NETWORK ATTACKS RELATED TO SMART HEALTHCARE AND THEIR IMPACT EVALUATION

Hiba EL FADILI ,Tomader MAZRI

National School of Applied Sciences, University Ibn Tofail, Kenitra, Morocco – (hiba.elfadili, tomader.mazri) @uit.ac.ma

KEY WORDS: Smart Healthcare, Internet of Things, Security Attacks, Security Strategy, Impact Evaluation, EBIOS Risk Analysis.

ABSTRACT:

The Internet of Things (IoT) has frequently been used by people as a way to facilitate their connection to all types of devices. Thanks to this technology, healthcare field can also benefit from a perfect interaction taking advantage of a better diagnostic and treatment that facilitate life for both patients and doctors. Unfortunately, and similarly to other domains based on technology, the smart healthcare does also use IT programs and wireless network to exchange and analyse data the fact that makes it highly exposed to malicious actions. Moreover, if a good security level is not provided in order to save patients information once hackers get access to the mentioned data, patients might be affected or even lose their lives. This paper presents an overview of the security issues in smart healthcare fields and gives a state of art of some well-known network attacks in the field of smart healthcare. We also propose an impact evaluation of those attacks by adopting four scales of evaluation ‘Minor’, ‘Significant’, ‘Serious’ and ‘Critical’ proposed by EBIOS Gravity assessment. The proposed evaluation is classified based on three criteria: sensor’s nature, application field and intervention time.

1. INTRODUCTION

Smart healthcare can be defined as a set of health services that uses different technologies like IoT and mobile Internet in order to allow communication happen between stakeholders in the health system, this process facilitates access to medical information anytime. An intelligent health system connects people (patients and medical teams), materials and institutions and then actively manages and meets the needs of the medical ecosystem in a smart way. It must ensure that all the participants get the services they need being allowed for a quick and easy decision-making and rational allocation of resources (Chacko and Hayajneh, 2018), (Tian et al., 2019).

To facilitate access to healthcare for patients, some IoT projects like intelligent health monitoring systems have been proposed for being equipped with "health sensors" that helps both the doctor and the patient to consult vital parameters like the level of the arterial pressure, the level of sugar and the heart rate, this system also warns the doctor immediately if it exceeds a threshold. This consultation involves sending the data to the cloud or fog server (Figure 1) allowing the doctor and nurses via their smartphones to monitor the patient's condition anytime and anywhere in the world (Pundir et al., 2020a).

The architecture of Smart healthcare has recently known an evolution in its systems by including lastly an intermediate layer in order to speed up the processing time and increase the real-time reactivity of such application. Figure 1 shows the smart healthcare system architecture in which we can distinguish between three types of layers: sensing, fog and cloud (Naresh et al., 2020).

However, many attacks can affect the normal behaviour of smart healthcare applications as a particular case of IoT systems. In this paper we will address the network related ones mentioning the details of their operating modes. We will then propose an impact evaluation of those attacks based on the EBIOS gravity assessment (ANSSI, 2019). The proposed evaluation is classified on three criteria sensor’s nature, application field and intervention time.

The rest of this paper is organized as follow: section 2 presents a state of art of some attacks that affect smart healthcare systems. Section 3 illustrates the different application fields of the smart healthcare systems. In section 4 we will present the proposed impact study of the attacks on the smart healthcare systems based on EBIOS gravity assessment. Finally, a discussion and conclusion are given as the last part of this work.

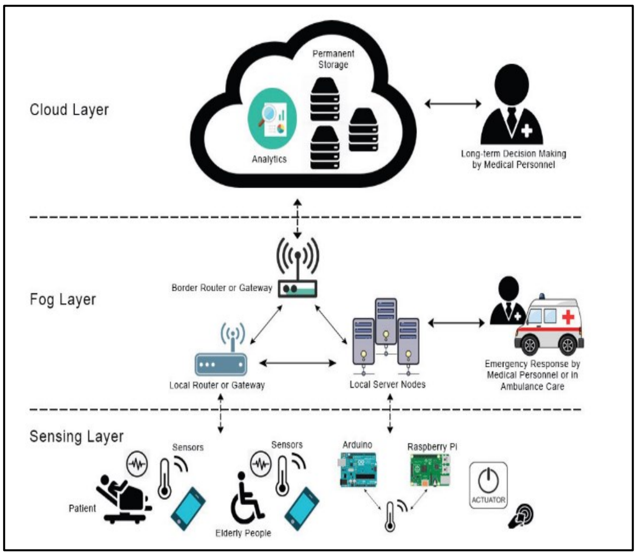

Figure 1: Smart healthcare system architecture (Naresh et al., 2020)

2. THE IMPORTANT NETWORK ATTACKS AGAINST SMART HEALTHCARE

2.1 Denial of Service Attack

This attack generally aims to influence the availability of a system and specifically an IoMT (Internet of Medical things) or medical device.

IoT devices are characterized by: low memory, bandwidth and battery capacity and limited disk space. This makes them very sensitive and easily affected by denial of service (DoS) attacks (Eken and Eken, 2018).

In healthcare systems, an adversary carries out denial of service (DoS) attacks to cause the loss or unavailability of the links used to communicate (Islam et al., 2015). Once launched, these attacks prevent legitimate patients from obtaining appropriate care, including life-saving drugs. These attacks also rob or delay physicians from accessing medical information and records (Yaacoub et al., 2020).

2.2 Hole Attacks

2.2.1. Sinkhole Attack: The Attacking nodes (noted SHA: Sinkhole attacker) begin their work by attracting the other legitimate nodes for the shortest path to the destination. Then legitimate nodes initiate the process of sending their packets through the same path (i.e. via SHA) while the attacking nodes start disrupting the flow of network traffic in four possible ways: not drop any packet (it expects to remain undetected by the IDS), not receiving the information required by the destination stations or receiving partial or modified information. Consequence: a reduction in network performance and degradation in the efficiency and reliability of communication (Pundir et al., 2020b).

Technically, the attacking node manipulates the routing algorithms by first announcing the best possible route (with less hop distance) to the destination (D) to attract its neighbours. Neighbours can then pass their traffic through the route announced by the attacking Sinkhole node. This attraction is not satisfied with the neighbours but can captivate other nodes that are closer to the hole than to the destination D. A scenario of this type of Sinkhole attack is illustrated in Figure 2.

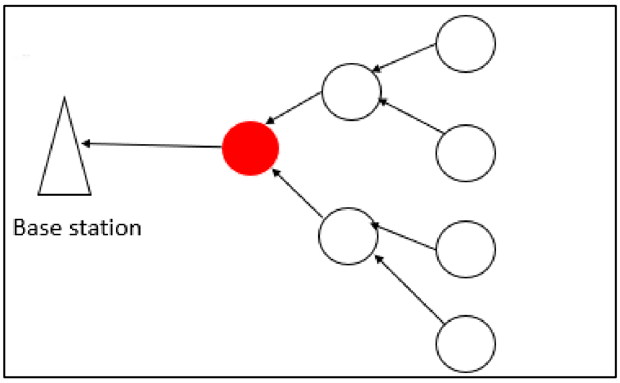

Figure 2. An illustration of the Sinkhole attack

As already explained when the attack is successful, three possibilities are imagined: messages can be dropped by the attacker node, or delayed, or modified. Hence, three types of sinkhole attacker nodes are possible (Wazid et al., 2016), (Butun et al., 2019):

- Sinkhole message modification nodes (SMD);
- Sinkhole message dropping nodes (SDP);
- Sinkhole message delay nodes (SDL).

2.2.2. Blackhole Attack: In this attack, the malicious node drops all the packets it receives from its neighbours and which are intended to be sent to subsequent nodes (figure 3). This attack is more harmful when the Blackhole node is also a Sinkhole. This leads to a halt in all data traffic around the Blackhole. In the literature, this attack is also called "Selfishness".(Butun et al., 2019).

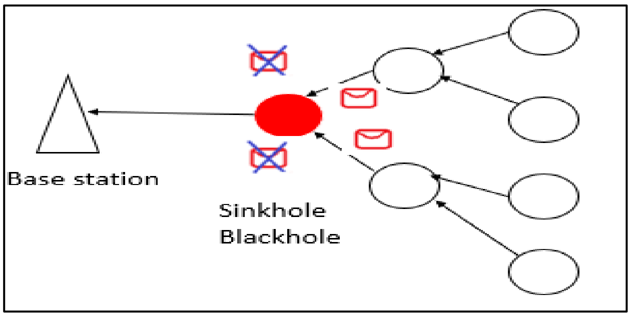

Figure 3. An illustration of the Blackhole attack

2.2.3. Greyhole Attack: This attack also named “selective forwarding” or “select and forwarding” attack is a variant of the Blackhole attack. In this case, the malicious node does not drop all the packets it receives, but some of them (Figure 4). This is an attack that is not easily detected by the IDS. In multi-hop networks Packet forwarding is a major responsibility of a routing node. However, in a selective forwarding attack, the opposing nodes can reject the forwarding of some messages by simply dropping them and ensuring that those packets are no longer handed over to the neighbours. In the Blackhole attack the attacker incurs the following risk: the neighbouring nodes will conclude that they have failed and they may decide to search for another route. In the Greyhole attack, part of the traffic being sent to neighbours, the attacker limits the suspicion of his malicious acts (Butun et al., 2019), (Ambarkar and Shekokar, 2020).

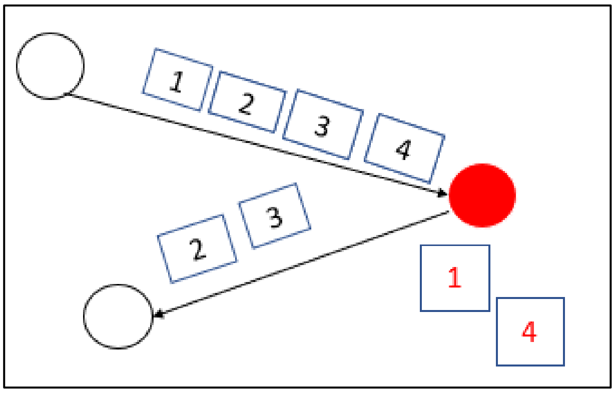

Figure 4. An illustration of the Greyhole attack

2.2.4. Wormhole Attack: This attack is performed when an attacker connects a malicious node in the network with connections that allow it to transmit packets faster than normal data transfer (Figure 5). This leads to the formation of a wormhole in the network (Ambarkar and Shekokar, 2020).

The Wormhole is a tunnel (called fast out-of-band transmission path) created between two nodes that can be used to transmit packets faster. In this way, two remote nodes in the network are advertised as neighbours to attract traffic from the neighbourhood. This makes all nodes that hear transmissions from the second malicious node believe that the node that sent the packets to the first malicious node is their direct neighbour. Other packets that follow the normal route arrive at the destination node later, so they are dropped because they do more hops.

Wormholes are very difficult to be detected and can negatively affect time synchronization, localization and data fusion (Butun et al., 2019).

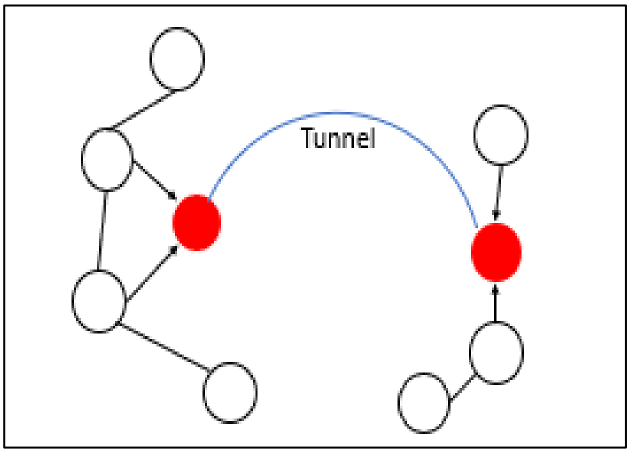

Figure 5. An illustration of the Wormhole attack

2.2.5 Abstract of Hole Attacks

As a summary of Hole Attacks: In Blackhole attack, the malicious node drops all incoming traffic, if the intruding node selects some packets and selectively drops them, it is a Greyhole attack, otherwise if it attracts all traffic to itself- in order to perform malicious actions, it is a Sinkhole attack. Finally, if there is a collaboration of two nodes using a separate fast channel other than the network itself, then it is called a Wormhole attack (Butun et al., 2019).

2.3 Sybil Attack

In this case, a node tries to illegally obtain various identities causing redundancies in the routing protocol. Sybil attacks degrade data integrity, security and resource usage. Sybil node attempts to communicate with neighbouring nodes using the identity of the normal node.

As shown in Figure 6, Sybil node can manage to form a new identity or behave as an already existing and legal one. This causes confusion in the network and leads to its collapses (Suriya et al., 2015) (Wadii et al., 2019).

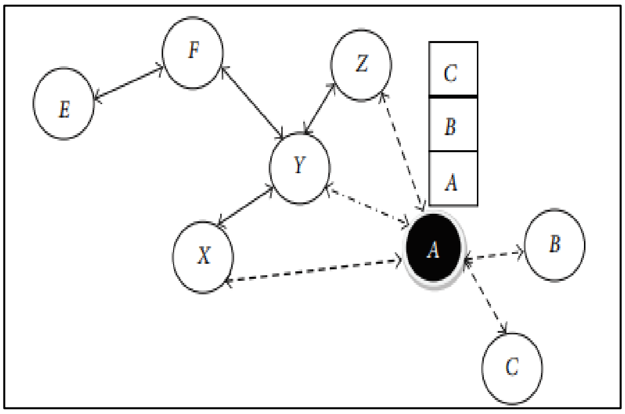

Figure 6. An illustration of the Sybil Attack (Suriya et al., 2015)

In the literature, Sybil attacks are divided into two classes based on the attack mode on the network (Suriya et al., 2015):

- **Direct and indirect attack**: In a direct attack, the real nodes and the Sybil nodes communicate directly. in the indirect attack, communication occurs via a malicious node.
- **Fabricated Attack and Stolen Identity Attack:** new illegal nodes are created using Legal Identities. detection can go through verifying identity replication.

2.4 Replay Attack

In this attack, the adversary can either steal or/and intercept information transmitted by redirecting them to another location. examples of damage can be caused to a given system, including medical systems. The intercepted packets are recorded at first place before being "played back" later on the receiving device. Two consequences are possible in this attack: theft and the leak or the disclosure of sensitive information to gain access to a given medical system (Yaacoub et al., 2020).

The principle of this attack is as follows: certain information are stored by a malicious node without any authorization and then retransmitted to the receiver in order to deceive the latter (Figure 7). The malicious sensor captures network traffic and then communicates with the receiver while acting as the original sender. It is mainly used to thwart authentication, in particular using certificates. In this case, even if the messages are encrypted, the attacker without knowing the real keys and passwords can access the network by retransmission of valid connection messages (Rughoobur and Nagowah, 2018).

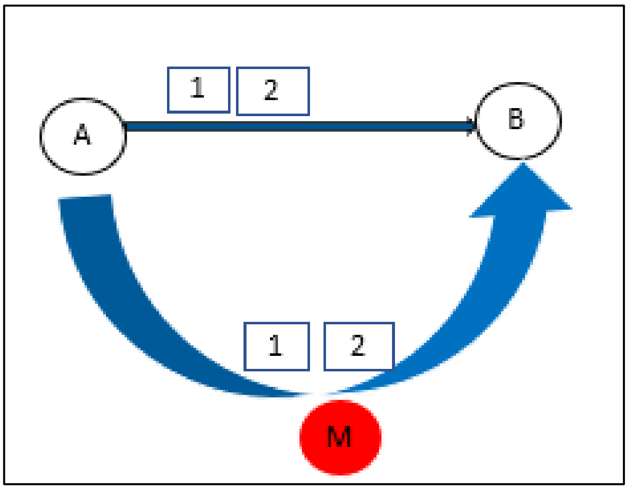

Figure 7. An illustration of the replay attack

2.5 Sensor Attack

Under normal network conditions and due to a lack of power, a sensor can die at any time. In this case, the smart attacker can easily replace the sensor and perform malicious activities. The attacker can modify patient data and insert a false one (Butt et al., 2019).

3. APPLICATION FIELDS

In this section, we will show the main applications of smart healthcare systems and will give the four labels used in the remaining of our risk gravity evaluation. The organization chart (Figure 8) illustrates the several applications of IoT-based healthcare which are divided into four fields, established by (Naresh et al., 2020).

The four domains illustrated in Figure 8 can be explained as follow:

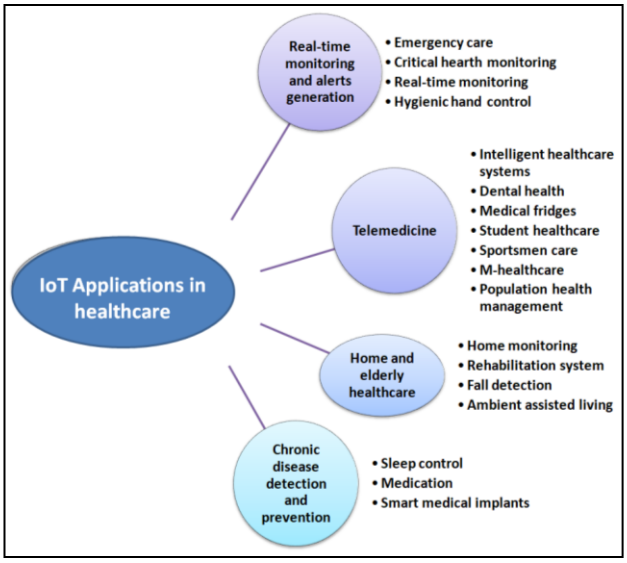

Figure 8. Different Application Fields of Smart Healthcare Systems (Naresh et al., 2020)

3.1 Real-time monitoring and alerts generation

The first application is considered as a continuous monitoring and surveillance of diverse parameters such as:

- Body temperature
- Cardiac activity
- Biochemical parameters like oxygen level in the blood.

These continuous measurements can be provided by deploying sensors in the human body and are controlled by IoT, which evaluates the functioning quality of organs, hence it detects anomalies in order to intervene as early as possible by proposing efficient solutions for the patient.

3.2 Telemedicine

Providing remote health care for patients using the Internet and communication technologies (ICT) significantly reduces operational costs of medical personnel and improves patient health. This system allows physicians to provide emergency and quality health care anytime.

3.3 Home and Elderly healthcare

IoT is a technology that simplifies doctors' immediate intervention in case of emergencies; this technology targets those who are elderly patients or experience difficulties in locomotion and helps save their lives.

3.4 Chronic disease detection and prevention

Chronic diseases such as diabetes, obesity, asthma, etc, are serious health problems that can lead to depression and several health complications. Detecting them earlier helps reducing their consequences. IoT is capable to do the prevention and can also propose the appropriate treatments and control smart medical implants which releases drugs automatically following a specific timing depending on each patient.

In the remaining work, we will adopt the following domain labels (as shown in Table 1).

Domain label	Domain name
D1	Real-time monitoring and alert generation
D2	Telemedicine
D3	Home and elderly healthcare
D4	Chronic disease detection and prevention

Table 1. Labelling of the four healthcare domains used for our gravity evaluation

4. THE PROPOSED IMPACT STUDY OF THE ATTACKS ON THE SMART HEALTHCARE SYSTEMS

In this section, we propose the following classifications of the impact of the attacks on the smart healthcare systems based on the three criteria: sensor's nature, application field and intervention time.

We will adopt the four scales of evaluation proposed by the EBIOS methodology (ANSSI, 2019). adapted for our smart healthcare applications (as shown in Table 2).

Scale	Gravity	Consequences for the smart healthcare applications
G4	Critical	*The inability to provide all or part of services to patients *Possible serious impacts on the safety of persons and property. *The IoT provider will likely not overcome the situation (its survival is threatened)
G3	Serious	*A sharp deterioration in the performance of the services to patients, * Probably a significant impact on the safety of persons and property. *The IoT provider will overcome the situation with serious difficulties (functioning in very degraded mode)
G2	Significant	*Degradation of service performances *Without impact on the safety of persons and property. * The IoT provider will overcome the situation despite some difficulties (functioning in degraded mode)
G1	Minor	* No operational impact on the performance of the services *No impact on the safety of persons and property. *The IoT provider will overcome the situation without too many difficulties

Table 2. Proposed gravity evaluation based on EBIOS methodology

4.1. Classification based on nature of sensors

The first proposed impact evaluation is based on the nature of sensors. According to the work of (Naresh et al., 2020) (Figure 9), sensors can be divided into two categories: 'clinical' and 'non-clinical'.

In a clinical setting, sensors are used to monitor patient vital signs such as:

- Temperature,
- The ECG,
- Blood pressure,
- Blood oxygen saturation,
- Etc.

It also helps physicians have a dashboard in order to visualize data. The sensors can be deployed and monitored remotely enabling remote healthcare.

In a non-clinical setting, sensors can be used to:

- Asset monitoring,
- Location of the doctor,
- Compliance with hygiene standards,
- Location of ambulances in case of emergency
- Operational efficiency by tracking assets, people inside the hospital, and providing real-time information for logistics.

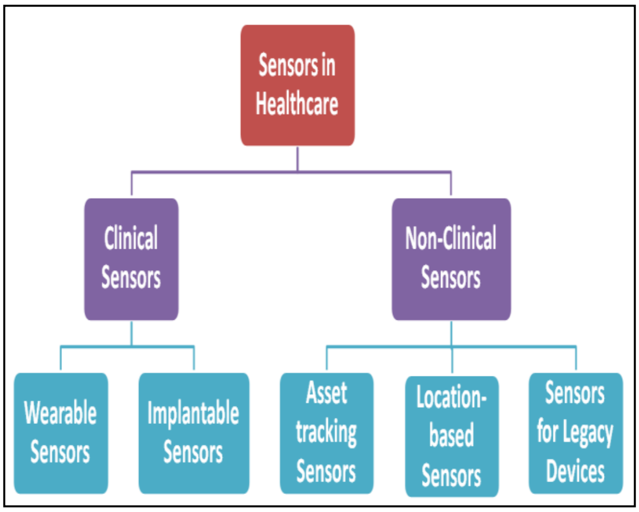

Figure 9. Classification of sensors in healthcare systems (Naresh et al., 2020)

Based on this classification we notice that the attacks on sensors that directly affect patients 'clinical ones' have more impact than on those 'non clinical' that affect assets, location of doctors…etc. Table 3 shows the impacts on the two sensors natures.

	Sensors nature	
	Clinical sensors	**Non-clinical sensors**
Impact Evaluation	**G4**	**G1 – G3**

Table 3.Impact of all the studied attacks on healthcare applications classified by nature of the sensors.

4.2. Classification based on application field

The second proposed classification is based on the application field. Table 4 shows the proposed impact evaluation.

Attack	Impact D1	Impact D2	Impact D3	Impact D4
Denial of Service	G1	G2 -G4	G2 -G4	G2 -G3
Sinkhole	G1	G2-G4	G2-G4	G2 -G3
Blackhole	G1	G2- G4	G2 -G4	G2- G3
Greyhole	G1	G2-G3	G2 -G3	G2
Wormhole	G1	G2 -G3	G2-G3	G2
Sybil	G1	G2 -G4	G2-G4	G2- G3
Replay	G1	G2 -G4	G2-G4	G2- G3
Sensor	G4	G4	G4	G4

Table 4. The proposed impact evaluation based on the application field.

We can conclude from Table 4 that the severity of impact differs from one attack to another as explained bellow:

4.2.1 Denial of Service Attack: Denial of service affects servers and makes them unavailable preventing them from being used by legitimate users. The influence of this attack on the 1st domain is minor because the Denial-of-Service attack does not affect the sensors but rather the servers.

As for the 2nd area, the attack can affect telemedicine with a significant level of severity and can even be critical as it makes the doctor unable to intervene or consult the condition of his patient.

While the 3rd domain, the DoS may cause the impossibility of providing home care since the servers are unavailable and may have a significant and critical severity level.

Finally for the 4th domain: chronic disease detection and prevention, DoS attack can impact with a significant level of severity and can be serious but not critical because chronic diseases treatments usually last for long term. Thus, its impact is less important compared to the 2nd and 3rd domains.

4.2.2 Hole Attacks: The influence of these attacks on the 1st domain always remains in the lower of severity level because they don't affect data collection while they can have an impact on alerts.

As for the 2nd domain the Sinkhole and Blackhole attacks will have the same influence on telemedicine with a "significant" level of gravity and even critical because the doctor would not manage to consult the state of his patient, therefore cannot intervene because of the deleted data or false alerts in the case of Sinkhole attack. As for the Greyhole and Wormhole, they impact telemedicine with a significant and serious level of severity but not critical because the part of the data that arrives can be useful for telemedicine even if another part is deleted.

The impact of the Sinkhole and Blackhole attack on the 3rd domain can be “significant” to “critical”, because doctors and nurses would not be able to intervene at home if they do not receive notifications on their server due to data being deleted or modified, this will generate false alerts.
As for Greyhole and Wormhole, they can impact with a significant and serious scale but not critical because the part of the data that arrives can be useful to intervene at home.

Concerning the 4th domain Sinkhole and Blackhole attacks can impact with a significant scale because the treatment of chronic diseases is long term process, but the scale can be serious due to deleted or modified data. The Wormhole and Greyhole attacks can have an influence on the 4th domain with a significant but not serious scale of gravity when compared to Sinkhole and Blackhole because some of the data arrives to the destination and also because the treatments of chronic diseases are long term which makes the impact less important.

4.2.3 Sybil and Replay Attacks: The same analysis used for Hole attacks and Denial of Service attack are applicable for the 1st domain, we notice that the gravity in domain 2 and 3 is greater compared to wormhole and Greyhole attacks.
As for the fourth domain we can apply the same analysis used in DoS, Sinkhole and Greyhole attacks.

4.2.4 Sensor Attack: The impact of the "Sensor" attack on the four domains is very serious because these attacks affect the nodes that collect data directly from the patient. As Data collection gets affected the rest of the process cannot take place. This explains G4 level for the four domains.

4.3. Classification based on intervention time

The third proposed classification is the impact based on the intervention time. Depending on the fact that the application necessitates a real-time reaction (cardiology, covid epidemic) or not (applications requiring medium or long-term care), the gravity of the impact will consequently increase (Table 5).

	Application nature	
	Real-time application	**Non-real-time application**
Impact Evaluation	**G4**	**G1 – G3**

Table 5. Impact of all the studied attack classified by intervention time

5. DISCUSSION

We can first note that the least impacted area is that of "Real-time monitoring and alert generation" because usually attacks affect the nodes that route the packets and also affect the servers in the cloud (except sensors attacks). For other attacks, the impact remains almost the same.

We also note that the most dangerous attacks for the healthcare systems are those which affect real-time health applications and more specifically those who affect sensors and the particular clinical sensors with a critical gravity level (G4). These attacks affect the collection of information and therefore if this collection does not take place the whole process of routing, storage, processing and healthcare will not take place anymore. This is why we can say that this type of attack is the most dangerous for all the system.

This means that we must pay more attention to attacks that affect the sensors and develop more mechanisms to protect them. This begins with the autonomy in energy and the verification of the duplication of identities on the network after the end of node’s autonomy.

The smart healthcare apparatus being frequently threaten by security attacks may affect the patient’s sensitive data or even lead to his death. Indeed, it is important to build a security strategy for making smart healthcare more secure against attacks. The first step in this process (Figure 10) will start by focusing on the attacks that represent the highest impacts on the system and by applying encryption (as a first mechanism) containing secret keys that use efficient cryptographic algorithms and protocols in a minimum of time in order to preserve the device battery autonomy. For those attacks (having great impacts), the authentication will be adopted (as a second mechanism) to preserve the confidentiality of data. The third mechanism is the fault tolerance that guaranties the persistence of services in case those attacks affect data availability.
In case the exchanged data over the Smart healthcare network has been accessed, this strategy will work to prevent the malicious attack from seeing or modifying the content of the transited traffic and messages.

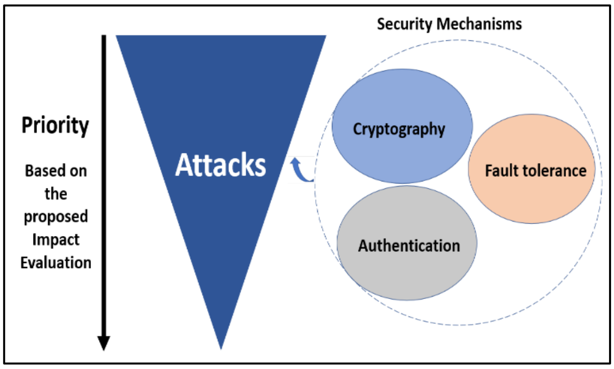

Figure 10. The adopted security strategy based on our impact evaluation

6. CONCLUSION

This paper presented a state of art on some well-known attacks in smart healthcare fields. We have proposed an impact evaluation of those attacks based on the EBIOS gravity assessment.

Our evaluation is classified on three criteria: sensor’s nature, application field and intervention time. This study will be useful, as a part of risk analysis, in the development of countermeasures adapted for each attack regarding its risk for the specific healthcare domain.

As a perspective of our work and since we have established a study of the impact of the underlined attacks, we will try in the next work to start our security strategy by prioritizing the attacks that have the highest impact on the healthcare systems and by implementing the corresponding security mechanisms including authentication, cryptography and fault tolerance. Furthermore, an internal audit and pentests can be periodically performed to update this security strategy.

REFERENCES

Ambarkar, S.S., Shekokar, N., 2020. Toward Smart and Secure IoT Based Healthcare System, Studies in Systems, Decision and Control. Springer International Publishing. https://doi.org/10.1007/978-3-030-39047-1_13

ANSSI, 2019. EBIOS RISK MANAGER - En [WWW Document].URL https://www.ssi.gouv.fr/uploads/2019/11/anssi-guide-ebios_risk_manager-en-v1.0.pdf (accessed 1.5.21).

Butt, S.A., Diaz-Martinez, J.L., Jamal, T., Ali, A., De-La-Hoz-Franco, E., Shoaib, M., 2019. IoT Smart Health Security Threats. Proc. - 2019 19th Int. Conf. Comput. Sci. Its Appl. ICCSA 2019 26–31. https://doi.org/10.1109/ICCSA.2019.000-8

Butun, I., Osterberg, P., Song, H., 2019. Security of the Internet of Things : Vulnerabilities , Attacks and Countermeasures. IEEE Commun. Surv. Tutorials PP, 1. https://doi.org/10.1109/COMST.2019.2953364

Chacko, A., Hayajneh, T., 2018. Security and Privacy Issues with IoT in Healthcare. EAI Endorsed Trans. Pervasive Heal. Technol. 4, 1–7. https://doi.org/10.4108/eai.13-7-2018.155079

Eken, C., Eken, H., 2018. Security Threats and Recommendation in IoT Healthcare. Proc. 9th EUROSIM Congr. Model. Simulation, EUROSIM 2016, 57th SIMS Conf. Simul. Model. SIMS 2016 142, 369–374. https://doi.org/10.3384/ecp17142369

Islam, S.M.R., Kwak, D., Kabir, M.H., Hossain, M., Kwak, K.S., 2015. The internet of things for health care: A comprehensive survey. IEEE Access 3, 678–708. https://doi.org/10.1109/ACCESS.2015.2437951

Naresh, V.S., Pericherla, S.S., Murty, P.S.R., Reddi, S., 2020. Internet of things in healthcare: Architecture, applications, challenges, and solutions. Comput. Syst. Sci. Eng. 35, 411–421. https://doi.org/10.32604/csse.2020.35.411

Pundir, S., Wazid, M., Singh, D.P., Das, A.K., Rodrigues, J.J.P.C., Park, Y., 2020a. Intrusion Detection Protocols in Wireless Sensor Networks Integrated to Internet of Things Deployment: Survey and Future Challenges. IEEE Access 8, 3343–3363. https://doi.org/10.1109/ACCESS.2019.2962829

Pundir, S., Wazid, M., Singh, D.P., Das, A.K., Rodrigues, J.J.P.C., Park, Y., 2020b. Designing efficient sinkhole attack detection mechanism in edge-based IoT deployment. Sensors (Switzerland) 20, 1–27. https://doi.org/10.3390/s20051300

Rughoobur, P., Nagowah, L., 2018. A lightweight replay attack detection framework for battery depended IoT devices designed for healthcare. 2017 Int. Conf. Infocom Technol. Unmanned Syst. Trends Futur. Dir. ICTUS 2017 2018-Janua, 811–817. https://doi.org/10.1109/ICTUS.2017.8286118

Suriya, U., Kumar, R., Vayanaperumal, R., 2015. Detecting and Preventing Sybil Attacks in Wireless Sensor Networks Using Message Authentication and Passing Method 2015. https://doi.org/10.1155/2015/841267

Tian, S., Yang, W., Grange, J.M. Le, Wang, P., Huang, W., Ye, Z., 2019. Smart healthcare: making medical care more intelligent. J. Glob. Health 3, 62–65. https://doi.org/10.1016/j.glohj.2019.07.001

Wadii, J., Rim, H., Ridha, B., 2019. Detecting and preventing Sybil attacks in wireless sensor networks. Mediterr. Microw. Symp. 2019-Octob. https://doi.org/10.1109/MMS48040.2019.9157321

Wazid, M., Das, A.K., Kumari, S., Khan, M.K., 2016. Design of sinkhole node detection mechanism for hierarchical wireless sensor networks. Secur. Commun. Networks 9, 4596–4614. https://doi.org/10.1002/sec.1652

Yaacoub, J.P.A., Noura, M., Noura, H.N., Salman, O., Yaacoub, E., Couturier, R., Chehab, A., 2020. Securing internet of medical things systems: Limitations, issues and recommendations. Futur. Gener. Comput. Syst. 105, 581–606. https://doi.org/10.1016/j.future.2019.12.028