Computers, Materials & Continua
DOI:10.32604/cmc.2021.014090
Article

Tech Science Press

A Formal Testing Model for Operating Room Control System Using Internet of Things

Moez Krichen[1], Seifeddine Mechti[2], Roobaea Alroobaea[3], Elyes Said[4], Parminder Singh[5], Osamah Ibrahim Khalaf[6] and Mehedi Masud[3,*]

[1]Faculty of CSIT, AlBaha University, AlBaha, Saudi Arabia & ReDCAD Laboratory, Sfax University, Sfax, Tunisia
[2]MIRACL Laboratory, Sfax University, Sfax, Tunisia
[3]Department of Computer Science, College of Computers and Information Technology, Taif University, Taif, 21944, Saudi Arabia
[4]International Institute of Technology of Sfax, Sfax, Tunisia
[5]School of Computer Science and Engineering, Lovely Professional University, Phagwara City, India
[6]Al-Nahrain Nanorenewable Energy Research Center, Al-Nahrain University, Baghdad, Iraq
[*]Corresponding Author: Mehedi Masud. Email: mmasud@tu.edu.sa

Received: 30 August 2020; Accepted: 18 October 2020

Abstract: Technological advances in recent years have significantly changed the way an operating room works. This work aims to create a platform to solve the problems of operating room occupancy and prepare the rooms with an environment that is favorable for all operations. Using this system, a doctor can control all operation rooms, especially before an operation, and monitor their temperature and humidity to prepare for the operation. Also, in the event of a problem, an alert is sent to the nurse responsible for the room and medical stuff so that the problem can be resolved. The platform is tested using a Raspberry PI card and sensors. The sensors are connected to a cloud layer that collects and analyzes the temperature and humidity values obtained from the environment during an operation. The result of experimentations is visualized through a web application and an Android application. The platform also considers the security aspects such as authorization to access application functionalities for the Web and the mobile applications. We can also test and evaluate the system's existing problems and vulnerabilities using the IEEE and owasp IoT standards. Finally, the proposed framework is extended with a model based testing technique that may be adopted for validating the security aspects.

Keywords: Communication; Internet of Things; control rooms; sensors; cloud; robot

1 Introduction

New information and communication technologies (NICTs) have experienced rapid development for several decades and they have been applied in the health sector in numerous ways. Telemedicine (telediagnosis, telesurveillance, telesupervision, telesurgery, etc.) profoundly changes

This work is licensed under a Creative Commons Attribution 4.0 International License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

medical practices and the relationships between a practitioner and his patient. E-health (information and services on the net, the online management of medical files, etc.) provides practitioners and patients with various sources of information and new services. Chip cards (vital cards, health professional cards) allow the computerized transmission of healthcare information, and they support other services and procedures. Technological advances in recent years have greatly changed the way an operating room works. The multiple possibilities offered to healthcare establishments by the miniaturization of technologies and new equipment have obliged healthcare professionals to rethink the operating theater and their intervention practices. The progress made in sectors such as imaging, robotics and materials, together with the importance of computerization and the use of networks in the management of hospital data, means that surgeons have undergone a major evolution in their way of working.

Today, radiology equipment with digital angiography, for example, is starting to be installed in operating theaters; this requires hybrid rooms to be designed that are capable of accommodating both surgery and radiology activity. The miniaturization of certain elements will lead to the installation of a greater number of technologies in blocks. Imaging improves the physician's vision, provides more information during an intervention, makes diagnosis faster and allows better treatment of the patient at a reduced cost. Certain technologies accessible to the general public are also present in operating theaters, such as large LED screens or 3D imaging. Virtual technologies also allow better communication and better traceability. Patient files arrive directly in the blocks via the network of the establishment. Any changes in data systems that affect the organization of the hospital also have an impact on operating theaters. This network logic encourages collaborative practices across major universities and hospitals.

In addition to maintaining comfort parameters, the purpose of air treatment facilities in operating theaters is to maintain acceptable values of temperature and humidity and to reduce the content of microorganisms, dust, and toxic gases in the air. This is achieved through air renewal at a suitable rate, with air whose purity characteristics have been obtained by various means. Airborne contamination (aero-bio-contamination) plays a significant pathogenic role in so-called clean surgery (Class I), and more particularly in surgery where implants are being placed. The architecture of the premises must comply with the requirements of ventilation techniques in order to prevent the introduction and stagnation of particles that could colonize the operating site. Inside the premises, humans are the main source of microorganisms and particles. The activity and number of people increase the risk of aero-bio-contamination. Therefore, the fight against nosocomial infections in the operating room is mainly based on rigor, with the rules of hygiene being applied by the entire team than the architecture of the premises.

In this work, we provide a solution for measuring, analyzing and controlling temperature and humidity inside operating rooms. For this purpose, we define a network of sensors connected to the Cloud and develop web and Android applications that collect and visualize the desired variables. More precisely, our main contributions in this work are:

- A network of sensors and electronic components for measuring temperature and humidity inside operating rooms ("Dht11" sensors [1], 6LowPan protocol [2] and a processing center "Raspberry card" [3]).
- A cloud layer based on Ubidots [4], which is used for storing and analyzing the data sent by the sensors through the Raspberry card.
- A web application developed using rest APIs, which is used by the hospital managers to detect variations in temperature and humidity in the operating rooms.

- An Android application developed with Android Studio that allows to monitor variations in temperature and humidity in operating rooms.
- A robot equipped with humidity and temperature sensors, controlled by a mobile device via Bluetooth, which sends the collected values to the Cloud using the node Mcu.
- A learning module that generates decision rules for controlling the heating and cooling engines of the operating rooms.
- A set of security measures that protect the developed system from possible external attacks.
- A possible extension that explores model-based testing techniques for validating the security properties.

The rest of this paper is organized as follows. Section 2 discusses related works. Section 3 presents the proposed solutions. Section 4 discusses the security aspects and the proposed mechanisms for protecting the system from attacks. Section 5 is dedicated to security aspects. Section 6 describes the proposed formal framework. Finally, Section 7 concludes the article and suggests directions for new contributions.

2 Related Work

2.1 IoT for Healthcare

The authors in [5] surveyed advances in IoT-based healthcare technologies and they reviewed the state of the art with regard to network applications, platforms, architectures and industrial trends in IoT-based healthcare solutions. Authors in [6] described the various IoT-enabled medical devices and their practices in the following areas: healthcare monitoring of critical patients, chronic care, medicine dispensers and operating rooms. Similarly, the authors in [7] provided an overview of the major medical sensors in IoT and they proposed a review of the existent state-of-the-art IoT projects and technologies required in healthcare. In addition, the authors in [8] described the "Wireless Body Area Network" (WBAN)-based IoT healthcare system and they reviewed the state of the art of the applications and network architecture topologies utilized in IoT healthcare systems. Moreover, the IoT for "Personalized Healthcare Systems" (PHS) was considered in [9]. The authors in [10] reviewed the use of RFID for application to centric body systems and they proposed a mechanism for the collection of information on the living environments of patients. Furthermore, the authors in [11] concentrated on the weaknesses and strengths of a wearable IoT medical system.

2.2 The IoT and Modern Technologies for Operating Rooms

The authors in [12] presented a so-called "Network function virtualization" (NFV)-enabled IoT architecture that enables the web-based automated management, control and orchestration of available resources for operating rooms. The authors in [13] proposed a new methodology for "Noncontact Imaging Photoplethysmography" using low-rank and chrominance features in "IoT Operating Rooms." Reference [14] proposed an IoT-based framework that promotes safety inside surgery rooms, the proper utilization of electrocautery, the standardization of surgical techniques and optimized use of surgical devices. Moreover, the authors in [15] proposed a solution for monitoring surgical operation theaters, keeping track of consumables and tracking surgical towels that are used in surgery. Similarly, the authors in [16] proposed an IoT-based technology for monitoring the sterilization process of surgical devices and instruments.

3 System Architecture

As illustrated in Fig. 1, our system is made up of four layers.

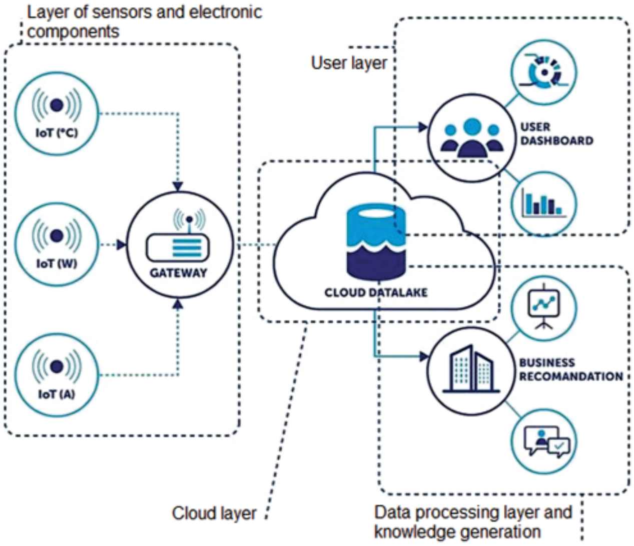


Figure 1: System architecture

3.1 Layer of Sensors and Electronic Components

This layer consists of a set of temperature and humidity sensors, "Dht11," connected through a sensor network based on the 6LowPan protocol and a processing center known as "Raspberry card."

3.1.1 6LowPan Protocol and Adaptation Layer

The sensor network is based on the 6LowPan, which is a cheap and simple communication protocol that allows wireless connectivity using an adaptation of the IPv6 protocol [17]. It is formed by a piece of equipment that is generally compatible with the IEEE802.15.4 standard [18] and is characterized by its short range, low speed, little memory, and low cost. The 6LoWPAN adaptation layer offers three main services:

- Fragmentation and reassembly of packages.
- Header compression.
- Forwarding when multi-hop is used by the link layer.

Fig. 2 shows an adaptation layer that is placed between the MAC layer and the network layer.

3.1.2 Routing

In the case of a sensor network, the network nodes consume a great deal of energy and they have memory constraints. For this reason, a new routing protocol called RPL ("IPv6Routing Protocol for Low-power and lossy networks") [19] has been developed for this type of network. RPL is a distance-vector IPv6 routing protocol that builds a DAG (Directed Acyclic Graph). Also, the LLN Border Router (LBR) [20] is a network border router. This LBR and all higher-ranking equipment form a DODAG (directed acyclic graph where the nodes want to reach a single destination) [21]. The LBR sends a DIO (DODAG information object) information message using multicast.

When a device receives a new version of DIO, it calculates its rank (compared to the one it has just received) and propagates its DIO. When viewed from a device, all devices with a lower rank can claim to be parents. The optimal "parent" routes within the DAG are obtained from metrics and constraints. The LBR periodically issues DIOs to update the DAG. When a device joins the network or loses the link to its "parent," it can wait for the next DIO or request the sending of a DIO using a DIS (DODAG Informational Solicitation) request message. At the end of this communication, the nodes send a DAO (Destination Advertisement Object) message to confirm their LBR roles. An example of a DODAG is shown in Fig. 3. We employed simulation to study the operating results of the sensor networks before implementation in a real environment. We used a Contiki system called Cooja [22] simulator to run the test. The latter makes it possible to simulate network connections and to interact with the sensors.

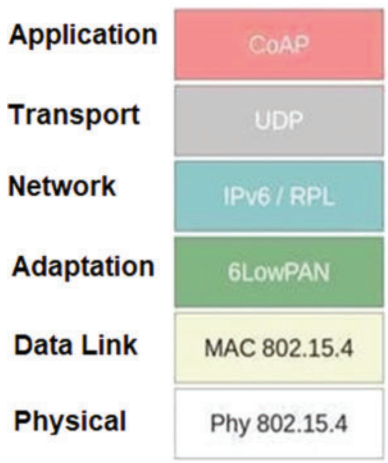


Figure 2: 6LowPan adaptation layer

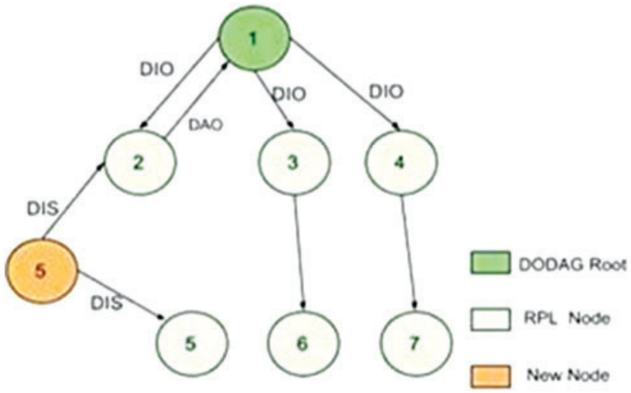


Figure 3: An example of a DODAG

3.2 Cloud Layer

This layer describes the cloud Ubidots used in our system, their services and the transfer of data between the Cloud and the Raspberry card. Ubidots is a private SaaS Cloud dedicated to IoTs. In our framework, its main role is to store the data sent by the sensors through the Raspberry card. These data are stored in variables identified by a name and an id. They represent the values sent by the sensors.

3.2.1 Ubidots Cloud Services

Ubidots is equipped with data analysis and cloud function tools, dashboard visualizations, device management tools, business intelligence (BI) events [23], alarm engines, and authentication/access for end users and operators. With Ubidots, users collect, improve, and deliver data from sensors, actuators, and tags (that matter to businesses and users) to make data-driven decisions that improve efficiency and effectiveness.

3.2.2 Data Transfer between Ubidots and Raspberry Card

Data transfer between the Cloud and the Raspberry card must go through 3 steps:

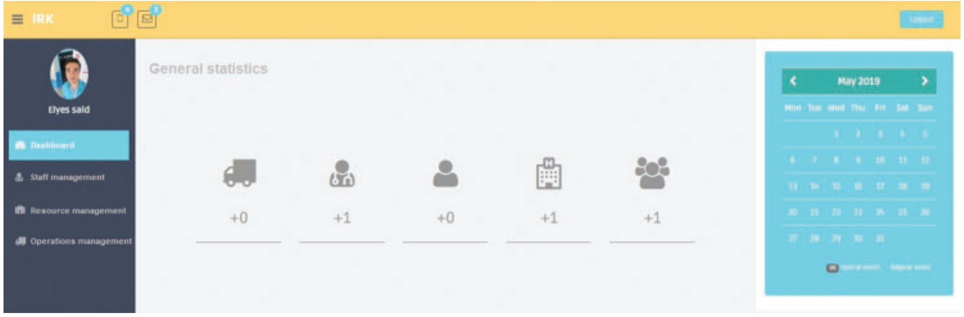
- Step 1: Installation of Ubidots cloud libraries on the Raspberry card so that a secure data transfer tunnel between the Raspberry card and the Cloud can be created.
- Step 2: Creation of a Python file in which the sensor's ipv6 address and the cloud variable id are defined. A script file filters the data sent by the sensor and extracts only the temperature and humidity values.
- Step 3: Running the python file in a closed loop to obtain the data sent by the sensor instantly without breaking, and to automatically create tunnels containing the temperature and humidity values of the sensors.

3.3 User Layer

The user layer forms an interface between the user, the Cloud and the sensors installed in the operating rooms. This layer is made up of 3 important parts.

3.3.1 Web Application

We developed a web application with Java JEE language (framework spring boot). The application helps hospital managers to manage work efficiently in the operating theaters. It also provides the facility to instantly detect any variations in temperature and humidity in the operating rooms in the form of statistics and through informative dashboards based on variables generated by the Ubidots Cloud using rest APIs. For the administrator to access our system, he must enter the login and password of the web application. After providing this information (Login and Password), the administrator is redirected to the dashboard interface. The latter displays the general statistics of the system in which one can find the total number of operating theaters, the number of doctors, the number of technicians, the number of operating heaters, and the number of managers. Fig. 4 shows the web dashboard interface.



General statistics

+0 +1 +0 +1 +1

Figure 4: Web dashboard interface

3.3.2 Android Application

This application is developed with Android Studio. The objective of the application is to support consultation about variations in temperature and humidity in the operating rooms via a mobile device. This application also uses APIs and variables generated by the Ubidots Cloud. To access the application, a user must be authenticated. Each user with an account on the web application can have an account on the mobile application. Hence, the mobile application uses the same authentication parameters as the web application. After entering the authentication parameters, a home page is displayed.

3.3.3 Robot

In the event of a sensor failure within the operating theaters, the robot can be moved using a mobile application. This application sends codes to the Arduino board, which is responsible for translating this code into an order or action for the robot motors. The robot used in the experiments is show in Fig. 5 and the manipulation interface of the robot is shown in Fig. 6. Orders and actions are sent via Bluetooth to activate the robot's own sensors. The collected values are sent to the Cloud using the node Mcu, which includes a micro-controller connected to Wifi. The objective of the robot is to ensure business continuity and minimize the damage caused by breakdowns.

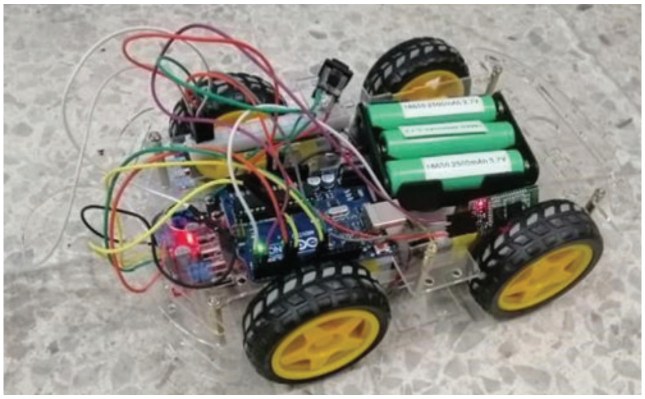


Figure 5: Robot connected to the Cloud via nodeMcu

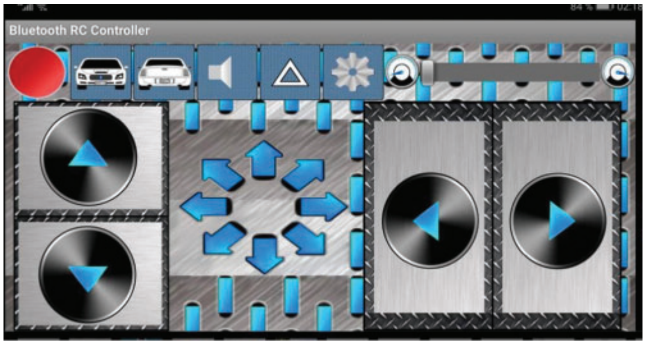


Figure 6: Robot manipulation interface

3.4 Data Processing Layer and Knowledge Generation

In each hospital, it is necessary to have an immense regulator that is given the role of managing the temperature within the operating rooms. Regulators are very expensive electro-mechanical components and it takes a long time to identify their faults. Therefore, we exploit data processing and the recognition generation by referring to a precise and detailed data analysis of the temperature and humidity values sent by the sensors installed in the prototypes. Then we rely on the rules provided by the experts. The experts are electro-mechanical engineers who help to identify the type of regulator failure in a quick and automatic manner. This saves time, money and ensures a stable and problem-free environment.

3.4.1 Rules Provided by Experts

The architecture of a regulator is based on two motors and electronic circuits. The first engine is responsible for cooling the operating rooms and the second one for heating. The rules are implemented based on temperature variation for a period of time relative to the value chosen in order to identify the source of the fault (in the cooling engine or the heating engine). The most important action in data analysis is defining the knowledge base. For this, we use knowledge tables.

3.4.2 Adopted Methods

The decision tree is a tool widely used in data mining. The construction of a decision tree is performed recursively. In the algorithm, the objective is to build a tree in which the leaves are associated with the classification of the labels.

3.4.3 The Result of Learning

The result of the REP-Tree algorithm's learning is that 87.4% of the given instances are correctly classified. In general, the result obtained can be improved by changing the chosen classification algorithm or by minimizing the classification attributes—this can be done by considering anomalies and learning problems such as over-learning.

4 Security of Operating Room Management System

4.1 Web Application Security

Web applications are the preferred target of hackers. Therefore, a poorly designed application allows access to confidential information or even entry to the company's IT system.

4.1.1 Spring Security

This framework [24] forms an infrastructure that provides both authentication and authorization to Java applications. The real strength of this framework lies in the ease with which it can be extended to meet custom requirements. The security implemented by Spring Security is based on two major steps:

- Authentication: The goal for Spring Security, at the end of this step, is to identify a main user—this can be a physical person, a device or any other system capable of performing one or more actions on our server.
- Authorization: Authorization is the process that determines whether or not our primary user has sufficient rights to perform an action within the application. This step is obviously only possible if the authentication has been successful.

4.1.2 Protection Against OWASP Top Ten Attacks

The OWASP Top 10 [25] is a valuable web application security awareness document. It reflects a broad agreement for web applications on the most important security risks. Spring Security solves at least the following OWASP TOP 10 problems:

- Sql injection: By providing mechanisms for secure authentication.
- Broken authentication and session management: By providing mechanisms for efficient and secure authentication and session management.
- Insecure direct object references: By providing authorization mechanisms in the application.
- Sensitive data exposure: The Spring Security cryptography module provides the necessary cryptography functionality.
- Access control at the missing function level: By providing authorization means in the user interface and on the server side.
- Cross-site request forgery (CSRF): Providing support for the generation and validation of tokens mitigating CSRF attacks.

4.1.3 Used Tools

In our case, we performed a vulnerability scan on our web application using the following tools:

- OWASP ZAP (Zed Attack Proxy): An open-source web application security scanner [26–28] that may be adopted by professional penetration testers.
- ACUNETIX: An end-to-end web security scanner [29,30] that offers a global view of an organization's security (web applications, web services, and APIs).

4.2 Mobile Application Security

At this level we adopted biometric authentication. The latter makes it possible to identify and authenticate a person based on a set of recognizable and verifiable, unique and specific data. The goal is to capture a piece of biometric data from that user. This can be a picture of their fingerprint, a recording of their voice, or a photograph of their face. This piece of data is then compared to the biometric data of other authorized users recorded in a database. In our mobile application, we have added a biometric authentication and identification extension for secure access.

5 A Formal Testing Framework Based on Timed Automata and Attack Trees

In this section, we present a model-based system for evaluating security properties [31,32]. A model-based methodology consists of automatically extracting test scenarios from a formal specification of either the system being tested, or the context of the system being evaluated. Our architecture is designed primarily on the use of two formalisms: "Attack Trees" (AT) and "Price Timed Automata" (PTA). An attack tree helps the malicious party to define the plan adopted to breach the protection of the considered system. An attack tree is converted into a PTA network. Using the UPPAALL platform, the product of the built PTA is then calculated. The timed automata product obtained acts as input for the algorithm employed for the generation of tests.

5.1 Attack Trees

Attack trees [33] employ a useful graphical formalism to analyze critical systems' defense. More specifically, an attack tree could be perceived as a graphical representation of the attacker's plan in a tree-shaped form. The root of the AT matches the objective that the attacker aims to achieve. The children of a node in the AT correspond to refinements into sub-goals of the target of the parent node. The refinement of an attack tree's internal node could be either conjunctive or disjunctive:

- A conjunctive refinement is adopted when the accomplishment of all the children's goals is required to accomplish the parent's goal. In this situation, an AND gate is associated with the parent node (Fig. 7a).
- A disjunctive refinement is adopted when the accomplishment of one of the children's goals is enough to accomplish the parent's goal. In this second situation, we associate an OR gate with the parent node (Fig. 7b).

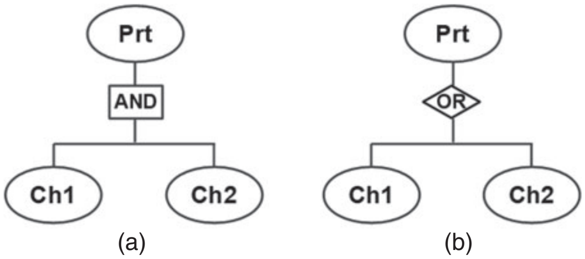


Figure 7: Different possible gates of an attack tree (a) AND gate (b) OR gate

An example of an AT is given in Fig. 8. The attacker's purpose here is to crack a secure file password. As seen in Fig. 8, the attacker's global target can be accomplished by:

- Either crack the password: one of three possible options (Dictionary, Guessing or Brute Force attacks) could accomplish this sub-goal.
- Or perform a password attack: a Social Engineering or a Key Logger attack will accomplish this sub-goal. In turn, the attack on social engineering is subdivided into two basic actions: Generic Reconnaissance and Trap Execution. Likewise, within these two basic actions the main logger assault is accomplished: Key Logger Installation and Password Intercept.

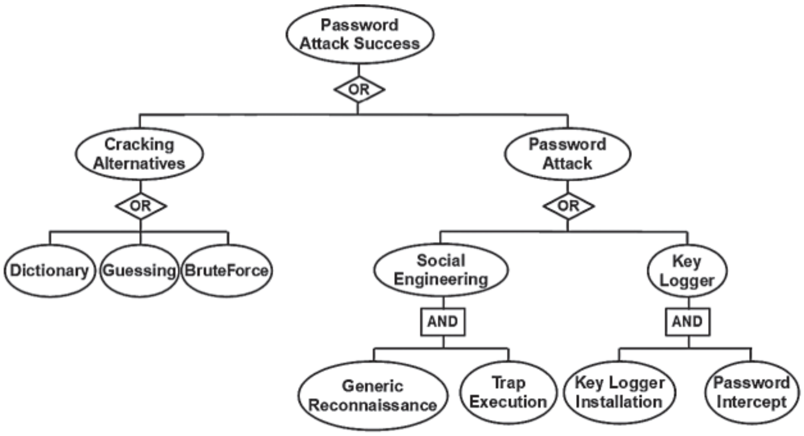


Figure 8: An example of an attacker tree inspired by the work of [29]

5.2 Transforming a Collection of ATs into a Network of PTA

The model of "Priced timed automata" (PTA) [33] is an extension of timed automata, obtained by associating costs with locations and actions. Here we explain how we transform a collection of ATs into a network of PTA. The suggested transformation will be borrowed from [33]. First in Fig. 9, we draw the PTA encoding a basic attack action.

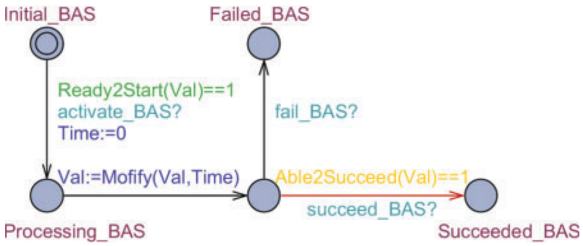


Figure 9: A PTA for a basic attack action

Fig. 10 demonstrates a timed automaton associated with a parent node connected to two children through an AND gate.

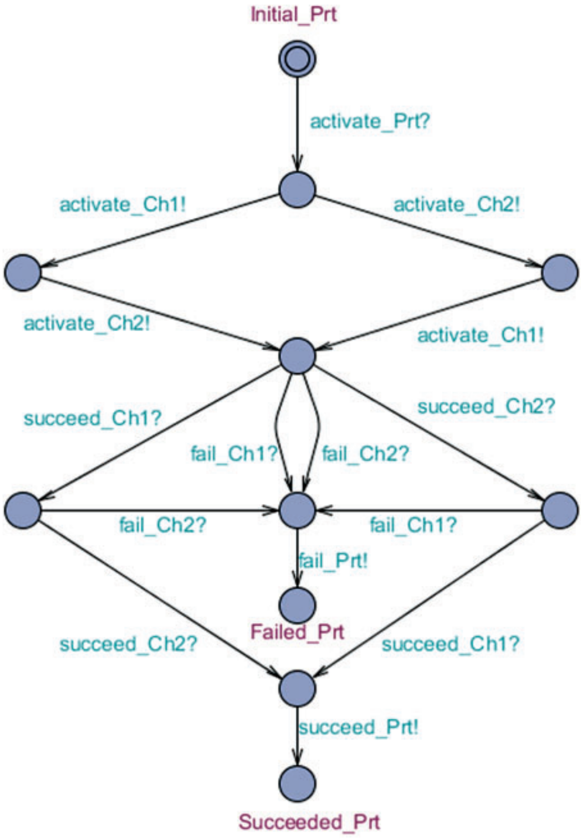


Figure 10: A PTA corresponding to an AND gate and a parent node possessing two children

Fig. 11 illustrates the timed automaton associated with a parent node connected to two children through an OR gate.

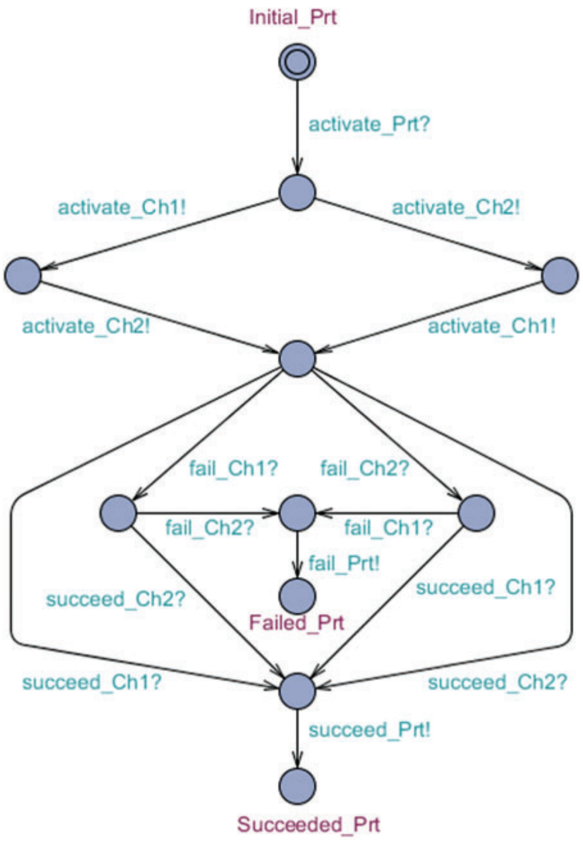


Figure 11: A priced timed automaton for an OR gate and a parent node having two children

Finally, the PTA presented in Fig. 12 is associated with the execution of the attacker's global goal. The generation of tests consists of extracting abstract tests from the PTA network constructed in the previous steps. To this end, we can adopt UPPAAL CORA [34], which is an extended version of the UPPAAL platform. This extension is supplemented with additional variables that are used for the optimal analysis of reachability.

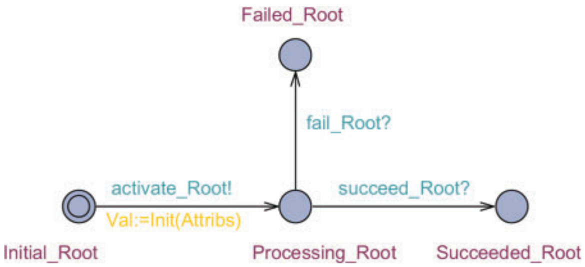


Figure 12: Priced timed automaton corresponding to the global goal of the attacker

6 Conclusion

In this paper, we developed two applications: an Android mobile application and an administrative web application. These two applications allow the management of operating rooms and sensors, and the monitoring of humidity and temperature values in the form of curves. All proposed functionalities have been developed and validated. Moreover, the proposed framework was extended with a model-based testing technique that is adopted to validate the security aspects. This work can be extended and improved by adding several other features, such as the detection of microbes in the operating room. Moreover, the proposed solution may be extended by considering sophisticated testing techniques for healthcare systems [35,36] based on standards like TTCN-3 [37], on formal and mathematical methods as in [38], and on cloud facilities as in [39].

Funding Statement: Taif University Researchers Supporting Project (TURSP-2020/36), Taif University, Taif, Saudi Arabia.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] N. Tianlong, “Application of single bus sensor DHT11 in temperature humidity measure and control system,” *Microcontrollers & Embedded Systems,* vol. 6, no. 26, pp. 1–6, 2010.

[2] N. H. M. Yusoff, N. A. Zakaria, A. Sikora and J. Sebastian, “6LoWPAN protocol in fixed environment: A performance assessment analysis,” in *Proc. 10th Int. Conf. on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications*, Metz, France, pp. 1142–1147, 2019.

[3] A. K. Dennis, “An introduction to the Raspberry Pi, Arduino, and home automation,” in *The Raspberry Pi Home Automation with Arduino,* 2nd ed., Birmingham, United Kingdom: Packt Publishing, pp. 7–18, 2013.

[4] L. Enciso and A. Vargas, “Interface with Ubidots for a fire alarm system using wifi,” in *Proc. 13th IEEE Iberian Conf. on Information Systems and Technologies*, Cáceres, Spain, pp. 1–6, 2018.

[5] S. M. Riazul Islam, D. Kwak, M. Humaun Kabir, M. Hossain and K. S. Kwak, “The internet of things for health care: A comprehensive survey,” *IEEE Access,* vol. 3, pp. 678–708, 2015.

[6] A. S. Yeole and D. Kalbande, “Use of Internet of Things (IoT) in healthcare: A survey,” in *Proc. 16th ACM Sym. on Women in Research*, New York, USA, pp. 71–76, 2016.

[7] N. M. M. AbdElnapi, N. F. Omran, A. A. Ali and F. A. Omara, “A survey of internet of things technologies and projects for healthcare services,” in *Proc. 2018 IEEE Int. Conf. on Innovative Trends in Computer Engineering*, Aswan, Egypt, pp. 48–55, 2018.

[8] M. M. Dhanvijay and S. C. Patil, “Internet of Things: A survey of enabling technologies in healthcare and its applications,” *Computer Networks,* vol. 153, pp. 113–131, 2019.

[9] J. Qi, P. Yang, G. Min, O. Amft, F. Dong *et al.,* “Advanced internet of things for personalized healthcare systems: A survey,” *Pervasive and Mobile Computing,* vol. 41, pp. 132–149, 2017.

[10] S. Amendola, R. Lodato, S. Manzari, C. Occhiuzzi and G. Marrocco, “RFID technology for IoT based personal healthcare in smart spaces,” *IEEE Internet of Things Journal,* vol. 1, no. 2, pp. 144–152, 2014.

[11] S. B. Baker, W. Xiang and I. Atkinson, “Internet of things for smart healthcare: Technologies, challenges, and opportunities,” *IEEE Access,* vol. 5, pp. 26521–26544, 2017.

[12] I. Miladinovic and S. Schefer-Wenzl, “NFY enabled IoT architecture for an operating room environment,” in *Proc. 4th IEEE World Forum on Internet of Things*, Singapore, pp. 98–102, 2018.

[13] H. Yue, X. Li, H. Wang, H. Chen, X. Wang *et al.,* “A new approach for noncontact imaging photo plethysmography using chrominance features and low-rank in the IoT operating room,” *IEEE Access,* vol. 7, pp. 284–112, 2019.

[14] Y. Ushimaru, T. Takahashi, Y. Souma, Y. Yanagimoto, H. Nagase *et al.,* "Innovation in surgery/operating room driven by internet of things on medical devices," *Surgical Endoscopy,* vol. 33, no. 10, pp. 3469–3477, 2019.

[15] A. E. Hasan, A. Schneider, A. Paulin and C. Thuemmler, "Future internet in surgical operating theatre," in *Proc. 12th Int. Conf. on Information Technology—New Generations,* Las Vegas, NV, pp. 580–585, 2015.

[16] L. P. Hung, C. J. Peng and C. L. Chen, "Using Internet of Things technology to improve patient safety in surgical instrument sterilization control," in *Proc. 11th Int. Wireless Internet Conf.*, Taipei, Taiwan, pp. 183–192, 2018.

[17] P. Loshin, "Theory, protocol, and practice guides readers through implementation and deployment of IPv6," in *IPv6: Theory, Protocol, and Practice,* 2$^{\text{nd}}$ ed. Burlington: Elsevier, 2003.

[18] T. Watteyne, J. Weiss, L. Doherty and J. Simon, "Industrial IEEE802. 15.4 e networks: Performance and trade-offs," in *Proc. 2015 Int. Conf. on Communications*, London, pp. 604–609, 2015.

[19] Q. D. Nguyen, J. Montavont, N. Montavont and T. Noël, "RPL border router redundancy in the internet of things," in *Proc. 15th Int. Conf. on Ad-Hoc Networks and Wireless*, Lille, France, pp. 202–214, 2016.

[20] J. Ko, J. Jeong, J. Park, J. A. Jun, O. Gnawali *et al.,* "DualMOP-RPL: Supporting multiple modes of downward routing in a single RPL network," *ACM Transactions on Sensor Networks,* vol. 11, no. 2, pp. 1–20, 2015.

[21] H. S. Kim, H. Kim, J. Paek and S. Bahk, "Load balancing under heavy traffic in RPL routing protocol for low power and lossy networks," *IEEE Transactions on Mobile Computing,* vol. 16, no. 4, pp. 964–979, 2016.

[22] A. Mahmud, F. Hossain, T. A. Choity and F. Juhin, "Simulation and comparison of RPL, 6Lowpan, and Coap protocols using Cooja simulator," in *Proc. Int. Joint Conf. on Computational Intelligence*, Sevelle, Spain, pp. 317–326, 2018.

[23] B. Wixom, T. Ariyachandra, D. Douglas, M. Goul, B. Gupta *et al.,* "The current state of business intelligence in academia: The arrival of big data," *Communications of the Association for Information Systems,* vol. 34, pp. 1–13, 2014.

[24] J. B. Ottinger and A. Lombardi, *Spring Security from Novice to Professional.* New York, NY: Apress Media, pp. 313–343, 2019. [Online]. Available: https://link.springer.com/content/pdf/10.1007%2F978-1-4842-4486-9.pdf.

[25] W. Bi, F. Yu, N. Cao, W. Huo, G. Cao *et al.,* "Research on data extraction and analysis of software defect in IoT communication software," *Computers, Materials & Continua,* vol. 65, no. 2, pp. 1837–1854, 2020.

[26] O. I. Khalaf and G. M. Abdulsahib, "Frequency estimation by the method of minimum mean squared error and *p*-value distributed in the wireless sensor network," *Journal of Information Science and Engineering,* vol. 35, no. 5, pp. 1099–1112, 2019.

[27] O. I. Khalaf and B. M. Sabbar, "An overview on wireless sensor networks and finding optimal location of nodes," *Periodicals of Engineering and Natural Sciences,* vol. 7, no. 3, pp. 1096–1101, 2019.

[28] G. M. Abdulsahib and O. I. Khalaf, "Comparison and evaluation of cloud processing models in cloud-based networks," *International Journal of Simulation—Systems, Science & Technology,* vol. 19, no. 5, pp. 1–6, 2018.

[29] D. Wiryawanet and S. Kom, "Implementation of the acunetix for testing the banking website," *Journal Information,* vol. 19, no. 6, pp. 1785–1792, 2016.

[30] K. A. Ogudo, D. N. Muwawa, O. I. Khalaf and H. K. Daei, "A device performance and data analytics concept for smartphones' IOT services and machine-type communication in cellular networks," *Symmetry,* vol. 11, no. 593, pp. 1–16, 2019.

[31] M. Krichen, "Improving formal verification and testing techniques for internet of things and smart cities," *Mobile Networks and Applications,* pp. 1–12, 2019.

[32] O. I. Khalaf, G. M. Abdulsahib, H. D. Kasmaei and K. A. Ogudo, “A new algorithm on application of blockchain technology in live stream video transmissions and telecommunications,” *International Journal of e-Collaboration,* vol. 16*,* no. 1*,* pp. 16–32, 2020.

[33] R. Kumar, E. Ruijters and M. Stoelinga, “Quantitative attack tree analysis via priced timed automata,” in *Proc. 13th Int. Conf. on Formal Modeling and Analysis of Timed Systems*, Madrid, Spain, pp. 156–171, 2015.

[34] G. Behrmann, K. G. Larsen and J. I. Rasmussen, “Priced timed automata: Algorithms and applications,” in *Proc. 3rd Int. Sym. on Formal Methods for Components and Objects*, Leiden, Netherlands, pp. 162–182, 2004.

[35] M. Krichen, A. J. Maâlej and M. Lahami, “A model-based approach to combine conformance and load tests: An eHealth case study,” *International Journal of Critical Computer-Based Systems,* vol. 8*,* no. 3/4*,* pp. 282–310, 2018.

[36] O. I. Khalaf, G. M. Abdulsahib and B. M. Sabbar, “Optimization of wireless sensor network coverage using the bee algorithm,” *Journal of Information Science Engineering,* vol. 36*,* no. 2*,* pp. 377–386, 2020.

[37] M. Lahami, F. Fakhfakh, M. Krichen and M. Jmaiel, “Towards a TTCN-3test system for runtime testing of adaptable and distributed systems,” in *Proc. 24th Int. Conf. on Testing Software and Systems*, Alborg, Denmark, pp. 71–86, 2012.

[38] M. Lahami, M. Krichen and M. Jmaiel, “Safe and efficient runtime testing framework applied in dynamic and distributed systems,” *Science of Computer Programming,* vol. 122*,* pp. 1–28, 2016.

[39] M. Lahami, M. Krichen and R. Alroobaea, “Towards a test execution platform as-a-service: Application in the e-health domain,” in *Proc. 19th Int. Conf. on Control, Automation and Diagnosis*, Marrakech, Morocco, pp. 1–6, 2018.