Submitted on: 15/03/2024

Revised form accepted on: 27/06/2024

Corresponding Author: rebbahmed@univ-mascara

Revue
Nature et Technologie
https://journals.univ-chlef.dz/index.php/natec

ISSN: 1112-9778 – EISSN: 2437-0312

A Security Model for Internet of Medical Things

Mohammed REBBAH*, Omar SMAIL, Omar SENOUSSAOUI and Rachid KHALLADI

Department of Computer Science, Faculty of Exact Science, University of Mustapha Stambouli, Mascara, Algeria

Abstract

The Internet of Things (IoT) represents an overarching ideology that blurs the boundaries between the physical and virtual worlds, encompassing a broad spectrum of computing systems and information technologies. IoT devices, such as wearable devices like smart watches and implantable medical devices, are connected to the Internet. Some IoT devices are even integrated into the human body. Generally, wireless communication technologies facilitate connectivity among intelligent and autonomous objects. However, security concerns within IoT pose significant challenges that impede its widespread adoption and evolution. This paper introduces a lightweight and robust security protocol designed to authenticate objects, ensure data integrity during transmission, and detect intrusions in case of attacks on the system.

Keywords: Internet of Things; Security; One Time Password; Mutual authentication; WSN

1. Introduction

The Internet of Things (IoT) has become an integral part of our daily lives, connecting billions of smart and autonomous devices worldwide. This paradigm shift blurs the lines between the physical and virtual worlds, facilitated by advancements in hardware and wireless communication technologies. The IoT is a culmination of various technological advancements, with wireless sensor networks (WSNs) playing a crucial role in enabling its success. However, the widespread adoption of IoT is hindered by significant security challenges, particularly concerning device authentication, data integrity, and intrusion detection

To address these challenges, this paper proposes a comprehensive security protocol tailored for IoT environments. Initially, our protocol focuses on ensuring device authentication to safeguard networks against identity theft. We introduce a Key Personalization system, which securely distributes pre-shared keys to prevent spoofing attacks. Additionally, the protocol includes a data integrity service using the HMAC-SHA256 algorithm to protect against data tampering. Authentication is achieved through robust and lightweight mechanisms such as one-time passwords and challenge/response algorithms, optimized for resource-constrained devices.

In its second iteration, the protocol enhances security by implementing mutual authentication between devices and Coordinators of Personal Area Networks (CPANs). This version improves upon key generation mechanisms, introduces a hidden broadcast key for secure broadcast messages, and strengthens overall system resilience.

Furthermore, this paper contributes to intrusion detection capabilities within IoT networks. It proposes methods to detect and mitigate unauthorized access and data breaches, crucial for maintaining the integrity and security of interconnected devices. The development of this security framework considers the inherent limitations of communication technologies and devices used within IoT ecosystems.

Our approach aims to establish robust security measures that ensure authentication services for connected objects, maintain data integrity, and effectively detect intrusions, thereby enhancing the trustworthiness and reliability of IoT deployments.

The structure of this paper is as follows: Section 2 provides an overview of existing IoT security frameworks and related works. Section 3 details the proposed security model, providing an in-depth exploration of its components and functionalities. Section 4 presents experimental results and comparative analyses with other solutions. Finally, Section 5 concludes with a summary of findings and avenues for future research in IoT security.

2. Related Works

Significant research efforts have been dedicated to enhancing the security of IoT systems. Below, we summarize several notable approaches related to our work.

Hernandez-Ramos *et al.* [1] introduced TinyTo, a protocol leveraging Public Key Infrastructure (PKI) for ensuring end-to-end security with mutual authentication. The protocol involves a series of handshake messages between the device and server to establish a session key for future communications. However, a notable drawback is the substantial memory requirement for certificate authority operations, and vulnerabilities to replay and denial-of-service attacks were not fully addressed.

In [2], a new shared key authentication Mechanism was proposed for both constrained (Cd) and unconstrained (Ud) IoT devices, eliminating the need for a gateway by utilizing a unified security policy agreed upon by participating entities. The method, relying on IPsec, is recognized for its robustness. Nevertheless, it has been noted vulnerable to Dos/DDos Attacks.

Jyh-Cheng and Yu-Ping [3] proposed an authentication system based on the Extensible Authentication Protocol (EAP), specifically designed for IEEE 802.1x technologies. This system requires entities to exchange IDs followed by authentication using methods like MD5 or TLS. While adaptable and standardized, it necessitates a trustworthy third-party authentication server, leading to high message transmission and resource consumption, making it unsuitable for resource-constrained IoT devices.

Sheetal and Sandeep [4] presented a mutual authentication protocol based on Elliptic Curve Cryptography (ECC) for securing communication between embedded devices and cloud servers using HTTP cookies. ECC offers robust security with efficient computations, but the protocol requires devices to support TCP/IP and HTTP, posing challenges for constrained IoT devices. Vulnerabilities include offline password guessing and insider attacks, alongside issues with device anonymity and session key agreement.

In [5], Ashok Kumar and Gireesh Kumar introduced S-OTP, a connection-less authentication mechanism tailored for mobile devices that does not rely on SMS. However, S-OTP imposes significant overhead due to multiple communication exchanges, limiting its suitability primarily to smartphones.

3. Proposed model

We propose an Intrusion Detection System (IDS) designed to identify malicious entities such as hackers or unauthorized objects attempting to illegitimately access the system. Our solution entails a comprehensive security framework that ensures authentication services for connected objects, preserves data integrity during exchanges, and proactively detects malicious activities before they can manifest.

The foundation of our approach leverages the "Open Communication protocol for Ad hoc Reliable Industrial Instrumentation" (OCARI) [6], commonly utilized in IoT and Wireless Sensor Network (WSN) systems [7]. An OCARI network comprises multiple sub-networks managed by key entities (e.g., gateways, servers, CPAN). To integrate a device into the network and facilitate data exchange, it must undergo an association phase with the CPAN of the respective network.

Our approach has evolved through several iterative phases or versions. Initially, we developed a protocol ensuring device authentication during association and safeguarding data integrity in unicast mode. Subsequently, enhancements were made to enable mutual authentication between devices and servers or entities, alongside integrity protection for all types of packets (both unicast and broadcast).

3.1. Problem Statement

In most IoT and WSN networks, devices such as sensors or actuators are managed by central entities (e.g., CPAN, routers, servers). When a new device seeks to join a WSN network, it must undergo mutual authentication with the network manager (server, CPAN). Following successful authentication, an asymmetrical secure channel is established to protect exchanged data. The challenge arises when an intruder masquerades as a legitimate device (by stealing credentials such as Uid, username, password), posing either from external or internal origins.

The critical issue at hand is detecting and mitigating intruders who illegitimately assume device identities. In the subsequent section (Contribution), we will delve into strategies for countering external attackers and safeguarding network integrity (see Figure 1).

The attacker initiates an association request using the Uid of a legitimate device. The server responds by generating a challenge and sending it to the device within an authentication request. The attacker intercepts this challenge and calculates the One-Time Password (OTP) and Ku (possibly a session key). Subsequently, the attacker sends the OTP to the server. If the server verifies the OTP and establishes a secure channel, the attacker gains unauthorized access equivalent to that of the legitimate device. However, if the OTP verification fails, the server denies access and sends an error response.

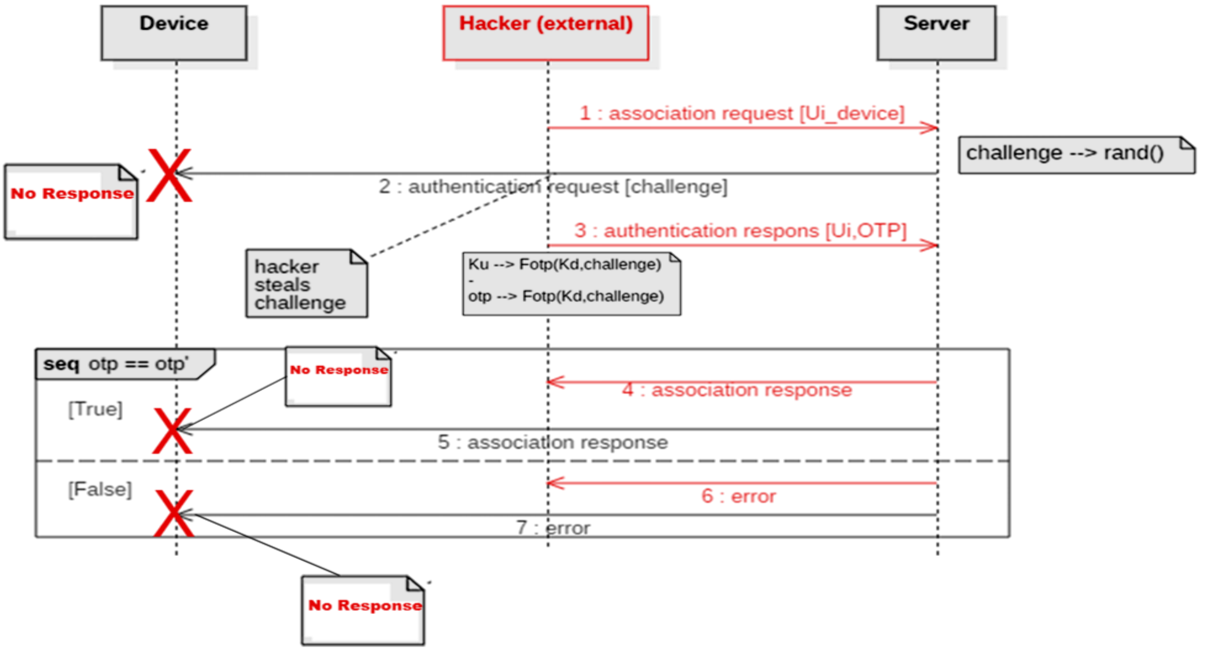

Figure 1: Hacking scenario

3.2. Solution

The major vulnerability highlighted in the previous problem occurs when a device receives an authentication request without having initiated an association request. Exploiting this weakness, an intruder could potentially manipulate the system. To address this critical issue, it is imperative that our devices respond to all authentication requests, regardless of whether they have initiated a request themselves (refer to Figure 2).

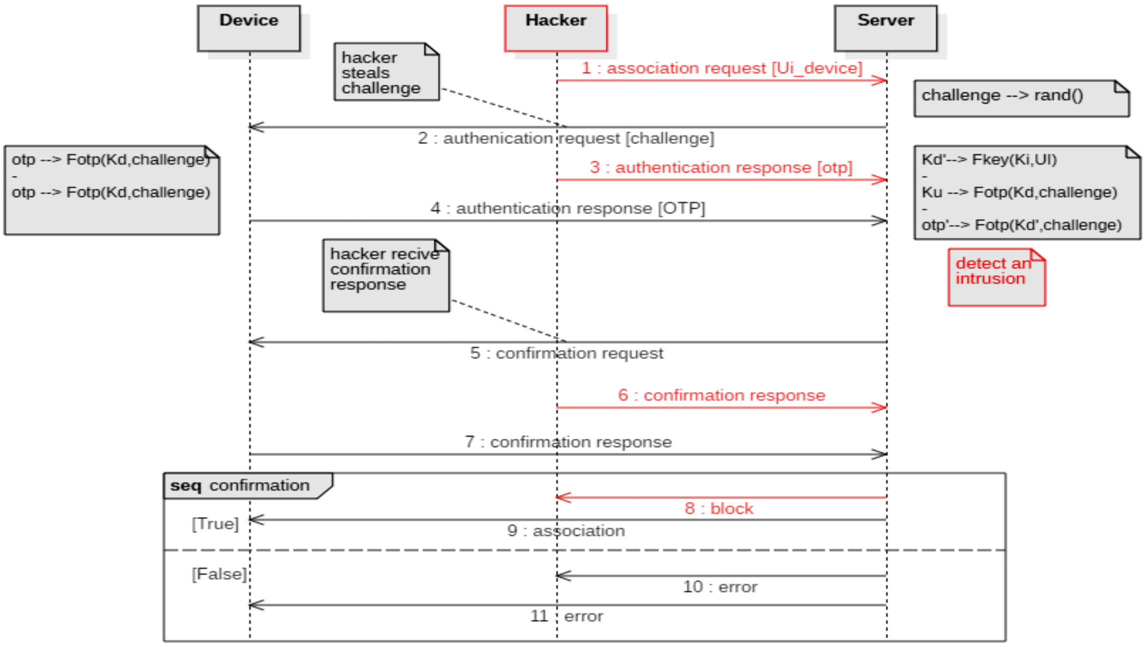
Device
Hacker
Server
hacker steals challenge
1 : association request [Ui_device]
challenge --> rand()
2 : authenication request [challenge]
otp --> Fotp(Kd,challenge)
-
otp --> Fotp(Kd,challenge)
3 : authentication response [otp]
Kd'--> Fkey(Ki,UI)
-
Ku --> Fotp(Kd,challenge)
-
otp'--> Fotp(Kd',challenge)
4 : authentication response [OTP]
hacker recive confirmation response
detect an intrusion
5 : confirmation request
6 : confirmation response
7 : confirmation response
seq confirmation
8 : block
[True]
9 : association
[False]
10 : error
11 : error

Figure 2: Security scenario

Citation : REBBAH M., SMAIL O., SENOUSSAOUI O. and KHALLADI R., (2024) A security model for internet of medical things, *Revue Nature et Technologie*, 16 (2): 01-06. https://journals.univ-chlef.dz/index.php/natec

When the server receives authentication responses from both the attacker and the legitimate device simultaneously, it detects this anomaly and initiates a confirmation request for further validation. The device, upon receiving this confirmation request, generates a response using a highly complex function or a result derived from a shared algorithm with the server.

The shared algorithm involves a common function or a shared variable known only to the server and internal devices. This ensures secure authentication and protection against external hackers. The algorithm is outlined as the following algorithm:

Algorithm 1 : Common function

```
Step1   :   R1 = HMAC-SHA256(username, password)
Step2   :   R2 = HMAC-SHA256(R1, Kd)
Step3   :   R3 = HMAC-SHA256(R2, Secretkey$_2$)
Step4   :   Return R3
```

And the secret key is hidden and know just for the device, and it’s very sensitive and this device encrypt (hide) this secret key by very strong encryption.

4. Experiment and Analysis

Our project was implemented and tested at a polyclinic in Biskra (About 400 km south-east of Algiers) [8].

We created a simulation model of a polyclinic located in Biskra (see Figure 3), comprising administrative staff and medical personnel including doctors and nurses. Both patients and medical professionals were equipped with devices enabling interaction and data exchange within the clinic. During the experiment, we introduced scenarios involving both internal and external intruders.

The application was designed to allow medical professionals to monitor patients closely and receive real-time data from connected devices.

We conducted tests to evaluate the system's response to internal and external intrusions. Specifically, we focused on measuring the association time factor, as detailed in Table 1.

Table 1
Authentication time

Version	Time without authentication (ms)	Time with authentication (ms)
Version 1[9]	20	32
Version 2[9]	43	54
Version 3	72	97

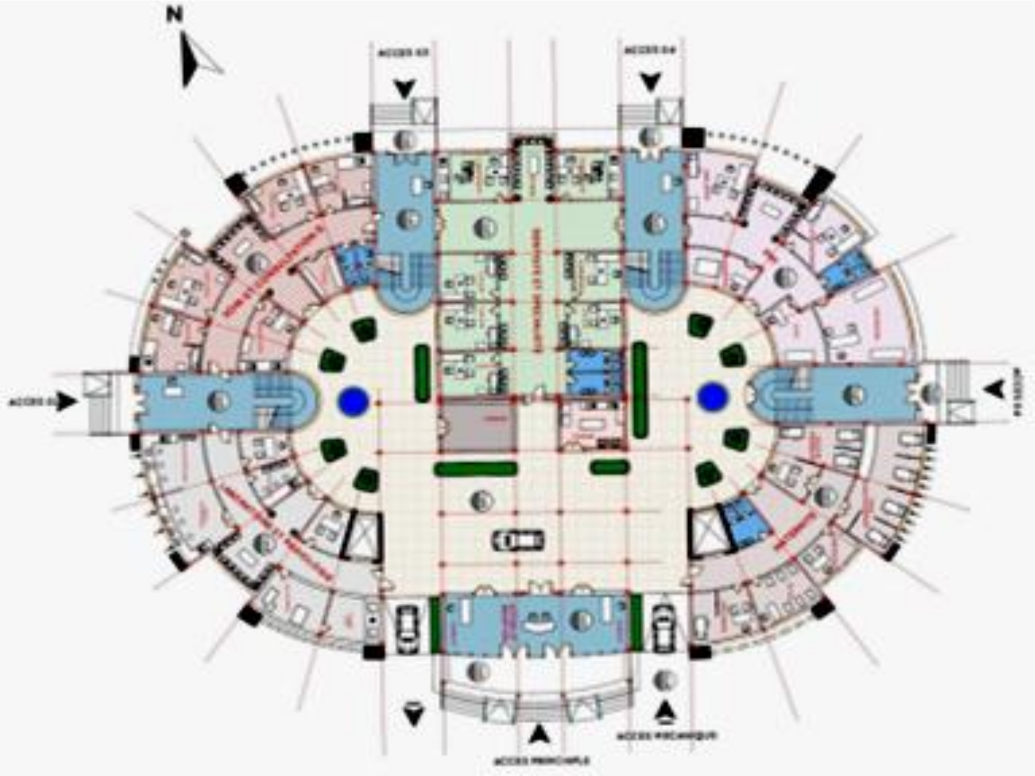

Figure 3: Polyclinic of Biskra

We conducted experiments involving various attacks from internal and external intruders, specifically focusing on detecting three association versions (see Table 2). Our findings indicate that version 3 yields superior intrusion detection results due to its more refined approach.

Table 2
Detection rate

Version	Internal intruder % detection	External intruder % detection
Version 1 [9]	60	54
Version 2 [9]	79	72
Version 3	98	95

External intruders pose a significant challenge in detection, primarily because their data is often absent from the database, complicating the identification process.

5. Conclusion and Future Works

The Internet of Things (IoT) integrates diverse fields such as computer science and electronics, resulting in a heterogeneous system that employs multiple technologies across various architectures and platforms. Deployed on a wide range of hardware, IoT systems utilize wireless communication technologies to interconnect intelligent and autonomous objects. However, the evolution and rapid deployment of IoT technologies are hampered by significant security challenges.

To address these issues, we developed a lightweight and robust security protocol designed specifically for IoT systems. This protocol ensures object authentication, guarantees data integrity, and incorporates intrusion detection capabilities to mitigate potential attacks. Our system has undergone iterative improvements, culminating in a solution tailored to the performance requirements of IoT environments.

In this study, we introduced an efficient security protocol capable of deployment across different IoT architectures and technologies, safeguarding systems and data from emerging threats. By enhancing security measures, we aim to facilitate the secure and widespread adoption of IoT technologies in diverse application domains.

Moving forward, our research will focus on several key areas to enhance and expand the capabilities of our security protocol. First, we plan to conduct extensive real-world testing in diverse IoT environments to evaluate the protocol's performance and effectiveness under various conditions. This will help identify potential areas for improvement and ensure robustness in practical applications.

Second, we aim to integrate advanced machine learning techniques to further enhance the protocol's intrusion detection capabilities. By leveraging AI, we can create adaptive security measures that respond dynamically to emerging threats, providing even greater protection for IoT systems.

Third, we will explore the development of a standardized framework for IoT security protocols, promoting interoperability and ease of adoption across different industries and platforms. This framework will serve as a foundation for creating universally accepted security practices, facilitating the global integration of secure IoT technologies.

Lastly, we will investigate the potential of blockchain technology to provide decentralized and tamper-proof security solutions for IoT networks. Blockchain can offer an additional layer of security, ensuring data integrity and transparency in IoT communications.

By pursuing these future works, we aim to continuously improve our security protocol, addressing new challenges and opportunities in the ever-evolving landscape of IoT technologies.

References

[1] Jose L Hernandez-Ramos, Marcin Piotr Pawlowski, Antonio J Jara, Antonio F Skarmeta, and Latif Ladid. (2015) Toward a lightweight authentication and authorization framework for smart objects. *IEEE Journal on Selected Areas in Communications*, 33 (4): 690–702
doi: 10.1109/JSAC.2015.2393436

[2] Riccardo Bonetto, Nicola Bui, Vishwas Lakkundi, Alexis Olivereau, Alexandru Serbanati, and Michele Rossi. Secure communication for smart IoT objects: Protocol stacks, use cases and practical examples. In 2012 IEEE international symposium on a world of wireless, mobile and multimedia networks (WoWMoM), pages 1–7. IEEE, 2012.
https://www.dei.unipd.it/~rossi/papers/IoT-SoS-2012.pdf

[3] Jyh-Cheng Chen and Yu-Ping Wang. Extensible authentication protocol (eap) and idée 802.1 x: tutorial and empirical experience. *IEEE communications magazine*, 43(12): supl–26, 2005.

[4] Sheetal Kalra and Sandeep K Sood. (2015) Secure authentication scheme for IoT and cloud servers. *Pervasive and Mobile Computing*, 24: 210–223.
https://doi.org/10.1016/j.pmcj.2015.08.001

[5] Ashok Kumar Mohan and T Gireesh Kumar. (2015) Secure seed-based sturdy OTP via convenient carry-on device. In *Artificial Intelligence and Evolutionary Algorithms in Engineering Systems*, pages 447–455. Springer.

[6] Khaldoun Al Agha, Marc-Henri Bertin, Tuan Dang, Alexandre Guitton, Pascale Minet, Thierry Val, and Jean-Baptiste Viollet. (2009) Which wireless technology for industrial wireless sensors network? The development of OCARI technology. *IEEE Transactions on Industrial Electronics*, 56 (10): 13.
https://doi.org/10.1109/TIE.2009.2027253

[7] Harsh Kupwade Patil and Thomas M Chen. Wireless sensor network security. In Computer and Information Security Handbook, pages 301–322. Elsevier, 2013.

[8] Tarhlissia Mohamed Islam. « *L'architecture fonctionnelle of polyclinique*" Master's thesis, University of Mohamed Khider de Biskra, Algeria, July 2019.

[HTML] http://archives.univ-biskra.dz/handle/123456789/14687?mode=full

[9] Mohamed Tahar Hammi, Erwan Livolant, Patrick Bellot, Ahmed Serhrouchni, Pascale Minet. A Lightweight IoT Security Protocol. 1st Cyber Security in Networking Conference (CSNet2017), Oct 2017, Rio de Janeiro, Brazil. https://doi.org/10.1109/CSNET.2017.8242001