Vulnerability and Threat Assessment Framework for Internet of Things Systems

Mohammad Beyrouti, Ahmed Lounis, Benjamin Lussier, Abdelmadjid Bouadallah, Abed Ellatif Samhat

Vulnerability and Threat Assessment Framework for Internet of Things Systems

Mohammad Beyrouti*, Ahmed Lounis*, Benjamin Lussier*, Abdelmadjid Bouadallah*
, Abed Ellatif Samhat†
*Aliance Sorbonne University, University of Technology of Compiegne, CNRS, Heudiasyc, UMR 7253, France
{Mohammad.beyrouti, Ahmed.lounis, Benjamin.lussier, Madjid.bouabdallah}@hds.utc.fr
†Faculty of Engineering-CRSI, Lebanese University
{Samhat}@ul.edu.lb

***Abstract*—The introduction of IoT technology in different domains and systems has led to a spectacular increase in the number of connected objects. However, this increase in resource-constrained devices was accompanied by numerous vulnerabilities, allowing attackers to penetrate deeply into IoT networks. As identifying these vulnerabilities is a difficult task, our work aims to propose a general threat and vulnerability assessment method, taking into consideration the IoT constraints to identify and assess the vulnerabilities and possible attacks on IoT networks. This method uses several existing databases but focuses on entries relevant to IoT components. We validate our approach using an IoT smart healthcare system as a case study. The suggested approach has produced an applicable methodology to provide a tool for users, vendors, and researchers to be aware of vulnerabilities and possible attacks on an IoT system.**

***Index Terms*—Vulnerability Assessment, Threat Assessment, MITRE Corporation, NVD database, CAPEC Attack Patterns**

I. Introduction

The idea behind the Internet of Things (IoT) is to connect everyday objects (e.g., sensors, actuators, control systems, machines, equipment, etc.) to collect, exchange, process, and access data or services over the internet. IoT networks can gather an enormous amount of data which can be used to have a more accurate representation of the current situations and allow the network or its human operators to take better decisions. This may improve the workspace productivity and avoid critical situations, or at least alleviate their consequences by allowing a faster and better-targeted response with lower costs. According to Gartner, there will be 25 billion IoT devices connected by 2025. Another study [**?**] shows that the growth of the Internet of Things devices should exceed 80 billion devices by 2030.

The vast growth of IoT devices has not come without consequences, particularly security challenges. These challenges mainly arise from the ill-designed and incomplete security of wireless sensors and actuators [**?**]. Many IoT providers do not have the prerequisite cyber-security knowledge and thus their IoT products often come with different weaknesses. The IoT Security Foundation [**?**] revealed that only 10% from more than 300 IoT companies had policies to disclose vulnerabilities in their products and patch them. Another study by HP revealed that 70% of the IoT devices connected to the Internet are vulnerable to numerous attacks with an average of 25 vulnerabilities per device [**?**]. Moreover, considering the combination of technologies used and IoT devices limited resources in terms of memory, energy, computing power, and communication protocols, IoT systems cannot take advantage of the traditional security mechanisms that are used in critical IT systems, thus exposing the system to critical vulnerabilities [**?**]. For example, the sensor nodes can implement various lightweight wireless communication protocols such as Bluetooth, Zigbee, or SigFox rather than the traditional ones that is supported with high security mechanisms [**?**]. In addition, the taxonomy of attacks in IoT systems differs from traditional IT, as the definition of 'remote access attack' in IoT could be only a few meters away from the vulnerable device to compromise, that is already inside the local network and beyond the firewall protection [**?**]. As a result, a wide range of IoT devices presently remain vulnerable to attacks in any IoT system.

One way to tackle these challenges is to conduct a cyber-security risk management analysis to be aware of the weaknesses severity and threats of one's IoT network. Unfortunately, the existing security risk analysis techniques had not initially been designed to be compatible with IoT systems, and their constraints [**?**]. For instance, [**?**] conducted an OCTAVE risk assessment method in the context of IoT healthcare systems, which handle modules and scoring metrics originally designed to identify and assess threats in IT, leading to the identification of few threats and vulnerabilities inaccurate assessment.

In this paper, we focus on assessing security in IoT networks, as previous works show that the number of IoT vulnerabilities is significant and there is no specific method that comprehensively identifies and assesses the severity of attack exploitation. We propose a novel method for identifying vulnerabilities with the highest risk and possible associated attack patterns in a specific IoT network. The method consists of three steps: the first step identifies significant weaknesses based on CWE and their severity. The second step identifies relevant CVE based on various IoT components and their associated CWE. The third step identifies attack patterns related to the CVE. This method could be used in security risk analysis as most methods require finding vulnerabilities in the system and possible attacks scenario, or in research work to confront new security methods in IoT networks with representative attacks.

The rest of the paper is organized as follows: Section II presents a background on the IoT architectures and security database resources used in our proposed method. Section III presents a state-of-the art of vulnerability databases and research work on IoT security. Section IV presents the design security assessment method that we suggest in IoT to evaluate vulnerabilities and attacks using OWASP[1], NVD[2], MITRE[3], and CAPEC[4]. Finally, the paper ends with a case study example in Section V to validate our approach and conclusions with future work perspectives in Section VI.

II. Concepts and Definitions

In this section, we provide a background knowledge about concepts of the Internet of Things (IoT) and discuss various databases and standards for identifying and assessing security vulnerabilities and threats. In addition, we discuss different vulnerability and threat assessment approaches used by researchers to analyze security in the IoT domain. Finally, we highlight some weak points in addressing security based vulnerability in IoT and explain the motivation for our work.

A. IoT Architectures:

In general, the architecture of an IoT network is typically divided into three layers depicted in figure 1 :

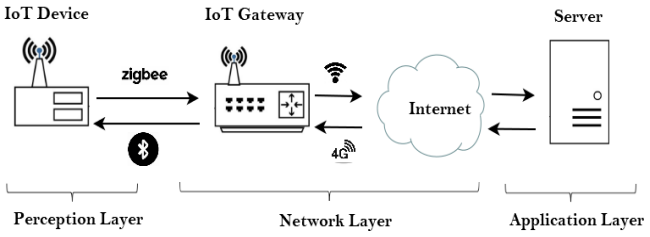

Fig. 1. Three Layers IoT Architecture

- The perception layer consists of physical objects, such as sensors and actuators that collect data and execute commands through the network.
- The network layer, also known as the transition layer, is responsible for transmitting information from the physical components to the information processing systems. We usually achieve communications with the physical objects with technologies, including ZigBee, or Bluetooth, while communications between the information processing systems are usually achieved with other wireless or wire technologies.
- The application layer manages information and provides decisions based on the data obtained from the physical components and the operator commands.

Few works outlined more detailed architectures. In [**?**], a standard IoT ISO architecture used by the SerIoT project contains five layers (the physical layer, the object layer, the communication layer, the application layer, and the user layer). [**?**] also discussed a five-layer architecture for IoT applications and services in several applications, such as smart homes, smart health care, smart city, etc. From the bottom to the top, these five layers are the device sensing layer, network management layer, service composition layer, application layer, and user interface layer.

B. Security Threat Taxonomy

The basic security terms are defined as follows [**?**], [**?**], [**?**], NIST[5]:

- **Vulnerability**: the occurrence of one or more weaknesses that a party can use to cause harm on the system.
- **Security Weakness**: faults in the software or hardware that, if not addressed, could possibly result in the system's assets being vulnerable to attacks.
- **Security Risk**: the probability of a threat source's exploiting vulnerability along with the severity impact of the adverse event on the system.
- **Vulnerability Assessment**: the process of identifying vulnerabilities relevant to system's assets followed by an estimation of the severity impact of exploitation.
- **Threat Assessment**: the method that users can develop to identify their potential cyber-security threats and the likelihood in order to overcome and mitigate the possible harmful consequences of these threats.

C. Open Web Application Security Project (OWASP) IoT:

The Open Web Application Project (OWASP) is an online publication that gives insights into the security weaknesses discovered in computing systems. Security experts across the globe have collectively identified these weaknesses after a thorough review of the existing state of affairs. It aims at educating network developers and users about potential vulnerabilities which they should be aware of so that they can take corrective action. In particular, OWASP proposes a top ten list of types of weaknesses in IoT systems. They obtained this list after evaluating reported cyber-attacks based on ease of exploitability, detectability, and the severity of the potential impacts on human safety. The list in Table I shows the Top 10 IoT weaknesses by OWASP 2018 in descending order of criticality. A brief detail for each category could be found on the OWASP website.

D. NIST, CVE and CVSS vulnerability scoring

The American National Vulnerability Database (NVD) is a database of vulnerabilities maintained by the National Institute of Standards and Technology (NIST). The database, referred to as the CVE (Common Vulnerability Exposure), identifies software vulnerabilities on any computer systems according to standardized codes. Every individual CVE acquires a timestamp of the date of publication of the vulnerability and a unique sequential number separated by hyphens, e.g., CVE-2022-26891. Furthermore, the Common Vulnerability Scoring

[1]https://owasp.org/
[2]https://nvd.nist.gov/
[3]https://cwe.mitre.org/
[4]https://capec.mitre.org/
[5]https://www.nist.gov/

TABLE I
OWASP TOP 10 IOT 2018

Category	IoT Weakness
C1	Weak, Guessable, or Hard-coded Passwords
C2	Insecure Network Services
C3	Insecure Ecosystem Interfaces
C4	Lack of Secure Update Mechanism
C5	Use of Insecure or Outdated Components
C6	Insufficient Privacy Protection
C7	Insecure Data Transfer and Storage
C8	Lack of Device Management
C9	Insecure Default Settings
C10	Lack of Physical Hardening

System (CVSS) is used as part of the NVD initiative to rate vulnerabilities. The CVSS ranges from 1 to 10 and reflects mainly the severity impact of exploiting a CVE vulnerability on the confidentiality, integrity, and availability attributes, the attack vector, and the attack complexity of exploiting a vulnerability. However, the CVSS score was originally designed to rate vulnerabilities in traditional systems, and it is not worth using it to assess CVE IoT vulnerabilities [**?**]. Additionally, the CVE details the vendors and products on which it was found. The CVE is a trusted source in the community and numerous other vulnerability databases depend on it.

E. MITRE, CWE, and CWSS Weakness Scoring System

The Common Weakness Enumeration (CWE) is a community-developed list of well known software and hardware weakness types managed by the Homeland Security Systems Engineering and Development Institute (HSSEDI) and operated by the MITRE Corporation. This list provides a baseline for the identification and classification of cyber weaknesses through well-defined codes and detailed lists for a universal type of weaknesses that concern the Information Technology (IT), Operational Technology (OT), and IoT systems. The CWE catalogs 1000 sorted entries that are identified using an ID number, e.g.: CWE-20. Each entry shares a piece of related information in a tree structure. These relationships are defined as ChildOf, ParentOf, MemberOf and give insight into similar weaknesses that may exist at higher and lower levels of abstraction. In addition, PeerOf and CanBeAlso relationships are defined to show similar weaknesses that share common characteristics. There exists another relationship, defined as chains and composites. It illustrates how CWE weaknesses can be combined to involuntarily contribute to a vulnerability. The CanFollow and CanPrecede relationships are used in chains to identify whether the weakness is primary or resultant. A Composite is a mix of several weaknesses that can create a vulnerability, but only if they all occur at once. In composite relationships, a Require is used by a composite to identify its component weaknesses, and IsRequiredBy relationship is used by the components of that composite. The NVD team performs manual study analyses on CVE description entries to pinpoint the type and cause of a vulnerability and to categorize the CVE under a specific existing CWE weakness. In a similar manner to CVSS, the Common Weakness Scoring System (CWSS) provides a mechanism for assessing the severity impact of CWE weaknesses. It ranges from 1 to 100 and demonstrates the technical impact, and the likelihood of exploiting the CWE weakness.

F. Common Attack Pattern Enumeration and Classification (CAPEC)

The Common Attack Pattern Enumeration and Classification (CAPEC) was established by the U.S. Department of Homeland Security to provide a publicly available catalog of common attack patterns that would help users to understand how attackers exploit weaknesses in systems and other cyber-enabled capabilities. Each attack pattern is assigned a number e.g.: CAPEC-34 and stores how specific parts of an attack are designed and executed, the attack steps that are taken to exploit a weakness, the likelihood, the typical severity impact, and the relationships with the CWE weaknesses. Additionally, it gives guidance on ways to mitigate the attack's effectiveness. CAPEC helps those developing applications, or administrating cyber-enabled capabilities, to better understand the elements of an attack and how to prevent them from succeeding. In addition, CAPEC attack patterns with their descriptions and characterizing context elements are a useful tool for threat assessment to be used in security analysis to build secure mechanisms.

III. RELATED WORKS

This section introduces databases that identify security vulnerabilities and are analogous to NVD, followed by a review of the literature on security assessment methods for IoT security.

A. Vulnerability databases

Various databases exist in the literature to describe and quantify vulnerabilities. For instance, the China National Vulnerability Database (CNVD[6]) is a general vulnerability database similar to CVE and regulated by the Chinese national CERT and they are rated using the CVSS score. The United States Computer Emergency Readiness Team (US-CERT[7]) provides also a vulnerability database, which includes references to the corresponding CVE. In addition, the US-CERT released the ICS-CERT[8] vulnerability advisories by product vendors related to the IoT industrial control systems and medical devices, respectively classified by the ICSA and ICSMA identifiers.
Other vulnerability databases exist in the literature, such as Japan's vulnerability notes ipedia vulnerability database (JVNDB[9]), China's national vulnerability database of information security (CNNVD[10]), and the Chinese industrial internet security emergency response center (CN-ICS-CERT[11]). However, the majority of entries of these databases are based on

[6]http://www.cnvd.org.cn/
[7]https://www.kb.cert.org/vuls/
[8]https://www.cisa.gov/uscert/ics/advisories-by-vendor
[9]https://jvndb.jvn.jp/en/
[10]http://www.cnnvd.org.cn/
[11]https://www.ics-cert.org.cn/

information from the NVD, and use scoring systems based on CVSS.

To sum up, in regard to IoT systems and devices, only the CN-ICS-CERT, US-CERT, and CNVD databases are at least partially focused on categorizing IoT vulnerabilities. The other databases do contain vulnerabilities affecting IoT products, but do not allow users to distinguish these vulnerabilities from the others.

B. Research Work on Security in IoT

1) Security surveys in IoT: In the literature, various research works discussed the security vulnerabilities and threats in IoT systems. For instance, Mosenia et Jha [**?**] provided a survey of a comprehensive list of threats, vulnerabilities, and possible countermeasures that target the edge layer (perception layer) of IoT architecture. They summarized this list based on discussing and summarizing various IoT model architectures, the potential motivation of attackers in addition to the possible attacks and threats in the edge layer, and the possible countermeasures to overcome these threats. Alaba et al. [**?**] presented a survey about security threats, attacks, and vulnerabilities in IoT, where they focused on the study criteria for discussing the taxonomies of security threats in terms of security in domain applications, IoT architectures, and communication. In addition, they provided possible challenges to existing solutions and security remediation techniques to improve IoT security. Samaila et al. [**?**] examined in a survey the security in nine domain applications of IoT. The authors illustrated the system models, including components, protocols, and technologies suggested in the literature for the nine applications. They analyzed the security in each domain based on defining the security requirements and threat models proposed per domain. In addition, they discussed the existing security mechanisms and other security solutions. Makhdoom et al. [**?**] presented a survey of various security threats and possible vulnerabilities in IoT. This survey is based on known defined threats in IoT architectures from the literature, focusing on the methods of IoT malware threat and DDoS attack strategy. In addition, they provided guidelines for security frameworks and best practices, highlighting the importance of risk and threat assessment, as well as the open security challenges. The aforementioned surveys constitute significant and useful efforts to study and improve the security of IoT systems by providing valuable information and taxonomies. Specifically, great work took place regarding analyzing the threats, vulnerabilities, and security requirements. However, they do not offer a means to rate these threats and vulnerabilities in terms of severity and likelihood of attacks, which is a necessary step in our work to know where to focus efforts to improve the system's security.

2) Security assessment in IoT systems: Diaz Lopez et al. [**?**] proposed an IoT security solution based on Security Information and Event Management (SIEM) to identify and detect security threats. The authors proposed a vulnerability and threat assessment method through a mapping between security events category, weakness types, and attack surfaces model by OWASP to define security events. In addition, they assigned the possible CAPEC attack patterns to the mapping criteria. Meneghello et al. [**?**] analyzed in a survey possible security risks and their countermeasures. The analysis explored security vulnerabilities, attacks, and implemented security mechanisms in the most popular IoT communication technologies. However, the authors provided risks without detailing their severity impact and likelihood, which are fundamental in every risk analyses. Grammatikis et al. [**?**] proposed quantitative and qualitative risk analysis methods to assess threat targeting protocols in the context of IoT. Based on the probability of a threat, its impact on security attributes, and deployed countermeasures, they provide an evaluation of risk level using a four-layer IoT architecture along with required countermeasures to mitigate the risks. However, the proposed method does not use a vulnerability assessment metric, which may cause the assessment to not be optimal for the considered system. Plenty of security assessment methods such as OCTAVE, PASTA, Trike, CRAMM, COBRA, CORAS, or STRIDE have been designed to identify and assess threats and vulnerabilities [**?**], [**?**]. However, most of these methods and tools do not target IoT systems specifically but are designed with scoring systems such as CVSS to assess threats and vulnerabilities in traditional systems. Qu et Chan [**?**] proposed to modify the base score equations of the CVSS scoring system to assess vulnerabilities in Bluetooth Low Energy (BLE) wireless communications in IoT networks. However, the modified scoring system remains limited to a specific IoT technology. Zahra et Abdelhamid [**?**] proposed a security risk analysis in IoT based on the EBIOS qualitative risk analysis method. The authors aimed to identify security risks based on the three layers of IoT architecture and provided severity impact and likelihood scoring metrics to evaluate risks. However, the authors neither present a complete adaptation of the EBIOS risk analysis steps nor a basic approach to identify and evaluate risks. In addition, the analysis lacked identification and assessment of weaknesses and vulnerabilities, and the method was originally designed for traditional IT systems [**?**].

Automatic tools, such as OVAL, are also used to identify and assess risks. For instance, Bronwyn et al. [**?**] designed an automatic risk assessment framework known as MedDecRisk for medical devices. The model combines the OVAL tool that reports whether a device is vulnerable or not based on assets, the STRIDE model defining threats, CVE/CVSS pairs, CWE, and CAPEC attack patterns to assess risks. However, as the databases provide few details on attacks and vulnerabilities and due to the uncertainty of machine learning algorithms to make decision classifications, automated identification and assessment may have insufficient data to produce all the possible vulnerabilities and attack patterns. In [**?**], Georgescu et al. proposed a machine learning method based on named entity recognition (NER) to detect vulnerabilities in IoT devices. The proposed model was trained using CVE training set vulnerabilities grouped by a search on keywords relevant to the domain. However, this search turned up certain training inputs that did not match the given IoT category which, according to our analysis, resulted in a precision mistake of more than 20%.

For instance, some CVE (e.g., CVE-2014-9877) are associated to the key term actuator, but in fact focus on vulnerabilities targeting the driver actuators in the Qualcomm components of Nexus Android smart phones rather than on vulnerabilities related to smart actuators in IoT.

As previously discussed, IoT systems face several security challenges that raise specific vulnerabilities. By proposing a vulnerability and threat assessment method to identify the vulnerabilities with the highest risk and possible associated attack patterns for IoT systems, we aim for security risk analyses to better know where to focus on threat mitigation and for researchers to identify representative attacks in order to confront with and validate newly developed security methods in IoT networks.

IV. A Novel Vulnerability and Threat Assessment Method for IoT

In this section, we present our method for identifying and assessing the severity of realistic security vulnerabilities with their relevant attack patterns for IoT systems. This method is a novel approach that can be applied to any IoT architecture and uses external databases and severity assessment studies to identify a list of the most severe vulnerabilities and related attack patterns for a specific IoT system. Our method gives the following outputs:

- a list of CWE to be focused on, ranked from the most severe to the less severe for the targeted system,
- for each CWE, a list of CVE that could target the system's components,
- for each CVE, attack patterns on one or more of the system's components.

The inputs of the method are the following:

- the Common Weakness Enumeration (CWE),
- the Common Vulnerability Enumeration (CVE),
- an attack pattern classification (for example CAPEC),
- one or several severity classification of security weaknesses for IoT systems (for example OWASP Top 10 for IoT),
- the list of components in the targeted IoT system.

Figure 2 represents a detailed block diagram of our proposed security assessment method, which consists of three steps:

- The first step is the CWE classification, which aims to select the particular CWE that are high threats to the targeted system.
- The second step uses the identified CWE and references them with the system components to identify and select the most relevant CVE.
- The third step uses the identified CVE to select specific attack patterns to the threatened components.

We will detail each of these steps in the following section.

A. Step 1: CWE IoT Classification and Assessment

In this first step, we aim to rate CWE depending on their severity on IoT systems. This would allow us to select and focus on the most severe CWE, depending on the time and

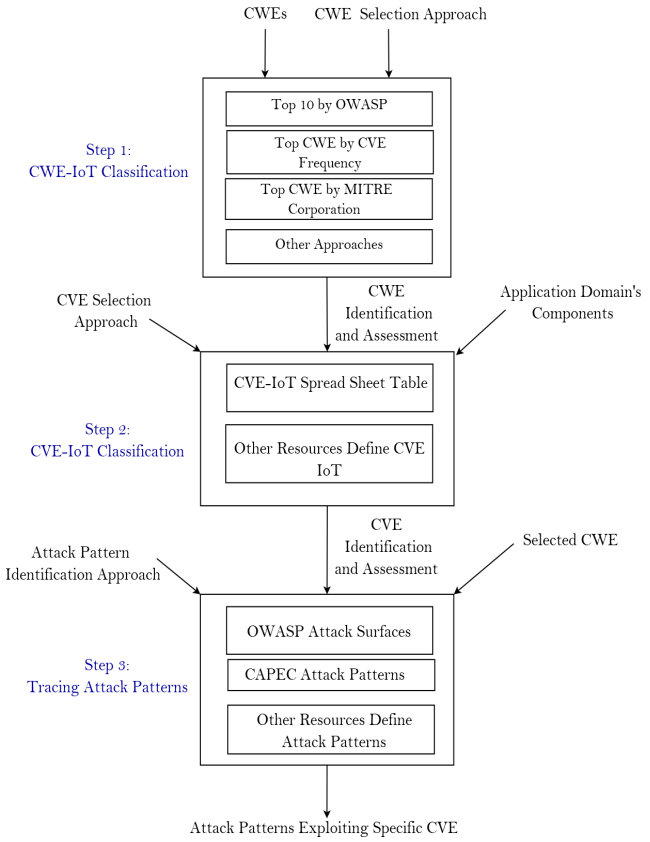

Fig. 2. IoT Vulnerability Assessment Model

resources available for our assessment. To do so, we can use one or more classification studies from the literature, for example, OWASP Top 10 IoT, the top CWE based on frequency of CVE, and the dangerous weaknesses defined by MITRE. This step takes as an input the CWE and external studies classifying the severity of attacks on IoT networks. The output of this step is the list of CWE weaknesses that we will focus on. The complete information on each CWE can be found on the MITRE corporation website. In the following subsections, we present severity classification studies that can be used in this first step.

1) Top 10 CWE Based on OWASP Top 10 IoT Weakness Categories: The known categories of IoT weaknesses are well documented and evaluated in the OWASP Top 10 IoT 2018. The categories of OWASP are dedicated to the IoT context, and it serves as a useful tool for assessing CWE entries for such systems. In addition, OWASP currently working on a project called OWASP CWE Toolkit for automatic mapping between CWE to OWASP categories. In the meantime, we proposed to map manually the CWE weaknesses with the OWASP top 10 IoT categories, to provide a comprehensive and useful list of OWASP weaknesses. Table II shows the results of this manual mapping.

2) Top CWE based on the relevant frequency of CVE in IoT devices: Various research works conducted statistical studies on CWE weaknesses in the domain of IoT to classify them

TABLE II
MAPPING BETWEEN OWASP TOP 10 IOT AND CWE

OWASP IoT Weakness Categories	CWE
C1: Weak, Guessable, or Hard-coded Passwords	CWE-261, CWE-260, CWE-521, CWE-259, CWE-257, CWE-798, CWE-522, CWE-321,CWE-256, CWE-523, CWE-307, CWE-640, CWE-255, CWE-345, CWE-287, CWE-257
C2: Insecure Network Services	CWE-287, CWE-276, CWE-255, CWE-522, CWE-269, CWE-295, CWE-120, CWE-20, CWE-598, CWE-419, CWE-22, CWE-434, CWE-1331, CWE-417, CWE-444, CWE-288, CWE-732, CWE-285
C3: Insecure Ecosystem Interfaces	CWE-79, CWE-20, CWE-89, CWE-377, CWE-427, CWE-352, CWE-650, CWE-287, CWE-327, CWE-601, CWE-598, CWE-307, CWE-284, CWE-319, CWE-77, CWE-78, CWE-119, CWE-295, CWE-311, CWE-319, CWE-325, CWE-94, CWE-125, CWE-787, CWE-416, CWE-306, CWE-862, CWE-427, CWE-94
C4: Lack of Secure Update Mechanism	CWE-295, CWE-940,CWE-15,CWE-1277
C5: Use of Insecure or Outdated Components	CWE-1233, CWE-1104, CWE-327, CWE-328, CWE-398, CWE-563, CWE-686, CWE-399, CWE-190, CWE-226, CWE-1240, CWE-693
C6: Insufficient Privacy Protection	CWE-359, CWE-200, CWE-295, CWE-311, CWE-312, CWE-325, CWE-326, CWE-327,
C7: Insecure Data Transfer and Storage	CWE-201, CWE-300, CWE-310, CWE-200, CWE-319, CWE-668, CWE-377, CWE-327, CWE-521, CWE-922, CWE-1240, CWE-388
C8: Lack of Device Management	CWE-909, CWE-910, CWE-920, CWE-770
C9: Insecure Default Settings	CWE-15, CWE-284, CWE-276, CWE-1068, CWE-269, CWE-521, CWE-295, CWE-1189, CWE-1231, CWE-1260, CWE-1262, CWE-1274
C10: Lack of Physical Hardening	CWE-1233, CWE-284, CWE-831, CWE-134, CWE-256, CWE-119, CWE-121, CWE-400, CWE-1300, CWE-1191, CWE-1244, CWE-1247, CWE-1256,- CWE-1332

based on repeating frequency in IoT devices. We present in the following the top CWE entries by frequency of CVE using different study analyses from the literature. For all the following works, we investigated from the literature, possible approaches to identify and assess the CWE weaknesses based on the frequency of detectability in the IoT context:

- *Top 6 CWE vulnerabilities the mostly exploited by IoT malwares:* The authors in [**?**], identify the top 6 CWE weaknesses, the one that is frequently exploited by IoT malicious malware codes.
- *Top 10 CWE weaknesses in most consumed IoT components:* In [**?**], the authors summarize the classification of the top 10 CWE by CVE frequency of detectability in different IoT devices, including routers, modems, gateways, IP cameras, and printers.
- *Top 3 CWE which occurred most often in IoT Operating Systems (IoT OS):* In [**?**], the authors outlines the Top 3 common weaknesses in IoT operating system source code.
- *Top 4 CWE which occurred most often in smart home applications:* The authors in [**?**], outline the Top 4 weaknesses that target the most commonly smart home IoT products such as wearables, IP cameras, routers, smart TV, smart controller hubs etc.

3) Recent 2022 Dangerous Software and Hardware CWE by MITRE Corporation: The MITRE corporation released a list of the 25 top dangerous Software CWE weaknesses in IT systems. The list was created based on a scoring system that combines the frequency of CVE per CWE, the Known Exploited Vulnerabilities (KEV[12]) count (CVE), and the average CVSS score related to each CWE. In addition, MITRE established an unranked list of the most important hardware weaknesses. They derived the list from many significant factors, mainly including the frequency of occurrence of the weakness. The tables of weakness can be found on the website of MITRE corporation.

For instance, we can find in the list of software weaknesses the CWE-798 (Use of Hard-coded Credentials) as entry 15 from the Top 25 most dangerous software weaknesses. Note, however, that the OWASP Top 10 IoT analyzed this type of weakness as in the top 1 category. This confirms that the assessment analysis of traditional IT systems (including CVSS) is not adequate to assess vulnerabilities in IoT systems and need further analysis.

4) Top CWE based on Multi-Assessment Classifications: There is no obligation to specifically use one of the previously presented classifications in our first step, one can use another classification, develop his own, or even combine several classifications to pinpoint the aspects according to the targeted system. For instance, if the target IoT system encompasses smart home applications, the IoT user can choose the OWASP top 10 classifications along with the top 4 CWE weaknesses targeting the smart home appliances to optimize their choice.

B. Step 2: CVE IoT Classification

In this subsection, we detail the second step of our method, which is based on a spread list[13] of CVE IoT vulnerabilities and their related CWE and target components. This step takes as input the selected CWE from step 1, our CVE spread list, and the target system's components. Its resulting output is the list of targeted IoT CVE vulnerabilities. The definition of each CVE can be found on the NVD database website.

To produce this cross-referencing spreadsheet, we investigated more than 300 CVE concerning the Internet of Things vulnerabilities on devices from different vendors from the NVD database. These CVE cover the following hardware and software categories: sensors, actuators, gateways, printers, IP cameras, smart hub controllers, medical devices, IoT technologies and protocols, smart wearable devices, smart vehicles, and smartphones.

For each CVE within a component category, we map its corresponding CWE. This approach will help the IoT users to identify the specific types of CVE vulnerabilities that they want to study and address in their system, depending on the CWE identified in the previous step and on the components in the targeted IoT system. Table IV presents an excerpt of the CVE spread list that targets the Medical Sensor Nodes and Low-range Wireless Communication Technologies.

[12]https://www.cisa.gov/known-exploited-vulnerabilities-catalog
[13]https://github.com/lounisShield/SRSEMS/blob/main/CVE IoT.pdf

C. Step 3: Tracing Attack Patterns From Selected CVE

This subsection presents the third step of our threat assessment method, aiming to identify the attack patterns by exploiting CVE vulnerabilities. It takes as input the identified CWE from step 1, identified CVE from step 2, and a list of attack patterns from a defined resource, such as CAPEC. It gives as output for each CVE possible IoT attack pattern targeting the system's components.

As previously stated, the Common Attack Patterns Enumeration and Classification (CAPEC) is a reliable and useful attack threat assessment method for this step. It identifies techniques of how an attacker can exploit a vulnerability present in the system along with the likelihood and mitigation strategies of these threats. Once the CWE and the related CVE are identified, the CAPEC attack patterns can give a different kinds of attacks stressing and affecting the security requirements of the system. A further advantage of this approach is that the CAPEC attacks are directly mapped to CWE, which provides a way to link the common attack schemes to the set of selected CVE vulnerabilities. However, one can use other alternate attack patterns lists for this step. For instance, OWASP provided a list of attack surfaces so that manufacturers, developers, security researchers, and user who wants to install or utilize IoT technology may be aware of how an attacker can take advantage of possible attack surfaces to exploit vulnerabilities.

V. Case Study of our method: IoT Smart Healthcare Application

In this section, we present a brief validation example of our system on a real IoT healthcare system [**?**]. We consider the implementation of a low-range wireless communication technology on a set of Body Sensor Networks (BSN) communicating with the IoT gateway device in the perception layer. To accomplish the first step, and to cover a comprehensive list of weaknesses in our system, we conduct two approaches targeting software weaknesses, which represent a majority concerning their number and criticality. We include the Top 10 IoT Weaknesses as defined by OWASP, which reflect the Top critical impact weaknesses on security and safety as defined in Table II as an input in addition to the Top 5 CWE weaknesses relevant to the medical devices. Table III classifies the top 5 CWE weaknesses in the domain of smart healthcare as analyzed by [**?**]. From these two studies, we identified as targets the CWE that are underlined in Table II.

In the second step, we give a classification (see tables) of CVE that targets the BSN nodes and the low-range wireless communication technologies to connect the sensor nodes to the IoT gateway. This step cross-references the chosen CWE from step 1 and the categories of the target system components on the CWE/CVE IoT spreadsheet. Table IV presents the resulting identified CVE.

In the third step, we trace the attack patterns relevant to the identified CVE. Based on the CAPEC database and the mapping criteria between CWE and CAPEC provided by MITRE, we investigated the possible attacks that could use the identified CVE vulnerabilities in wireless sensor nodes and low-range wireless communication technologies. However, the mapping process between CVE and CAPEC still requires significant work to be done as the number of CVE could be numerous in a system. Table V identifies the resulting possible attacks. The complete information on each CAPEC attack pattern can be found on the CAPEC website.

TABLE III
Top 5 weaknesses in Medical devices

Rank	Weaknesses Type	CWE-ID
Top 1	Authentication (28/89 entries)	CWE-287, CWE-345, CWE-259, CWE-798, CWE-321
Top 2	Information leak (20/89 entries)	CWE-200, CWE-256, CWE-668, CWE-257, CWE-260, CWE-319, CWE-522, CWE-311, CWE-377, CWE-312
Top 3	Malicious Data Injection (10/89)	CWE-78, CWE-20, CWE-427, CWE-94
Top 4	Memory Access (8/89 entries)	CWE-121, CWE-120, CWE-125, CWE-119
Top 5	Access Control (7/89 entries)	CWE-284, CWE-285, CWE-732

TABLE IV
CVE-IoT Selection

CVE Vulnerability Identification and Assessment		
Device or Technology	OWASP IoT Category: CWE-IoT	CVE-IoT
Medical Sensor Nodes	C2: CWE-287	CVE-2020-15486
	C2: CWE-311	CVE-2018-10825
	C3: CWE-78	CVE-2020-27373
	C3: CWE-319	CVE-2020-11539
	C1: CWE-798	CVE-2018-8870
Low-range Wireless Communication Technology	C2: CWE-287	CVE-2019-19194, CVE-2020-25183
	C2: CWE-120	CVE-2019-19196
	C3: CWE-20	CVE-2019-19192, CVE-2015-6244, CVE-2015-8732
	C1: CWE-345	CVE-2020-10137
	C6: CWE-311	CVE-2020-9058, CVE-2020-9057
	C2: CWE-285	CVE-2020-9061

TABLE V
CAPEC-IoT Attack Patterns

Tracing CAPEC-IoT	
CVE-IoT	CAPEC-IoT
CVE-2020-15486	CAPEC-94, CAPEC-148, CAPEC-155, CAPEC-151
CVE-2018-10825	CAPEC-15 CAPEC-148
CVE-2020-27373	CAPEC-88, CAPEC-115
CVE-2020-11539	CAPEC-155, CAPEC-94, CAPEC-148
CVE-2018-8870	CAPEC-507, CAPEC-114
CVE-2020-25183	CAPEC-114, CAPEC-151, CAPEC-148
CVE-2019-19194	CAPEC-114, CAPEC-100
CVE-2019-19196	CAPEC-100, CAPEC-114
CVE-2019-19192	CAPEC-100, CAPEC-25
CVE-2020-15802	CAPEC-668, CAPEC-94, CAPEC-114
CVE-2015-6244, CVE-2015-8732	CAPEC-540
CVE-2020-10137	CAPEC-115, CAPEC-100
CVE-2020-9058, CVE-2020-9057	CAPEC-115, CAPEC-94

VI. Conclusion and Future Work

In this paper, we proposed a vulnerability and threat assessment method that can be used to identify possible attacks by analyzing and rating important IoT vulnerabilities and threats. The method consists of three steps, the first of which identify significant weaknesses based on CWE. The second step identify relevant CVE through a thorough classification of real CVE vulnerabilities that have been identified in various IoT components and their associated CWE to help focus on vulnerabilities specific to the targeted system. The third step identifies attack patterns that exploit the identified CVE. We applied our proposed method to some components of an IoT healthcare system. This method acts as a helpful and flexible tool to be used in risk analyses to identify and assess security risks in IoT systems, or in research work to find realistic attacks to confront with or validate new security components or processes. For future perspectives, we expect to conduct a vulnerability and threat assessment on a complete IoT case study based on our approach to establish threat scenarios. We also aim to improve on taking into account the relationships between weaknesses and attack patterns to propose more elaborate and complex attacks. Finally, we intend to propose alternatives to select significant CAPEC from CVE that would require less work from the security experts.

Acknowledgment

This work was funded by the International Research Project Adonis and the French region Hauts-de-France.

References

[1] B. B. Gupta and M. Quamara, "An overview of internet of things (iot): Architectural aspects, challenges, and protocols," *Concurrency and Computation: Practice and Experience*, vol. 32, no. 21, p. e4946, 2020.

[2] P. Anand, Y. Singh, A. Selwal, P. K. Singh, R. A. Felseghi, and M. S. Raboaca, "Iovt: internet of vulnerable things? threat architecture, attack surfaces, and vulnerabilities in internet of things and its applications towards smart grids," *Energies*, vol. 13, no. 18, p. 4813, 2020.

[3] I. S. Foundation, "Understanding the contemporary use of vulnerability disclosure in consumer internet of things product companies," Available online: https://www.iotsecurityfoundation.org/wp-content/uploads/2018/11/Vulnerability-Disclosure-Design-v4.pdf, accessed on 29 May 2022.

[4] HP, "Hp fortify," https://www.hp.com/go/fortifyresearch/iot, 2017.

[5] M. Rytel, A. Felkner, and M. Janiszewski, "Towards a safer internet of things—a survey of iot vulnerability data sources," *Sensors*, vol. 20, no. 21, p. 5969, 2020.

[6] I. Makhdoom, M. Abolhasan, J. Lipman, R. P. Liu, and W. Ni, "Anatomy of threats to the internet of things," *IEEE communications surveys & tutorials*, vol. 21, no. 2, pp. 1636–1675, 2018.

[7] A. Ur-Rehman, I. Gondal, J. Kamruzzuman, and A. Jolfaei, "Vulnerability modelling for hybrid it systems," in *2019 IEEE International Conference on Industrial Technology (ICIT)*, 2019, pp. 1186–1191.

[8] F. Hashmat, S. G. Abbas, S. Hina, G. A. Shah, T. Bakhshi, and W. Abbas, "An automated context-aware iot vulnerability assessment rule-set generator," *Computer Communications*, vol. 186, pp. 133–152, 2022.

[9] M. B. Ali, T. Wood-Harper, A. S. Al-Qahtani, and A. M. A. Albakri, "Risk assessment framework of mhealth system vulnerabilities: A multi-layer analysis of the patient hub," *Communications and Network*, vol. 12, no. 2, pp. 41–60, 2020.

[10] P. E. Gelenbe, "Reference architecture for secure and safe internet of things by the seriot project, seriot project," https://seriot-project.eu/2019/01/14/reference-architecture-for-secure-and-safe-internet-of-things-by-the-seriot-project/, accessed on May 14 2022.

[11] S. Pal, M. Hitchens, T. Rabehaja, and S. Mukhopadhyay, "Security requirements for the internet of things: A systematic approach," *Sensors*, vol. 20, no. 20, p. 5897, 2020.

[12] K. Kandasamy, S. Srinivas, K. Achuthan, and V. P. Rangan, "Iot cyber risk: A holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process," *EURASIP Journal on Information Security*, vol. 2020, no. 1, pp. 1–18, 2020.

[13] V. Malamas, F. Chantzis, T. K. Dasaklis, G. Stergiopoulos, P. Kotzanikolaou, and C. Douligeris, "Risk assessment methodologies for the internet of medical things: A survey and comparative appraisal," *IEEE Access*, vol. 9, pp. 40 049–40 075, 2021.

[14] P. Napolitano, G. Rossi, M. Lombardi, F. Garzia, M. Ilariucci, and G. Forino, "Threats analysis and security analysis for critical infrastructures: Risk analysis vs. game theory," in *2018 International Carnahan Conference on Security Technology (ICCST)*. IEEE, 2018, pp. 1–5.

[15] A. Mosenia and N. K. Jha, "A comprehensive study of security of internet-of-things," *IEEE Transactions on emerging topics in computing*, vol. 5, no. 4, pp. 586–602, 2016.

[16] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of things security: A survey," *Journal of Network and Computer Applications*, vol. 88, pp. 10–28, 2017.

[17] M. G. Samaila, M. Neto, D. A. Fernandes, M. M. Freire, and P. R. Inácio, "Challenges of securing internet of things devices: A survey," *Security and Privacy*, vol. 1, no. 2, p. e20, 2018.

[18] D. Diaz Lopez, M. Blanco Uribe, C. Santiago Cely, A. Vega Torres, N. Moreno Guataquira, S. Morón Castro, P. Nespoli, and F. Gómez Mármol, "Shielding iot against cyber-attacks: An event-based approach using siem," *Wireless Communications and Mobile Computing*, vol. 2018, 2018.

[19] F. Meneghello, M. Calore, D. Zucchetto, M. Polese, and A. Zanella, "Iot: Internet of threats? a survey of practical security vulnerabilities in real iot devices," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8182–8201, 2019.

[20] P. I. R. Grammatikis, P. G. Sarigiannidis, and I. D. Moscholios, "Securing the internet of things: Challenges, threats and solutions," *Internet of Things*, vol. 5, pp. 41–70, 2019.

[21] P. Griffioen and B. Sinopoli, "Assessing risks and modeling threats in the internet of things," *arXiv preprint arXiv:2110.07771*, 2021.

[22] Y. Qu and P. Chan, "Assessing vulnerabilities in bluetooth low energy (ble) wireless network based iot systems," in *2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS)*. IEEE, 2016, pp. 42–48.

[23] B. F. Zahra and B. Abdelhamid, "Risk analysis in internet of things using ebios," in *2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC)*. IEEE, 2017, pp. 1–7.

[24] J. Mcdonald, N. Oualha, A. Puccetti, A. Hecker, and F. Planchon, "Application of ebios for the risk assessment of ict use in electrical distribution sub-stations," in *2013 IEEE Grenoble Conference*. IEEE, 2013, pp. 1–6.

[25] B. J. Hodges, "Attack modeling and mitigation strategies for risk based analysis of networked medical devices," Ph.D. dissertation, University of South Alabama, 2019.

[26] B. Xie, G. Shen, C. Guo, and Y. Cui, "The named entity recognition of chinese cybersecurity using an active learning strategy," *Wireless Communications and Mobile Computing*, vol. 2021, 2021.

[27] A. Hamou-Lhadj and A. Razgallah, "An analysis of the use of cves by iot malware," in *Proceedings of the International Symposium on Foundations and Practice of Security (FPS)*, vol. 12637, 2021, p. 47.

[28] X. Feng, Q. Li, H. Wang, and L. Sun, "Acquisitional rule-based engine for discovering {Internet-of-Things} devices," in *27th USENIX Security Symposium (USENIX Security 18)*, 2018, pp. 327–341.

[29] A. Al-Boghdady, K. Wassif, and M. El-Ramly, "The presence, trends, and causes of security vulnerabilities in operating systems of iot's low-end devices," *Sensors*, vol. 21, no. 7, p. 2329, 2021.

[30] F. Reitz, "Weaknesses and risks of the consumer internet of things," 2019.

[31] D. Dias and J. Paulo Silva Cunha, "Wearable health devices—vital sign monitoring, systems and technologies," *Sensors*, vol. 18, no. 8, p. 2414, 2018.

[32] H. Debar, R. Beuran, and Y. Tan, "A quantitative study of vulnerabilities in the internet of medical things." in *ICISSP*, 2020, pp. 164–175.