Online-Journals.org

iJOE International Journal of Online and Biomedical Engineering

iJOE | eISSN: 2626-8493 | Vol. 21 No. 9 (2025) | OPEN ACCESS

https://doi.org/10.3991/ijoe.v21i09.55517

PAPER

STRIDE-Based Threat Modeling and Risk Assessment Framework for IoT-enabled Smart Healthcare Systems

Zineb Nadifi[1], Mariyam Ouaissa[1](✉), Mariya Ouaissa[2], Mohamed Alhyan[1], Ali Kartit[1]

[1]LTI, Chouaib Doukkali University, El Jadida, Morocco

[2]LISI, Cadi Ayyad University, Marrakech, Morocco

ouaissa.mariyam@ucd.ac.ma

ABSTRACT

The increase in the evolution of Internet of Things (IoT) architectures and their use in different domains, such as agriculture, smart cities/homes, industry, transport and logistics, and others, has triggered a proportional increase in vulnerabilities, threats, and security risks that violate security objectives. The criticality of the information circulating in the architecture and assets exposed to public networks such as the internet imperatively implies effective management beforehand of the factors that can put a system at risk. This article focuses mainly on the IoT in the healthcare sector and uses it as a pilot for an in-depth study of vulnerabilities using a threat modeling approach based on the spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege (STRIDE) method. This will be carried out by carefully following the steps of explaining the use case, drawing a data flow diagram (DFD) using the tool offered by Microsoft Threat Modeling (MTM) tool, and identifying the assets in question. This is followed by an identification of the threats linked to the DFD and identified assets, then an assessment of the risks caused, and finally proposals for security patches to be applied as far as possible to ensure the efficient and secure use of an architecture that offers many advantages in terms of services and ease of management of modern domains but which at the same time puts at risk all the assets that can cause significant damage and impact if they are exposed to malicious hands.

KEYWORDS

Internet of Things (IoT), healthcare, threat modeling, spoofing, tampering, repudiation, information disclosure, denial of service and elevation of privilege (STRIDE), data flow diagram (DFD), Microsoft threat modeling (MTM), common vulnerability scoring system (CVSS)

1 INTRODUCTION

The Internet of Things (IoT) is a modern concept that focuses on the creation and formation of an ecosystem that connects different local and internet-based

Nadifi, Z., Ouaissa, M., Ouaissa, M., Alhyan, M., Kartit, A. (2025). STRIDE-Based Threat Modeling and Risk Assessment Framework for IoT-enabled Smart Healthcare Systems. *International Journal of Online and Biomedical Engineering (iJOE)*, 21(9), pp. 63–80. https://doi.org/10.3991/ijoe.v21i09.55517

Article submitted 2025-03-14. Revision uploaded 2025-04-26. Final acceptance 2025-04-29.

© 2025 by the authors of this article. Published under CC-BY.

equipment and devices to create a more controllable and supervised environment [1]. This environment can refer to artificial intelligence (AI) and intelligent techniques to make decisions based on the inputs it receives as information and predefined thresholds. The control, analysis, supervision, and decision-making mechanism is ensured by instantaneous exchanges of information and data between the devices in the IoT architecture; on the other hand, this circulation and transmission puts the privacy and confidentiality of the data at risk in view of its exposure on a public network such as the Internet, which leads to a better examination and analysis of the structure of the IoT architecture in question in order to avoid or at least minimize the threats that may face the secure transmission of information, hence the need for a prior phase that can ensure this task, which is threat modeling [2].

The benefits of IoT architecture are increasing more and more, given the services and facilities offered by the IoT and the diversity of areas it touches. However, despite this fact, the deployment of the solution is still improvised and requires prior study to properly investigate the vulnerabilities that can cause security impacts during the data transmission, analysis, and exchange process [3]. This article will discuss the importance of threat modeling in threat prevention, following one of the famous and effective approaches, spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege (STRIDE), which will be carefully applied in the field of healthcare.

Attackers are increasing the rate of cyberattacks launched against IoT architectures because they are aware of the criticality of the healthcare sector. Data transmission really has no tolerance for error, because even a simple change in a blood pressure value, heartbeat, or other factor can have an impact on the decisions taken by doctors and nurses, which can have catastrophic consequences for a patient's health–a change in a diabetic patient's blood sugar level can be life-threatening! A mix-up or alteration in patient results can pose a serious threat to either the patient's life or the reputation of the health organization and can also result in legal action by the patient's family against the hospital in question [4].

A direct deployment of the architecture leads to an improvised management of the security problems that can occur and that can negatively impact the effectiveness of the architecture, which requires a prior study of the threat scenarios and vulnerabilities that can be exploited by attackers and a good awareness of the impact of the risks in the event of compromise. This will help enormously in the management and maintenance of a stable and effective architecture. In this article, a study in threat modeling format will be applied to a healthcare prototype in an IoT environment, and a possible risk assessment will be carried out, as well as a proposed mitigation and correction plan for the threats identified [5]. The aim of this research is to shed light on a number of points that could serve as a future reference and basis for another research in the same field. Below are some of the main objectives targeted by this paper:

1. Identify vulnerabilities and threats related to IoT in the healthcare sector.
2. Based on the STRIDE methodology, propose an effective threat modeling framework, using the Microsoft Threat Modeling (MTM) Tool to draw the data flow diagram (DFD).
3. Detail the assets, access points, and threat scenarios that can be covered by domain healthcare.
4. Apply risk assessment and their impact on confidentiality, integrity, availability, and other security objectives if the identified vulnerabilities are exploited.

5. Apply risk assessment and their impact on confidentiality, integrity, availability, and other security objectives if the vulnerabilities identified are to be exploited using the common vulnerability scoring system (CVSS) and 5 by 5 matrix.
6. Promoting a better understanding of the emerging risks associated with IoT technologies in healthcare.
7. Propose security countermeasures that can deal with the threats identified to ensure optimal and secure use of the IoT in healthcare.

The structure of this paper is as follows: The subsequent section provides an overview of previous works. Section 3 discusses the threat modeling methodology and tools. We present the proposed methodology in Section 4. Section 5 presents the results along with discussion. Conclusions are drawn in Section 6.

2 RELATED WORK

Given the importance, topicality, and richness of the subject, it has been the subject of various research and articles and has been tackled from different nails and approaches. The study in [6] started with the importance of defining security levels in an IoT environment, then it defined the domains that the IoT can act in, such as healthcare, commerce, and smart homes, and then it identified the vulnerabilities and threats for each of the three types, calculating the score of their criticality with CVSS, to finally give recommendations of measures to follow in each domain.

Authors in [7] dealt with the area of healthcare in an IoT environment by combining the STRIDE and DREAD approaches, identifying threats using the STRIDE methodology, assessing them using DREAD, and proposing mitigations at the end.

The work in [8] focused on medical devices, starting by defining an example of attack graph models to deduce risks for medical devices, tracing threats on a body surface area reference, namely wireless body area networks, Bluetooth attacks, Android attacks, and also giving corrective solutions for these attacks.

Authors in [9] indicated that the Secure and Resilient Scheme for Telecare Medical Information Systems (SRSTMIS) framework offers a secure and resilient solution thanks to White-Box Cryptography (WBC) and a protocol validated against various attacks. It also used STRIDE to announce the threats identified and, in return, the solutions proposed by SRSTMIS as security measures.

The research in [10] focused on medical cyber-physical systems (MCPS) and the criticality it presents in terms of data confidentiality, integrity, and availability, and therefore used MCPS stakeholders to identify threats via a trust model. The threats were effectively classified according to their violation of the three security objectives: confidentiality, integrity, and availability, leading to remedies to guarantee a secure MCPS with the minimum possible attack surfaces.

The paper [11] presented the telehealth system according to the STRIDE methodology, starting with an explanation of the telehealth system and its zones, namely Point-of-Care, which presents the patient's environment and sensor, Health & Care Services, which is based on the healthcare professional's environment, and Health Information Services (HIS) Infrastructure, which presents the cloud part where all the data is transmitted, processed and analyzed before being sent to doctors/nurses, processed and analyzed before being sent to doctors/nurses, then [10] gave an overview of the assets and access points, the threats identified according to the STRIDE categorization extracted from the Data Flow

Diagram of the MTM Tool, and a presentation at the end of a mitigation plan and countermeasures.

Authors in [12] focused on mHealth, giving a prototype presentation of its architecture, which he used to define the assets, then presented the types of threats according to the STRIDE approach, and traced the DFD, and presented each asset with the impact that could cause its compromise, then using the DREAD methodology, he qualified the level of impact of each threat, with a final description of possible mitigation strategies.

The work in [13] spoke about modern medical devices (MMDs) and MEDICALHARM as a model designed to identify and manage threats specific to MMDs, combining risk analysis and shift-left security using different approaches and tools, namely STRIDE, a 5 by 5 matrix, common vulnerability scoring system.

The authors in [14] discuss the importance of strengthening cybersecurity in the healthcare sector, given that with increasing digitization (electronic medical records, telemedicine), hospitals have become prime targets for cyberattacks. To do this, it details the impact of cyber threats in the healthcare sector, the methodologies that can be used in the study (PASTA, STRIDE, VAST, etc.), and the importance of risk assessment in decision-making after integrating threat modeling with scenario and contingency planning, and an examination of the results.

This article will address a healthcare prototype in the IoT environment, applying threat modeling following the STRIDE methodology, and assessing beforehand the risks of the impacts that may be caused in the event of threats identified from the DFD on the MTM tool with the two methods CVSS and 5 by 5 matrix, based on which recommendations for countermeasures will be proposed at the end of the work.

3 THREAT MODELING

Threat modeling is a proactive step in a scenario of deploying a new architecture or changing and/or updating a current system; it is a preventive step that aims to number the vulnerabilities present in an environment beforehand while citing the threats that may arise if these vulnerabilities are not addressed [15]. Threat modeling can be applied in a number of ways, including:

DREAD: Potential for damage, reproducibility, usability, affected users, and discoverability.

PASTA: Attack simulation and threat analysis process.

LINDDUN: Linking, identifying, non-repudiation, detecting, data disclosure, unawareness, and non-compliance.

STRIDE: Spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege.

Each approach aims at a different perspective and will be adequate and effective in some environments more than others; this paper will focus on STRIDE as a method. STRIDE is a threat modeling approach that aims to classify vulnerabilities into six categories, hence its nomenclature [16].

S (Spoofing): This type of attack refers to the usurpation of the user's identity. It enables the attacker to gain the privileges and rights of the target. This type of attack is equivalent to identity theft.

T (Tampering): This is the unauthorized modification or change of information, which may be a transmitted message, a database, code, user input, etc. This type of behavior directly affects the system. This type of behavior directly affects integrity.

R (Repudiation): the act of denying one's actions, i.e., when users carry out modifications, additions, or deletions and dispute their actions, this can have a remarkable impact on traceability and the organization of responsibilities.

I (Information disclosure): the leakage of information and its disclosure, giving access to resources or data to people and entities who are not authorized to have them. The presence of vulnerabilities of this type has an impact on confidentiality.

D (Denial of service) is explained by the inability to access a resource or data in a moment of need following a constraint on the target. The target will either be bombarded and occupied by the processing of requests and requests arriving from a harmful source or disconnected altogether following a sudden overload that has finally brought the target's processing to a standstill. This type of threat impacts the target's availability.

E (Elevation of privilege): corresponds to a vertical movement in accounts, which consists of migrating from an account with limited privileges to another with more rights and more freedom to execute commands and access resources without being detected or alerted by monitoring tools.

4 PROPOSED METHODOLOGY

To study the threat modeling model in one of the modern domains, the following steps will be taken (see Figure 1).

Fig. 1. Proposed threat modeling methodology steps

4.1 Use case explanation

The IoT domain that will be represented in this paper is healthcare. Its architecture is made up of the following parts [17, 18].

The sensor perimeter. This perimeter contains sensors that interact following indicators received and captured from the environment in which they are installed. These sensors can be connected watches, patches, bracelets, etc., worn by the patient or placed in their environment, which record body movements, measure heart rate, oxygen saturation, body temperature, etc. In reality, these sensors are supported by an application installed on the patient's mobile. The application is supposed to both arrange the data collected from sensors (watches, thermometers, etc.) and offer forms to be filled in manually by the patient to provide greater clarification and visibility regarding their state of health. All this data and information will then be sent to a gateway for further processing. Various sensors can be implemented or worn by the patient (refer to Table 1).

Table 1. Description of sensors

Sensor Type	Description
Heart Rate Monitor (HRM)	Captures and measures heart rate (beats per minute) to detect human heart rhythm.
Electrocardiogram Sensor (ECG)	Measures the electrical activity of the heart using electrodes placed on the skin, and presents the heartbeat rate in the form of a diagram called an electrocardiogram. It is often used to detect cardiac disorders in patients, such as arrhythmias or atrial fibrillation, and requires the intervention of a medical expert to analyze its results.
Electronic Blood Pressure Meter (BP)	Allows measurement of systolic and diastolic blood pressure (in mmHg), and blood pressure in the patient, used for people suffering from hypertension, detect variations in pressure
Oxygen Saturation Sensor (SpO_2)	Measures the percentage of oxygen in the blood, and is used in patients suffering from respiratory problems or lung diseases. It was very much in demand during the COVID-19 period, as the virus had an impact on the lungs, to determine whether the percentage of oxygen circulating in the blood is normal (greater than or equal to 95%).
Thermometer	Measures the variation in patients' body temperature to detect hyperthermia, or early signs of infection or fever.
Spirometer	Used to measure respiratory rate (number of breaths per minute).
Continuous Glucose Monitoring (CGM)	Tracks blood glucose (sugar) levels over time, especially useful for diabetics.
Electromyography (EMG)	Measure the electrical activity of muscles, to assess muscular and nervous conditions, or in rehabilitation to monitor muscle contractions.
Accelerometer	Measure movements and changes in body posture, used to monitor patients with reduced mobility, to detect their movements and prevent them from falling.
pH and ion concentration sensors	Determines alkalinity or acidity and pH levels or concentration of specific ions in body fluids (e.g. blood pH, potassium concentration).
GPS trackers	Indicates the position at the moment the patient takes a measurement by tracking its location.
Electrooculography (EOG)	Measure the corneo-retinal standing potential that exists between the front and the back of the human eye.

Gateway. The gateway acts as an intermediary between the perimeter of the sensors and the IoT architecture in the cloud. It first receives the data collected by the sensors and/or the forms filled out by the patients via communication protocols wireless such as Bluetooth, Wi-Fi, Zigbee, or LTE. It then processes this data at its level to aggregate the data and format it. It also ensures initial filtering to avoid the massive sending of non-essential information and optimize consumption bandwidth. The gateway can be smartphones, home hubs, or IoT routers.

IoT cloud architecture. After gathering the information and data collected by the sensors and/or entered by the patient via his mobile application through the gateway, it performs an initial filtering before sending the data via an internet network to the IoT cloud architecture. This mass of information is supposed to be collected and processed by the electronic and personal health record systems (EHRs, PHRs). The data and information received are stored in the cloud or on local server, or in a hybrid way. Each one of the three ways has its own advantages and inconveniences, Storage locally is more secure and can be fully controlled but is still limited and expensive in terms of maintenance and scalability, the one in the cloud is cheaper in terms of infrastructure cost and maintenance, and also the local users don't have to carry out the updates; however, the problems related to security, privacy, and regulatory non-compliance are still big issues for storage in the cloud. Azure, AWS, and Google are famous examples of these service providers. The hybrid mode is a solution that take from both -local and cloud- advantages and mix them up by storing the critical information in local servers and leaving secondary data in the cloud. The percentages, rates, and indications on the instant health state of the patient presents a large mass of information which must be analyzed and processed carefully so that

doctors can make the right decisions regarding standard thresholds, the care of the information is ensured by monitoring services and Artificial Intelligence to provide help and support to doctors to better manage their decision-making/actions, given that medical staff can sometimes manage several cases remotely, which minimizes or even reduces the error rate.

Medical personal area. This scope is specific to healthcare staff (doctors and nurses), who base their decisions on the results of analyses and conclusions received from the IoT area architecture presenting the patient's state of health. Healthcare professionals consult the status of their patient at any time from the application installed on their mobile phone, and can also have dashboard views of the patient's condition.

To summarize the use case sequence, and as shown in Figure 2, the transmission and processing of the patient's health is as follows: the various sensors within the patient's perimeter detect and measure physical quantities (temperature, gesture movement, eye contact, etc.) depending on their nature. According to their nature, these sensors are supported on a mobile application of the patient, who can still use it to fill out a form that answers questionnaires related to his state of health. This information will then be sent to a gateway for an initial filtering before it will be stored, processed, and analyzed in the IoT architecture cloud via electronic and personal health record systems (EHRs, PHRs), AI, and storage units. The results of these analyses will be visible on the application installed on the medical staff's mobile phones, which, based on them, can make decisions about adjusting, adding, or modifying medical parameters or taking action.

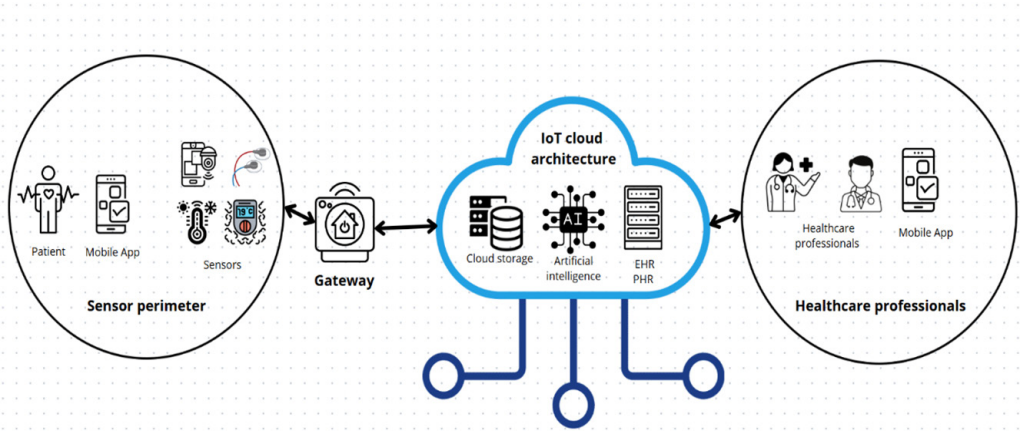

Fig. 2. IoT prototype architecture for healthcare domain

4.2 Security requirements

According to this case study, there is a set of prerequisites to be validated in the architecture, from the patient's environment to the healthcare professionals. To avoid any risk of access to the mobile phone that supports the sensors and on which the application is installed, the phone must be protected with an access method that is either biometric or at least a schema or pin code, and then the application must also be protected by identifiers to be entered that will be examined at the level of a database server, for example, Azure. The same applies to healthcare professionals, so the deployment of solutions that help to maintain and ensure confidentiality, integrity, availability (CIA) security objectives, and others [19].

4.3 Data flow diagram

The DFD is a graphical presentation that explains and details how the healthcare architecture works in an IoT environment [20]. Simplifying the processes via the DFD makes it easier to understand the sequence of information exchanges, and above all to identify the vulnerabilities and threats linked to the assets in the architecture, which then helps to propose a mitigation and correction plan, either by eliminating the threat altogether, or by reducing it, or by circumventing it to better manage the impact that may be caused in case it is exploited (see Figure 3).

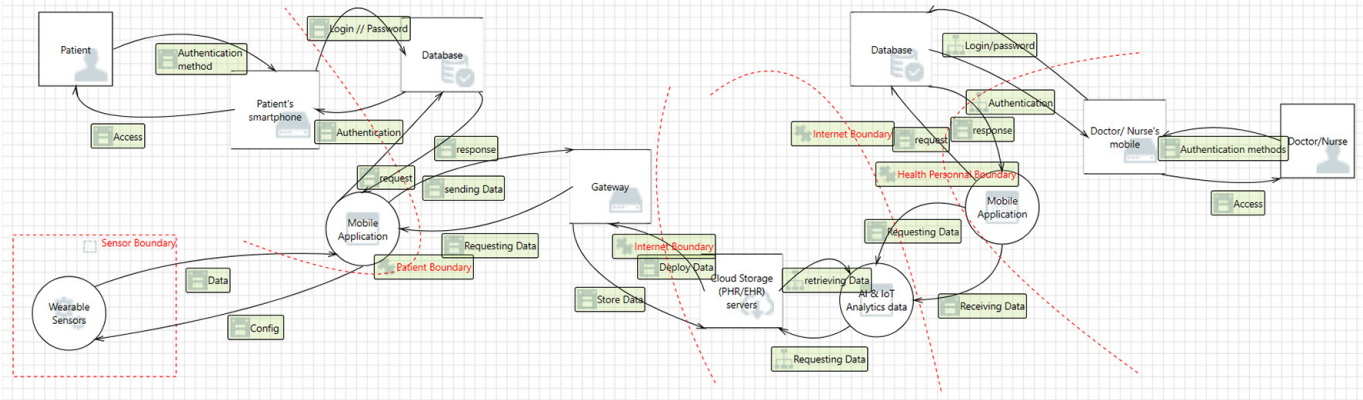

Fig. 3. Data flow diagram of the key components and security boundaries of a healthcare system modeled using the Microsoft threat modeling tool

4.4 Asset identification

Asset identification is a critical step in threat modeling for IoT-enabled smart healthcare environments, as it lays the foundation for understanding and protecting the key components of the system. In such environments, assets include a wide range of interconnected elements, such as wearable devices, medical sensors, healthcare applications, cloud platforms, patient data repositories, and network infrastructure. Each asset plays a vital role in delivering efficient, real-time healthcare services, making them potential targets for cyber threats. Identifying these assets involves categorizing them by their function, value, and interaction within the system, as well as recognizing their dependencies and vulnerabilities. This process ensures that critical assets, like patient records, life-support systems, and diagnostic equipment, are prioritized in threat mitigation strategies. By thoroughly mapping and classifying assets, healthcare providers can enhance system resilience, ensure regulatory compliance, and safeguard the trust and well-being of patients [21].

4.5 Threat identification

Following the application of the threat modeling approach, the next step is threat identification, as illustrated in Figure 3. By employing the STRIDE threat modeling technique within the MTM tool, a detailed threat report was generated for each component in the DFD. Subsequently, all identified threats were documented separately in Section 5 of the results. These listed threats highlight how specific components can be compromised by various threats. We also detailed the assets impacted

by each STRIDE threat and their correlation with security requirement violations. After cataloging all the threats identified through the STRIDE technique, we further analyzed which of these threats could lead to attacks [22].

4.6 Risk assessment

Risk assessment is a critical component of threat modeling, enabling organizations to prioritize and mitigate potential vulnerabilities effectively. By systematically identifying and analyzing risks, threat modeling offers a structured approach to improving system security. Two widely used methods for quantifying and visualizing risks are the CVSS and the 5×5 risk matrix. CVSS provides a standardized framework for evaluating the severity of vulnerabilities based on factors such as exploitability, impact, and environmental modifications. Complementing this, the 5×5 matrix visualizes risks by categorizing them according to likelihood and impact, offering a straightforward and intuitive decision-making tool. Together, these methods enable security teams to balance quantitative precision with practical prioritization, ensuring that mitigation efforts focus on the most critical threats. This article delves into the integration of CVSS and the 5×5 matrix, highlighting their synergy in building a comprehensive risk assessment framework [23].

4.7 Threat mitigation

After identifying threats and the risk assessment in IoT healthcare, the next step is to propose appropriate mitigation techniques. Threat mitigation involves reducing or eliminating potential risks within a system. To develop effective mitigation strategies, we analyzed various existing approaches and, based on these studies, selected the most suitable remedies to protect the IoT smart healthcare use case from these potential threats, as discussed in Section 5.4.

5 RESULTS AND DISCUSSION

In this section, we conduct experiments using the MTM tool to identify threats through the STRIDE methodology and evaluate the risk assessment. As previously discussed, STRIDE categorizes and maps the identified threats based on the use case. To achieve thorough threat identification, we integrated findings from both STRIDE methodologies to more effectively evaluate all potential threats in our IoT smart healthcare use case. Subsequently, we propose mitigation techniques to enhance the security of smart healthcare against possible attacks.

5.1 Asset identification

An asset is a valuable entity that the user needs to protect and secure against any type of attack in order to maintain it in a good condition that ensures it is usable and available in the event of need. Assets can be either physical, such as mobile phones, computers, servers, etc., or software, such as applications and operating systems, or commercial, when it is a question of the reputation and image of the entity seeking to protect it, or informational, such as any kind of document that may contain valid information, for example, configuration files, commitment charters, photos, videos, etc.

Although the assets have an important and indispensable value, they obviously become the main goal of the attackers who seek access points to one of the assets; hence the need to identify the assets and their entry points to have a view of an attacker and gain more visibility in relation to the axes, which can then be exploited by them to guarantee illegal and unauthorized access to a given system or architecture (refer to Table 2).

Table 2. Description of assets

Asset	Description
Wearable sensors	Sensors dedicated to capturing the patient's physical parameters.
Patient's smartphone	The smartphone, from which the sensors are supported, and from which the patient can fill in the forms.
Patient Credentials	The patient's login details, enabling them to access the application on their smartphone.
Patient's personnel data	Information relating to the patient, i.e. surname, first name, date of birth, patient ID, as well as the data that the patient will enter in the forms.
Storage server (PHR/EHR)	The Patient's data is transmitted to the PHR/HER servers for storage, and treatment
Healthcare professionals' mobile	The smartphone of the doctor/nurse where the application is installed on.
The application	The application installed on the Healthcare professionals' mobile that shows all the information and statistics regarding the patient's health state, and on the patient's smartphone so he can field the forms and receive the data from the sensors.
The Healthcare professionals' credentials	The login and password used by the doctors/nurses to access to the application, and to the mobile.
Data flowing	Data circulating in the architecture network.

5.2 Threat identification

According to STRIDE, the threats can be categorized under six categories following each letter of it, and each one impact one of the security's objectives (refer to Table 3).

Table 3. STRIDE model threat and security objective violation

Letter	Threat	Security Objective's Violation
S	Spoofing	Authentication
T	Tampering	Integrity
R	Repudiation	Non-repudiation
I	Information disclosure	Confidentiality
D	Denial of service	Availability
E	Elevation of privilege	Authorization

Below are descripted the threats identified from the diagram classed by the approach STRIDE (refer to Table 4).

Table 4. Threat identification following STRIDE approach

STRIDE	Asset	Threat
S ➔ Spoofing	Data Store Patient's smartphone	**V.S.1** – Patient's smartphone may be spoofed by an attacker and this may lead to incorrect data delivered to patient.
	Wearable Sensors/Mobile Application	**V.S.2** – Wearable Sensors/Mobile Application may be spoofed by an attacker and this may lead to unauthorized access to Wearable Sensors/Mobile Application.
	Cloud Storage (PHR/EHR)	**V.S.3** – Cloud Storage (PHR/EHR) servers may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of Cloud Storage (PHR/EHR) servers.
T ➔ Tampering	Wearable Sensors	**V.T.1** – The information and measure provided by the sensors to the application mobile may be modified, either by a direct human interaction, or by a change of the sensor's threshold settings. If Wearable Sensors is given access to memory, such as shared memory or pointers, or is given the ability to control what Mobile Application executes (for example, passing back a function pointer.), then Wearable Sensors can tamper with Mobile Application.
	Data flow	**V.T.2** – Data flowing across Data may be tampered with by an attacker. This may lead to a denial-of-service attack against Mobile Application or an elevation of privilege attack against Mobile Application or an information disclosure by Mobile Application. Failure to verify that input is as expected is a root cause of a very large number of exploitable issues.
	Mobile Application	**V.T.3** – Mobile Application could be a subject to a cross-site scripting attack if it does not sanitize untrusted input.
	Mobile Application	**V.T.4** – Mobile Application could be a subject to a persistent cross-site scripting attack if it does not sanitize data store 'Database' inputs and output.
	Database server	**V.T.5** – SQL injection is an attack in which malicious code is inserted into strings that are later passed to an instance of SQL Server for parsing and execution. Any procedure that constructs SQL statements should be reviewed for injection vulnerabilities because SQL Server will execute all syntactically valid queries that it receives. Even parameterized data can be manipulated by a skilled and determined attacker.
R ➔ Repudiation	Mobile Application/AI & IoT Analytics data	**V.R.1** – Mobile Application/AI & IoT Analytics data claim that it did not receive data from a source outside the trust boundary.
	Patient's smartphone/Healthcare professionals' mobile	**V.R.2** – Patient's smartphone claims that it did not write data received from an entity on the other side of the trust boundary.
I ➔ Information Disclosure	The patient's data/Cloud Storage (PHR/EHR) servers	**V.I.1** – Improper data protection of Patient's smartphone/Cloud Storage (PHR/EHR) servers can allow an attacker to read information not intended for disclosure.
	Data flowing	**V.I.2** – Data flowing across Data may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations.
	Patient's credentials/The Healthcare professionals' credentials	**V.I.3** – Credentials on the wire are often subject to sniffing by an attacker. For example, sending a zip file with the password in the email.
D ➔ Denial of Service	Mobile Application	**V.D.1** – Mobile Application crashes, halts, stops or runs slowly; in all cases violating an availability metric.
	AI & IoT Analytics data/Cloud Storage (PHR/EHR)	**V.D.2** – If AI & IoT Analytics data or Cloud Storage (PHR/EHR) servers may be a victim of control resource consumption if they deadlock instead of they do timeout.
E ➔ Elevation of Privilege	Wearable Sensors	**V.E.1** – Mobile Application may be able to impersonate the context of Wearable Sensors in order to gain additional privilege.
	Mobile application/AI & IoT Analytics data	**V.E.2** – An attacker may pass data into Mobile Application/AI & IoT Analytics data in order to change the flow of program execution within Mobile Application/AI & IoT Analytics data to the attacker's choosing.

5.3 Risk assessment

Risk assessment is a process that involves assessing the threats identified through threat modeling, quantifying the risks, and putting in place measures to mitigate them in order to ensure the protection of resources and assets, reduce financial losses, improve decision-making, and other reasons.

Common vulnerability scoring system. The risk assessment of the threats and vulnerabilities identified above can be carried out using the CVSS, which rates the risk of vulnerabilities on a scale of 0 to 10 in ascending order according to the severity and impact of the vulnerability. The division of the score with respect to the severity and the hierarchy of the criticality of the vulnerability is presented in Table 5.

Table 5. Allocation of vulnerability severity scores according to CVSS

Severity	Score
None	0
Low	0.1 ➔ 3.9
Medium	4.0 ➔ 6.9
High	7.0 ➔ 8.9
Critical	9.0 ➔ 10.0

Following CVSS v3.1 Calculator, the score is calculated by calling up the following parameters in Figure 4 and Table 6.

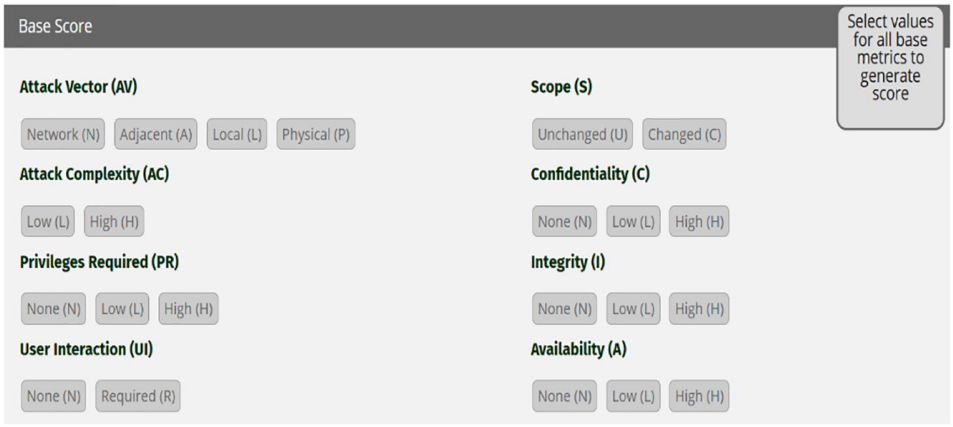

Fig. 4. The base score parameters

Attack vector (AV): Defines the level of proximity required by the attacker to exploit the vulnerability.

Attack complexity (AC): Indicates the difficulty of exploiting the vulnerability.

Privileges required (PR): Reflects the level of access privileges an attacker needs before exploiting the vulnerability.

User interaction (UI): Describes whether an interaction of the user is needed in the exploit process.

Scope (S): Indicates if exploitation affects components outside the vulnerable component's security scope.

Confidentiality (C): Describes the potential impact on the confidentiality of data.

Integrity (I): Reflects the impact on the accuracy and reliability of data.

Availability (A): Describes the impact on the availability of the affected component.

Table 6. The threats score following CVSS v3.1 calculator

Vulnerabilities	AV	AC	PR	UI	S	C	I	A	Score	Severity
V.S.1	N	L	N	N	C	N	H	N	7.1	High
V.S.2	N	L	N	N	C	H	H	H	10	Critical
V.S.3	N	L	N	N	C	H	H	N	10	Critical
V.T.1	L	L	L	N	C	L	H	L	7.9	High
V.T.2	N	L	N	N	C	H	H	H	10	Critical
V.T.3	N	L	N	R	C	L	L	N	6.1	Medium
V.T.4	N	L	N	R	C	H	H	L	9.6	Critical
V.T.5	N	L	N	N	C	H	H	H	10	Critical
V.R.1	N	L	N	N	C	H	L	L	9.9	Critical
V.R.2	N	L	N	R	C	H	L	L	8.8	High
V.I.1	N	L	N	N	C	H	N	N	8.6	High
V.I.2	N	L	N	N	U	H	N	N	7.5	High
V.I.3	N	L	N	N	U	H	N	N	7.5	High
V.D.1	N	H	L	R	U	L	N	H	5.4	Medium
V.D.2	N	L	L	N	U	L	N	H	7.1	High
V.E.1	N	L	L	N	C	H	H	N	9.6	Critical
V.E.2	N	L	N	N	U	H	H	L	9.4	Critical

5 by 5 risk matrix. 5 by 5 risk matrix is a useful tool used in risk assessment which aims to assess threats by combining their impact and likelihood grated from low to extreme, in order to identify and prioritize assets before conducting the assessment. The impact is defined as how severe would the outcomes be if the risk occurred, and the likelihood is presented by what is the probability the risk will happen.

The risk is calculated using the equation ➔ Risk rating = Impact * Likelihood, and can be categorized as low, medium, high, or extreme and color-coded in green, yellow, orange, and red respectively as shown in the matrix in Figure 5.

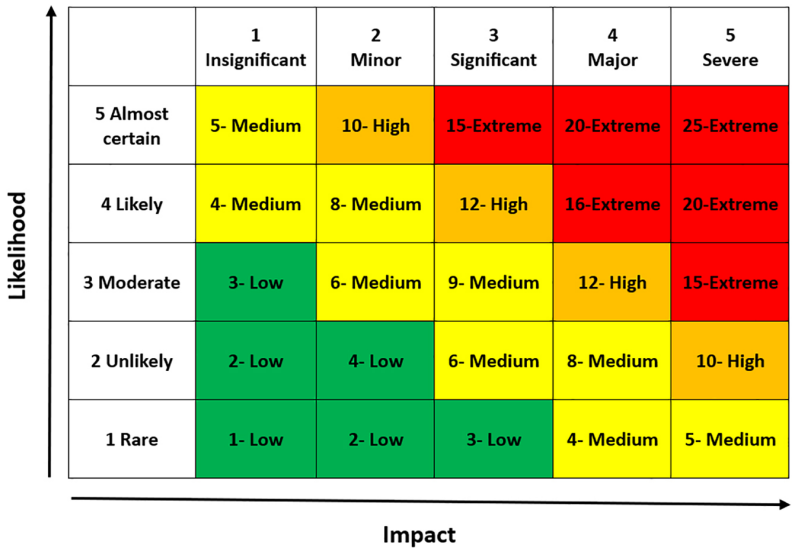

Fig. 5. 5 by 5 Risk Matrix representing the likelihood and impact of identified threats in the healthcare system

Based on the 5×5 matrix, a threat assessment was carried out, and summarized in the Table 7.

Table 7. Risk rating based on 5 by 5 risk matrix

Threat	Likelihood	Impact	Risk Rating
V.S.1	3 (Moderate)	3 (Significant)	9 (Medium)
V.S.2	4 (Likely)	4 (Major)	16 (Extreme)
V.S.3	4 (Likely)	5 (Severe)	20 (Extreme)
V.T.1	3 (Moderate)	4 (Major)	12 (High)
V.T.2	4 (Likely)	5 (Severe)	20 (Extreme)
V.T.3	3 (Moderate)	3 (Significant)	9 (Medium)
V.T.4	4 (Likely)	4 (Major)	16 (Extreme)
V.T.5	4 (Likely)	5 (Severe)	20 (Extreme)
V.R.1	3 (Moderate)	3 (Significant)	9 (Medium)
V.R.2	2 (Unlikely)	3 (Significant)	6 (Medium)
V.I.1	4 (Likely)	5 (Severe)	20 (Extreme)
V.I.2	4 (Likely)	4 (Major)	16 (Extreme)
V.I.3	4 (Likely)	4 (Major)	16 (Extreme)
V.D.1	3 (Moderate)	4 (Major)	12 (High)
V.D.2	3 (Moderate)	5 (Severe)	15 (Extreme)
V.E.1	3 (Moderate)	4 (Major)	12 (High)
V.E.2	4 (Likely)	5 (Severe)	20 (Extreme)

The risk assessment of threats is often very high either in CVSS or 5 by 5 matrix because of the healthcare sector, which requires great vigilance in terms of data confidentiality, integrity, and availability; the criticality of the information circulating in the architecture; and the impact that can be caused in the event of compromise and false decision or consultation that can lead to a serious error in the patient's health, which increases the rate of each risk.

5.4 Threat mitigation

Once the threats have been identified and classified according to the STRIDE approach, it's time to propose a list of mitigation measures to limit the impact that can be caused if one of the threats is exploited (refer to Table 8).

Table 8. List of mitigation countermeasures

Threat	Countermeasure
S ➔ Spoofing	– *Strong password*: Patients and Healthcare professionals must use passwords that meet security requirements such as: avoid using sequential numbers, dates of birth, names and words found in the dictionary, avoid reusing passwords, or storing them in files on the computer, or on a pad of paper, use at least twelve letters combined with numbers, upper case, lower case, digits and special characters. – *MFA*: Use of two-factor authentication, the first with a password, and the second with a notification sent by email or SMS, or by a biometric index. – *Digital certificates*: Use of PKI for certificate management to verify the identity of each device before it is connected to the network, with periodic renewal of certificates to ensure they are not compromised.
T ➔ Tampering	– *Hash*: In view of the fact that tampering violates integrity, and therefore to prevent data from being altered, it is recommended to use a strong hash of the information circulating in the network. – *Memory isolation and management*: In order to prevent from access to memory such as shared memory or pointers, double check whether if the functions could work with less access to memory, such as passing data rather than pointers. Copy in data provided, and then validate it. – *Input validation*: Use of approval lists (whitelisting) by using validation APIs, check that file paths and data points are correct and secure (path validation) by using for example absolute paths instead of relative paths in order to avoid 'path traversal attacks', Data type validation and size control. – *Filter database input*: Applying a special character filtering, deny extended URLs, sanitize data and limit special characters can help prevent SQL injection and cross-site scripting (xss) attacks. – *Role-based access management (RBAC)*: Restrict access to data and systems to people who need them for their jobs.
R ➔ Repudiation	– *Audit logs and timestamps*: Use of logs/events/logs to track actions taken (additions/modifications/deletions) on networks; these logs are injected by default into a group of security tools such as IDS, IPS, firewalls, computers, etc. – *Log audit*: Regular auditing of events generated by security tools can circumvent problems that have arisen within a favorable timeframe. – *SIEM tool*: use of a SIEM solution to correlate the logs linked to all the security tools implemented in the network, i.e. IPS, IDS, NDR probes, EDR, etc.
I ➔ Information disclosure	– *Encryption*: Use data encryption algorithms and protocols such as SSL/TLS to guarantee the confidentiality of information. – *Authentication mechanism*: Use a strong authentication mechanism such as a strong password, MFA…etc. – *File and directory permissions management*: Verification of the rights granted to users over files and folders to ensure that access is restricted, especially to critical and sensitive files.
D ➔ Denial of service	– *Next-generation firewall*: using NGF helps to detect attacks such as DOS, since it is based not only on traffic filtering but also on analyzing the conformity and homogeneity of the user's session. This is ensured by integrating other blades such as IDP/IPS, anti-spam, anti-malware, etc. – Using a timeout in resource response instead of deadlock.
E ➔ Elevation of privilege	– *Privilege management*: Establish Appropriate Privileges and Strict Access. – *Separation of responsibilities*: Avoid giving full access and authority to a profile so as not to risk losing all privileges in the event of a compromise. – *EDR*: use of EDR to monitor all activities, including the elevation of privilege on an account, in real time.

6 CONCLUSION

This paper sheds light on the threats that can put an IoT architecture at risk. The area covered is healthcare, which is a critical and sensitive area given that it affects patients' health directly, and the right to make mistakes is very intolerable and can lead to catastrophic consequences; hence the importance of modeling the threats before deploying the architecture in order to study and assess the possible risks, and this work proposes countermeasures and solutions to the threats identified. This paper has been written in the hope that it will serve as a point of reference for other work on the same subject and to provide a basis for further research. By identifying development-level threats specific to the IoT healthcare context and correlating them with appropriate mitigation strategies, the proposed approach enhances the overall security posture of IoT systems. As IoT continues to evolve, proactive and comprehensive threat modeling will be crucial in safeguarding against emerging security risks and ensuring the resilience of IoT healthcare environments. This work can be further enhanced by implementing the proposed mitigation techniques in a real-world system, allowing for deeper insights into securing the underlying infrastructure against attacks.

7 REFERENCES

[1] Z. Nadifi, M. Ouaissa, M. Ouaissa, M. Alhyan, and A. Kartit, "Security, privacy, and trust in IoT networks," in *Artificial Intelligence for Blockchain and Cybersecurity Powered IoT Applications*. Boca Raton, FL: CRC Press, vol. 19, 2025. https://doi.org/10.1201/9781003497585-2

[2] A. R. Mahlous, "Threat model and risk management for a smart home IoT system," *Informatica*, vol. 47, no. 1, 2023. https://doi.org/10.31449/inf.v47i1.4526

[3] M. Ouaissa and M. Ouaissa, "Cyber security issues for IoT based smart grid infrastructure," *IOP Conference Series: Materials Science and Engineering*, vol. 937, no. 1, p. 012001, 2020. https://doi.org/10.1088/1757-899X/937/1/012001

[4] W. Xiong and R. Lagerström, "Threat modeling – A systematic literature review," *Computers & Security*, vol. 84, pp. 53–69, 2019. https://doi.org/10.1016/j.cose.2019.03.010

[5] M. Ouaissa and M. Ouaissa, "Analyzing and mitigating attacks in IoT smart home using a threat modeling approach-based STRIDE," *International Journal of Interactive Mobile Technologies*, vol. 19, no. 2, pp. 126–142, 2025. https://doi.org/10.3991/ijim.v19i02.52377

[6] S. Rizvi, R. Pipetti, N. McIntyre, J. Todd, and I. Williams, "Threat model for securing internet of things (IoT) network at device level," *Internet of Things*, vol. 11, p. 100240, 2020. https://doi.org/10.1016/j.iot.2020.100240

[7] A. Omotosho, B. Ayemlo Haruna, and O. Mikail Olaniyi, "Threat modeling of internet of things health devices," *Journal of Applied Security Research*, vol. 14, no. 1, pp. 106–121, 2019. https://doi.org/10.1080/19361610.2019.1545278

[8] P. Luckett, J. T. McDonald, and W. B. Glisson, "Attack-graph threat modeling assessment of ambulatory medical devices," *arXiv preprint arXiv:1709.05026*, 2017.

[9] S. S. Ahamad, M. Al-Shehri, and I. Keshta, "A secure and resilient scheme for telecare medical information systems with threat modeling and formal verification," *IEEE Access*, vol. 10, pp. 120227–120244, 2022. https://doi.org/10.1109/ACCESS.2022.3217230

[10] H. Almohri, L. Cheng, D. Yao, and H. Alemzadeh, "On threat modeling and mitigation of medical cyber-physical systems," in *2017 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE)*, 2017, pp. 114–119. https://doi.org/10.1109/CHASE.2017.69

[11] M. Abomhara, M. Gerdes, and G. M. Køien, "A stride-based threat model for telehealth systems," *Norsk informasjonssikkerhetskonferanse (NISK)*, vol. 8, no. 1, pp. 82–96, 2015.

[12] M. Cagnazzo, M. Hertlein, T. Holz, and N. Pohlmann, "Threat modeling for mobile health systems," in *2018 IEEE Wireless Communications and Networking Conference Workshops (WCNCW)*, 2018, pp. 314–319. https://doi.org/10.1109/WCNCW.2018.8369033

[13] E. Kwarteng and M. Cebe, "MEDICALHARM-A threat modeling designed for modern medical devices," in *2023 IEEE 22nd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 2023, pp. 1147–1156. https://doi.org/10.1109/TrustCom60117.2023.00157

[14] A. A. Salami, U. T. I. Igwenagu, C. E. Mesode, O. O. Olaniyi, and O. B. Oladoyinbo, "Beyond conventional threat defense: Implementing advanced threat modeling techniques, risk modeling frameworks and contingency planning in the healthcare sector for enhanced data security," *Journal of Engineering Research and Reports*, vol. 26, no. 5, pp. 304–323, 2024. https://doi.org/10.9734/jerr/2024/v26i51156

[15] A. Seeam, O. S. Ogbeh, S. Guness, and X. Bellekens, "Threat modeling and security issues for the internet of things," in *2019 Conference on Next Generation Computing Applications (NextComp)*, 2019, pp. 1–8. https://doi.org/10.1109/NEXTCOMP.2019.8883642

[16] Z. Abuabed, A. Alsadeh, and A. Taweel, "STRIDE threat model-based framework for assessing the vulnerabilities of modern vehicles," *Computers & Security*, vol. 133, p. 103391, 2023. https://doi.org/10.1016/j.cose.2023.103391

[17] V. S. Naresh, S. S. Pericherla, P. S. R. Murty, and S. Reddi, "Internet of things in healthcare: Architecture, applications, challenges, and solutions," *Computer Systems Science & Engineering*, vol. 35, no. 6, pp. 411–421, 2020. https://doi.org/10.32604/csse.2020.35.411

[18] N. Kumar, "IoT architecture and system design for healthcare systems," in *2017 International Conference on Smart Technologies for Smart Nation (SmartTechCon)*, 2017, pp. 1118–1123. https://doi.org/10.1109/SmartTechCon.2017.8358543

[19] I. Lee, "Internet of Things (IoT) cybersecurity: Literature review and IoT cyber risk management," *Future Internet*, vol. 12, no. 9, p. 157, 2020. https://doi.org/10.3390/fi12090157

[20] S. Raja, S. S. Manikandasaran, and R. Doss, "Threat modeling and IoT attack surfaces," in *Immersive Technology in Smart Cities: Augmented and Virtual Reality in IoT*. Cham: Springer, 2022, pp. 229–258. https://doi.org/10.1007/978-3-030-66607-1_11

[21] S. Madanian, T. Chinbat, M. Subasinghage, D. Airehrour, F. Hassandoust, and S. Yongchareon, "Health IoT threats: Survey of risks and vulnerabilities," *Future Internet*, vol. 16, no. 11, p. 389, 2024. https://doi.org/10.3390/fi16110389

[22] A. Konev, A. Shelupanov, M. Kataev, V. Ageeva, and A. Nabieva, "A survey on threat-modeling techniques: Protected objects and classification of threats," *Symmetry*, vol. 14, no. 3, p. 549, 2022. https://doi.org/10.3390/sym14030549

[23] L. Zhang, A. Taal, R. Cushing, C. de Laat, and P. Grosso, "A risk-level assessment system based on the STRIDE/DREAD model for digital data marketplaces," *International Journal of Information Security*, vol. 21, pp. 509–525, 2022. https://doi.org/10.1007/s10207-021-00566-3

8 AUTHORS

Zineb Nadifi is currently a Professor/Trainer at Institute specializing in new information and communication technologies. She received her engineer's degree in Network and Telecommunications in 2015. She is a PhD student at ENSA, Chouaib Doukkali University El Jadida, Morocco. Her research interests include Network, Cybersecurity, and Internet of Things.

Mariyam Ouaissa is currently an Asssitant Professor in Netwroks and Systems at ENSA, Chouaib Doukkali University El Jadida, Morocco. She is a Ph.D. in Computer Science and Networks graduated in 2019 from Moulay Ismail University, ENSAM, Meknes, Morocco. Her main research topics are IoT, M2M, WSN, Vehicular Networks, Cellular Networks. She is mainly working on M2M congestion overload problem, security and the resource allocation management. She has published more than 70 research papers. She is Editor in several books (Springer, De Gruyter, RGN Publications) and Guest Editor in several special issues of journals (E-mail: ouaissa.mariyam@ucd.ac.ma).

Mariya Ouaissa is a Professor in Cybersecurity and Networks at FSSM, Cadi Ayyad University, Marrakech, Morocco. She is a Ph.D. graduated in 2019 in Computer Science and Network from ENSAM, Moulay Ismail University, Meknes, Morocco. Her main research topics are Cybersecurity, IoT, M2M, D2D, WSN, Cellular Networks, Vehicular Networks. She has published over than 90 papers (Book Chapters, International Journals, and Conferences/Workshops), 30 Edited Books, and 10 Special Issues as guest editor.

Mohamed Alhyan is currently a Professor/Trainer at Institute specializing in new information and communication technologies. He received his engineer's degree in Network and Telecommunications in 2017. He is a PhD student at ENSA, Chouaib Doukkali University El Jadida, Morocco. His research interests include Network, Security, Cloud and Vehicular Networks.

Ali Kartit earned his Ph.D. in Computer Science, specializing in computer network security, from the Faculty of Sciences at Mohamed V University in Rabat. He is currently an Assistant Professor at Chouaib Doukkali University. With over 14 years of experience in the field of computing, he has spent the past decade in technical and vocational education as a computer network trainer, particularly focusing on the module 'Computer Network Security Principles'.