Threat Level Assessment of Smart-Home Stakeholders Using EBIOS Risk Manager

N'guessan Yves-Roland Douha, Doudou Fall, Yuzo Taenaka, and Youki Kadobayashi
Division of Information Science
Nara Institute of Science and Technology
Ikoma, Japan
email:douha.nguessan_yves-roland.dn6@is.naist.jp, doudou-f@is.naist.jp, yuzo@is.naist.jp, youki-k@is.naist.jp

***Abstract*—The smart home is among the emerging technologies designed to improve in-house quality of life by supplying many services, such as home automation, healthcare, and energy management. Recent cyberattacks on smart homes affecting home dwellers' privacy, safety, and security could slow down smart homes' adoption. To identify smart-home attack surfaces, we propose to use a risk analysis method called Expression of Needs and Identification of Security Objectives - Expression des Besoins et Identification des Objectifs de Sécurité (EBIOS) Risk Manager to evaluate the threat level of smart-home stakeholders in the role of threat agents. The contributions of this paper are assessing smart-home stakeholders and identifying attack scenarios in which they could be involved to extend the reflection on smart home security. We are the first to estimate the threat level of fourteen smart-home stakeholders through assessing many metrics. We use a 5-point Likert scale to collect data from security professionals to conduct this assessment. We classify the smart-home stakeholders into various threat zones and find that smart-home inhabitants and home automation service providers have the highest threat agent levels. This investigation will contribute to designing security systems and policies for strengthening the smart-home ecosystem's security.**

Keywords-EBIOS RM; Internet of Things; Smart Home; Stakeholder; Security.

I. INTRODUCTION

A smart home is an Internet of Things (IoT) application that promotes technology-based living places. It includes various technologies such as devices (e.g., sensors, actuators, multimedia), networking (e.g., wireless, wired), mobile and web applications, cloud computing, and artificial intelligence [1] [2]. Statista estimates that the worldwide revenue of smart homes, US$78.9 billion in 2020, will increase to US$182.3 billion by 2025 [3]. This technology-based home attracts considerably, not only normal users, but also attackers. Recent cyberattacks exploiting home devices have revealed security risk concerns in smart homes [4] [5]. Hence, carrying out a risk assessment becomes necessary to identify and address the security flaws in smart homes to withstand future cyberattacks.

Recent research have shown interests in the risk assessment of the smart home security. Jacobsson et al. [6] propose an empirical evaluation and scenario-based study. Wongvises et al. [7] propose a Fault Tree Analysis to quantify security risks. Most studies have only focused on assets such as devices and networks. However, Cherdantseva et al. [8] emphasize that a risk assessment needs to include stakeholders to provide a complete set of risks. As stated in International Organization for Standardization (ISO) 27005, a stakeholder is a "person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity [9]." To the best of our knowledge, prior work have not focused on smart-home stakeholders-based threat analysis so far. As mentioned by Bregman [10], the smart home intelligence requires developers, suppliers, and users to cooperate, specifically to transfer information. If one or many of these stakeholders get compromised by attackers or fail to secure information transmission, the smart home security could be affected. Stakeholders play an essential role in the smart home operations and could, without realizing it, contribute to the fulfillment of attack scenarios. Securing a smart home could require a deep understanding of every stakeholder connected to the smart home. Therefore, an assessment of how easy it is for an attacker to exploit a stakeholder to conduct a cyberattack on a smart home may provide security perspectives to reduce the attack surfaces.

Our approach uses EBIOS Risk Manager, referred to as EBIOS RM. It is a method based on the risk analysis and management methodology called EBIOS, which has proven to be effective for risk management in critical information infrastructures [11]. Furthermore, it includes stakeholder analysis.

The main contributions of this research are as follow:

- We introduce stakeholder-based risk analysis for smart home security.
- We evaluate the threat level associated with smart-home stakeholders to identify strategic scenarios that attackers could exploit.
- We propose an approach of threat classification for risk managers and compare our results with two other classification methods, including the EBIOS RM's.
- We identify and describe potential high-level attack scenarios that could involve smart-home stakeholders.

We organize the rest of the paper as follows: Section II describes the related work. Section III introduces EBIOS RM. Section IV analyzes the threat level of smart-home stakeholders using EBIOS RM. Section V discusses our results. Section VI concludes the paper.

II. RELATED WORK

This section presents previous work on smart home and stakeholder security risks.

A. Smart-Home Security Risk

Wongvises et al. [7] use Fault Tree Analysis (FTA) to quantify security risks in a smart home. They show that security risks in smart homes might be high through the

 ISBN: 978-1-61208-919-5

assessment of lighting systems. Ali et al. [12] use Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Allegro to analyze information security risks in smart homes. The authors identify ten critical information assets (e.g., user credentials, log information, mobile application data, and various smart home-related information) and evaluate the risk scores associated with these information assets. We note that the paper does not present the calculation of risk scores. Kavallieratos et al. [13] use the Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege (STRIDE) model to identify threats to smart homes. They identify threats that relate to devices such as IP cameras, smartphones, and alarm systems. The paper does not evaluate the threat levels. Jacobsson et al. [6] evaluate the risk exposure of a smart home by applying the Information Security Risk Analysis (ISRA) approach described in [14]. They used a questionnaire to collect the opinions of nine participants, including security experts, domain experts, and system developers of smart homes. The authors recognize that third-party stakeholders can access the whole smart home and collect private data on inhabitants.

The previous work show that risk assessment is essential to address smart home security. Furthermore, we can notice a lack of study on stakeholders assessment whereas Bregman [10] shows that they play a critical role in a smart-home environment.

B. Stakeholder Security Risk

Grimble et al. [15] describe stakeholder analysis as a powerful tool for policy analysis and formulation that help understanding a system, and changes in it, by identifying and assessing key actors or stakeholders. Stakeholder assessments have been explored in many areas, such as human resource development, business management, or natural resource management [16]. However, the related papers in the cybersecurity area are limited. Mollaeefar et al. [17] propose a multi-stakeholder cybersecurity risk assessment for data protection. They focus their research on the estimation of the relation between the impact levels and risk exposures. We note that they consider the likelihood as the same for every stakeholder. Even if this consideration could be effective in the proposed configuration, it cannot be realistic in many areas, such as a smart home where stakeholders have various interests, intentions, and behaviors.

The limitations mentioned above motivate us to leverage a risk analysis method that complies with international cybersecurity standards and includes identifying and evaluating security issues associated with stakeholders. To the best of our knowledge, the related work has not explored this perspective. In this research, we adopt the EBIOS RM method to identify and assess the threat level of threat agents (stakeholders).

III. Research Method

This section presents the background of EBIOS RM, the method used in this research.

A. Method

We often express information security risk as a combination of the consequences (impacts) of an information security event and the associated likelihood of occurrence [9]. This research focuses on the likelihood assessment, and we use EBIOS RM to evaluate the threat level of stakeholders in the role of threat agents. We choose EBIOS RM because it is a flexible method covering any system, regardless of its size and sector of activity and whether it is under development or already developed. Furthermore, unlike most qualitative risk analysis methods, EBIOS RM introduces a new calculation of the threat level and an approach to identify and evaluate threat agents and attack scenarios.

Note that EBIOS is a methodology that was created in 1995 for risk management of information system security. It is maintained by the National Cybersecurity Agency of France - Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) with the support of Club EBIOS [18]. This methodology is a comprehensive tool that complies with security management policies and international standards such as ISO 27001, 27005, and 31000. Furthermore, it was used to address risk management in critical information infrastructures [11] and we believe it could be effective for a critical environment such as a smart home where the absence of dedicated cybersecurity teams to support home users could facilitate attackers activities to access users' privacy.

B. EBIOS Risk Manager

Available since 2018, the so-called EBIOS Risk Manager (EBIOS RM) is the latest version of the EBIOS methodology. This method is iterative and includes two approaches: An approach through "conformity" that identifies the security baseline and through "scenarios" that analyzes potential attack scenarios based on the point of view of attackers. EBIOS RM comprises five workshops described as follows.

1) Workshop 1 (scope and security baseline): This workshop aims to identify the scope of our study, its assets, and its primary missions. Then, it determines the severity of feared events associated with its assets.
2) Workshop 2 (risk origins): The second workshop aims to identify the RO/TO pairs. This pair comprises risk origins (RO) and their high-level targets, namely target objectives (TO).
3) Workshop 3 (strategic scenarios): This workshop includes the threat level assessment, establishes a mapping of threat agents, and provides high-level scenarios, called strategic scenarios. These scenarios describe the attack paths a risk origin could use to reach its target objective.
4) Workshop 4 (operational scenarios): The purpose is to define technical scenarios that include the methods of attack that risk origins can use to carry out the strategic scenarios. This workshop also assesses the risk of each operational scenario.
5) Workshop 5 (risk treatment): In this workshop, the goal is to summarize all the identified risks, then define a risk

 ISBN: 978-1-61208-919-5

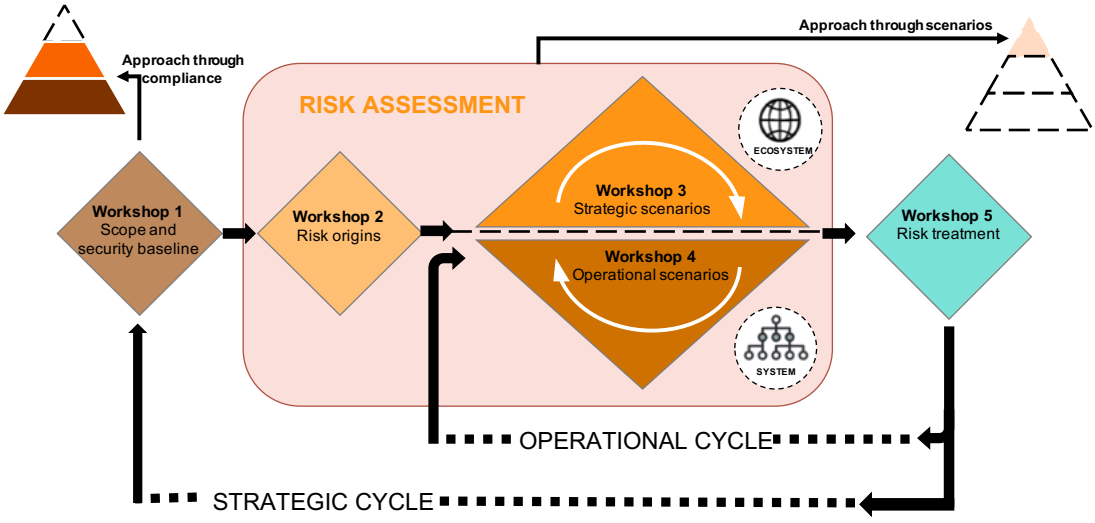

Fig. 1. A description of the general workflow of the EBIOS Risk Manager methodology [18].

treatment strategy. This workshop ends with a summary of the residual risks and the framework for monitoring risks.

Figure 1 shows the general flow of EBIOS RM. It presents two risk management cycles. The strategic cycle includes every workshop, and the operational relates only to Workshop 3, Workshop 4, and Workshop 5. We can see that Workshop 3 plays an indispensable role that consists of assessing threat agents and determining scenarios involving these agents. Furthermore, this workshop provides most of the information required to identify the operational scenarios (Workshop 4) and the appropriate risk treatment (Workshop 5).

We will focus exclusively on the first three workshops because our purpose is to evaluate the threat level of smart-home stakeholders.

IV. Data Collection and Analysis

This section describes the participants of the study and presents data collection and analysis.

A. Participants

In total, 17 participants (Academic Researcher (11.8%), Cybersecurity Specialist (29.4%), Chief Information Security Officer (5.9%), and IT Department/Information Management Team (52.9%)) responded to our survey questionnaire. Furthermore, 47.1%, 47.1%, and 5.8% of participants have respectively less than 5 years, between 5-10 years, and more than 10 years of experience in cybersecurity. 76.5% of participants are certified in one or many certifications: Cisco Certified Network Associate (CCNA), Certified Ethical Hacker (CEH), Certified Information Security Manager (CISM), Certified Information Systems Security Professional (CISSP), Control Objectives for Information and Related Technology (COBIT) 5 Foundation, ISO 27001, Information Technology Infrastructure Library (ITIL) V3, ITIL V4. These certifications are attributed to individuals who can distinguish IT services, analyze and mitigate risks, understand cyberattack methods, design security countermeasures, and prevent unauthorized intruders from accessing network systems.

We also interacted directly in private messages with six respondents who wanted to get more details in our research. Four of them were security professionals who wanted to confirm that our study is real and legitimate. The two others were IoT/smart home professionals who informed us that they do not have the required skills for risk analysis. In a nutshell, the participants are likely to be qualified and experienced enough to assess the security of complex IT systems. Therefore, we assume that they are all eligible to evaluate the threat level of smart-home stakeholders.

B. Data Collection

We created an online Google Form and carried out the survey questionnaire over two weeks through two primary social networking services: LinkedIn for professionals and researchers and ResearchGate for academic researchers. We choose this short period of time to prevent eligible individuals to repeatedly take the only form and ineligible individuals to fill out the form. Our target was to reach cybersecurity professionals, top managers, and IoT/smart home specialists. To ensure the representativeness of the sample, we identified several private groups on LinkedIn related to IoT security/Cybersecurity, IoT/smart home professionals, risk managers, and Chief Information Security Officer (CISO).

The survey questionnaire provided six pages for a total of 13 questions, including five grid questions, which can be filled in 15-20 minutes. The questions we asked included:

C. Data Analysis

First, we asked the participants' opinions regarding the stakeholders we selected. To the question *"Do you think that these stakeholders are part of the smart home ecosystem?"*, more than 70% of participants responded *"Yes, I*

 ISBN: 978-1-61208-919-5

TABLE I
DESCRIPTION OF SEVERITY LEVELS REGARDING THE POTENTIAL IMPACTS OF FEARED EVENTS.

Severity level	Description
S4 (Critical)	Incapacity for the smart home to ensure all or a portion of its functioning. Severe impacts on the safety and security of dwellers, data, and assets.
S3 (Serious)	High degradation in the performance of the smart home. Significant impacts on the safety and security of dwellers, data, and assets.
S2 (Significant)	Degradation in the performance of the smart home. No direct impact on the safety and security of dwellers, data, and assets.
S1 (Minor)	Minor or no impact on operations or performances of the smart home. Minor or no impact on the safety and security of dwellers, data, and assets.

do" to 10 out of 14 propositions: *Energy service provider* (76.5%), *Healthcare service providers* (76.5%), *Home automation service providers* (88.2%), *Courier service providers* (23.5%), *Network service providers* (88.2%), *IoT cloud service providers* (88.2%), *Sensor/IoT device manufacturers* (70.6%), *IoT application developers* (88.2%), *IoT/smart home regulators* (97.1%), *Real estate agents* (11.8%), *Dwellers friends* (17.7%), *Dwellers collaborators* (11.8%), *Smart home owners (dwellers)* (76.5%), and *Other smart home inhabitants (dwellers)* (70.6%). We can see that three stakeholders, i.e., *Courier service providers*, *Real estate agents*, *Dwellers' friends*, and *Dwellers' collaborators*, did not get many favorable votes.

Furthermore, we asked the participants: *"Please rate the Dependency, Penetration, Cyber Maturity, and Trust levels between each stakeholder and the smart home on a scale of 1 to 5."* to measure the metrics recommended by EBIOS RM and calculate the threat levels. We used a five-point Likert scale to measure the participants' responses. The choice of this measure is motivated by Boone et al. [19], who stated that if one designs a series of questions that, when combined, measure a particular trait, then one has created a Likert scale. In this case, the authors recommended the mean and standard deviation to describe the scale.

V. THREAT LEVEL ASSESSMENT OF STAKEHOLDERS

This section describes the threat level assessment of smart-home stakeholders using EBIOS RM.

A. Scope and Security Baseline

The scope of this investigation is about the smart-home services (functions) that relate to stakeholders. According to Mendes et al. [20], we can distinguish four functions (i.e., energy efficiency and management, healthcare, entertainment, and security) in a smart home. The analysis of smart home devices discussed in [21] guided us to consider five essential functions in a smart home: energy management, safety and security, healthcare, home automation, and entertainment. These functions could be associated with one or many feared events (FEs). For each essential function identified, we associate the feared events, their impacts, as well as their severity. Table I summarizes each instance of severity.

Energy management: This function helps to avoid wasting energy and to supply power when a power failure occurs.

- FEs: *Triggering power outage*, *tampering consumed energy amount*, and *alteration of heating, ventilation, and air conditioning*. These FEs could impact the quality of service (QoS), comfort, safety, security of dwellers, and financial losses (Severity: S3 or S4).

Safety and security: The goal of this function is to ensure data and information confidentiality, integrity, and availability.

- FEs: *Disabling of alarm system*, *smart door lock*, or *network security services*, and *detection of human activities by an attacker*. These FEs could impact the QoS, data security, privacy, safety, and security of dwellers (Severity: S2, S3, or S4).

Healthcare: This function remotely monitors and manages the health of dwellers in the smart home.

- FEs: *Leaking medical data records of dwellers* and *altering medical data records*. These FEs could impact the safety and privacy of dwellers and involve financial losses (Severity: S3 or S4).

Home automation: Smart homes automate the in-home daily tasks of dwellers. This function controls and manages the smart home appliances. Furthermore, it automatically monitors and manages dwellers' activities in the smart home.

- FEs: *Altering the automation configuration and remote control by an attacker*. These FEs could impact the comfort, privacy, safety, and security of dwellers (Severity: S1, S2, or S3).

Entertainment: This function provides amusement moments (e.g., music, movies, games) to dwellers.

- FEs: *Leaking personal data of dwellers*. These FEs could impact the safety and privacy of dwellers and involve financial losses (Severity: S3 or S4).

Our research does not include the security baseline because it is only necessary for risk treatment in Workshop 5, which is beyond this research scope. However, it is essential to note that the security baseline of smart homes may include ISO 27030 and ISO 24391, which are currently under development.

B. Risk Origins

Bugeja et al. [22] classify the attacker profiles into six profiles: *"State-related", "terrorist", "competitor and organized crime", "hacktivist", "thief", and "hacker"*. In addition to this classification, we consider the *"amateur"* profile as script kiddies who use malicious codes and programs created

 ISBN: 978-1-61208-919-5

TABLE II
DESCRIPTION OF RO/TO PERTINENCE.

Identification		Scoring		Assessment
Risk origins (RO)	Target objectives (TO)	Motivation	Resources	Pertinence
Amateur	Challenge	Low	Limited	Low
Avenger	Obstacle to functioning; Spying	Low	Limited	Low
Competitor and organized crime	Profit; Strategic pre-positioning; Terrorism	High	Significant	Fair
Hacker	Challenge; Profit; Spying; Strategic pre-positioning	High	Significant	Fair
Hacktivist	Terrorism	Fair	Significant	Fair
Inadvertent attacker	N/A–does not intend to attack	Very low	Limited	Low
Specialized outfits	Profit; Challenge; Spying; Strategic pre-positioning	High	Considerable	High
State-related	Terrorism; Spying	High	Unlimited	High
Terrorist	Terrorism; Spying	Highly motivated	Considerable	High
Thief	Spying; Obstacle to functioning; Profit	Fair	Significant	Fair

by more experienced attackers, the "avenger" corresponding to profiles in bad relations with smart home inhabitants. An example of an avenger could be a disgruntled service provider. Furthermore, we consider the *"specialized outfits"* profile as cyber-mercenaries who are often at the origin of the design and creation of attack kits and tools. Lastly, we consider the *"inadvertent attacker"* profile as another risk origin because many recent attacks were due to human errors [23].

Note, the target objectives of attacker profiles are mostly well-known and could relate to *challenges* (e.g., fun, curiosity, or social recognition), *profit* (e.g., moneymaking by selling dwellers' private information), *spying* (e.g., access to dwellers' privacy), *obstacle to functioning* (e.g., making smart home services unavailable), *strategic pre-positioning* (e.g., using smart home devices to perform another attack–case of DDoS attacks), or *terrorism* (e.g., impacting smart home dweller security for political or economic purposes.).

Detecting risk origins (ROs) and target objectives (TOs) led us to determine the most critical attacker profiles to the smart home security. We assess the RO/TO pertinence as described in Table II by relying on the motivation level (i.e., very low, low, fair, or high) and potential financial, technical, human, and time resources (i.e., limited, significant, considerable, or unlimited) of attackers to compromise a smart home. Based on this assessment, the most relevant ROs are *terrorists*, *specialized outfits*, and *States-related*. Next, the least relevant but pertinent ROs are *thieves*, *hacktivists*, *hackers*, and *competitors and organized crimes*. Finally, the least pertinent ROs are *inadvertent attackers*, *avengers*, and *amateurs*. We will build the strategic scenarios on the most relevant ROs and the smart-home stakeholders.

C. Strategic Scenarios

1) Smart-Home Stakeholders: EBIOS RM recommends distinguishing internal stakeholders to the system from the externals to identify the stakeholders to be taken into account. Regarding the internal stakeholders, we decided to choose dwellers, i.e., people living in smart homes. They comprise smart-home owners and other smart-home inhabitants such as children. About the external stakeholders, the information collected in various academic papers [20] [24]–[26], led us to consider service providers, manufacturers, IoT developers, IoT/smart home regulators, real estate agents, dwellers' friends, and dwellers' collaborators. Note that services providers enrich smart homes with many services. They are energy providers, home automation providers, healthcare service providers, courier service providers, network service providers, and IoT cloud service providers. Manufacturers provide smart homes with actuators, sensors, and IoT devices. Developers create web and mobile applications that control one or more aspects of the smart home. Then, IoT or smart home regulators contribute to ensuring the quality of services by accreditation. Real estate agents encourage people that seek new properties to buy smart homes. Home dwellers' friends or collaborators may have direct or indirect access, depending on their intimacy with smart homes' owners and other dwellers.

2) Assessment of Stakeholders: This assessment is based on a formula recommended by EBIOS RM. The formula comprises four metrics (i.e., *Dependency*, *Penetration*, *Cyber Maturity*, and *Trust*). *Dependency* and *Penetration* represent the level of exposure to the system. More specifically, *Dependency* evaluates the degree of relationship between the stakeholder and the smart home. *Penetration* assesses how far the stakeholder could access the smart home assets (including physical and remote access). Then, *Cyber Maturity* and *Trust* give information on cyber reliability. *Cyber Maturity* measures the ability of stakeholders to understand and implement cybersecurity best practices in their daily activities. *Trust* measures the level of confidence the system should have regarding the intention of stakeholders. Each metric is scored on a scale from 1 to 4. When the threat level score of threat agents (stakeholders) is close or equal to 4, it is highly feasible that an attacker exploits the related stakeholder to compromise a smart home.

$$Threat\ Level = \frac{Dependency \times Penetration}{CyberMaturity \times Trust} \quad (1)$$

[18]

3) Measurement of Threat Levels: The EBIOS RM method recommends an assessment on a scale of 1 to 4 for each metric: *Dependency*, *Penetration*, *Cyber Maturity*, and *Trust*. As we used a five-point Likert scale in our survey questionnaire, we consider the participants' evaluations in the range of 0 to 4

 ISBN: 978-1-61208-919-5

TABLE III
EVALUATION OF THE "DEPENDENCY" (D), "CYBER MATURITY" (M), "PENETRATION" (P), AND "TRUST" (T) METRICS WITH MEANS AND STANDARD DEVIATIONS FOR EACH SMART HOME STAKEHOLDER.

	Number of n-points					Total points	Means	Standard Deviations
	0-point	1-point	2-points	3-points	4-points			
	(D) (M) (P) (T)	(D) (M) (P) (T)	(D) (M) (P) (T)	(D) (M) (P) (T)	(D) (M) (P) (T)	(D) (M) (P) (T)	(D) (M) (P) (T)	(D) (M) (P) (T)
Energy service providers	(0) (0) (0) (0)	(1) (5) (2) (2)	(5) (8) (7) (11)	(6) (4) (7) (3)	(5) (0) (1) (1)	(49) (33) (41) (37)	(2.88) (1.94) (2.41) (2.18)	(0.90) (0.73) (0.77) (0.71)
Healthcare service providers	(0) (0) (0) (0)	(0) (7) (3) (1)	(8) (7) (9) (9)	(5) (3) (5) (6)	(4) (0) (0) (1)	(47) (30) (36) (41)	(2.76) (1.76) (2.12) (2.41)	(0.81) (0.73) (0.68) (0.69)
Home automation service providers	(0) (0) (0) (0)	(0) (2) (1) (3)	(1) (7) (6) (10)	(10) (7) (8) (4)	(6) (1) (2) (0)	(56) (41) (45) (35)	(3.29) (2.41) (2.65) (2.06)	(0.57) (0.77) (0.76) (0.64)
Courier service providers	(5) (5) (3) (1)	(6) (9) (4) (7)	(4) (2) (9) (8)	(2) (1) (1) (1)	(0) (0) (0) (0)	(20) (16) (25) (26)	(1.18) (0.94) (1.47) (1.53)	(0.98) (0.80) (0.85) (0.70)
Network service providers	(0) (0) (0) (0)	(0) (1) (1) (4)	(1) (0) (5) (9)	(6)(12) (7) (3)	(10) (4) (4) (1)	(60) (53) (48) (35)	(3.53) (3.12) (2.82) (2.06)	(0.61) (0.68) (0.86) (0.80)
IoT cloud service providers	(0) (0) (0) (0)	(0) (0) (2) (3)	(2) (2) (4) (8)	(7) (11) (8) (5)	(8) (4) (3) (1)	(57) (53) (46) (38)	(3.35) (3.12) (2.71) (2.24)	(0.68) (0.58) (0.89) (0.81)
Sensor/IoT device manufacturers	(0) (0) (0) (0)	(1) (1) (3) (1)	(2) (7) (9) (12)	(7) (7) (2) (3)	(7) (2) (3) (1)	(54) (44) (39) (38)	(3.18) (2.59) (2.29) (2.24)	(0.86) (0.77) (0.96) (0.64)
IoT application developers	(0) (0) (0) (0)	(1) (1) (4) (4)	(5) (7) (6) (10)	(6) (8) (5) (3)	(5) (1) (2) (0)	(49) (43) (39) (33)	(2.88) (2.53) (2.29) (1.94)	(0.90) (0.70) (0.96) (0.64)
IoT/smart home regulators	(0) (0) (0) (0)	(1) (1) (4) (0)	(3) (8) (9) (8)	(9) (6) (3) (9)	(4) (2) (1) (0)	(50) (43) (35) (43)	(2.94) (2.53) (2.06) (2.53)	(0.80) (0.78) (0.80) (0.50)
Real estate agents	(3) (4) (3) (0)	(7) (10) (7) (8)	(5) (2) (7) (7)	(1) (0) (0) (2)	(1) (1) (0) (0)	(24) (18) (21) (28)	(1.41) (1.06) (1.24) (1.65)	(1.03) (0.94) (0.73) (0.68)
Dwellers friends	(4) (5) (2) (4)	(6) (8) (6) (6)	(5) (3) (6) (6)	(2) (0) (3) (1)	(0) (1) (0) (0)	(22) (18) (27) (21)	(1.29) (1.06) (1.59) (1.24)	(0.96) (1) (0.91) (0.88)
Dwellers collaborators	(4) (4) (4) (4)	(6) (8) (9) (6)	(6) (4) (4) (6)	(1) (1) (0) (1)	(0) (0) (0) (0)	(21) (19) (17) (21)	(1.24) (1.12) (1) (1.24)	(0.88) (0.83) (0.69) (0.88)
Smart home owners (dwellers)	(0) (3) (0) (0)	(1) (7) (2) (1)	(4) (5) (7) (9)	(4) (1) (8) (7)	(8) (1) (0) (0)	(53) (24) (55) (40)	(3.12) (1.41) (3.24) (2.35)	(0.96) (1.03) (0.68) (0.59)
Other smart home inhabitants (dwellers)	(1) (5) (0) (1)	(1) (6) (3) (2)	(5) (4) (1) (8)	(2) (1) (6) (6)	(8) (1) (7) (0)	(49) (21) (51) (36)	(2.88) (1.24) (3) (2.12)	(1.23) (1.11) (1.08) (0.83)

rather than 1 to 5. Thus, metrics that obtained 1 point during the assessment will get 0 points.

Mean and *standard deviation* describe the scale of the dataset.

$$\bar{x} = \frac{\sum x}{N} \tag{2}$$

The mean evaluates the average of points–where x is the point value for each evaluation and N represents the number of evaluations.

$$\sigma = \sqrt{\frac{\sum_{i=1}^{N}(x_i - \bar{x})^2}{N}} \tag{3}$$

Standard deviation is a statistical measurement that evaluates dataset variability. It helps to understand the distribution of the dataset relative to the mean.

Table III presents the evaluation results of the *Dependency (D)*, *Penetration (P)*, *Cyber Maturity (M)*, and *Trust (T)* metrics. We calculate the means and standard deviations and evaluate the threat level of each stakeholder using the obtained means.

4) Threat Classification: It provides a clear insight into how critical the threats are and contribute to prioritizing the countermeasures. Table IV presents the results of threat level assessments.

Figure 2 maps the threat levels of smart-home stakeholders according to the classification provided by EBIOS RM, i.e., the danger (red) zone is determined by considering 10% of the stakeholders with the highest threat levels. The control (yellow) zone is determined by considering 40% of the following stakeholders. The watch (green) zone is determined by considering 40% of the next stakeholders. The remaining

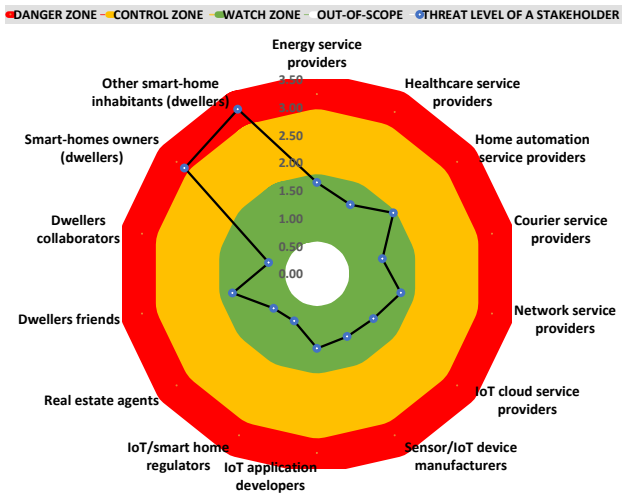

Fig. 2. A description of threat agents using EBIOS RM classification.

10% covers the out-of-scope. This classification indicates that the danger zone contains *Smart-homes owners (dwellers)* and *Other smart-home inhabitants (dwellers)*. The watch zone contains the other stakeholders.

Given that the EBIOS RM recommends a threat assessment in the range 1-4, a simplified classification could follow this pattern: Danger zone ($3 \leq$ Threat level ≤ 4); Control zone ($2 \leq$ Threat level < 3); Watch zone ($1 \leq$ Threat level < 2); Out-of-scope ($0 \leq$ Threat level < 1). Figure 3 maps the threat levels. According to this classification, the danger zone contains *Smart-home owners (dwellers)* and *Other smart-home inhabitants (dwellers)*, the out-of-scope contains *Dwellers collaborators* and *IoT/smart home regulators*. The watch zone

TABLE IV
LIKELIHOOD ASSESSMENT OF SMART HOME STAKEHOLDERS.

	Dependency	Cyber Maturity	Penetration	Trust	Threat Level
Energy service providers	2.88	1.94	2.41	2.18	1.64
Healthcare service providers	2.76	1.76	2.12	2.41	1.38
Home automation service providers	3.29	2.41	2.65	2.06	1.76
Courier service providers	1.18	0.94	1.47	1.53	1.21
Network service providers	3.53	3.12	2.82	2.06	1.55
IoT cloud service providers	3.35	3.12	2.71	2.24	1.30
Sensor/IoT devices manufacturers	3.18	2.59	2.29	2.24	1.26
IoT applications developers	2.88	2.53	2.29	1.94	1.34
IoT/smart home regulators	2.94	2.53	2.06	2.53	0.95
Real estate agents	1.41	1.06	1.24	1.65	1.00
Dwellers friends	1.29	1.06	1.59	1.24	1.56
Dwellers collaborators	1.24	1.12	1	1.24	0.89
Smart home owners (dwellers)	3.12	1.41	3.24	2.35	3.05
Other smart home inhabitants (dwellers)	2.88	1.24	3	2.12	3.29

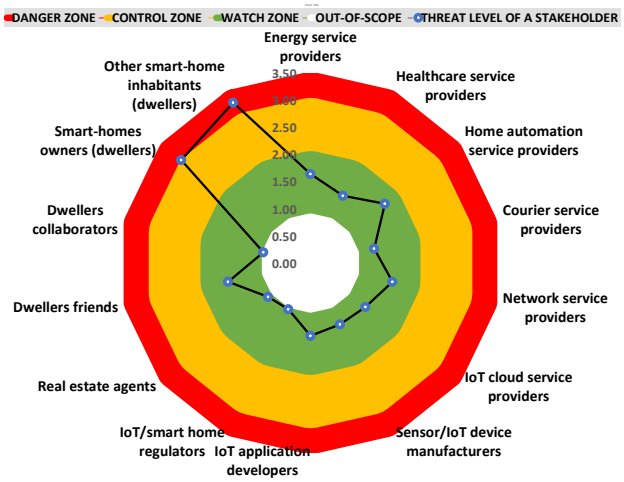

Fig. 3. A description of threat agents using a simplified classification.

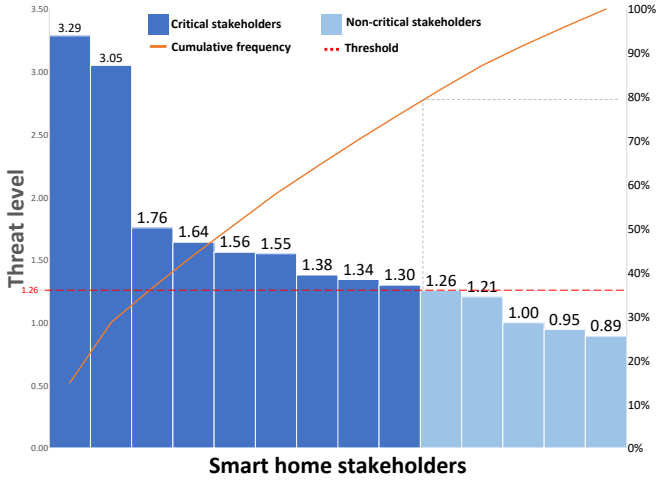

Fig. 4. A description of distinction between the critical and non-critical threats using a Pareto chart.

contains the other stakeholders.

We can notice that Figures 2 and 3 give different results. Furthermore, they do not distribute the threats onto each threat zone, which could be troublesome for decision-makers.

To cope with this limitation, we propose to use the Pareto principle [27] to determine the threat zones associated with each stakeholder. According to the Pareto principle or "80/20 rule", only a few vital inputs contribute to the greatest outputs. In our context, this principle contributes to identifying the most critical stakeholders who represent 80% of the total threats. Figure 4 presents a distinction between the critical and non-critical threats using a Pareto chart. Our proposed classification consists of iterating the Pareto Chart three times to determine respectively the stakeholders included in the following zones: *out-of-scope*, *watch*, *control*, and *danger*. We present the first iteration in Figure 4. The *non-critical stakeholder* obtained represents the *out-of-scope*. The second iteration uses the *critical stakeholders* obtained in the first iteration to identify the *non-critical stakeholders* included in the *watch zone*. Then, the third iteration uses the *critical stakeholders* obtained in the second iteration to identify the *non-critical stakeholders* included in the *control zone*. Finally, the remaining *critical stakeholders* of the third iteration is included in *danger zone*. Figure 5 presents the outcome when we classify the smart-home stakeholders per threat zone using a three-level Pareto chart. The danger zone contains *Smart-homes owners (dwellers)* and *Other smart-home inhabitants (dwellers)*, and *Home automation service providers*. The control zone contains *Energy service providers*, *Dwellers friends*, and *Network service providers*. The watch zone contains *Healthcare service providers*, *IoT application developers*, and *IoT cloud service providers*. The out-of-scope contains *Sensor/IoT device manufacturers* and *Courier service providers*, *Real estate agents*, *IoT/smart home regulators*, and *Dwellers collaborators*.

We summarize and compare the results of each classification method in Table V. The table illustrates that the Pareto-based classification can distribute the stakeholders' threats to every threat zone identified. Hence, a three-level Pareto chart can

TABLE V
COMPARISON OF THREE CLASSIFICATION APPROACHES OF THREAT AGENTS DISTRIBUTION PER ZONE.

	Danger zone		Control zone		Watch zone		Out-of-scope	
	Range of the likelihood (L)	Number of stakeholders	Range of the likelihood (L)	Number of stakeholders	Range of the likelihood (L)	Number of stakeholders	Range of the likelihood (L)	Number of stakeholders
EBIOS RM's classification	4≥ L ≥2.96	2	2.96 > L ≥1.77	0	1.77 > L ≥0.59	12	0.59 > L ≥0	0
Simplified threat classification	4 ≥ L ≥3	2	3 > L ≥2	0	2 > L ≥1	10	1 > L ≥ 0	2
Proposed Pareto's classification	4 ≥ L > 1.64	3	1.64 ≥ L > 1.38	3	1.38 ≥ L > 1.26	3	1.26 ≥ L ≥ 0	5

TABLE VI
DESCRIPTION OF THREE CRITICAL ATTACK PATHS.

	Risk Origins (RO)	Target Objective (TO)	RO/TO Pertinence	Fear Events (FEs)	Severity	Threat Agents (Smart-Home Stakeholders)	Likelihood
Attack path 1	Specialized outfits	Profit	High	Leaking personal data of dwellers; Leaking medical data records.	S4	Smart-home dwellers; Smart-home dwellers' friends.	Danger zone; Control zone.
Attack path 2	Terrorists	Terrorism	High	Triggering power outage; Disabling of network security services.	S4	Energy service providers; Network service providers.	Control zone; Control zone.
Attack path 3	State-related	Spying	High	Leaking personal data; Leaking medical data records; Altering medical data records.	S4	Home automation service providers; Network service providers; Smart-home dwellers' friends.	Danger zone; Control zone; Control zone.

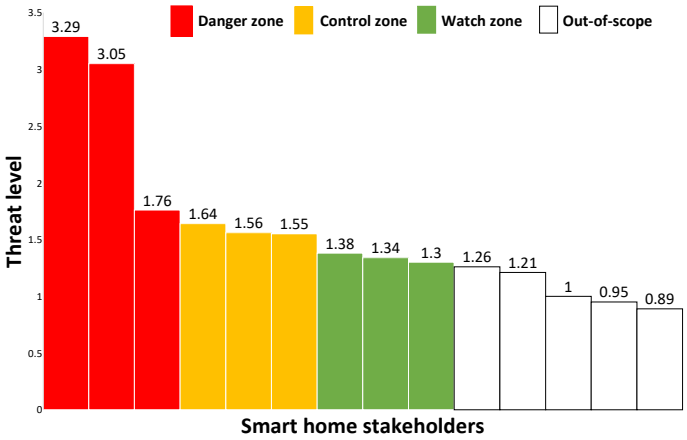

Fig. 5. A description of threat agents using a Pareto chart.

provide better results than the two other approaches.

5) Identification of Strategic Attack Scenarios: The attack scenarios present briefly which attacker's profile may want to exploit a particular vulnerability in smart homes, for what purpose, and how they can realize that. Table VI describes the needed information (e.g., RO/TO pertinence, feared events, and threat level) to identify three strategic attack scenarios.

Strategic attack scenario 1: *Experienced hackers with specialized outfits use social engineering techniques (e.g., phishing) to trick smart-home dwellers or their friends and get unauthorized access to a smart home. The attackers could sell their personal data or medical data records on the dark web to make profit (Severity: S4).*

Strategic attack scenario 2: *Terrorists put many smart homes out of service and spread fear among citizens by disabling access to Internet-based services after attacking network service providers or triggering power outages of many smart homes simultaneously after compromising the infrastructure of energy service providers (Severity: S4).*

Strategic attack scenario 3: *A government spies and gets confidential and sensitive information on opposition leaders or other state leaders to blackmail them for national security, political or economic purposes. The state-related profile performs the attack after taking advantage of the strategic positions of home automation service providers, network service providers, and dwellers' friends (Severity: S4).*

Figure 6 summarizes the three strategic attack scenarios.

VI. DISCUSSION

There are no easy solutions when discussing the security issues of complex systems such as smart homes. We are aware of the importance of developing robust systems to empower the security of home networks, mobile apps, and IoT software and hardware. Furthermore, we believe that attackers are continuously looking for weak links to achieve their ends. As in the recent attacks on the European aerospace giant Airbus in which attack scenarios first targeted Airbus' suppliers (external stakeholders) [28], attackers could take advantage of one or many stakeholders to harm a smart home and its inhabitants. Hence, to prevent such attack scenarios, we used EBIOS RM to evaluate the threat levels to which an attacker could compromise a smart-home stakeholder.

Threat level calculation: In our work, we have used the threat level equation proposed by EBIOS RM to evaluate the likelihood of threat agents. However, in risk assessment, many authors estimate the likelihood without the use of an equation. For example, Nurse et al. [29] used a 3-point Likert scale to estimate the likelihood directly, without considering an estimation of relevant metrics. As these authors mentioned, it is difficult to estimate the likelihood of risks. We believe that an approach, such as that of EBIOS RM, that evaluates many metrics to calculate the likelihood may provide more reliable results than a direct assessment. We encourage future research to investigate and provide new metrics and equations to estimate the likelihood of threat agents and cyberattacks in qualitative risk assessment.

Threat level of stakeholders: Our results showed that the security education of smart-home dwellers is crucial to reduce attack scenarios targeting these internal stakeholders. Further-

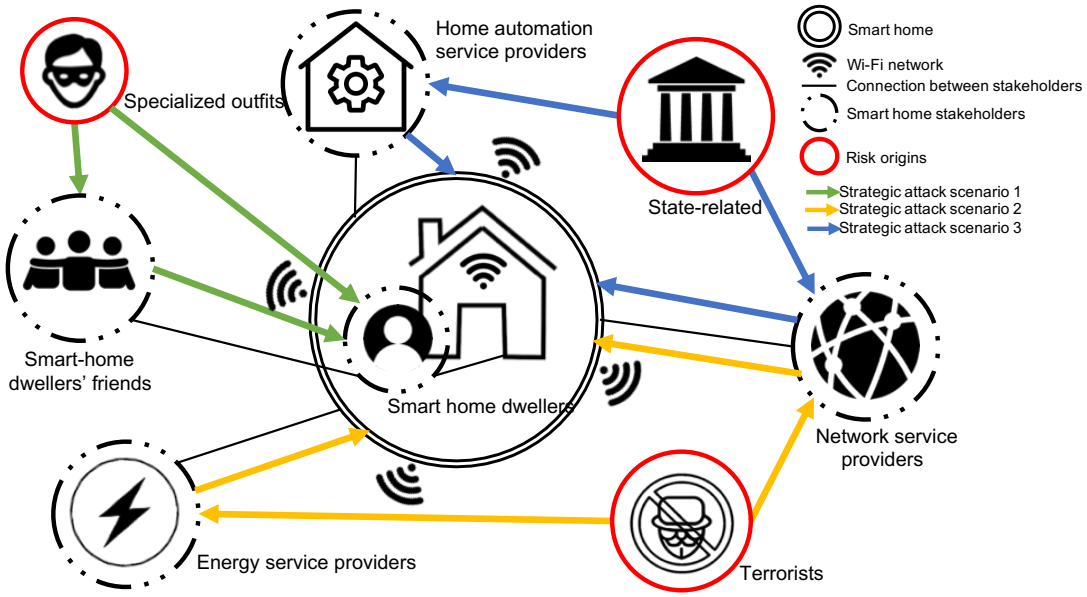

Fig. 6. A description of proposed attack scenarios on smart homes involving stakeholders.

more, there is an imperative necessity to set up a regulatory agency to check on home automation service providers and the other smart-home stakeholders to ensure they comply with the security standards of smart homes for the benefit of all. This cybersecurity compliance will increase the values of *Cyber Maturity* and *Trust*, and reduce the *Threat Level* given the calculation proposed by EBIOS RM.

Classification of stakeholders: Risk managers always have to make crucial decisions based on priorities to ensure the security of the assets they are in charge of. As presented in Table V, EBIOS RM could not distribute the stakeholders in every threat zone. To address this issue and provide a more effective classification to risk managers, we proposed a three-level Pareto chart. By extension, an $(n-1)$ level Pareto chart could distribute the threat agents on (n) threat zones effectively.

Attack scenarios: We defined the strategic attack scenarios based on information (e.g., risk origins, target objectives, fear events, threat agents, and threat level) we collected through our investigation. These scenarios support our claim regarding the importance of assessing the stakeholders for smart home security. However, it could be challenging to discuss how realistic these scenarios are. To address these issues, note that EBIOS RM recommends an assessment of every strategic attack scenario in Workshop 4, which is out of the scope of this paper.

Limitations: Given the complexity of smart home ecosystems, one limitation of this paper could be the identification of key smart-home stakeholders. "The Principle of Who or What Really Counts" rests upon the assumptions and perception of risk managers [30]. That being said, a comprehensive survey study to identify the smart-home stakeholders in regards to critical attributes, such as *power*, *legitimacy*, and *urgency* proposed by [30], is necessary. Moreover, the results of our research, especially those described in Table III and Table IV, rely on the stakeholders we choose and participants' responses to our questionnaire. Since we used an online questionnaire, we could not guarantee the integrity of the collected data. Furthermore, the results could have changed with fewer or more stakeholders and participants. It is necessary to remark that risk assessment is evolutionary. Threats are constantly evolving, and ecosystems are changing. Therefore, our results are not timeless. We recommend a more global investigation with considerable financial and human resources to perform a benchmark for significant smart-home stakeholders in many countries and collect evaluations of thousands of participants to provide more robust and reliable results.

Our findings sound the alarm on the security of smart homes, but mostly its stakeholders. This research fills a gap in the literature since none of the previous works have considered this perspective.

VII. Conclusion and Future Work

Cyberattacks regularly involve sophisticated means that could be challenging to detect, mainly when they target a dynamic and complex environment such as a smart home. This paper elaborates the security risk analysis of a smart home using EBIOS RM with a focus on the threat level assessment of smart-home stakeholders in the role of threat agents. The goal is to identify realistic attack scenarios to smart homes involving these stakeholders. We provide high-level attack scenarios involving smart-home stakeholders after a step-by-step process to identify risk origins, target objectives, fear events and their severity, threat agents and their threat level, as recommended by EBIOS RM. This perspective of the smart home security with a focus on stakeholders security issues have not been explored in the previous studies.

 ISBN: 978-1-61208-919-5

We develop a questionnaire based on a 5-point Likert scale to assess the threat level of threat agents. We propose a three-level Pareto chart to classify the smart-home stakeholders into different threat zones. This approach distributes the threat agents into every threat zone, unlike the proposed distribution suggested by EBIOS RM. Our results show that the threat levels of successful attack scenarios involving smart home inhabitants and smart home automation service providers are very high.

Forthcoming work will cover the identification and risk assessment of each operational scenario (Workshop 4) and the risk treatment (Workshop 5). More broadly, the present findings might contribute to extending the discussions on smart home security to the security of stakeholders who make smart home operations effective. Including stakeholders when rethinking the security design of smart homes becomes essential. Furthermore, multi-layered security cooperation for smart home security could be possible in the future. Future work will cover the designing of security systems and policies considering stakeholders for smart home security. We invite interested readers to engage in smart-home stakeholders analysis to provide other perspectives and results.

ACKNOWLEDGMENT

Part of this study was funded by the ICS-CoE Core Human Resources Development Program.

REFERENCES

[1] M. R. Alam, M. B. I. Reaz, and M. A. M. Ali, "A review of smart homes—Past, present, and future," *IEEE transactions on systems, man, and cybernetics, part C (applications and reviews)*, vol. 42, no. 6, pp. 1190–1203, 2012.

[2] P. P. Gaikwad, J. P. Gabhane, and S. S. Golait, "A survey based on Smart Homes system using Internet-of-Things," in *2015 International Conference on Computation of Power, Energy, Information and Communication (ICCPEIC)*. IEEE, 2015, pp. 0330–0335.

[3] Statista, "Smart Home Report 2021," 2021, retrieved: October, 2021. [Online]. Available: https://www.statista.com/study/42112/smart-home-report/

[4] Proofpoint, "More than 750,000 Phishing and SPAM emails Launched from "Thingbots" Including Televisions, Fridge," 2014, retrieved: October, 2021. [Online]. Available: https://www.proofpoint.com/us/proofpoint-uncovers-internet-things-iot-cyberattack

[5] E. Blumenthal and E. Weise, "Hacked home devices caused massive Internet outage," 2016, retrieved: October, 2021. [Online]. Available: https://www.usatoday.com/story/tech/2016/10/21/cyber-attack-takes-down-east-coast-netflix-spotify-twitter/92507806/

[6] A. Jacobsson, M. Boldt, and B. Carlsson, "A risk analysis of a smart home automation system," *Future Generation Computer Systems*, vol. 56, pp. 719–733, 2016.

[7] C. Wongvises, A. Khurat, D. Fall, and S. Kashihara, "Fault tree analysis-based risk quantification of smart homes," in *2017 2nd International Conference on Information Technology (INCIT)*. IEEE, 2017, pp. 1–6.

[8] Cherdantseva et al., "A review of cyber security risk assessment methods for scada systems," *Computers & security*, vol. 56, pp. 1–27, 2016.

[9] ISO, "ISO/IEC 27005:2011(en) Information technology — Security techniques — Information security risk management," 2011, retrieved: October, 2021. [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso-iec:27005:ed-2:v1:en

[10] D. Bregman, "Smart home intelligence–the ehome that learns," *International journal of smart home*, vol. 4, no. 4, pp. 35–46, 2010.

[11] W. Abbass, A. Baina, and M. Bellafkih, "Using EBIOS for risk management in critical information infrastructure," in *2015 5th World Congress on Information and Communication Technologies (WICT)*, 2015, pp. 107–112.

[12] B. Ali and A. I. Awad, "Cyber and physical security vulnerability assessment for IoT-based smart homes," *Sensors*, vol. 18, no. 3, p. 817, 2018.

[13] G. Kavallieratos, V. Gkioulos, and S. K. Katsikas, "Threat analysis in dynamic environments: The case of the smart home," in *2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS)*. IEEE, 2019, pp. 234–240.

[14] T. R. Peltier, *Information security risk analysis*. CRC press, 2005.

[15] R. Grimble and K. Wellard, "Stakeholder methodologies in natural resource management: a review of principles, contexts, experiences and opportunities," *Agricultural Systems*, vol. 55, no. 2, pp. 173–193, 1997, socio-economic Methods in Renewable Natural Resources Research. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0308521X97000061

[16] R. M. Yawson and B. Greiman, "Stakeholder analysis as a tool for systems approach research in hrd," in *Leading Human Resource Development through Research. Proceedings of the 21st Annual AHRD International Research Conference in the Americas. Houston, Texas, USA*, 2014.

[17] M. Mollaeefar., A. Siena., and S. Ranise., "Multi-stakeholder cybersecurity risk assessment for data protection," in *Proceedings of the 17th International Joint Conference on e-Business and Telecommunications - SECRYPT*, INSTICC. SciTePress, 2020, pp. 349–356.

[18] ANSSI, "EBIOS Risk Manager – The method," 2021, retrieved: October, 2021. [Online]. Available: https://www.ssi.gouv.fr/en/guide/ebios-risk-manager-the-method/

[19] H. N. Boone and D. A. Boone, "Analyzing likert data," *Journal of extension*, vol. 50, no. 2, pp. 1–5, 2012.

[20] T. D. Mendes, R. Godina, E. M. Rodrigues, J. C. Matias, and J. P. Catalão, "Smart home communication technologies and applications: Wireless protocol assessment for home area network resources," *Energies*, vol. 8, no. 7, pp. 7279–7311, 2015.

[21] V. Williams, S. Terence J., and J. Immaculate, "Survey on internet of things based smart home," in *2019 International Conference on Intelligent Sustainable Systems (ICISS)*, 2019, pp. 460–464.

[22] J. Bugeja, A. Jacobsson, and P. Davidsson, "An analysis of malicious threat agents for the smart connected home," in *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*. IEEE, 2017, pp. 557–562.

[23] S. Harris, "China's cyber-militia," 2008, retrieved: October, 2021. [Online]. Available: https://www.nextgov.com/cio-briefing/2008/05/chinas-cyber-militia/42113/

[24] M. R. Alam, M. B. I. Reaz, and M. A. M. Ali, "A review of smart homes—past, present, and future," *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, vol. 42, no. 6, pp. 1190–1203, 2012.

[25] R. H. Jensen, Y. Strengers, J. Kjeldskov, L. Nicholls, and M. B. Skov, *Designing the Desirable Smart Home: A Study of Household Experiences and Energy Consumption Impacts*. New York, NY, USA: Association for Computing Machinery, 2018, p. 1–14. [Online]. Available: https://doi.org/10.1145/3173574.3173578

[26] S. Ul Rehman and S. Manickam, "A study of smart home environment and its security threats," *International Journal of Reliability, Quality and Safety Engineering*, vol. 23, no. 03, p. 1640005, 2016. [Online]. Available: https://doi.org/10.1142/S0218539316400052

[27] V. Pareto, *Trattato di sociologia generale [The mind and society]*. G. Barbèra, 1916, vol. 2.

[28] AFP, "Airbus Hit by Series of Cyber Attacks on Suppliers: Security Sources," 2019, retrieved: October, 2021. [Online]. Available: https://www.securityweek.com/hackers-target-airbus-suppliers-quest-commercial-secrets

[29] J. R. C. Nurse, A. Atamli, and A. Martin, "Towards a usable framework for modelling security and privacy risks in the smart home," in *Human Aspects of Information Security, Privacy, and Trust*, T. Tryfonas, Ed. Cham: Springer International Publishing, 2016, pp. 255–267.

[30] R. K. Mitchell, B. R. Agle, and D. J. Wood, "Toward a theory of stakeholder identification and salience: Defining the principle of who and what really counts," *The Academy of Management Review*, vol. 22, no. 4, pp. 853–886, 1997. [Online]. Available: http://www.jstor.org/stable/259247

 ISBN: 978-1-61208-919-5