Scenario-based Vulnerability Analysis in IoT-based Patient Monitoring System

Neila Mekki[1], Mohamed Hamdi[2], Taoufik Aguili[1] and Tai-Hoon Kim[3]

[1] *CommunicationsSystems Laboratory, (SysCom), National Engineering School of Tunis, (ENIT), University of Tunis El Manar, (UTM), Tunisia*

[2] *Elgazala Technopark, Higher School of Communication of Tunis, Sup'Com, University of Carthage, Tunisia*

[3] *School of Information Science, University of Tasmania, Australia*

Keywords: Healthcare, Internet of Things, Scenario, Security Requirements.

Abstract: The Internet of Things (IoT) is one of the revolutionary technologies for healthcare. However, this flourishing still faces too many challenges including security and privacy preservation information. To address these problems, our contribution is to present a scenario of diabetes disease assume a matching between the situation of the patient and the relevant data from monitoring point view. This scenario describes how a patient can collect enormous of vital sign and activity. Wireless Body Sensor Networks (WBSN) is one of the IoT building blocks in which a patient can be monitored using a collection of sensor nodes to improve the patients quality of life. This technology in healthcare applications should not ignore security requirements. The aim of this paper is, (1) to design a healthcare architecture for a patient monitoring system, and (2) to explore the major security requirements in WBSN.

1 INTRODUCTION

Today the number of people with chronic diseases such as diabetes, cardiovascular diseases, and hypertension is growing exponentially according to the World Health Organisation (WHO, 2017). This is due to sedentary lifestyle and different risk factors such as unhealthy diet, physical inactivity, tobacco, alcohol consumption, and oxidative stress. It is said (WHO, 2016) that diabetes is considered to be one of a major cause of stroke, blindness, heart attacks, kidney failure, and lower-limb amputation. It will be the 7^{th} leading cause of death by 2030.

However, diabetes can be actively treated and monitored if an early diagnosis is available. Such as for many years, the only standard exams consisted of measuring the glucose level in the health center. Thanks to technology, it is possible today with a variety sensor to read vital signs such as heart rate monitor and blood pressure to take the patient with their vital sign daily. The main challenge is to detect chronic diseases early enough to implement efficient mechanism.

Now, according to (Islam et al., 2015) and (Al-Fuqaha et al., 2015), Internet of Things (IoT) is expected to be a potential alternative to cope with this serve. It provides a dynamic environment in which anything can be able to communicate with other in anywhere and at any time.

Such as Wireless Body Sensor Networks (WBSN), (Gope and Hwang, 2016) is one of the most commonly-used technologies in IoT-based healthcare systems. It is used to collect a human body function and also surrounding environment.

However, in transit and stored data in healthcare application, an attacker for example (Huang et al., 2017) can be damage health devices or services by providing a wrong information or remove integrity data. Therefore, the challenge is to identify and predict all possible attacks and vulnerabilities associated to IoT in a healthcare application. To deal with this challenge our major contribution is organized as follows:

- To propose a new IoT healthcare monitoring architecture, by allowing distributed security strategy.
- To describe the interaction between various actors and patient monitoring system based IoT, in which the patient is generated heterogeneous data based WBSN deployed in this ambient environment. This methodology is proposed to identify

Mekki, N., Hamdi, M., Aguili, T. and Kim, T-H.
Scenario-based Vulnerability Analysis in IoT-based Patient Monitoring System.
DOI: 10.5220/0006473005540559
In *Proceedings of the 14th International Joint Conference on e-Business and Telecommunications (ICETE 2017) - Volume 4: SECRYPT*, pages 554-559
ISBN: 978-989-758-259-2

the typology of the data collected from the patients environment based on a scenario-based approach.

- To evaluate the security requirements according to time is thoroughly studied. The importance of our scenario can be used to implement context-aware techniques in WBSN-based healthcare solutions.

Therefore this paper is organized as follows. After the introduction, we give and specify in Section 2 a new healthcare architecture for the patient monitoring system. In Section 3, we present a scenario of a diabetic patient in which we identify the security requirements. Finally, we provide concluding remarks and future prospects in Section 4.

2 PROPOSED ARCHITECTURES

From the literature (Al-Fuqaha et al., 2015), (Islam et al., 2015) we can distinguish that a general architecture IoT can basically consist of three layers, perception layer, network layer, and application layer.

In this sense, our main contribution in revising the literature is to present a new healthcare architecture for IoT, which describes how a patient can collect enormous of vital sign and activity. We explain also how doctors can remotely use the patient monitoring system to the remote. For that, we can find a lot of possibilities to improve the security for IoT Architectures in health context such as (Valera et al., 2010), (Hassanalieragh et al., 2015), (Catarinucci et al., 2015), and (Horn et al., 2016). However, most of the proposed architecture are over to focus in only one building blocks in WBSN, Gateway, or cloud. The challenge is to propose a new architecture, for IoT vulnerability following in each step.

Therefore, our healthcare system architecture as shown in Figure 1 consists of three building blocks.

- A perception layer: to collect a physiological state and movement context, by using Wireless Body Sensor Network (WBSN).
- Network layer: to transmit data to the remote center, by using Smart Health Gateway.
- Application layer: to explain a good decision or to monitoring information. While data mining (Chun-Wei Tsai and Yang, 2014) and machine learning (Abu Alsheikh et al., 2014) can be used to provide smart services IoT, this lies outside the scope of this paper.

The goal of the research is to design the embedded security framework for IoT and to model the jamming attack and design the defensive technique for Wireless Sensor Network (WSN)-based IoT. Our contribution is inspired us to propose a scenario to collect and monitor the workout routines measurement according to diabetes disease patient up at 7:00 in a section below.

3 SCENARIO DIABETIC PATIENT IN IOT HEALTHCARE

In this section, we focus on describing the scenario a healthcare application IoT, in which a patients health profile and vital signs are captured sensor attached to his or her body as shown in Figure 2.

The sensor will also be used to collect somatic data as the reference to monitor their conditions such as eating and others risk factors, such as Weight measuring, Blood glucose (sugar), Electrocardiogram (ECG), and Heartbeat rate.

It is important at this level to mention that, diabetes is a metabolic disease in which patient have a high blood glucose (sugar) level over prolonged period. In a normal subject, the fasting blood glucose level is about 1g/l.

Moreover, we assume that a person needs to move from one context to others. Different means of transportation are generally available to include walking, public transport, and vehicle transport.

Our contribution is twofold. We provide a matching between the situation of the patient (i.e., step in the scenario) and the relevant data from the monitoring point of view. Second, we associate a set of security requirements to each of the data a set too.

The result is very important from the adaptive security prospection since we provide a set of requirements on which dynamic security techniques can be built to while taking into consideration the variation of the security requirements.

3.1 Narrative Scenario Remote Diabetic Patient Monitoring

In this section, we develop a scenario of patient monitoring medical data to remote healthcare center, a find to implement the context-aware technique in WBSN based healthcare solutions. According to, (Viswanathan et al., 2012), and (Islam et al., 2015)) less research challenge over context-aware has been developed. And our challenge is inspired us to explain a good decision to devise healthcare solution into three generic level:

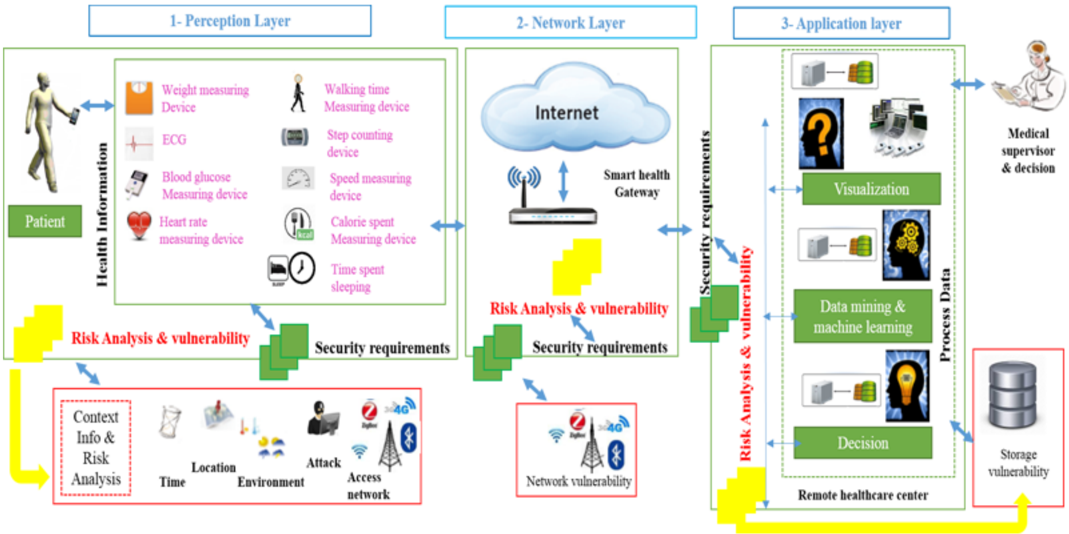

Figure 1: Proposed Adaptive architecture Remote healthcare IoT.

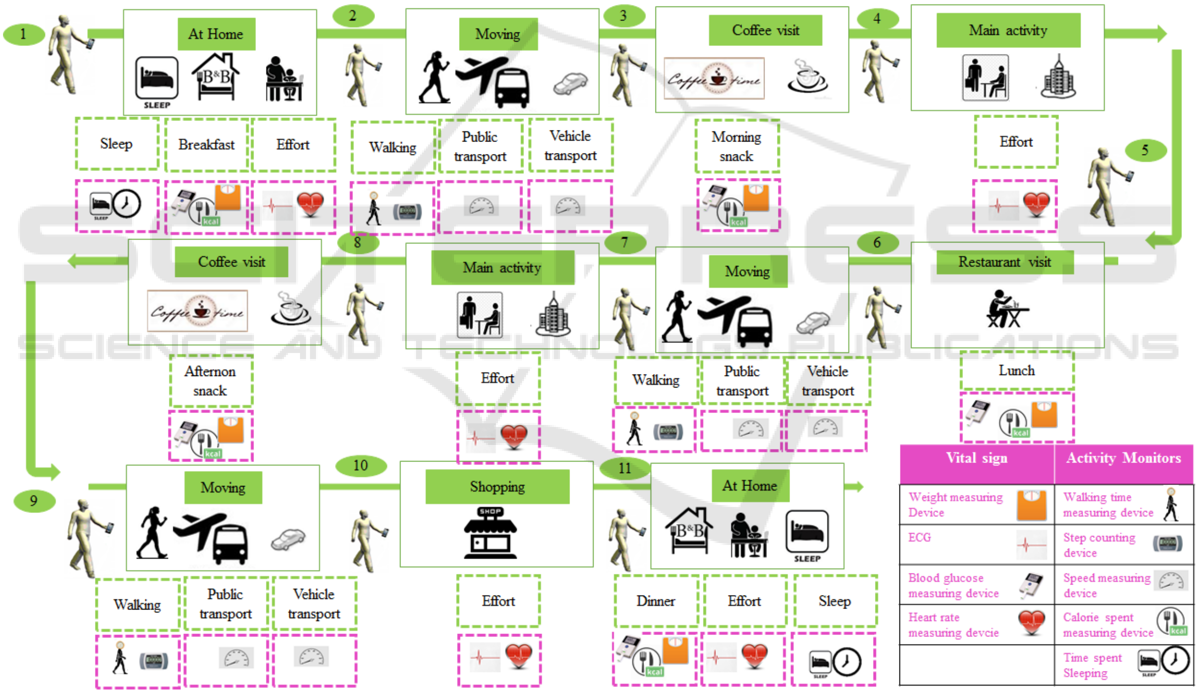

Figure 2: Scenario diabetes disease.

- The context of the patient: at home, moving, coffee visit, main activity, restaurant visit, and shopping.
- The activity monitoring: sleeping, eating, walking, moving.
- Information capture: blood glucose, weight measuring device, ECG, heartbeat rate measuring devices, time spent of sleeping, walking time measuring device, step counting devices, speed measurement device, calorie spent measuring devices.

A brief description of core scenario is given as follows:

At Home. WBSN is used to monitor the patient at home. This scenario includes some other sub-scenarios such as sleeping, eating (breakfast or dinner) or others household activity (effort). For each sub-scenario, the objective is to monitor the patient.

Moving. The patient can be moving from one context to other by walking, using public transport or his or her vehicle transport.

Coffee Visit or Restaurant Visit. The patient may visit a coffee or restaurant.

Shopping the patient visits the market to buy various goals.

3.2 Security Requirements Remote Diabetic Patient Monitoring

The challenge at this terms is to ensure security requirements diabetes disease. A features component, security requirements based (Islam et al., 2015) are described as following:

- Confidentiality: has to ensure the inaccessibility of medical information for unauthorized users.
- Integrity: has to ensure that received medical data are not altered in transit by an adversary.
- Authentication: has to enable an IoT health device to verify the identity of the peer with which it is communicating.
- Availability: has to ensure the availability of IoT healthcare services to authorized parties when needed even under denial-of-service attacks.
- Data freshness: has to associate exchanged data to a specific session.
- Non-repudiation: has to prove that an action has been performed by an entity.
- Authorization: has to ensure that only authorized nodes can access services or resources.
- Data Privacy: has to ensure that only authorized person that allow specific a purpose of sharing can access to information.
- Resiliency: has to guarantee that if a set of entities are compromised then a security scheme should still protect the network, device or information from any attack.
- Fault tolerance: has to guarantee that a security scheme should continue to provide respective security services even in the presence of a fault.

In this sense, our objective is to evaluate the security requirement and to implement resilient security. It can be divided into two steps: Security requirements depending on information nature, and Security requirements depending on the context. In this sub-section below, we describe as following these two categories.

3.2.1 Security Requirements Depending on Information Nature

It depends on sensors or activity used to monitor to interact patient shown in Table 1.

To be more specific we address two categories:

To Monitor Chronic Disease Management such as cardiovascular and diabetes. It involves the lifestyle of the patient via continuous monitoring. The sensor used in this case include ECG sensor, blood glucose sensor, heartbeat rate sensor. These sensors should respect some requirements, case to people with diabetes will be considered a higher risk compared to non-diabetics for insurance companies. Such as they should pay more. It requires protecting content from eavesdroppers, which aims to ensure inaccessibility information for unauthorized users.Moreover, the modification of vital information can cause very dangerous case, in which can resist a false alert and false information or no alarm. So, the system should diving attackers based on replay such as the submission of alarm messages related to previous sessions.

To Monitor Personal Health and Fitness Management such as the system monitor a patient who is self-motivated and takes steps to stay healthy and fit. This provides some consequent avoid by regular screening applied by monitoring application and appropriate treatment. For this type, the objective is to continuous remote monitoring patient to improve the quality life, which can define some security requirements. Our objective is to find and ensure availability and efficient information. In this sense, a goal is to counteract his or her activity a find to collect human body function (weight measuring device, and activity monitors) such as eating, walking and moving. In order to integrate this functionality, the challenge is to respect requirements security. In such case, a solution is to assure these two major requirements authentication and availability a find to secure communication. There are the two most important requirements in any IoT. A find to assure identify patient and respect requirement availability of information at anytime and anyplace. However, for another requirement, the impact factor of not respect can be treated as function as to impact factor attacker and if the patient should respect or not.

Table 1: Information Nature Security Requirements.

Requirement	Blood glucose	Weight measuring device	ECG	Heart beat rate measuring device	time spent of sleeping	walking time measuring device	step counting device	speed measuring device	calorie spent measuring device
Confidentiality	+	-	+	+	-	-	-	-	-
Integrity	+	-	+	+	-	-	-	-	-
Authentication	+	+	+	+	+	+	+	+	+
Availability	+	+	+	+	+	+	+	+	+
Data freshness	+	-	+	+	-	-	-	-	-
Non-repudiation	-	-	-	-	-	-	-	-	-
Authorization	+	-	+	+	-	-	-	-	-
Data privacy	+	-	+	+	-	-	-	-	-
Resiliency	+	-	+	+	-	-	-	-	-
Fault tolearance	-	-	-	-	-	-	-	-	-

3.2.2 Security Requirements Depending On The Context

The patient in nature didn't have the static place. For example, he or she moves from home to another provider. In this case, different networks have different security configurations and settings.

Such as, when patient walking or moving by public transport or vehicle transport many other people, the neighbourhood can intercept by the active or passive attack. This attack can be potential affect patient in which depends on user class patient. For example, political user has a higher potential attack compares to the simple user. So, the other problem that can be allowed is what is the solution when the connectivity is not possible.

The challenge is to ensure availability information at anytime and at anyplace, to allow security requirements resist to various threat and attack that can modify, impersonation and eavesdropping or be replaying information. The challenge is to ensure availability information at anytime and at anyplace, to allow security requirements resist to various threat and attack that can modify, impersonation and eavesdropping or be replaying information.

Therefore, developing mobility security requirements can be a serious challenge. According to the Table 2, the context can be divided into six categories: at home, moving, coffee visit, main activity, restaurant visit, and shopping. Therefore for each category, they can be classified into four other categories that involved as following:

- Time: Refers to the specific period in which the patient interacts with the system to monitor an activity of workouts routines or measuring some diseases. It constant supervision by vital sign monitors or activity monitors.
- Neighborhood: Depends on environment patient and other people can intercept by the active or passive attack.
- User Class: Depends user class patient such as a political user or a simple user.
- Access Network: Depends on to the location of the patient in or out home. The system should be able to ensure the availability information.

Due to the sensitive nature of the sensor, WBSN could be easily replayed by the adversary. In this case, we need to ensure minimize security threats as following: Confidentiality, Authorization, Integrity, Resiliency, Authentication, Availability, Data freshness, and Data privacy. So, the other problem that can be allowed is what is the solution when the connectivity is not possible.

Challenge Access Network. Wireless Body Sensor Networks was used to measuring blood glucose (BG) a find to monitor a diabetic patient in the different context of at home moving, coffee visit, main activity, restaurant visit, and shopping.

4 CONCLUSION

This paper proposed two major contributions are twofold. First, we proposed a design a healthcare application in IoT. Second, we discuss to identify the as-

Table 2: Context Security requirements.

Requirement	At home	Moving	Coffe visit	Main activity	Restaurant visit	Shopping
Confidentiality	+	+	+	+	+	+
Integrity	+	-	-	+	-	-
Authentication	+	+	+	+	+	+
Availability	+	+	+	+	+	+
Data freshness	+	+	+	+	+	+
Non-repudiation	-	-	-	-	-	-
Authorization	+	+	+	+	+	+
Data privacy	+	+	+	+	+	+
Resiliency	+	-	-	+	-	-
Fault tolearance	-	-	-	-	-	-

sociations between the varying vulnerabilities related to the data collected while a patient is operating in normal life and the security threats he or she is exposed to the major result consists in a mapping between the steps of the generic life scenario and the security requirements. This result is very useful of adaptive security approaches.

ACKNOWLEDGMENT

This research has collaborated with innovation centre (Elgazala technopark).

REFERENCES

Abu Alsheikh, M., Lin, S., Niyato, D., and Tan, H.-P. (2014). Machine learning in wireless sensor networks: Algorithms, strategies, and applications.

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., and Ayyash, M. (2015). Internet of things a survey on enabling technologies protocols and applications. In *IEEE Communications Surveys Tutorials*.

Catarinucci, L., Donno, D. d., Mainetti, L., Palano, L., Patrono, L., Stefanizzi, M. L., and Tarricone, L. (2015). An iot-aware architecture for smart healthcare systems.

Chun-Wei Tsai, Chin-Feng Lai, M.-C. C. and Yang, L. T. (2014). Data mining for internet of things: A survey,.

Gope, P. and Hwang, T. (2016). Bsn-care: A secure iot based modern healthcare system using body sensor network. In *IEEE Sensors Journal*.

Hassanalieragh, M., Page, A., Soyata, T., Sharma, G., Aktas, M., Mateos, G., Kantarci, B., and Andreescu, S. (2015). Health monitoring and management using internet-of-things (iot) sensing with cloud-based processing: Opportunities and challenges. In *IEEE International Conference on Services Computing,*.

Horn, G., Eliassen, F., Taherkordi, A., Venticinque, S., Martino, B. D., Bcher, M., and Wood, L. (2016). An architecture for using commodity devices and smart phones in health systems. In *IEEE Symposium on Computers and Communication (ISCC),*.

Huang, h., Gong, T., Ye, N., Wang, R., and Dou, Y. (2017). Private and securedmedical data transmission and analysis for wireless sensing healthcare system. In *IEEE Transactions on Industrial Informatics*.

Islam, S. M. R., Kwak, D., Kabir, M. H., Hossain, M., and Kwak, K. S. (2015). The internet of things for health care: A comprehensive surveys. In *IEEE Access*.

Valera, A. J. J., Zamora, M. A., and Skarmeta, A. F. G. (2010). An architecture based on internet of things to support mobility and security in medical environments. In *IEEE Consumer Communications and Networking Conference,*.

Viswanathan, H., Chen, B., and Pompili, D. (2012). Research challenges in computation, communication, and context awareness for ubiquitous healthcare.

WHO (2017). The global burden of chronic. In *Nutrition*. http://www.who.int/nutrition/topics/2_background/en/.

WHO (November 2016). Diabetes. In *Global report on diabetes*. http://www.who.int/mediacentre/factsheets/fs312/en/.