Advanced IoT Network Topologies to Optimize Medical Monitoring Platforms based on a Constrained and Secured IOT Application Protocol CoAP

Fatima Zahra Hamza[1,] , Sanaa EL Aidi[2] , Abderrahim Bajit[3] , Siham Beloualid[4] , Habiba Chaoui[5] and Ahmed Tamtaoui[6]*

[1]Laboratory of Advanced Systems Engineering (ISA), National School of Applied Sciences, Ibn Tofail University. Kenitra, Morocco
[2]Laboratory of Advanced Systems Engineering (ISA), National School of Applied Sciences, Ibn Tofail University. Kenitra, Morocco
[3]Laboratory of Advanced Systems Engineering (ISA), National School of Applied Sciences, Ibn Tofail University. Kenitra, Morocco
[4]Laboratory of Advanced Systems Engineering (ISA), National School of Applied Sciences, Ibn Tofail University. Kenitra, Morocco
[5]Laboratory of Advanced Systems Engineering (ISA), National School of Applied Sciences, Ibn Tofail University. Kenitra, Morocco
[6]National Institute of Posts and Telecommunications (INPT-Rabat), SC Department, Mohammed V University. Rabat, Morocco

Abstract. The Internet of Things (IoT) became, and still an important and critical element during the covid-19 pandemic, and this paper was written within that framework, as it proposes a synchronized medical IoT platform that is used to monitor citizens' access to public areas, and where the access is only authorized if one of the three following conditions is fulfilled: Be vaccinated (which is verified via a QR code), having a negative PCR test (valid for only 48 hours), undergoing a body temperature measurement. Of course, a confirmation of identity with a facial recognition test is mandatory. This automatic process will allow us to reduce the possibility of spreading the disease due to the congestion of the checkpoints, as well as to detect citizens who could be potential patients of the covid-19 virus.

1 Introduction

IoT gives digital and physical worlds an opportunity to interact with each other through sensors, that collect information for storage and processing [1]. This work proposes a medical IoT platform to monitor citizens' access to a public area in order to minimize the spread of Covid-19. In this platform, we apply a set of tests that are divided into three cases. In the first case, we check the citizens who are vaccinated by the QR code of the vaccine pass and facial recognition. We move to the second case when the citizen does not possess a vaccine pass, where we check the PCR test that should not overpass 48 hours. If this test is valid, we apply a facial recognition test. If the citizen does not have a PCR test, we move to the third case, to check in the database if he/she is already registered by his/her RFID's UID, if yes, we apply the facial recognition test. If one of these cases' tests are valid, we authorize the access to the citizen, if not, we deny it.

The IoT devices collect the data needed about the citizen to process it and finally act appropriately on the citizen's right to access public space. The platform is also capable of analyzing the facial structure of the human face and comparing it to the information related to it in the database to eventually recognize the detected person.

To make this synchronized, secure, and intelligent platform work properly we implemented four IoT nodes: the first IoT node consists of detecting the presence of a person using the PIR sensor, the second node allows us to measure the body temperature of the detected person by the temperature sensor, the third node is for the identification of the data using an RFID tag, and the fourth node is the camera IoT client node that used for different purposes which are reading the QR code of the vaccine pass, reading the barcode of the PCR test, and finally facial recognition test. These IoT devices communicate with each other through Constrained Application Protocol CoAP, which's payloads are secured RSA and AES cryptography algorithms combined with SHA256, which gives the data transferred a security layer. We have also based the platform on three kinds of network topologies namely Star, Tree, and Mesh. This will allow us to choose the approach that is more efficient, secure, and reliable for the realization and implementation of our platform.

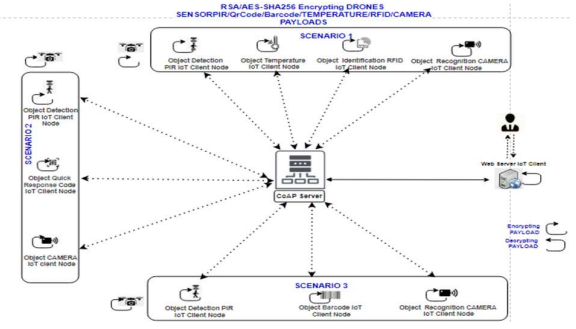

Fig. 1. Supervising Medical IoT Platform Architecture.

* Corresponding author: Fatimazahra.hamza@uit.ac.ma

2 Supervising Medical IoT Cases

Our platform discusses three cases to decide if a citizen is authorized to access a public area or not. The following figure shows the steps of each case scenario.

We start by checking if the person is vaccinated against covid-19, and that is by scanning the QR code on the vaccine pass. The QR codes used in our platform contain a unique number. If it is a valid number, we make sure that this person is indeed the one on the vaccine pass, by performing a facial identification test, which is based on Artificial Intelligence and is a way of identifying or confirming a person's identity using their face. Only if this test is valid can we allow access to the citizen.

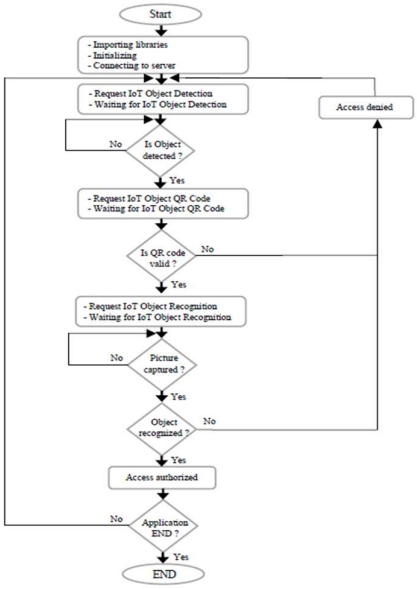

Fig. 2. Functional algorithm of the first case.

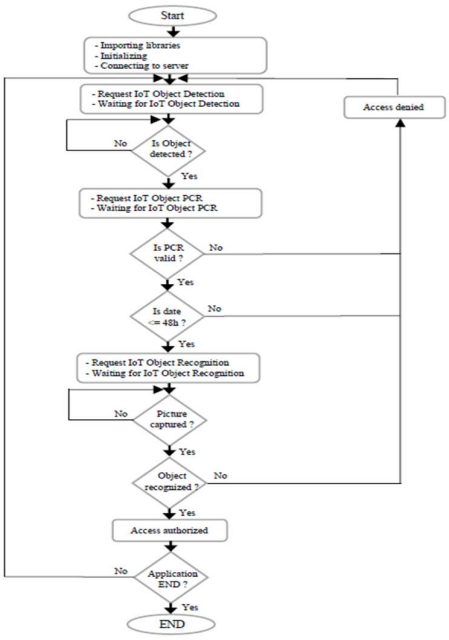

Fig. 3. Functional algorithm of the second case.

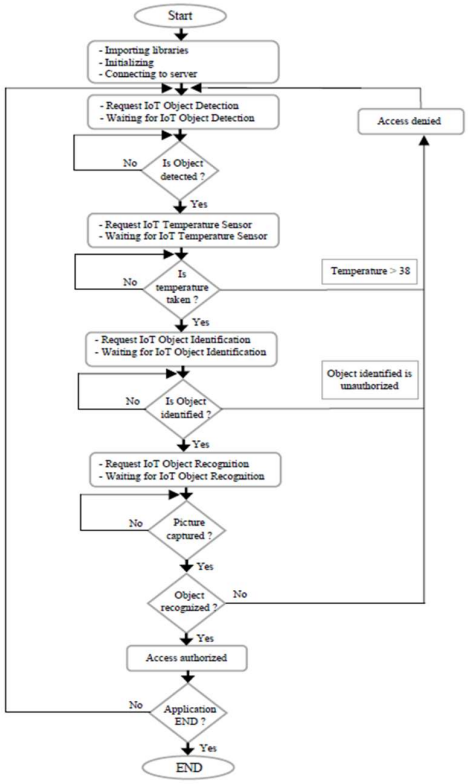

Fig. 4. Functional algorithm of the third case.

The second case is performed when the person does not possess a vaccine pass, where we see if he/she has a PCR test that is used to detect the presence of the virus. When the barcode in the PCR test is scanned, we verify that only less than 48 hours have passed for the test, or else the access is denied. We then perform the facial identification test to verify the identity of the individual.

The third case is applied when the citizen is not vaccinated and also doesn't have a PCR test, so we check the body temperature as well as the unique number of his/her RFID and perform a facial identification test.

3 Methodological Approach

To complete our research, we built our platform and based it on different approaches from which we deducted comparative results, that will allow us in the end to extract the approach that fits the requirements of our platform when it comes to the communication protocol, cryptography algorithm, and network topology, in regards of reliability, security, time consumption, memory occupation, and power consumption. So, for the communication protocol, we have made a light comparison between MQTT and CoAP to ensure communication of the nodes, for the cryptography algorithms we compared RSA/SHA256 and AES/SHA256, and for the network topologies, we compared Star, Tree, and Mesh.

3.1 Constrained Application Protocol

The Constrained Application Protocol (CoAP) is a standard web transfer protocol [2]. It is a lightweight protocol that is intended for resource-constrained environments, thanks to the fact that it is built over UDP which has a smaller packet size and lower overhead compared to TCP which MQTT is built upon. This leads to less resources consumption and allows long-life batteries for the IoT devices [1,3].

CoAP feels very much like HTTP, but for constrained environments. It uses the same mechanism and features as HTTP to transfer the data but with less resources consumption. Furthermore, CoAP is also a restful protocol, this means that establishing a connection between these two protocols can be easily done through cross-protocol proxies [4].

3.2 Cryptography Algorithms

To add a security layer to the data shared in the network we have secured it with two different cryptography methods namely RSA and AES, both combined with SHA256.

RSA is an asymmetric key cryptosystem that uses a key pair for encryption and decryption; which are the public key that serves to encrypt data shared to the senders, and the corresponding private key, which is kept private, that serves to decrypt the received data. The factorization of prime numbers allows the RSA algorithm to hand out a great level of security. However, it is very slow since it uses large keys, especially in the case where large amounts of data must be encrypted or decrypted [4].

The Advanced Encryption Standard (AES) is a symmetric cryptography algorithm that only needs one key to encrypt and decrypt data. This feature makes AES encryption more effective to use in resource-constrained environments than RSA. AES encryption aims to prove the authenticity of the data and prove that it was not modified or transformed from its original state during its transfer. AES is a common security algorithm, used for a variety of applications, for the security level it provides and its special mechanism of how the data is encrypted and decrypted [1,5].

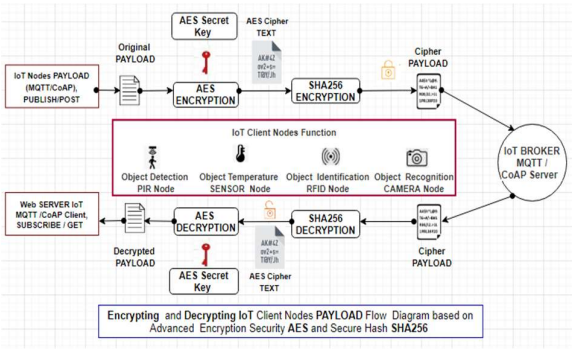

Fig. 5. Encrypting/decrypting a payload using AES-SHA256.

3.3 IoT Network Topologies

The network topology describes how the communication between the different IoT components is established. When choosing to implement a network topology, it is mandatory to first learn how and see the impact of it on the platform, in terms of resources consumption, complexity, latency, and fault resiliency.

Star topology allows a point-to-point connection, where each IoT device is directly connected to the coordinator of the network [6]. The implementation of star is very simple compared to other topologies. In addition, end-points operate separately from the other ones and so the network will not be touched when one of them fails or is attacked which increases the network security [7].

In tree topologies, the devices are connected and arranged exactly like the structure of a tree [8]. This topology has a root node, and all other nodes are connected to it in a form of branches, and each branch has its own parent, leading it to form a hierarchical structure [9]. The hierarchy demands a minimum of three levels [10]. In addition, the hierarchical structure offers the ease of adding more nodes if needed, and the ease to find and troubleshoot errors [11].

A mesh topology offers multiple paths for the data to pass through. In other words, in a mesh topology the nodes are all interconnected with each other and implemented so every node is within the transmission range of at least one other node, and so, the data may have to pass multiple nodes to reach its destination [4]. Mesh networks can be full or partial mesh [12].

4 Results and Discussion

Our goal is to apply the AES and RSA algorithms on our platform, as well as develop it based on different topologies to study the impact of each one on the platform, knowing that it is a high constraint resources platform so it is necessary to preserve the energy of the IoT nodes, as well as decrease their memory occupation and execution time. Figures 4 and 5 show the comparative results of each case that our platform provides: QR code that is used in the vaccine pass + facial recognition, barcode that is used in the PCR test + facial recognition, body temperature check + UID check which is contained in the RFID tag + facial recognition.

When it comes to the security of the payload that we added thanks to RSA/AES-SHA256, it is clear, in all the scenarios, that RSA algorithm costs considerably in terms of memory occupation and execution time, as it consumes a lot of time, memory and power, and this is greatly remarkable in the results. Whereas AES encryption algorithm is the best choice since it almost does not affect or impact the effectiveness of the platform, in addition that it's a robust cryptography method that uses only one key for encryption and decryption.

As for the results of the network topologies, we can see that star topology has a very low execution time and memory consumption compared to the tree and mesh topologies. Star is a solution that is reliable, and easy to implement and manage, but only for nodes that are close to each other, in that if the communication link between the central node and the end node is long, that means that more energy must be spent to relay messages, which is the opposite of what we are looking for in our medical IoT platform. A tree topology is a hierarchy of network nodes, with the root node providing services for client nodes, that in turn provide services for other lower-level nodes. In this arrangement, each layer of nodes can form a star network with the nodes it serves. In this case, the structure of tree topology incorporates the drawbacks of star topology. Also, looking at the results of both tree and mesh topologies, their execution time and memory occupation is almost similar, which leads to a conclusion that adopting a mesh topology for this platform is better, in terms of efficiency, resources consumption, reliability (since the multiple paths between the nodes make the network resistant to fails as there is more than one passage between any two nodes), security (since the setup is secure from being compromised), execution time and memory consumption, as seen in the previous results.

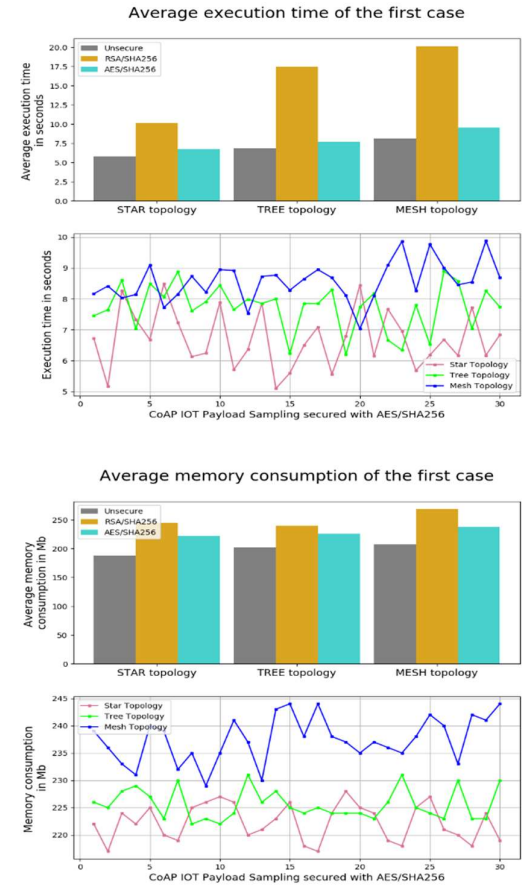

Fig. 6. The average time and memory consumption of 1st case.

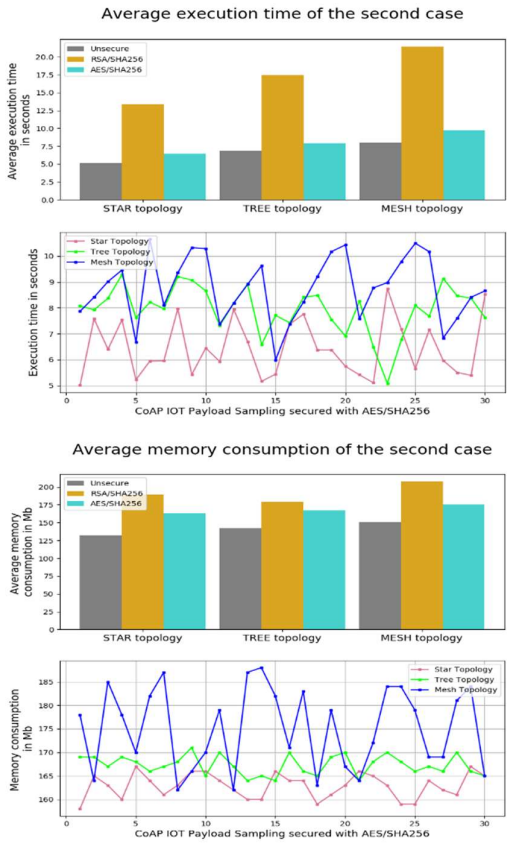

Fig. 7. The average time and memory consumption of 2nd case.

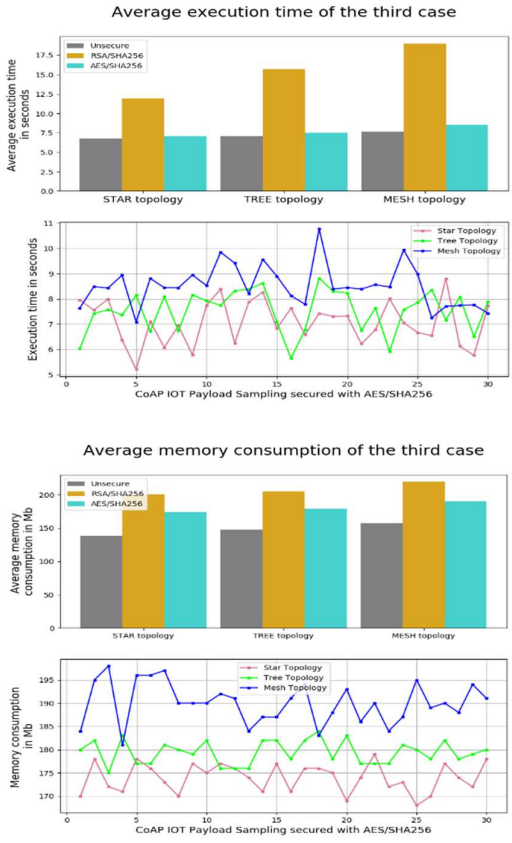

Fig. 8. The average time and memory consumption of 3rd case.

5 Conclusion and perspectives

This research enabled us to create a medical platform that helps control citizens' access to public spaces which will decrease the fast spread of Covid-19. And that is by subjecting the individual to three cases of access control.

As a reliable communication protocol between the nodes, we chose the Constrained Application Protocol and implemented the platform on three network topologies, star, tree, and mesh, and two different cryptography algorithms namely RSA and AES combined with SHA256. Finally, we have opted for the AES-SHA256 algorithm with mesh topology to ensure the requirements of the platform.

In the upcoming works, we will propose an architecture of blockchain which will allow us to store all transactions made [13], also encrypt the payloads with other cryptography algorithms such as ECC and ECIES, and try different communication protocols like 6LowPan which is used in low power wireless communications for IoT [14].

References

1. An Advanced Encryption Cryptographically-Based Securing Applicative Protocols MQTT and CoAP to Optimize Medical-IOT Supervising Platforms S. El Aidi, A. Bajit, A. Barodi, H. Chaoui, A. Tamtaoui. *Lecture Notes on Data Engineering and Communications Technologies*, 2021, 72, pp. 111–121 (2021)
2. M. Farsi, A. Daneshkhah, A. Hosseinian-Far, & H. Jahankhani (Eds.). (2020). *Digital Twin Technologies and Smart Cities.* Internet of Things. doi:10.1007/978-3-030-18732-3
3. An Optimized Security Vehicular Internet of Things -IoT-Application Layer Protocols MQTT and COAP Based on Cryptographic Elliptic-Curve S. El Aidi., A. Bajit, A. Barodi, H. Chaoui, A. Tamtaoui (2020) *IEEE 2nd International Conference on Electronics, Control, Optimization and Computer Science*, ICECOCS 2020, 2020, 931457
4. The basics of IoT's Constrained Application Protocol (CoAP), https://www.embedded.com/the-basics-of-iots-constrained-application-protocol-coap/ , last accessed 2021/07/09
5. KOTHMAYR, Thomas. A security architecture for wireless sensor networks based on DTLS. Master's Thesis in the Software Engineering Elite Graduate Program at the University of Augsburg, (2011)
6. What is network Topology in Internet of Things (IoT) https://engineering.eckovation.com/what-are-network-topology-in-iot/ , last accessed 2021/07/11
7. Mesh vs. Star Topology https://behrtech.com/blog/mesh-vs-star-topology/ , last accessed 2021/07/11
8. Tree topology https://www.computerhope.com/jargon/t/treetopo.htm , last accessed 2021/07/11
9. Type of Network Topology: Bus, Ring, Star, Mesh, Tree, P2P, Hybrid https://www.guru99.com/type-of-network-topology.html , last accessed 2021/07/11
10. Tree Topology | Advantages And Disadvantages Of Tree Topology https://learntechit.com/tree-topology/ , last accessed 2021/07/11
11. Comprehensive Guide on Network Topology, Types, and Tools https://www.tek-tools.com/network/best-network-topology-software , last accessed 2021/07/11
12. What Is Network Topology? Best Guide to Types and Diagrams https://www.dnsstuff.com/what-is-network-topology#tree-topology , last accessed 2021/07/11
13. R. K. Kodali, & N. V. S. Narasimha Sarma (2013). Energy Efficient ECC Encryption Using ECDH. *Emerging Research in Electronics, Computer Science and Technology*, 471–478. doi:10.1007/978-81- 322-1157-0_48
14. What is 6LoWPAN - the basics www.electronics-notes.com/articles/connectivity/ieee-802-15-4-wireless/6lowpan.php