). But BLE is still an unproven technology. BLE implementation has 2 types such as single mode and dual-mode.

D. Radio Frequency Identification (RFID)

RFID is using together with the wireless sensor network in healthcare devices, especially for monitoring systems. These sensors are using to monitor physical or environmental conditions such as temperature, sound, vibration, pressure, humidity. Motion or pollutants at different locations.

Together RFID and wireless sensor network can use for remote monitoring of patients at home, collecting information such as blood pressure, heart rate, temperature, glucose level, analysing and making decisions. When trying to read RFID tags metals and liquids can cause problems if devices are in the vicinity of the distribution centers such as forklifts and walkies-talkies interruption may occur (Ajami, 2013). Use of the RFID in the healthcare industry alone will be faced with various issues.

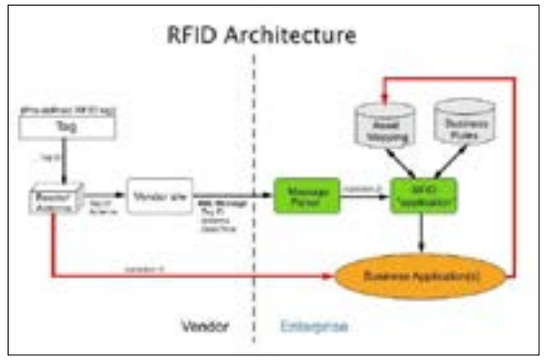

Figure 3. Architecture of RFID

Initially, item-tags are scanned by the Reader. Secondly, back-end transmitted data which are coming from an antenna. The signals are coming as RF waves. They have been recognized by the RFID-based system. The system acts as a middleware communication gateway among items, Reader, and the Databases. In the final step, it filters out and stores data in databases for checking the data faults and relevant operations.

E. Wireless Sensor Network (WSN)

A wireless sensor network (WSN) is a network which consists by a large number of sensor nodes where each node is equipped with a sensor to detect physical environmental things such as pressure, temperature, light, pH value. Today WSNs include sensor nodes, actuator nodes, gateways, and clients. The number of sensor nodes is deployed randomly inside of or near the monitoring area assuming the sensor nodes transfer the collected data to one another. During this transmission process to get to the gateway node, monitored data may be handled by multiple nodes. After multi-hopping, finally, it reaches the management (main) node through the internet or satellite (Gavrilovska, 2010). The one who handles the management node is publishing monitoring missions and collected monitored data.

Table 1. Technology comparison

Technology	State	Range (m)	Current rate	Bandwidth (Mbps)	Sharing			
					Data	Audio	Video	Voice
Wi-Fi	no	32	M	11	Y	Y	Y	VoI P
Zigbee	yes	100	-	0.2 5	N	N	N	N
Blueto oth	no	10-100	M	0.8	Y	Y	N	N
BLE	yes	15-30	-	1	N	N	N	N
RFID	no	1	L	1-11	-	-	-	-

Medium – M Large – L Yes -Y No - N

As other technologies, WSN also has security issues. Hackers can easily hack the network because WSN is working with nodes, they need to be charged at regular

intervals. So, the battery life of the nodes may very low. Like Wi-Fi and ZigBee, this technology also has low communication speed. And also, wireless sensor networks keep distracting from other wireless devices.

F. Cloud Computing

Cloud computing is widely used for delivering the applications over the internet as services. It is rooted in the internet search engine platform. It is an elastic resource which is scaled up or down effectively and efficiently. Also, a metered service so that consumers can pay only for what they use. There are three kinds of services in cloud computing such as IaaS (Infrastructure as a service), SaaS (Software as a service), PaaS (Platform as a service) (Armbrust, 2009). In the healthcare industry, cloud computing is used for population health management, care management and diagnostic, image handling services and laboratory services.

G. Global Positioning System

Global Positioning System(GPS) is a satellite-based navigation system which made up of at least 24 satellites. By using GPS tracking systems, that will make it easier for law enforcement to recover stolen property. When using GPS on a battery operated medical devices, there may be a battery failure and may need an external power supply which is not always possible. Also, in some cases, the GPS signals are not accurate due to some obstacles to the signals such as buildings, trees and sometimes by extreme atmospheric conditions such as geomagnetic storms.

III. IDENTIFIED CHALLENGES OF IOMT TECHNOLOGIES

Considering the above discussed technologies, five common problems were identified as follows,

i. Security issues
ii. Privacy challenges
iii. Limited processing power
iv. Limited data storage
v. Data integrity issues

A. Security Issues

As a growing number and variety of connected devices are introduced onto IoT (Internet of Things)-generation, the potential security threats are increased. IoT improves the quality of people's lives but also increases the potential attack surfaces for hackers and other cyber criminals. With the increase in the need for mobile systems, the current electronic market has also been filled with tabs, RFID devices, healthcare devices, laptops and many Wi-Fi enabled decides. Thus, the security of wireless networks such as Wi-Fi, Bluetooth, RFID, Zigbee has been increased. These wireless networks are prone to various attacks. The main reason for these security issues is that the wireless networks are open networks (Karygiannis, 2002). Most common security issues are,

i. Attack by hackers
ii. Intruders come into the network
iii. Data theft
iv. Virus attacks
v. Trojans and malware passed from one end-device to another
vi. Expose sensitive information to the open world

Security of wireless networks against such vicious attacks becomes the priority for the network industry. This is because not all networks are equally secure. The security depends on what security methods are used in the network, where and how this network is being used.

B. Privacy Challenges

There are privacy concerns in the wireless networks. The data transmitting in the wireless networks must be encrypted end-to-end device. If there is not proper encryption over the wireless network, sensitive data can be exposed to the outer world. The data that transmitting over the wireless networks should be stored securely, or else intruders and unauthorized persons can access the data, thus compromising the privacy of the users. Also, in actions like wireless hacking or some malicious attacks, if the sensitive information like patient records, patient contact details, payment information, history records, user identity, etc. are exposed or stolen, the privacy and confidentiality will be compromised.

C. Processing Power

Considering the transmission speed of the above technologies, Wi-Fi, Bluetooth, ZigBee, RFID, and WSN have a low rate of data transmission. ZigBee takes time to send a set of data by up to four times compared to other mentioned technologies. Most of these technologies access to the internet using access point (AP). However, the system has a difficulty of communication due to the traffic overload caused by communication through AP. (Jin, 1--2)

D. Data Storage Issue

Data storing is a very important fact in the healthcare sector. Because, the medical data are sensitive and confidential, hence the enhancements to privacy and security should be required. Most of the medical applications use local databases and management systems to store their data. It is easy for the third-party attackers to enter the systems. So that, Security and privacy enabled cloud-based systems are encouraged to use in the healthcare sector.

E. Data Integrity

Data integration in healthcare is about collecting, auditing and monitoring data. It goes beyond simple reporting of an organizational performance. It is not a simple task to integrate all the patient medical records universally. So that, there is a necessity for a method to integrate the data in an effective and efficient manner.

IV. CRITICAL TECHNOLOGY ISSUES FOR IOT BASED MEDICAL DEVICES IN HOSPITALS

A. Lacking medical device control

Healthcare device adoption simply indicates the growth of Machine-To-Machine (M2M) and Machine-To-People (M2P) automation. With such progress of medicinal workflow, IT functions have to focus beyond continuous connectivity with key applications and clinical employees. For each healthcare devices on the network, there is an application data flow between application and the system.

Variableness into medical device connectivity, locations, capabilities, as well as designs of activity is essential for optimizing medical care. Also, this is important for optimizing the infrastructure and for both of those short- and long-term planning for medical device automation.

B. Managing device diversity and interoperability

There are a number of healthcare devices are using in the medical field for different reasons. So that, healthcare stakeholders have to manage the different devices according to the different situations which create the need for technology experts in hospitals and medical centers. So before using medical devices they can give a training to the stakeholders who are going to use the device so that they can reduce the number of mistakes can happen. Not like normal mobile healthcare applications, there are huge devices like ECG monitoring devices, IoT based medical healthcare monitoring systems, ubiquitous medical healthcare systems.

C. Need of medical expertise

For some advanced medical devices, they need expertise in that area. In that case, the number of healthcare stakeholders can be reduced. So that it will optimize the flexibility of the device.

D. Hardware implementation issues

Hardware implementation part is the costliest in the healthcare domain. There are a number of sides in implementation they have to think like there are sensor-based devices, scanning devices which should have best quality materials, technology for hardware implementation, facilities to use those technologies, experiments, different conditions to use those devices in hospitals.

V. CONCEPTUAL MODEL

In this research, it has proposed a model for overcoming these issues in those technologies that are used in many healthcare applications and systems. In this proposed model, it uses Cloud Computing as a method to solve the storage capacity and processing power issues. And then to address the privacy issues, the proposed model is using a method called Attribute-based encryption (ABE). To overcome the security issues, the proposed model uses the Advanced Encryption Standard (AES) to encrypt the data before sending and storing in the cloud. And finally, to ensure the data integrity of the medical data that are collected from those technologies, the proposed model is using a method called Provable Data Possession (PDP).

Figure 4. Proposed conceptual model

VI. ABOUT THE ALGORITHM

The algorithm that implemented to overcome the data integrity, security and privacy issues in cloud computing has five main parts.

i. Advanced Encryption Standard (AES) Encryption
ii. Attribute-base Encryption (ABE) Encryption
iii. Advanced Encryption Standard (AES) Decryption
iv. Attribute-base Encryption (ABE) Decryption
v. Provable Data Possession (PDP)

The figure 3 illustrates the proposed security mechanism. In the first part of the algorithm, the data (text, image, sound, video and etc.) is encrypted using a symmetric cipher the Advanced Encryption Standard (AES). Then, the encryption of files is created using AES and generate AES-key. In this process, the AES encryption security level will take according to the specified security level in the algorithm which can be minimum (128 bits), medium (192 bits) or high (256 bits).

After encrypting the data and generating both the AES key and asymmetric cipher of the raw data using the AES encryption algorithm, this AES-key is used to the ABE Encryption. The AES-key is protected using ABE encryption. Here, we are using the CP-ABE (Ciphertext-Policy Attribute-Based Encryption. CP-ABE uses different pairing constructions to match the AES security levels of 128, 192 and 256-bits. In the CP-ABE encryption method, the data have associated with a set of attributes defined by the user. This creates an access structure policy for the encrypted data. The encrypted data is defined by a set of

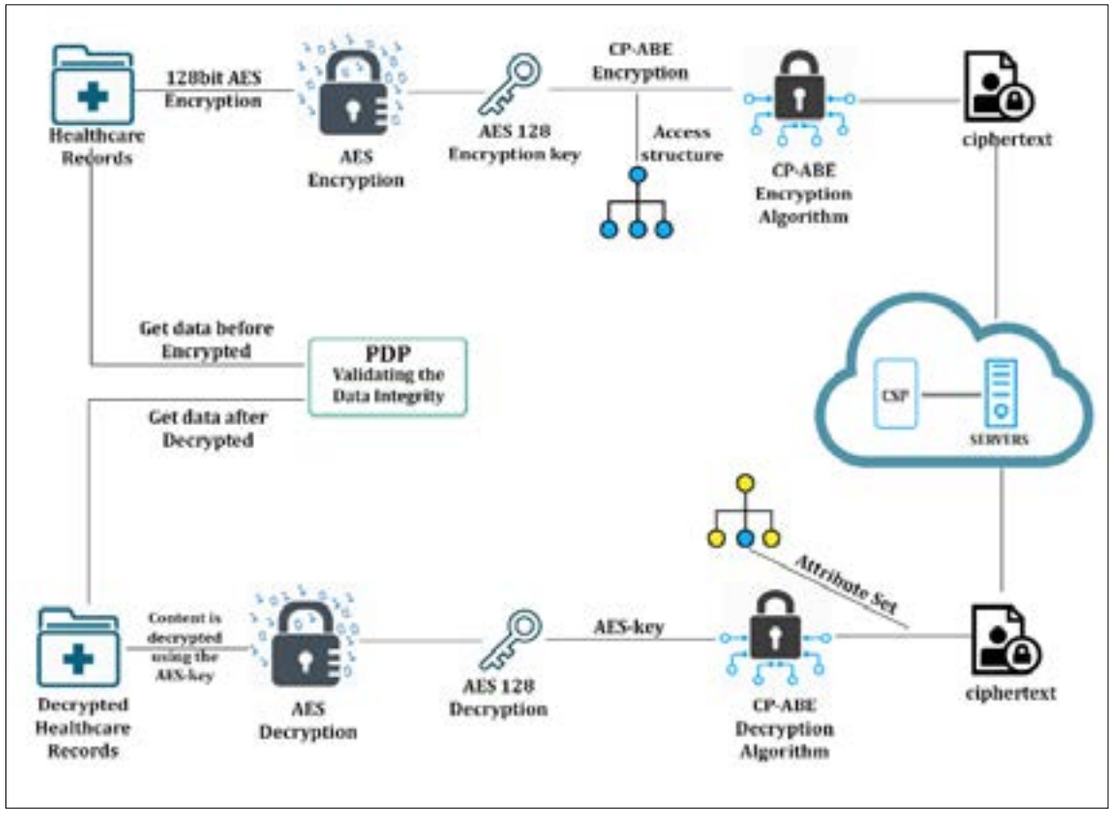

Figure 5. Proposed Security Mechanism

attributes, and access rule contained in the user's private key. If a set of attributes of data matches the structure of access to the user's private key, the data can be decrypted. After that, encrypted data will go to the cloud.

Once encryption is performed, the encrypted data (with AES) together with the encrypted AES-key (with CP-ABE) can be securely distributed over insecure networks or stored in an honest but curious untrusted third party (i.e. Cloud storage provider). Thus, the algorithm allows to achieving confidentiality and CP-ABE enable fine-grained control access mechanisms.

When decryption is performed, the AES-key is first decrypted using the ABE decryption key that matches the encryption policy. Then the content is decrypted using that AES-key. Only those authorized entities with a valid set of attributes could decrypt and recover the AES-key to launch the AES decryption process over the encrypted data. Under this solution approach, typical applications as securing digital medical records or storing and sharing of digital documents in the Cloud could be easily implemented.

Finally, the PDP method ensures the data integrity of the files that encrypted using the AES and ABE. This method enables a user to verify that the server possesses his data, without retrieving the entire data. Inside this method, it checks and validates whether the input raw data correctly store to the cloud and kept by comparing the encrypted stored data in the cloud a raw input data.

VII. CONCLUSION

The Internet of Medical Things (IoMT) is changing day by day. The world needs to prepare than with a value-based care. With the rapid growth of the IoMT the vulnerabilities of healthcare devices also increasing

day by day. This paper provides an overview of the IoT technologies, the key challenges in the healthcare sector and an adaptive solution to preventing the identified issues. There are five key challenges such as Data integrity, Security, Privacy, Storage issues and Processing power issues. The proposed model consists of 2 security methods such as Attribute-based Encryption (ABE) and Advanced Encryption Standard (AES) along with the data integrity method called Provable Data Possession (PDP). For the future work, it needs to enhance the effectiveness of the methods, as to deliver convenient usage to medical stakeholders. Further, we will look to use Artificial Intelligence-based encryption cryptography algorithms such as Neural cryptography to achieve more robust and efficient encryptions for data security and privacy of the healthcare organizations.

ACKNOWLEDGEMENT

This research is supported by Department of Computing & Information Systems, Sabaragamuwa University of Sri Lanka. And I am grateful to my supervisor Dr.(Mrs) M. S. Karunarathne for her immense support and guidance. I would like to thank my parents and friends who supported me to complete this research successfully.

REFERENCES

Ahamed, S., 2009. THE ROLE OF ZIGBEE TECHNOLOGY IN FUTURE DATA COMMUNICATION SYSTEM.. *Journal of Theoretical \& Applied Information Technology*, Volume 5.

Ajami, S. a. R. A., 2013. Radio Frequency Identification (RFID) technology and patient safety. *Journal of research in medical sciences: the official journal of Isfahan University of Medical Sciences*, p. 809.

Alliance., Z., 2006. ZigBee Security Specification Overview. *ZigBee Alliance. Wireless Control That Simply Works.*

Armbrust, M. a. F. A. a. G. R. a. J. A. D. a. K. R. H. a. K. A. a. L. G. a. P. D. A. a. R. A. a. S. I. a. o., 2009. *Above the clouds: A berkeley view of cloud computing*, s.l.: Technical Report UCB/EECS-2009-28, EECS Department, University of California, Berkeley.

Bhagwat, P., 2001. Bluetooth: technology for short-range wireless apps. *IEEE Internet Computing*, pp. 96--103.

Cordeiro, C. a. A. D. a. P. M., 2010. IEEE 802.11 ad: Introduction and performance evaluation of the first multi-Gbps WiFi technology. In: *Proceedings of the 2010 ACM international workshop on mmWave communications:* from circuits to networks. s.l.:s.n., pp. 3--8.

Gavrilovska, L. a. K. S. a. M. V. a. S. I. a. T. R., 2010. Application and multidisciplinary aspects of wireless sensor networks: concepts, integration, and case studies. In: s.l.:Springer Science \& Business Media.

Haartsen, J. a. N. M. a. I. J. a. J. O. J. a. A. W., 1998. Bluetooth: Vision, goals, and architecture. *ACM SIGMOBILE Mobile Computing and Communications Review*, pp. 38--45.

Horowitz, M. D. a. R. J. A. a. J. C. A., 2007. Medical tourism: globalization of the healthcare marketplace. *Medscape General Medicine*, p. 33.

Jin, C. a. C. J.-W. a. K. W.-S. a. Y. S., 1--2. Wi-Fi Direct data transmission for wireless medical devices. In: *Consumer Electronics (ISCE 2014), The 18th IEEE International Symposium on.* s.l.:s.n., p. 2004.

Kanwar, A. a. K. A., 2012. ZigBee: The new bluetooth technology. *ZigBee: The new bluetooth technology*, pp. 2319--7242.

Karygiannis, T. a. O. L., 2002. Wireless network security. *NIST special publication*, Volume 800, p. 48.

Li, J. a. Z. X. a. T. N. a. S. J., 2010. Study on ZigBee network architecture and routing algorithm. In: *Signal Processing Systems (ICSPS), 2010 2nd International Conference on.* s.l.:s.n., pp. 382--389.

Wells, J., 2009. Faster than fiber: The future of multi-G/s wireless. *IEEE microwave magazine*, Volume 10.