

SECURITY THREATS IN SMART HEALTHCARE

EL BAKKOURI Najlae¹, TOMADER Mazri²

¹University Ibn Tofail, National School of Applied Sciences Kenitra, Morocco – najlaeelbakkouri@gmail.com

²University Ibn Tofail – National School of Applied Sciences Kenitra Morocco – Tomader20@gmail.com

KEY WORDS: Smart Health, Internet of things, smart environment, IoT Attacks, Smart Healthcare, threat security.

ABSTRACT:

The Internet of Things had become more usually those recent years, it helps the human to be connected to every devices, to The Internet of Things had become more usually those recent years, it helps the human to be connected to every devices, to communicate and to share information for each other, the IoT gives many benefits to HealthCare systems and applications, it help to diagnostic and to monitor patients more closely and easier, but as other domain based on technologies, the smart Health use IT programs and Wireless network to exchange and analyse data which may be stouling by attackers if it doesn't secured and controlled permanently, as a fact of this weakness, it's possible to injure or kill some patient without being detected, this article discussing the Smart Health system, its benefits and examples of its using, also, it gives a view about security issues that can touch to this domain and best practice to follow for securing, detecting and avoiding security risks.

1. INTRODUCTION

Smart Things, this word is becoming more and more used by several people and in several fields, it was born to follow the rapid development of technology aiming at the simplification of the procedures, the speed of the treatments and the efficiency of the rendered work.

Smart Things build an ecosystem that encompasses all areas and environments, so we can talk about: smart cities, smart school, smart university, smart campus, smart transport, smart health ... etc.

Generally, all of this can be integrated into the smart environment which can be defined by a physical world integrating a very large number of invisible sensors, actuators, screens and calculation elements.

These IT elements are generally seamlessly integrated into everyday objects and networked with each other. It is connected objects or the Internet of Things (IoT) which aim to improve existing processes, ease and permission of scenarios which cannot be implemented before, helped to control and manage the physical world at using sensors which will make it possible to detect, collect, analyze, transmit and process data (C.Gomez et al, 2019).

In this article, we will focus our work on the field of *Smart Health*, this large vital system which includes several participants, such as doctors, patients, hospitals and medical research institutes.

We will give more details on the use of Smart Health, the health benefits by adopting and using this system, but also the risks that can be generated in the event of misuse or fraudulent manipulation of the data and this system in general.

The article will be organized as follows:

Smart Health overview in the section 1, then we will see a general description of the IoT for Health in the section2, after, we will talk about security in the Smart Health and also describe some attacks that could damage a Smart Health system in section 3, and next, we will recommend some defense security measures in

section 4. Concluding by a discussion and conclusion in section 5 and 6.

2. SMART HEALTH OVERVIEW

As mentioned in the introduction of this article, the Smart Healthcare is a service that brings together several stake holders and includes several participants, such as doctors, patients, hospitals and medical research institutes. Its appearance has allowed a revolution in the field of health, it has enabled a very effective evolution for the health of humanity and has made it possible to fight against several diseases and to cope with several constraints where even detection was previously impossible (Glob. Health J., 2019).

The figure bellow show components and the different participants on the Smart health system:

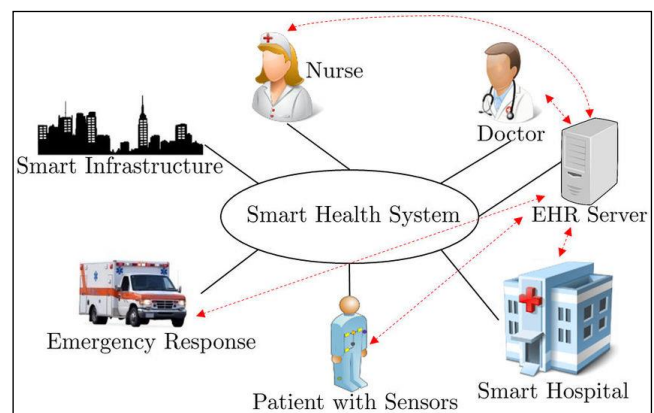


Figure 1: Smart health System components

In what follows, we will talk about the evolution that accompanied Smart Healthcare.

2.1 Smart Health Evolution

Firstly, we will discuss about electronic health (e-health) which is the way we apply service via information and communications

technology (ICT) in the healthcare field. The concept of e-health also helps to increase efficiency and reduce costs.

It is linked to mobile health (m-health), which can be defined by the provision of health services via mobile communication devices and digital applications (hardware and software), which allow the patient, his entourage and different health care providers to collect, view, share and use intelligently and permanently information related to health and well-being (A. Solanas et al., 2014).

E-health and m-health are supported by mobile devices, such as mobile phones, patient monitoring devices, personal digital assistants (PDAs) and other wireless devices.

Stilling in the health field, and as an evolution, we experienced the appearance of Smart Health (s-health), it is the key concept of intelligent health including both and integrating e-health and m-health.

In Smart Health, healthcare is defined by technology that leads to better diagnostic tools, better treatment for patients and devices that improve the quality of life for everyone with real-time monitoring and immediate alerts in the event of a problem, even without the appearance of symptoms of an illness (Y. Zhang et al, 2018).

Smart Health provides health services remotely and even at home.

Via connected objects, we can monitor blood pressure, do a cardiology, performance of the humanitarian system and other permanent health measures in real time and build an individual database which can be used to anticipate several illnesses and to react effectively in case of a disease or damage on an organ of the human.

The figure below gives an overview of the connected objects used in the Smart Health system:

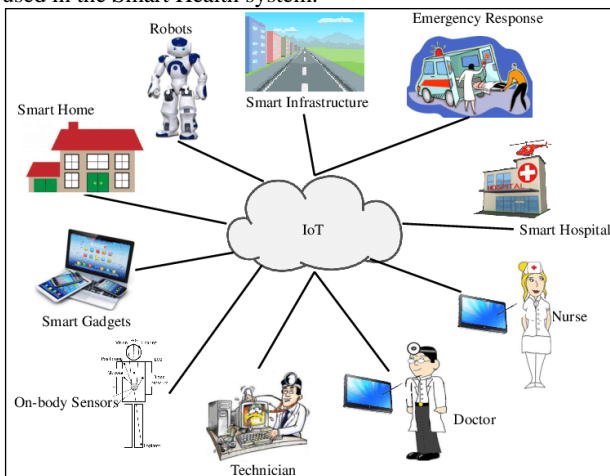


Figure 2: IoT on Smart Health System

According to this description of Smart Health, what are the benefits and advantages behind this system?

2.2 The Benefits Of Smart Health

Smart health has significant, positive results and great efficiency in health all over the world, although it is not generalized everywhere and its ecosystem still requires a lot of work in order to equip hospitals, ambulances, local medical operations, medical

staff and patients by connected objects and smart technologies (A. Srilakshmi et al, 2019).

Regarding the benefits of smart health, we quote:

- Less errors: With smart health technology doctors can gain access to near real-time information and take a data-driven approach to ensure better success rates.
- Time reduce: the patient thinks that waiting in the hospital is a huge wasting of time to exchange information with the doctor, in fact the patient today wants better interaction with the doctors and less time wasted.
- Provide more data: It quite difficult for the human (doctor or nurse) to collect all the patient's information consistently and continuous, but with the smart Health technologies the data are collected easier and reliably.
- Monitoring data for a longer period: Smart health technologies have the ability to stock the information which make them visible for years seamlessly in the dashboard in an easy to use format.

Also, Smart Health system permit:

- Regular and permanent monitoring of patient health
- Regular test against diseases and spread of viruses
- Test and analysis for several people at the same time
- Anticipation of diseases even without symptoms
- Avoid direct contact with contagious disease patients

To conclude this part, according to the benefits and advantages of Smart Health, what may a description of IoT and smart environment for health will look like?

3. GENERAL DESCRIPTION OF SMART ENVIRONMENTS FOR HEALTH

Let have a look on how the IoT and smart environment works for health and how to enable technologies and application for the healthcare.

We give this example where set of sensors are integrated to the environment of a person or worn by him, these sensors and captures will acquire data continuously or periodically, then, process them to be able to firstly give some information or some feedback to the concerned person and secondly inform the medical staff, the family or some other authorized persons of the health status (C.Gomez et al, 2019).

This example is explained on the below figure.

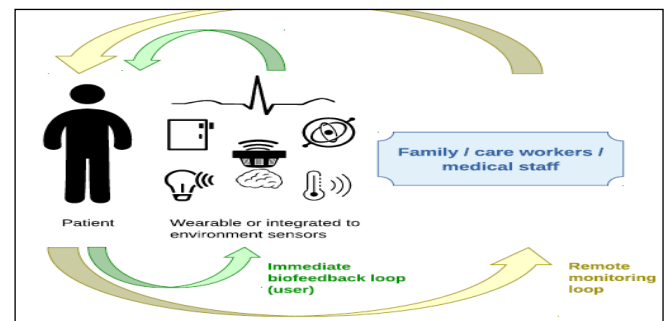


Figure 3: Smart Environment for healthcare

All these new technologies have brought many advantages in the field of health, whether for speed, efficiency, quality, diagnosis and patient management and also for the doctor's task, as we have described in the overview section. However, with all its benefits, there are new security concerns that can threaten patients' health and privacy.

If the system is hacked, the confidentiality of patient data will no longer be protected, disclosure of sensitive data will be at the fingertips of unauthorized individuals and this will compromise important critical data.

As statistics show, health care is the most pirated industry in the United States. For example, a study shows that more than 13 million records were exposed through around 350 data breaches in 2018 and 89% of healthcare facilities have experienced a data breach in the past two years, despite sophisticated measures implemented by suppliers to prevent data breaches and secure the information system (Source: Dizzion).

4. SECURITY IN SMART HEALTHCARE

Like any computer system, Smart Environment in general are affected by security risks. Smart health is one of those environments that can be attacked or outright broken by individuals or hackers.

Given the sensitivity of the data which contains and which transits in a large network of which the Internet is a part, and given the large number of devices and IoT which constitutes it, the risk of having a large number of vulnerabilities will always remain current if the necessary measures are not applied and are taken into consideration throughout the deployment project of the Smart Health system. Also, rigorous monitoring, regular and periodic audit plans are necessary to ensure that the system is always safe from attacks and that these components comply with security, configuration and hardening standards (Shancang Li, Li Da Xu, 2020).

In order to ensure the security of the Smart HealthCare system, security requirements must be provided. The system must meet all of the following security requirements: confidentiality, integrity, authentication, authorization, availability and non-repudiation (see the figure 4):



Figure 4: Goals of system information security

Confidentiality refers to the fact that an unauthorized user sees the hidden information, in other words it means that an intruder adversary access to the data.

Integrity means that patient's data will not be changed by an unauthorized attacker.

Authorization is the function of specifying access rights/privileges to resources or system.

Authentication alludes to the identification of the person which attempt to access the system.

Availability means when authorized users get access to the smart health system and to the services they need.

Non-repudiation is the assurance that someone cannot deny something. Typically, nonrepudiation refers to the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated.

In medicine, a small mistake or a security threat can end a human's life. To combat this and ensure patient safety, the Smart HealthCare system must meet all of the requirements listed above.

Despite this, we still find attackers and hackers who are researching and developing new ways with the goal of gaining access, controlling the system, disclosing and obtaining confidential data and information.

As mentioned before, the large number of devices and IoTs used in this environment, make the system vulnerable to the majority of attacks and known security risks (Kristen Gloss, 2020), such as:

- Problems with system and firmware updates
- Use of end-of-life devices
- Listening to the network and intercepting traffic
- The denial of service
- Man in the Middle Attacks (MITM)
- Location-based attack and routing attack
- ... Etc.

In this paper, we will focus and deal with the following two attacks:

- Location-based attack
- Routing attack

The intruders in location-based attack tries to target the destination of the node to services of the system such as:

- Denial of Service attack

In the other hand an attacker that use a Routing Attack mostly targets the route of the data to drop or send data packets (S. A. Butt et al, 2019) such as:

- Select and forwarding attack
- Replay attack and router attack

The figure below shows a summary of these attacks.

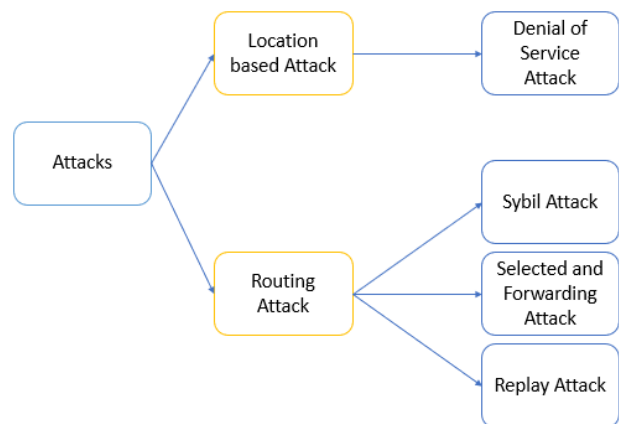


Figure 5: Taxonomy of attacks in Smart Health System

In what follows, we will deal in detail with the two attacks chosen for this paper.

1. Location based attack

A. Denial of service

Denial of service (DoS) attacks can affect health-care systems and affect patient safety. It tries to cause a capacity overload in the target system by sending multiple requests with unknown

traffic. Dos attack can be used to disable or slow a service so the resources won't be accessible for the patient and the doctor either, due the busy channel the other nodes wouldn't be able to send their information. A DOS attacker aims to ruin the operation of the nodes. According to the IEEE 802.11 standard the nodes doesn't counter check every one of the flags in control frames, for that reason, it will be hard to detect such kind of attack. The Denial of Service attack makes the channel of data system busy so that the other sensors in the network won't be able to receive information. Also, the patient can gain access without authentication. The attacker of Denial of Service can add or send false information of a patient causing a false treatment, a false diagnostic, a false status of the patient and may be a false emergency call to the doctors. Consequently, causing patient Death.

The figure bellow shows the denial of service attack.

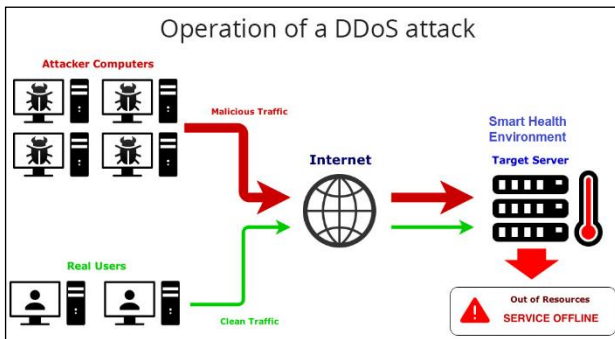


Figure 6:Denial of service attack

2. Routing attack

A. Sybil attack

In this attack, the intruder tries to get a node claims multiple fake identity (Udaya S., Rajamani V., 2020), this attack is classified into two forms as describing bellow:

- **Direct Attack and Indirect Attack:** in the direct attack the real node communicate directly with the Sybil node. Whereas in the indirect attack the communication between the Sybil node and the real node is done by a malicious node.
- **Stolen and fabricated node identities attack:** in this type of attack an illegal node is using a fake identity to communicate with the other nodes, a sensor node with ID of 16-bit integers makes the same ID of 16 bits, which are fabricated nodes. The IDs taken by the Sybil node are destroyed by examining the identity replication.

In other words, an adversary tries to have one or large number of nodes IDs to act and function as a distinct node. Sybil attacks degrade data integrity, security, and resource utilization it could affect harmfully in the context of a Smart HealthCare System. The attacker could receive patient's privacy information update it and perhaps send false data, consequently, cause a call and a fake emergency (John F. Buford, Eng Keong Lua, 2020)(A. Rajan, J. Jithish, et S. Sankaran,2017).

The figure below shows the Sybil attack:

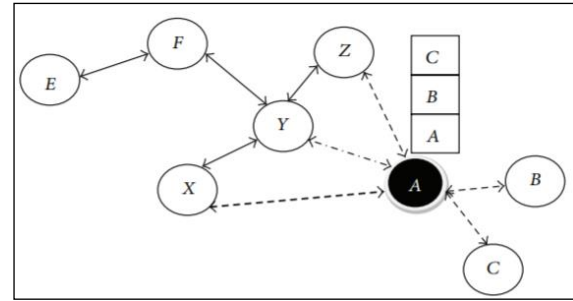


Figure 7:Sybil attacks with multiple ID

B. Select forwarding:

This type of attack is also called "Gray hole attack" it's a special type attack of black hole attack, in which the attacker gain access to single or multiple malicious nodes and behave like normal nodes (I. Butun et al, 2020) in most time but selectively drop not all the packet receives but sensitive packets and the ones selected as showing in the figure 8, just like that the attacker expects to not detected by the IDS (message identities).

There are two ways that the intruder can follow to attack the target system:

- **Insider Attack:** The authentication of the authorized sensor nodes might be compromised or the adversary might steal some key or information from the nodes and attack the whole network.
- **Outsider Attack:** the attacker tries to jump the routing path between legitimate nodes

There are different types of Select forwarding attack such as bellow:

- When the unauthorized nodes do not forward information and decides to drop them randomly, then send their own packets to the other nodes. This kind of attack is titled by **Neglect and Greed**.
- When an unauthorized node delays the messages flowing through them to delude the routing data between the nodes.
- When a packet is forwarded from a legitimate node to a malicious node, it guarantees the legitimate node that the information is forwarded to next node and ultimately drops the packet without being noticed. This attack is called **blind letter attack**.

This attack affects the system very badly, because of the dropped packets by the SF attack, it will be very difficult to recognize the cause of packet drop. The medical health staff may not see the entire picture with uncomplete information, therefore, this can be harmful for the patient or for the medical health system by having a wrong treatment for the patient.

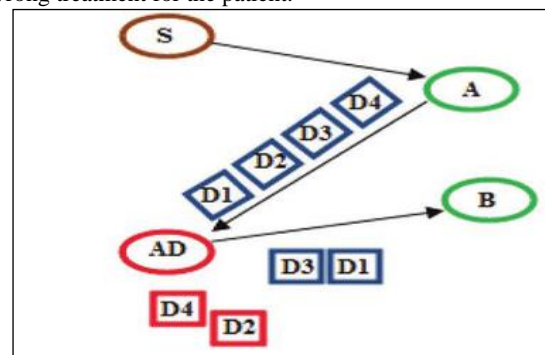


Figure 8: Drops Selected packets of a node

C. Replay Attack

In this type of attack an unauthorized user get access to the Smart Health system, the intruder captures the network traffic and send the message to the receiver acting as the original sender (P. Rughoobur et L. Nagowah, 2017) as showing in the figure 9. The attacker aims to acquire the trust of the system, a replay attack describes as an infraction of security in which some data is stored with no permission and the retransmitted to receiver. This attack can affect bad on a Smart Healthcare System by get an unauthorised access and then stealing patient's informations which they can be very confidentially to diffuse (Bo Yu, Bin Xiao, 2006).

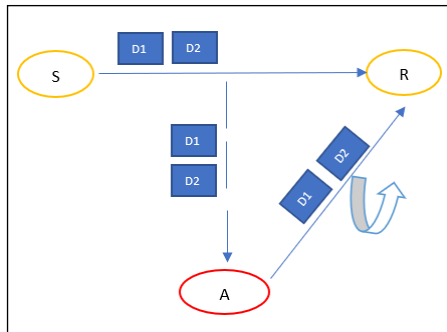


Figure 9:Replay Attack Demonstration

5. SECURITY RECOMMENDATION

The technologies of Smart environment and IoT add many benefits for Smart Health, but they present also new risks, security issues and vulnerabilities, with the fact that the Smart Health devices and sensors are more usually now than before. Those risks include possible harm to the patient's safety and health and unfortunately it may cut a life (A. Chacko et T. Hayajneh, 2020). There are some steps to follow for mitigate the security threats:

1. **Secure storage and management for certificate keys:** cryptography is from the best methods to protect data, it a process that convert the plan text into unintelligible text and vice-versa using keys. Certificate key it an electronic document use to the ownership of the user so he can access to the services that he needs (Digicert.com, 2020).
2. **Updates to cryptographic curves, algorithms, and hashes:** hashes it is the fact of applying mathematical functions to an amount of data.
3. **Conducting a secure boot:** to make sure that when a device is turned on, none of its configurations have been modified.
4. **Authentication:** make sure that there is a proper access control in place of limit unauthorized access to the information.
5. **Smart card:** the role of the smart card is to carry the data in an electronic memory with a available large capacity, however, the data stored on a smart card are secured against being read by anyone unless the person who enable a code and by an authorised reader system Even when the reader system is given the enabling code (R. Neame, 1997) the card may be configured to reveal only some of the data it holds depending on the classification of the user. Smart health cards can also include biometrics to offer strong biometric authentication making sure health services are being delivered to the right patient (Thalesgroup.com,2020).
6. **Strong protocol:** The use of a strong protocol is very important to ensure safety of data stored or exchanged.
7. **Update of the operating systems, devices firmware and applications:** all these systems should be maintained up to

date, its musts be checked regularly and followed by a technical team.

8. **System hardening:** the system hardening should be applied over all the environment components and the hardening procedure must be updated even a new vulnerability or weakness is detected.
9. **Devices and systems end of life:** The replacement of all equipment, devices and systems with end of life and support should be maintained to ensure always updates and new releases on the system.

6. DISCUSSION

The introduction of technology and IoTs in the health field gave birth to Smart Health, this field which is in full expansion especially in the last months and with the appearance of COVID-19 epidemy.

The world is increasingly in need of smart devices and sensors to monitor and examine the patient, so we have seen new technologies that:

- Measure the temperature
- Nursing robot to serve the sick
- Drones to detect contaminated people
- Face recognition systems to alert people
- Smart robots and devices to disinfect offices and places
- Robots to test dozens of people at the same time
- Mobile applications to track the movements of people with the virus
- ... Etc.
-

All these systems and technologies have many advantages for the health and development of humanity, but how can we confirm that these projects respect security standards and that they adopt and apply measures to guarantee the confidentiality of data, especially when we are talking about big data and sensitive information of millions and millions of people?

Is security evolving and following the increasing speed of application development and IoT deployment?

The fraud, attacks and disclosures of sensitive data that our world knows are not enough to stop and go back and think seriously about other alternative and solution to protect information systems from attack and unauthorized access?

Who can guarantee that the data collected is only used for health reasons?

Can development and technology always guarantee us reliable results that have no negative impact on people's health and lives? Everyone is aware that there is no 100% secure system, but do states and domain officials deploy the resources necessary to ensure a tolerable level of security?

Are the secure development standards respected?

All these questions are very important and will always remain valid whether for Smart Health or other environments based on the same technologies.

What is certain is that we must take security seriously, audit systems periodically, trace all actions and accesses made on the data and ensure the permanent evolution of the solutions used and deployed in the different sectors of the world.

7. CONCLUSION

this paper discuss about the Smart Environments and their use which is growing more and more, then it was moved to the Smart Health field and gave an overview of it, this article discusses also about the benefits of Smart Environment for patients, how it helps and facility the health field, added value and all advantages which offer to humanity.

This paper also talks over the important item regarding security and gave a list of requirements that the smart health system should meet to guarantee the security of important and vital data stored, exchanged, and manipulated.

The paper includes a description of two serious attacks that could damage the Smart health system and disclose confidentiality of data.

some security recommendations are given to take into consideration to mitigate security attacks and to maintain patient privacy.

In the future work we will concentrate all the research about how a Smart Healthcare system can prevent and automatically block these kinds of attacks by presenting new security measures and strategies to protect patient's data and life.

REFERENCES

A. Chacko et T. Hayajneh, « Security and Privacy Issues with IoT in Healthcare », *EAI Endorsed Trans. Pervasive Health Technol.*, vol. 4, no 14, juill. 2018, Consulté le: mai 27, 2020. [En ligne]. Disponible sur: <https://eudl.eu/doi/10.4108/eai.13-7-2018.155079>.

A. Rajan, J. Jithish, et S. Sankaran, « Sybil attack in IOT: Modelling and defenses », in *2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, sept. 2017, p. 2323-2327, doi: 10.1109/ICACCI.2017.8126193.

A. Solanas et al., « Smart health: A context-aware health paradigm within smart cities », *IEEE Commun. Mag.*, vol. 52, no 8, p. 74-81, août 2014, doi: 10.1109/MCOM.2014.6871673.

A. Srilakshmi, P. Mohanapriya, D. Harini, et K. Geetha, « IoT based Smart Health Care System to Prevent Security Attacks in SDN », in *2019 Fifth International Conference on Electrical Energy Systems (ICEES)*, févr. 2019, p. 1-7, doi: 10.1109/ICEES.2019.8719236.

Bo Yu, Bin Xiao, « Detecting selective forwarding attacks in wireless sensor networks | Request PDF », ResearchGate. https://www.researchgate.net/publication/220951840_Detecting_selective_forwarding_attacks_in_wireless_sensor_networks (consulté le mai 27, 2020).

C. Gomez, S. Chessa, A. Fleury, G. Roussos, et D. Preuveneers, « Internet of Things for enabling smart environments: A technology-centric perspective », *J. Ambient Intell. Smart Environ.*, vol. 11, no 1, p. 23-43, janv. 2019, doi: 10.3233/AIS-180509.

Digicert.com, « Security Solutions for Healthcare IoT | DigiCert.com », DigiCert. [/internet-of-things/healthcare/](https://internet-of-things/healthcare/) (consulté le mai 29, 2020).

Glob. Health, J., « Smart healthcare: making medical care more intelligent », *Glob. Health J.*, vol. 3, no 3, p. 62-65, sept. 2019, doi: 10.1016/j.glohj.2019.07.001.

I. Butun, P. Österberg, et H. Song, « Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures », *IEEE Commun. Surv. Tutor.*, vol. 22, no 1, p. 616-644, Firstquarter 2020, doi: 10.1109/COMST.2019.2953364.

John F. Buford, Eng Keong Lua, « Sybil Attack - an overview | ScienceDirect Topics », <https://www.sciencedirect.com/topics/computer-science/sybil-attack> (consulté le mai 28, 2020).

Kristen Gloss, « Healthcare IoT security issues: Risks and what to do about them », *IoT Agenda*. <https://internetofthingsagenda.techtarget.com/feature/Healthcare-IoT-security-issues-Risks-and-what-to-do-about-them> (consulté le mai 29, 2020).

P. Rughoobur et L. Nagowah, « A lightweight replay attack detection framework for battery depended IoT devices designed for healthcare », in *2017 International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions) (ICTUS)*, déc. 2017, p. 811-817, doi: 10.1109/ICTUS.2017.8286118.

R. Neame, « Smart cards—the key to trustworthy health information systems », *BMJ*, vol. 314, no 7080, p. 573, févr. 1997, doi: 10.1136/bmj.314.7080.573.

S. A. Butt, J. L. Diaz-Martinez, T. Jamal, A. Ali, E. De-La-Hoz-Franco, et M. Shoaib, « IoT Smart Health Security Threats », in *2019 19th International Conference on Computational Science and Its Applications (ICCSA)*, juill. 2019, p. 26-31, doi: 10.1109/ICCSA.2019.000-8.

Shancang Li, Li Da Xu, « Chapter 9. Confidentiality and Security for IoT Based Healthcare - Securing the Internet of Things [Book] », <https://www.oreilly.com/library/view/securing-the-internet/9780128045053/xhtml/chp009.xhtml> (consulté le mai 28, 2020).

Thalesgroup.com, « Health card and eHealthcare solutions ». <https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/health> (consulté le mai 31, 2020).

Udaya Suriya, Rajamani Vayanaperumal, « (PDF) Detecting and Preventing Sybil Attacks in Wireless Sensor Networks Using Message Authentication and Passing Method », ResearchGate. https://www.researchgate.net/publication/281822967_Detecting_and_Preventing_Sybil_Attacks_in_Wireless_Sensor_Networks_Using_Message_Authentication_and_Passing_Method (consulté le juin 01, 2020).

Y. Zhang, D. Zheng, et R. H. Deng, « Security and Privacy in Smart Health: Efficient Policy-Hiding Attribute-Based Access Control », *IEEE Internet Things J.*, vol. 5, no 3, p. 2130-2145, juin 2018, doi: 10.1109/JIOT.2018.2825289.