A Secure Emergency Framework in an IoT Based Patient Monitoring System

Neila Mekki[1], Mohamed Hamdi[2], Taoufik Aguili[1] and Tai-hoon Kim[3]
[1]*Communications Systems Laboratory ,(SysCom), National Engineering School of Tunis, (ENIT), University of Tunis El Manar, (UTM), Tunisia*
[2]*Cytekia, Higher School of Communication of Tunis, Sup'Com, University of Carthage, Tunisia*
[3]*School of Information Science, University of Tasmania, Australia*

Keywords: Internet of Things, Healthcare, Monitoring, Patient, Doctor, Diabetic, Security, Authentication.

Abstract: Today, the Internet of Things (IoT) in healthcare has become more productive to reduce the gap between doctors and patients. If any problem has occurred to the patient, then the doctor approaches the patient and gives the appropriate treatment. In this context, the main research question is how to identify the methodological choice (paradigm, approach, and method) in coherent with theoretical foundation of the Internet of things. Our objective is to involve better management of public IoT healthcare application by following a prevention methodology. To address this need, we adopt the design science research (DSR) methodology to implement a smart healthcare application. The ultimate goal is to enable the dynamic prediction and/or detection of the patient health deterioration, which taking into consideration the patient health evolution. So the prototyping process suggests some important factors to monitor and assist living diabetic patient at any time. The doctor have the ability to easily monitor and manage the patient health and can save precious minutes every day. Without having to manually visit each patient, the doctor can give a remote diagnosis and track the medical assets. To this purpose, we provides a theoretical contribution which the DSR assists in identifying an intelligent healthcare application based on IoT technology.

1 INTRODUCTION

The Internet of Things (IoT) is an emerging paradigm that enhance our everyday life through automation and optimization tasks related to transport healthcare domain, smart-home and smart-enterprise, and so forth. IoT is a huge network of things, which can recognize, manage, and control all kinds of objects around us through sensors and embedded devices. According to Gartner (Sallabi and Shuaib, 2016), in 2020, there will be 26 billion things for a market exceeding $300 billion. This new market has been invested by big companies, such as Samsung, Amazon or Google, that are developed things for the IoT and try to stay ahead concurrent by proposing emerging and innovative products.

However, the traffic monitoring system is prone to some cyberattacks. A malicious user may control a sensor to upload forged information to the system, which may cause traffic chaos.

In particular, we address those challenges in healthcare application context. Healthcare is among the fastest-growing domains since it affects the whole world population. A continuous monitoring and real-time communication of patients have always been the mean idea of smart healthcare services of cardiac (ren, 2018), Diabetes mellitus (Al-Taee et al., 2017), or respiratory problems (Mukhopadhyay et al., 2018).

Despite that security and privacy of client's data remain a tremendous challenge to address (Ida et al., 2016) (Sowmiya et al., 2016), the psychological and environmental factors interact in decision making and behavior (Alaiad and Zhou, 2017). Such as, psychosocial problems (Ferrer and Mendes, 2018) are most common in diabetes patients (Chew et al., 2014) that often result in serious negative impacts.

Additionally, our previous recherche works were done on describing the scenario a healthcare application (Mekki et al., 2017), solving the noise problem due to multiple sensor applied WBAN and providing an authentication protocol to correctly identify the communication requests from legitimate user (Mekki et al., 2018),(Mekki et al., 2023) .

For this purpose, our challenge is to allow a com-

Mekki, N., Hamdi, M., Aguili, T. and Kim, T.
A Secure Emergency Framework in an IoT Based Patient Monitoring System.
DOI: 10.5220/0012138400003555
In *Proceedings of the 20th International Conference on Security and Cryptography (SECRYPT 2023)*, pages 844-849
ISBN: 978-989-758-666-8; ISSN: 2184-7711

plete regroup hardware system that gives users control and check the existence of a threshold event invoked by a particular sensor (e.g ECG or blood glucose). However, a design model which gives users control and lets them check their physical condition by themselves was not yet mentioned.

Our contribution consists on how do we construct a secure protocol to achieve security between users and sensor nodes? Moreover, how do we transform data raw into cognitive knowledge information shared between IoT system components?

To answer those questions, we illustrate our methodology for a diabetic patient based on Design Science Research Methodology (DSRM)(March and Smith, 1995). The DSRM supports a research paradigm that calls the creation of innovative artifacts to solve real-life problems. We present the empirical study, which begins with researching the adequate methodology in coherence with research objectives and theoretical foundations.

Among others, the following components must be set:

- The key security requirements and challenges in IoT with a specific focus on healthcare applications.
- The balance between security and functionality by explaining our system model and methodology.

The ultimate goal of this methodology is providing a flexible smart IoT-based system able to perceive the collected data and provide decisions.

This paper is organized as follows. First in Section 2, we begin by some overview of exiting work in IoT for healthcare application. Second, in section 3, we propose our adaptive methodology a find to involve better management of public IoT healthcare application. Finally, concluding and future trends are drawn in Section 4.

2 RELATED WORK

In the past few years, IoT has become most productive in the area of healthcare, to improve the quality of care to the patient. Such as diabetes can be actively treated and monitored if an early diagnosis is available.

In this context, some contributions have addressed the focuses on developing an IoT healthcare system, in which are summarized in table 1 .

Compared to those previous researches, some of a prior studies did not adopt any sensors (Khan, 2020) (Rghioui et al., 2021), while some others studies using these sensor (Islam et al., 2023) technologies for collecting real-time data.

Different from all the previous researches, our contribution combine security requirement and DSR to monitor the diabetic patient.

Such as, **our challenge is to provide a secure emergency framework for healthcare application** , which include a biomedical sensors, an android interface for monitoring real-time sensor data, and a cloud infrastructure for processing the real-time data.

3 PROPOSED ADAPTIVE METHODOLOGY

In this section, we illustrate detailed information including the methodology of our system architecture for diabetic patient-based Design Science Research Methodology (March and Smith, 1995). Following the proposed methodology, we have combined emotion and Cognitive IoT for developing a flexible monitoring system. The research aims to create an artifact to support the decision making for smart healthcare framework. To build an artifact-based design science paradigm, we consider two basic activities: build and evaluate as follows respectively:

- Build: is the process of constructing an artifact for a specific purpose. We build an artifact to perform a specific task.
- Evaluate: is the development of criteria performance evaluation.

IoT methodologies can be divided into two categories: bottom-up approaches and top-down approaches.
The Bottom-Up Approaches: consist of selecting a priory the residual risk, i.e. the degree of protection of the system and implementing the countermeasures that allow reaching it.
The Top-Down Approaches: define scheduled tasks that are intended to reduce the identified threats.

Both development approaches use the same toolchain, and can thus be applied to best suit the needs of the particular feature development project. It is also possible to start development with the bottom-up approach and complete it with the top-down approach.

However, the challenge encountered while implementing our approach, is to achieve and maintain mobility without attacks or vulnerability. Besides, how the collected data are transformed into insights and interact with domain experts for better decisions.

We describe as our methodological contribution in coherence with some elements of qualitative approaches (case study and narrative analysis (Mekki et al., 2017)), to design and implement a monitoring system in IoT-Based on WBAN for a diabetic patient.

Table 1: Benchmarking overview of exiting work in IoT for healthcare.

Ref	Embedded platform	emergency alerts	Sensor
(Khan, 2020)	Client computer with IoT sensors	No	Not done
(Rghioui et al., 2021)	IoMT Based cloud infrastructure	No	Not done
(Islam et al., 2023)	Android Device with Iot wearable Device	Yes	Done

Our main focus is to equip the methodology with human cognition, which is capable of performing intelligent decision making independently.

These artifacts then become the object of the study. The methodology followed in our research is classified into four methods and activities, linked with the corresponding steps of the DSR approach. DSR artifact can include: Construct, Models, Method, and Instantiation.

3.1 Construct

Let's consider our smart IoT-based healthcare scenario, in which a medical IoT device publishes the physical condition (such as ECG or blood glucose) of a diabetic patient to a remote healthcare center periodically.

Despite their large deployment, security issues, mainly related to data privacy, are often considered as potential obstacles that might limit the extent of such solutions. Hence, the constructed artifact itself presents a challenge to explain how and why it works. Hence, the attacker blocks critical health information from being transmitted to physicians, threatening the life of the patient.

Context: In general, the IoT-base healthcare system collects sensitive data. The platform must ensure an adequate level of security to data access and management. At this stage, management analysis must clarify and define functional requirements and design constraints. Functional requirements define quality (how good), environment (know-that), availability (how often) and the procedural knowledge (know-how) to make decisions. To ensure such functionalities, the system should be able to understand the meaning of the received data and history as well as the disease management strategies to provide the right decisions.

Problem: If we consider deploying and activating all the monitoring processes for each patient, this requires increasing the cost. Moreover, hard coding of all rules causes maintainability problems. Besides, privacy is also a primary concern in the remote health monitoring system, as health data are highly relevant to the patient being monitored.

Solution: To deal with those challenges, our methodology design, are used to combine knowledge and security analyses. We defined within this methodology a set of (1) delineating the security dynamic coordination of the management processes to deal with the system's context changeability and (2) cognitive abilities to IoT-based systems to interact with the human through generating new insights and to solve problems as human do.

3.2 System Model

In this sub-section, we illustrate the system model of our case study of the diabetic patient. It is depicted by figure 1, which consists of: (i) a trusted domain with sensors and IoT devices under a single administrative domain (e.g. at home, or outside the home), and (ii) an untrusted domain connected via the public Internet, including the illegal user.

Note that we consider the application logic to be separate from its implementation: while the design of the application logic can be separately verified, vulnerabilities can still be introduced due to implementation bugs.

Proposing a system model for the patient monitoring system should take into account the key characteristics of IoT. The techniques should be asking enough to various context. Thus, the IoT system must have strong security guarantees.

We propose the bottom-up approach for verifying the security of the software stack in an IoT system, to provide a guarantee for how the software is secure.

We plan to verify the security of the actual (source and machine) code that will run on IoT devices. By bottom-up approach, we mean that the security of software needs to be established at every level of abstraction: at the OS (Operating System), implementation, and functional design levels.

Specifically, the choice of our methodology refers to a pluralistic methodological approach (case studies, architecture, and narratives approach).

As shown the figure 1, the arrow model presents the precedence relationship between the eight processes; denoted by 1- Context; 2-Activity monitoring; 3-Information Capture; 4-Vulnerability; 5-Threats; 6-Risk; 7-Reduces /Countermeasures; 8- Security requirements.

- 1-Context: It refers to the vast amount of information processing that normally takes place outside conscious awareness, even during sleep. Our methodology should be asking enough two motivating factors.

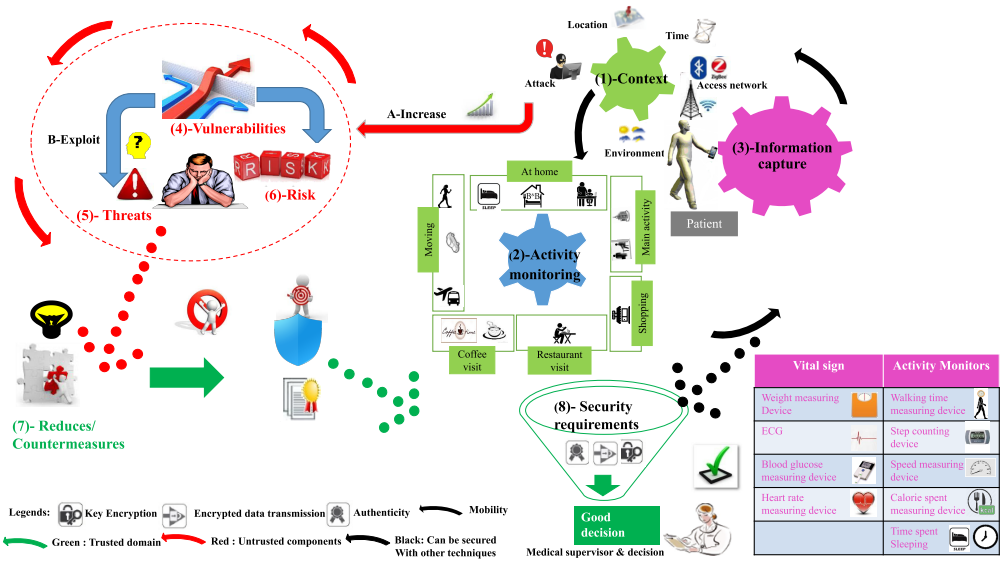

Figure 1: Proposed Adaptive methodologies Patient Monitoring System.

- Attack structure depends on context patient, time, environment and access network.
- The importance of security requirement may constitute countermeasure selection. For to this purpose, the key security requirement can be divided into two steps: Information nature security requirement, and context security requirement (As it has been introduced, in our previous works (Mekki et al., 2017)).

• 2-Activity monitoring: This process aims to monitor and to achieve a good decision patient over time. In this sense, our goal is to counteract his or her activity to collect human body function. It is a very important step, to understand what happened and devise response strategy. Therefore, it is the association between context and information capture. The monitoring of physical activity facilities the development of adaptive healthcare research. The real-time decision, based on which the future action is taken, is made by the cognitive module. The cognitive healthcare framework is sufficiently intelligent to make corresponding decisions. Thereafter, the cognitive system makes a real-time decision on the activities to be provided to patients based on their state. Such as patients living with diabetes are not constantly watched, like in a clinic or a hospital, but are managing their disease largely by themselves. Therefore, patients need to make best-individualized care decisions about the daily management of their diabetes. The objective is to adapt and personalize the lifestyle behaviors based on the collected data. More specifically, positive emotions, such as happiness, excitement, and contentment result in better health behaviors and improved adherence to treatment regimens

• 3-Information Capture: It is stimulated to measure and collect a physiological and movement by using wireless body area networks (WBAN).

• 4-Vulnerability: Weaknesses and security breaches of the analyzed system are identified at this level.

• 5-Threats: this process aims to identify the attacks that threaten the analyzed system. Unlike vulnerabilities, threats are measurable as each of them can be represented by its frequency and its severity. Threat rates and impacts depend on the environment.

• 6-Risk: This process aims to identify the risk that may threaten the asset of the analyzed system based on the identified vulnerabilities and threats. This process can be divided into the following steps:

  - Identify the global (main) attacks corresponding to the asset.
  - Build the attack scenario for every main attack.

• 7-Reduces /Countermeasures: It has been also demonstrated that security countermeasures can be viewed as the pseudo inverse of attacks concerning the composition law. These criteria may include:

  - The efficiency or the degree of protection
  - The feasibility of the countermeasure.

- 8-Security requirements: This process aims to react to security requirements to reduce attacks. The security requirements become an exigency to reduces and adapt the implementation of the countermeasure such as key encryption, encrypted data transmission, and authenticity.

Our model should implement cognitive capabilities that allow good decisions at the right time.

3.3 Method

In this section, we study methods to improve an emergency framework in an IoT based patient monitoring system. To make it possible, we propose to create a secure authentication in a given temporal and spatial environment of the subject's life. By using sensors, the data will be captured and compared with the predefined threshold. Our study focuses on blood glucose and heartbeat rate, thus in case of emergency notification will be sent to the doctor mobile.

Our challenge is to design the embedded security framework, by factors good performance, robustness to attacks and low energy consumption.

3.4 Instantiation

Designing an IoT-health system is a burdensome assignment because we should respect some key concerns such as:

- A providing authentication protocol to identify and authorize the communication requests from a legitimate user.
- Designing an authentication protocol to minimize the power consumption of the smart device (e.g. blood glucose).

To meet all the requirements and make software available as soon as possible, the software development for embedded the system often uses V-model. It enables also to perform tests at any time during the development of our healthcare application. Here, the development method influences the entire development, from requirements definition to software release. In the first step, is to meet all functional requirements but not yet the restrictions of the target hardware. Such as the functional requirement are checked using a model methodology based on a bottom-up approach.

In the next step, the function and the model are optimized for target two use cases of service analytic capabilities of our application inside or outside home.

However, the capability to perform software tests faster and more efficiently is of utmost importance to healthcare application. We plan to introduce a safety application and front-load more tasks to detect errors early.

In fact, we develop a Management Application (MA), is based PHP and Nginx web server easily configurable and accessible via a web browser. Specifically, an MA can receive and reply to any request, coming from the user, in JSON format. A MySql database, store the information retrieved from WBAN.

Our solution consists of two parts: the first part is the web service restful that run in the cloud accessible by the smart gateway. It was developed by using PHP and deployed on the Nginx server. The second part consists of an android application which acts as the client of our web service restful.

For those reasons, users (patients or doctors) need to be authenticated before the access to the platform, accessible via smartphone. such as the proposed model of a secure authentication protocol based on Restful approach for monitoring the diabetic patient has been already introduced in our previous work (Mekki et al., 2023).

Note That, these interfaces implement restful services, which allow the user to communicate with WBAN through the Smart Health Gateway (SHG). It offers two main functionalities depending on two possible users (patient or doctors) as shown in Figure 2.

Patient interface: it allows the patient to register to SAA. Furthermore, the patient can be equipped with a smartphone and running application, named MobiDiabetic, a customized Android Application with specific privilege access.

Doctor interface: it allows medical staff to register to SAA. Furthermore, doctors can be equipped with a smartphone and running the same healthcare Application, to check and interact with patient vital signs. Since the system collects sensitive and confidential data to ensure the adequate security level.

4 CONCLUSION

In this paper, we have exposed our methodology for the diabetic patient in IoT healthcare. We discuss the main process of our adaptive methodology. Our methodology is mainly guided by knowledge information carried by events and objects.

We emphasize describe the systems at multiple levels and from a variety of perspectives. such as we plan to validate our MobiDiabetic application through controlled evaluations taking into account the clinical environment, to assess its performance, reliability and safety by the nursing staff.

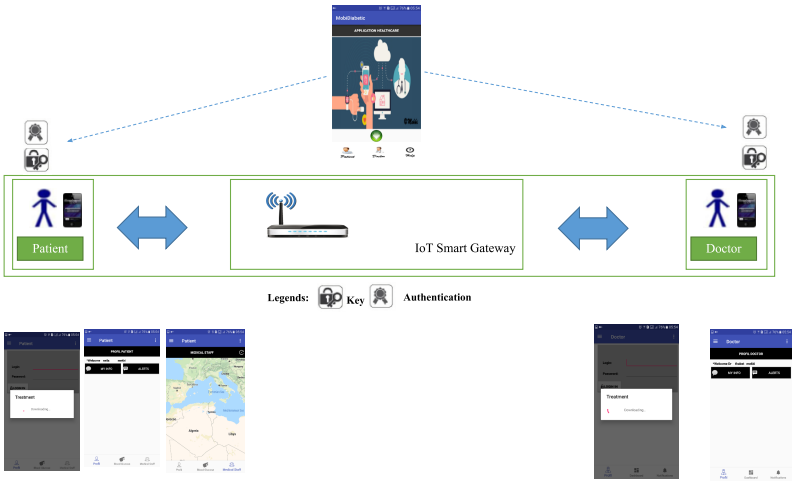

Figure 2: Users interface visualization.

REFERENCES

(2018). A Novel Cardiac Auscultation Monitoring System Based on Wireless Sensing for Healthcare. 6:1–12.

Al-Taee, M. A., Al-Nuaimy, W., Muhsin, Z. J., and Al-Ataby, A. (2017). Robot Assistant in Management of Diabetes in Children Based on the Internet of Things. *IEEE Internet of Things Journal*, 4(2):437–445.

Alaiad, A. and Zhou, L. (2017). Patients' Adoption of WSN-Based Smart Home Healthcare Systems: An Integrated Model of Facilitators and Barriers. *IEEE Transactions on Professional Communication*, 60(1):4–23.

Chew, B.-H., Shariff-Ghazali, S., and Fernandez, A. (2014). Psychological aspects of diabetes care: Effecting behavioral change in patients. *World Journal of Diabetes*, 5(6):796–808.

Ferrer, R. A. and Mendes, W. B. (2018). Emotion, health decision making, and health behaviour. *Psychology & Health*, 33(1):1–16.

Ida, I. B., Jemai, A., and Loukil, A. (2016). A survey on security of IoT in the context of eHealth and clouds. In *2016 11th International Design Test Symposium (IDT)*, pages 25–30.

Islam, M. N., Raiyan, K. R., Mitra, S., Mannan, M., Tasnim, T., Putul, A. O., and Mandol, A. B. (2023). Predictis: an IoT and machine learning-based system to predict risk level of cardio-vascular diseases. 23(1):171.

Khan, M. A. (2020). An IoT framework for heart disease prediction based on MDCNN classifier. 8:34717–34727. Conference Name: IEEE Access.

March, S. T. and Smith, G. F. (1995). Design and natural science research on information technology. *Decision Support Systems*, 15(4):251–266.

Mekki, N., Hamdi, M., Aguili, T., and Kim, T.-H. (2017). Scenario-based Vulnerability Analysis in IoT-based Patient Monitoring System. pages 554–559.

Mekki, N., Hamdi, M., Aguili, T., and Kim, T.-H. (2018). A Privacy-Preserving Scheme Using Chaos Theory for Wireless Body Area Network. In *2018 14th International Wireless Communications Mobile Computing Conference (IWCMC)*, pages 774–779.

Mekki, N., Hamdi, M., Aguili, T., and Kim, T.-H. (2023). An authentication protocol for healthcare application: A case study of a diabetic patient. pages 434–445.

Mukhopadhyay, B., Sharma, O., and Kar, S. (2018). IoT Based Wearable Knitted Fabric Respiratory Monitoring System. In *2018 IEEE SENSORS*, pages 1–4.

Rghioui, A., Naja, A., Mauri, J. L., and Oumnad, A. (2021). An IoT based diabetic patient monitoring system using machine learning and node MCU. 1743(1):012035. Publisher: IOP Publishing.

Sallabi, F. and Shuaib, K. (2016). Internet of things network management system architecture for smart healthcare. pages 165–170.

Sowmiya, E., Malathi, L., and Selvi, A. T. (2016). A Study on Security Issues in Healthcare Applications Using Medical Wireless Sensor Network and Iot. *Iioab Journal*, 7(9):575–583. WOS:000397199100004.