A Metamodel-Based Approach for Eliciting Security Requirements in Cyber-Physical Systems within the Context of Industry 4.0

Shafiq ur Rehman[††]

College of Computer and Information Sciences, Imam Muhammad bin Saud Islamic University (IMSIU)
Riyadh, Saudi Arabia

Abstract
The increasing significance of Cyber-Physical Systems (CPS) within the framework of Industry 4.0 have not only present numerous new opportunities but have also become an integral component of the contemporary world in recent years. Hence, the process of implementing security requirements engineering for CPS is more complex as compared to the traditional software applications. Consequently, the formulation of security requirements, which delineate a system's functionality to uphold security protocols, must be customized to meet the specific needs of these advancing technologies. Such systems are intended to directly interact with human beings, which makes security implementation an important factor for safety of human lives. This paper presents detailed overview of security requirements engineering issues present in CPS within context of industry 4.0. To handle the security issues, a metamodel for eliciting security requirements is presented. This metamodel concludes seven different aspects in which every one of them is illustrated separately. Since it is important to use the metamodel correctly, a case study is presented and applied to every component to validate the proposed metamodel to elicit security requirements for cyber-physical systems.

Keywords:
Cyber-Physical Systems (CPS), Security, Security Requirements Engineering, Human Machine Interface, Supervisory Control, Data Acquisition.

1. Introduction

Cyber-Physical Systems (CPS) have become integral components of the contemporary world [1,2]. Smart homes and automated car parking systems stand out as prevalent instances of CPS [3,4]. These systems can be comprehensively characterized as the integration of global technology (Cyber) with the physical environment, operating predominantly autonomously 24 hours a day. Core devices in these systems include sensors for data acquisition and actuators for effecting changes in the physical environment. Some common examples of such components are fingerprint sensors employed for entry control and automated sprinklers responsible for watering a garden [5]. These components collectively exemplify the fusion of cyber and physical elements within the CPS framework, where the interaction between software and the tangible world yields sophisticated functionalities. Cyber-Physical Systems is used to bridge the cyber and the physical world, through this interconnection, physical de- vices can be controlled throughout cyber commands. In the context of IOT systems or Cyber-Physical Systems (CPS), Industry 4.0 assumes a crucial role in expediting the decision-making process [6,7,8]. It promotes collaboration among various departments, ensuring timely and informed decisions accessible to authorized personnel. A few examples of CPS integrated with industry 4.0 in various fields of life are shown in figure 1. The integration of Industry 4.0 not only enhances efficiency but also boosts productivity within the system. However, The four foundational principles of Industry 4.0 interoperability, information transparency, decentralized decisions and technical assistance intro- duce novel attack surfaces susceptible to exploitation by malicious actors [9]. Like any evolving system, the adoption of new technologies brings forth security challenges. These challenges vary from manage- able and dismissible threats to severe risks capable of rendering the entire system inoperable [10]. As these systems offer a new, physical dimension, ensuring their security poses a significant challenge. Consequently, applying the security requirements engineering process is not as straightforward as it is with conventional software. Therefore, security requirements, defining a system's behavior to enforce security measures, must be tailored to align with the demands of these emerging technologies. The inherent heterogeneity of Cyber-Physical Systems distinguishes them from common software. These systems are composed of various third-party components grouped together to form a new software entity. Frequently, these components consist of legacy software, implying that they are over

Manuscript received November 5, 2025
Manuscript revised November 20, 2025
https://doi.org/10.22937/IJCSNS.2025.25.11.3

a decade old and might not be current [11,12,13]. Consequently, legacy software often harbors unpatched vulnerabilities, and the fundamental design of CPS is built upon potentially faulty software [14].

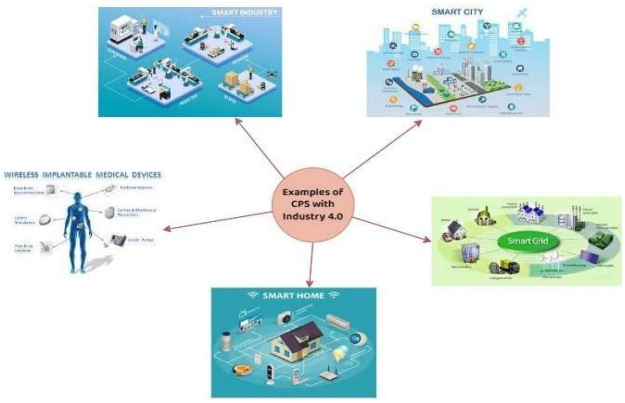

Fig. 1. Different examples of CPS integrated with industry 4.0

CPS normally designed for continuous operation; face challenges due to the need for uninterrupted functionality. Unlike common software that can be easily shut down for updates, these systems, often integral to critical infrastructure, cannot be easily suspended [15]. This presents a challenge in promptly addressing security flaws through updates, leaving the system vulnerable to potential malicious attacks. Another major issue in CPS is in communication, particularly within sensor networks, poses challenges. The small size of modern sensors, coupled with limitations in power, memory, and computational capabilities, impede the implementation of robust security measures [16,17].

As previously mentioned, Industry 4.0 relies on CPS along with various technologies. Like any other system, the integration of new technologies introduces security challenges. These challenges span from mi- nor threats that can be easily addressed or overlooked to more severe threats capable of rendering the entire system unusable [9]. Given that CPS involve direct interaction with humans, the primary focus extends beyond information security to ensuring the physical safety of individuals [7,18]. This imperative is evident in critical infrastructures like modern railway systems, where unauthorized access could pose life-threatening risks [9,7]. This research is focused on prioritizing human safety comprehensively, addressing key challenges such as the inability to install updates seamlessly and the security limitations in wireless sensor communication due to resource constraints. The critical need for security research in various forms of CPS underscores the urgency to establish a metamodel for eliciting security requirements, ensuring that security measures can be effectively applied to safeguard hu- man well-being at all times. This is to help developers eliciting security requirements and reducing complexity of the security requirements engineering process. Since a fully developed list of security requirements is an important characteristic of a secure system, a metamodel to elicit security requirements for cyber-physical systems is presented. This metamodel consists out of 7 different components. Each of them rep- resents an essential aspect of security which needs to be considered. This metamodel can also directly serve the overlaying organizations and improve the quality of their product. Customers can be sure that the Cyber-Physical Systems has at least a certain level of security since it is based on the metamodel presented in this paper.

The subsequent sections of this paper are structured as follows: Section II provides an overview of the background and existing research. Section III out- lines the methodology of the proposed approach in de- tail. In Section IV, the case study is presented to evaluate the methodology. Following that, Sections V present the conclusion and discussion.
The primary contributions of this paper can be out- lined as follows:

- Outlined significant challenges related to security in Cyber-Physical Systems within the context of Industry 4.0.
- Presented a metamodel for creating security requirements of Cyber Physical Systems.
- A case study (smart home) has been developed to validate the presented metamodel.
- The seven concepts of presented metamodel for security of CPS are further explained individually using smart home example.

2. Literature Review

The broad spectrum of technology encompassed by Industry 4.0 with CPS allows businesses to consistently improve best practices within the sector. This is facilitated by their ability to manage and analyze extensive data, spanning from customer orders to the production and output of products [19]. In a research [20] the authors explain two of the three basic general components of Cyber-Physical Systems, the Human- Machine Interface (HMI) and Supervisory Control and Data Acquisition (SCADA). The HMI software dis- cussed in that article is iFIX version 4.5. Since iFIX 4.5 has like every other software vulnerability, too, principles of the security requirements engineering process are introduced and the importance of security requirements, especially for Cyber Physical Systems, are clarified. In the next part, a case study is used, focusing on vulnerabilities, particularly targeting authentication issues, and discusses them in detail.

In another article [21], authors states that software security is a relatively new and evolving field, not yet fully matured or explored. The authors emphasize the distinction between software security and secure software, noting that vulnerabilities are inherent, and security mechanisms do not assure 100% security. The core focus of the article revolves around providing an overview of best practices in software security within the context of the traditional waterfall model. These practices are initially summarized in a visual representation and subsequently elucidated in detail.

Julie Greensmith's presented a paper [22], in which he explains three distinct security measures, commencing with an overview of firewalls. The article provides a brief explanation of firewalls in general and delves into the detailed discussion of three common types: packet-filtering firewalls, circuit level gate- ways, and application gateways. Additionally, the article illustrates intrusion detection systems, with a focus on both network-based and host-based intrusion detection systems. While these security measures—firewalls, intrusion detection systems, and anti- virus scanners—may seem similar in function, the article concludes by elucidating the key differences among them.

In another research [23], different flaws of sensors using biometric data are presented. To get a deeper knowledge of vulnerabilities of biometric sensors, previously developed models of possible attack points are introduced. According to these models, the author creates a threat-vector framework concluding 18 different threat vectors against biometric sensors. Since these threat vectors are equally important, each of them is explained in detail afterwards. In this paper a table of several solution possibilities is presented, where each solution is clarified in a separate section.

Article [24] explores the viability of three fundamental security mechanisms—cryptography, steganography, and physical layer secure access in wireless sensor networks, considering the limitations of small sensors with restricted processing, memory, and battery power. The authors define security threats and is- sues, providing explanations and examples of the most prevalent ones. To address these threats, a table is presented which outline various security schemes. In another article [25], the authors present the IRIS Metamodel for usable security requirements, emphasizing that security can be achieved through correct system usage but may be compromised if utilized un- expectedly. The metamodel comprises essential com- ponents such as task, goal, risk, and responsibility. The task metamodel encapsulates the concept of usable security requirements, addressing individual interactions with the system. To validate the IRIS metamodel, a case study is developed and applied, providing practical insights into its effectiveness.

A framework is proposed in 2018 [6] that defines a specific set of attributes for each subsystem within a Cyber-Physical System (CPS). These attributes con- tribute to creating detailed models enabling the evaluation of the system's security posture. The framework is constructed by analyzing historical vulnerability data from databases, referred to as evidence, and aligning it with the system model based on the identified at- tributes. The paper demonstrates that this framework achieves model sufficiency by mapping potential at- tack vectors, using the example of an NMEA GPS and radio module.

In a recent survery [26], The growing demand for sophisticated security techniques and strategies to

identify and prevent attacks on the Internet of Things (IoT) and Cyber-Physical Systems (CPS) is evident. The paper outlines research challenges and provides insights into future directions in this domain. In this survey they emphasized on need of more research in this area.

Similarly in another recent research paper [27], vulnerabilities, attacks, and threats to Cyber-Physical Systems (CPS) security are comprehensively analyzed. The analysis scrutinizes the limitations of current security measures and their impact on people's lives. The paper explores the principal types of security threats and attacks in CPS, providing analysis. Lastly, it discusses the challenges in CPS, proposes potential solutions, and identifies areas for future research, high-lighting the global significance of security in designing robust and efficient CPS.

3. Proposed Methodology

This research is focused on handling the security requirements and challenges in CPS for industry 4.0.

3.1. Challenges in CPS

The following highlights several fundamental challenges in Cyber-Physical Systems security, emphasizing the greater difficulty in securing them compared to typical software.

3.1.1. Legacy Software

Cyber-Physical Systems get often referred to the term "System of Systems". They basically consist out of many different third-party systems which are grouped together and create a new system themselves [28]. They encompass systems over a decade old, poses numerous security challenges. Justifications such as the current functionality and cost-effectiveness contribute to the widespread use of legacy software. However, older software of- ten includes unaddressed vulnerabilities and insecure protocols. Consequently, building a new system upon a flawed legacy one can perpetuate its vulnerabilities. Rectifying these issues becomes exceedingly challenging, as the original developers may be unreachable, and the current team might lack knowledge about the legacy software. This compromised integration can create new points of vulnerability, introducing potential attack vectors [29].

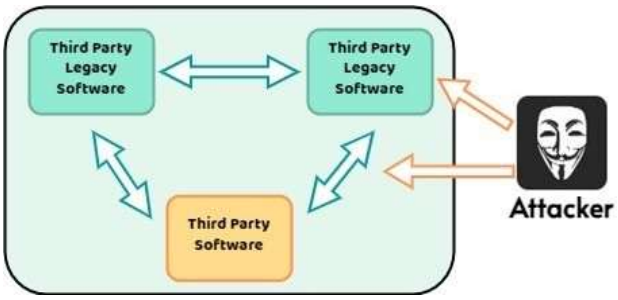

Fig. 2. System of Systems (CPS)

3.1.2. 24-hour runtime

A fundamental requirement and one of the most alarming challenges in CPS for industry 4.0 is their continuous operation, necessitating a 24/7 runtime. Unlike conventional software, which can be temporarily shut down for updates, certain systems like a pace- maker, vital to its user, cannot afford such interruptions. Similarly, a smart home relies on a network, which in turn depends on electricity. Owing to these intricate dependencies, the imperative for a continuous 24-hour runtime becomes critical. Any failure in even a single component could lead to a system-wide crash [29].

3.1.3. Myths on CPS security

Initially, developers of the first CPS believed these systems were safe from malicious threats due to their specialized techniques. This optimistic perspective led to a lack of security mechanisms in the early phase [30]. However, the rapid occurrence of attacks, exemplified by the Maroochy Water Breach where an employee hacked into a wastewater system, disapproved the argument that CPS were too complex to attack [31].

3.2. Security Requirements Engineering

Security requirements engineering aims at generating a nearly complete list of security requirements to guarantee best possible security for the concerning system. Security requirements are arrangements de- scribing behaviour of the system that enforces security. The significance of software security is on the rise in the development of CPS for industry 4.0, with a primary focus on ensuring the continuous and accurate operation of the software under various circumstances. These scenarios range

from natural disasters to acts of vandalism, terrorism, or malicious attacks [21].

3.2.1. Threat

A software threat exploits design flaws in a system, posing a security risk that software security aims to counter. Threats are categorized by their source, tar- get system, attacker's motive, attack vector, and con- sequences. Each threat has a likelihood and impact, requiring diverse security measures in CPS [2,28].

3.2.2. Vulnerability

In contrast, a vulnerability is a system weakness susceptible to exploitation through threats. The vulnerability life cycle involves four phases. Initially, it is detected by a third-party user or the development team. If a malicious third party identifies vulnerabilities at this stage, they have ample time to exploit them, given their exclusive awareness. Once the developers have fixed the issue and released a patch, the third phase has been started. A patch is an update which can be installed by the user. Since the user is not forced to download and install the latest up- dates from the vendors and is often not aware of the importance of them, the last phase of the life-cycle will usually not be reached [32].

3.2.3. Asset

A crucial aspect of security in Cyber-Physical Systems involves effectively managing all assets. Assets encompass anything, tangible or intangible, that holds value for the organization [33]. Broadly, assets can be categorized into three groups as shown in the Figure 3. The first category includes the utilized hardware, such as Programmable Logic Controllers and various servers within Cyber-Physical Systems. Even physical devices employed by developers are considered as- sets, as they play a vital role in the organization's success. The second category pertains to the software system developed during the development process and the third category encompasses stakeholders—individuals who have influence over the operation's success.

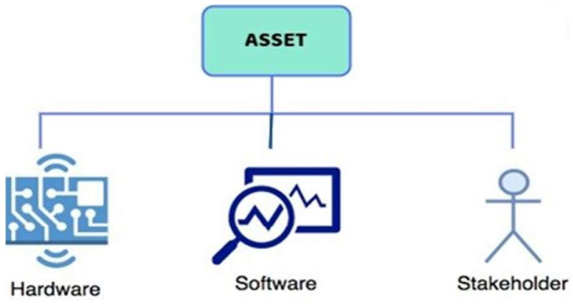

Fig. 3. Asset: Three Groups

3.2.4. Risk

In software engineering a risk arises when a threat has exploited a vulnerability in the system and attacked a certain asset. Once a risk has been exposed, the total risk impact (R) can be calculated throughout the product of the likelihood (L) and the impact (I) of the corresponding threat as shown in the Figure 4. Therefore, the impact will be higher if either the likelihood or the impact rises and a low-cost high impact risk can be as problematic as a high-cost low impact one [34,18].

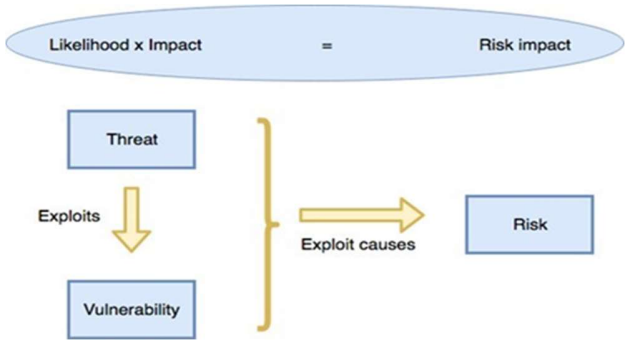

Fig. 4. Risk

3.3. CPS Security Requirements Engineering for Industry 4.0

As mentioned earlier, achieving security in Cyber- Physical Systems is crucial yet challenging, and absolute security is nearly impossible. According to CERT- SEI & CERT-UK (Computer Emergency Response Team), vulnerabilities and threats surged by 2493 % from 1997 to 2015. As software complexity increases and CPS provides physical gateways, retrofitting security to an already deployed system becomes impractical. Security should be an ongoing process through- out the development life cycle, starting on day one and persisting until the system is

no longer in use. While the intensity of security management may vary, the primary focus should be on investing significant effort into security requirements early in the development process. However, developers must remain vigilant to address security issues at any point in the system's life cycle. Security requirements engineering aims to systematically create secure software by generating a comprehensive set of detailed security requirements. Due to the potential for costly and risky consequences resulting from incomplete security requirements, it is crucial to consider a wide range of conceivable vulnerabilities and threats. Unforeseen weaknesses may be detected through improper user usage, highlighting the need to establish not only explicit software and hard- ware security requirements but also requirements pertaining to developers, architects, users, and other fac- tors that may not be immediately apparent [21,35].

3.4. CPS Metamodel

Models have always played an important part in many different aspects of the world and are usually created to present a human understandable image of a specific aspect throughout abstraction. Since a model needs specific rules how it must be created and how it must be read, every model is designed with a specific modelling language which serves a template for syn- tax and semantic. Especially the development process of Cyber-Physical Systems offers good possibilities to reduce the complexity by models. Metamodels on the other hand, are a specific kind of modelling. The difference is, that the information presented in metamodels are models themselves [36]. Metamodeling is the analysis, construction and development of the rules, constraints and models applicable and useful for modeling a special class of problems. In this paper, a CPS Metamodel is presented which includes seven different metamodels helping to identify security requirements for Cyber Physical Systems. The first metamodel which is presented in the figure 5 is the most abstract one and concludes seven entities referring to another, lower abstracted metamodel. Each CPS has at least one asset, one security goal, one threat, one hard- ware endpoint, one sensor communication medium and one risk. Securing the network communication is only preferable, but not inevitable necessary.

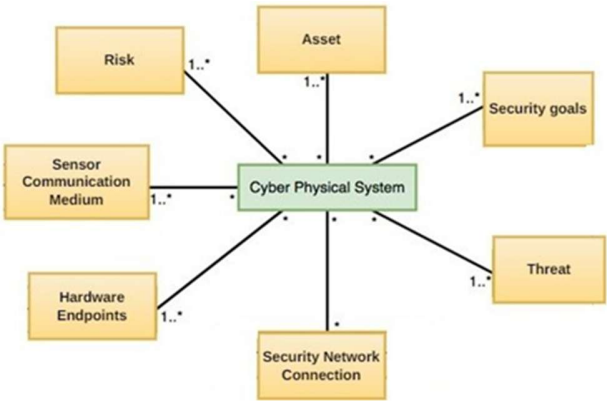

Fig. 5. CPS Metamodel

3.4.1. Asset Metamodel

The primary metamodel at this abstraction layer is the asset metamodel as shown in the Figure 6. Assets, encompassing software, hardware, and stakeholders, contribute value to the system and can be associated with certain threats and vulnerabilities. Software assets may include components like Kerberos or operating systems such as Microsoft Windows. Stakeholders, comprising individuals or organizations influencing the system, are classified into two types: those actively involved in the project (e.g., developers, management) and those affected by the project who utilize its artifacts. Since some assets are more important than others, they can be marked by values.

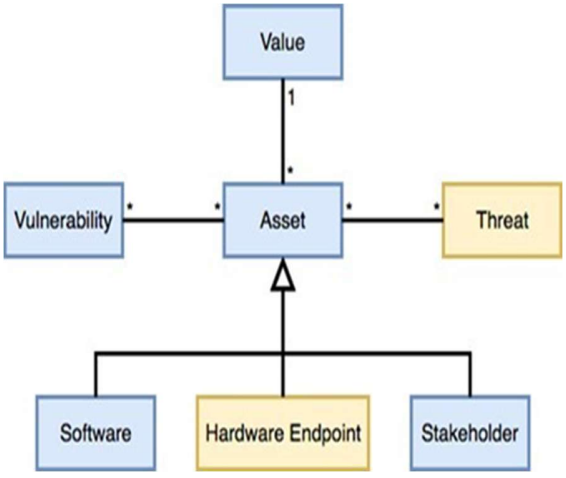

Fig. 6. Asset Metamodel

3.4.2. Security Goal Metamodel

Typically, security goals are identified through requirements gathered from stakeholders and developers, often associated with specific contexts and assets. Context, in this context, refers to the physical environment, users, or the operational world of the software. Occasionally, non-functional requirements, such as quality requirements, may not be linked to a specific context or asset. Despite variations in project-specific requirements, the fundamental security goals—confidentiality, availability, integrity, and access control—are consistently present in every security policy. Security goals can be identified not only through requirements from stakeholders and developers but also by analyzing how tasks are executed within the system. Ensuring security for all users, including those with different levels of efficiency and satisfaction, involves testing tasks against various personas, representing prototype characters. To guarantee best possible security, as many security goals as possible should be elicited. Therefore, a security goal not necessarily needs an obstacle since the malware for that security goal may not have been invented yet. The more security goals the safer is the system, even if some of them seem unnecessary or duplicated.

3.4.3. Threat Metamodel

Each threat originates from a malicious attacker aiming to achieve specific objectives, which can be inferred from one or more motives of various natures. Economic motivations, involving attempts to improve the attackers' financial situation, are commonly observed. Additionally, politically motivated at- tacks, gaining attention, may involve extremist groups spreading propaganda or even entire states pursuing such motives. Next to the motive, the attacker chooses an attack vector, which is the mechanism used to con- duct the attack. Along classic vectors like malware, Cyber-Physical Systems offer sensors, which can be tricked by using fake data. Depending on the attack vector and the capabilities of the attacker, sooner or later consequences are deduced. Especially in Cyber Physical Systems, these consequences can be catastrophic. It is desired to have 100 percent secure system, however, realistically this is not possible as a system will never be that secure and free from vulnerabilities. Threats can be categorized throughout two values. First, the likelihood that the event happens and second the impact of the loss when the event happens. Once a threat finally exploits a vulnerability, the result would be a risk, which will be explained later in section 3.4.7.

3.4.4. Secure Network Communication Metamodel

Effective network communication relies on robust security mechanisms. Firewalls, particularly packet- filtering firewalls within networks, enable the filtration of both incoming and outgoing network packets. With firewalls, network intrusion detection systems play its role. These systems monitor the traffic of the network and in case of unusual activity it triggers alarms. They monitor the network traffic and cause alarm, if suspicious activities are discovered. Additionally, communication within wireless sensor networks is characterized by unreliability, leading to frequent packet damage or loss. Given that various protocols exhibit distinct characteristics, the selection of protocols can play a crucial role in enhancing overall security significantly [37].

3.4.5. Hardware Endpoint Metamodel

In CPS, where real-time communication is imperative, sensor nodes must ensure the freshness of data. Moreover, CPS may operate in diverse and uncertain environments characterized by varying conditions such as temperature. To excel in every scenario, sensors must exhibit exceptional robustness despite their compact sizes, and they should incorporate security mechanisms for enhanced protection [38]. The level of security in Cyber-Physical Systems depends on the specific system employed, as some systems may guarantee security by preventing attackers from accessing the hardware endpoints altogether.

3.4.6. Sensor Communication Medium Metamodel

Due to their inexpensiveness of resources and their ability to be implemented decentralized, Network Intrusion Detection Systems and Network Intrusion Prevention Systems provide a good basis for sensor communication mediums [39]. Encryption techniques, on the other hand, have been devised for traditional networks. Modern encryption schemes need many re-sources in form of memory, battery and processing power which, once again, are rare in sensors systems.

3.4.7. Risk Metamodel

Every potential risk is fundamentally rooted in a specific threat. Consequently, the resulting risks can

be systematically prioritized based on the probability of occurrence and the potential impact of the loss associated with the connected threat. Once the risks are prioritized, response strategies aimed at mitigating either the likelihood or the impact of the threat can be implemented. Risk prevention is probably the best, but also the hardest solution. The intention here is to avoid negative affects impacting the system which may involves applying major changes to the project design. If the development process is near to completion and an unexpected risk arises that would necessitate significant changes to the system design, risk mitigation measures can be implemented. Another approach is transferring the responsibility for a certain risk to a third party. Although this measure is rather costly, it offers savings in time, since the developers of the system do not have to deal with that particular problem. However, if the risk's impact is low but costly to mitigate, it can be appropriate to simply accept that risk by either ignoring it or at least monitoring its current status [18,39]. In the next section, figures of all these meta-models are shown using a case study based on smart home.

4. Case Study and Discussion

The presented metamodel above can serve as a framework for generating security requirements in the development process of CPS for industry 4.0. To validate this approach, a case study is introduced, and subsequently, an example will be applied to each meta- model. Ultimately, the security requirements generated will be summarized.

4.1. Smart Home

Smart homes play a significant role in future house planning approaches since the requirements and possibilities have evolved beyond basic convenience functionality. Modern smart homes consist out of many devices which are connected to the local network [40]. A few of them are presented in Figure 7. Fingerprint sensors for keyless entry, smart sprinklers watering the garden automatically or smart refrigerators keeping track of the current food items expiry dates are just a few of basic characteristics of a smart homes. However, besides the positive features of a smart home, it should be considered that they offer several security issues. Since they are connected to the Internet, smart homes are no more attackable simply through- out physical intruders, but also throughout cyber criminals. Lacks in security of the software or hardware used can cause direct damage to the human beings living in that house.

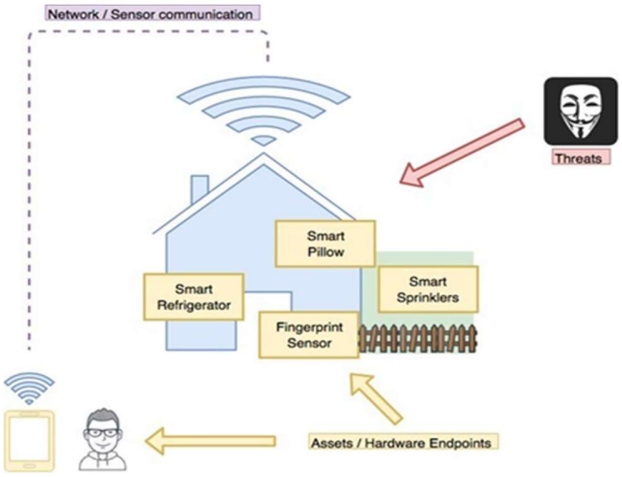

Fig. 7 Smart Home

4.2. Appliance

To validate the CPS Metamodel and demonstrate its correct application, the case study is systematically applied to each aspect of the CPS Metamodel. Each element of the metamodel is exemplified using corresponding details from the case study.

4.2.1. Asset Metamodel for smart home

Every CPS, smart homes offer several assets (Figure 7). The first possible attack point of a smart home system can be the software used, in this example Samsung's SmartThings which is a mobile application to control PLCs in the belonging smart home (Figure 8). As every software program, SmartThings offer some vulnerabilities. For instance, it requests more privileges than used and makes itself attackable against different threats which can exploit these unnecessary privileges.

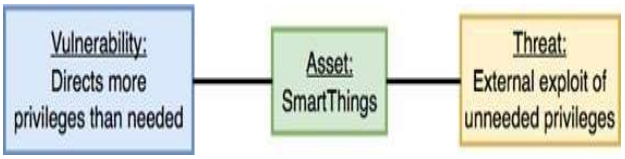

Fig. 8. Asset Metamodel applied to case study

In the context of this case study, stakeholders, who essentially represent the users of the system, may have conflicting requirements. For instance, two residents have distinct requirements. Resident 1 prioritizes maximum security for the house, while Resident 2 desires windows to automatically open during rain- free summer days. Recognizing that both requirements cannot be fully met simultaneously, a compromise be- comes necessary. A potential security requirement to address this issue could involve the implementation of motion sensors in each window, capable of detecting any attempt to enter the house. This compromise aims to balance the security concerns of Resident 1 with the comfort preferences of Resident 2.

4.2.2. Security Goal Metamodel for smart home

The requirement of resident 1 leads among others to the security goal, that only authorized persons can access the house. Consequently, a task dealing with entering the fingerprint at the fingerprint sensor can be deducted. In this context, two personas have been created. Resident 1, who uses the sensor correctly and resident 2, who has never used one be- fore and inserts his finger upside down. Both personas are authorized and must be granted access to the house. Thus, the fingerprint sensor must be able to detect resident 2's fingerprint as valid, without raising the possibility for a third, malicious persona trying to enter the house unauthorized. A security goal can have numerous obstacles. If the database where the authorized fingerprints are stored is not secure and a malicious at- tacker could gain access to this information, he could easily insert the house unauthorized.

4.2.3. Threat Metamodel for smart home

Threats against Cyber Physical Systems are basically the intention for eliciting security requirements. Several threats can be deduced, even knowing that there always exist more than the developers will be aware of.

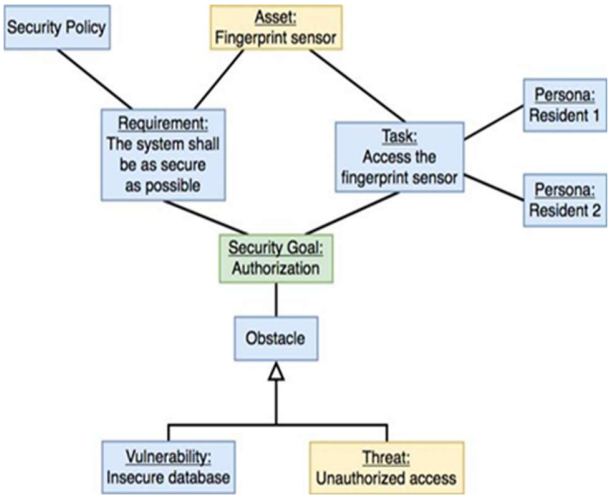

Fig. 9. Security Goal Metamodel applied to case study

The following example should clarify, how this metamodel can be applied to create security requirements. The smart home concerning to this case study offers a fingerprint sensor to grant access to the house. A malicious attacker with the intention of financial gain may want to rob the house and could now think of several threat possibilities. One of them is fake biometric data. Threat Model using this case study is shown in the Figure 10. Imagine the system is vulnerable in that kind of way, that it cannot separate a real finger from a fingerprint printed on a paper sheet. The burglar could copy the fingerprint of an authorized per- son and gain himself access to the house easily.

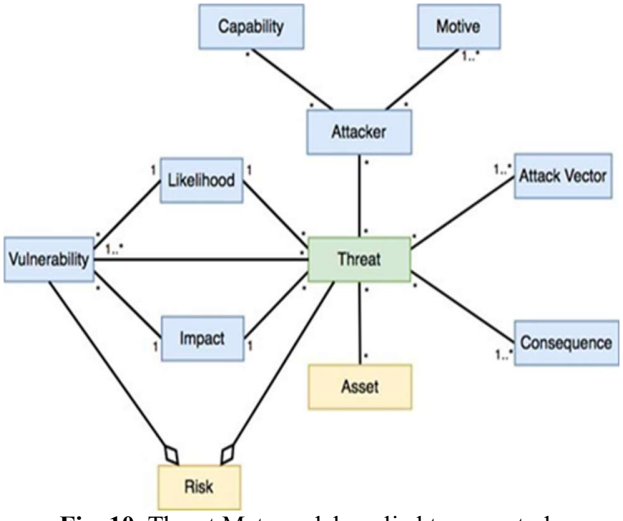

Fig. 10. Threat Metamodel applied to case study

On a scale from one to ten, where one is the lowest possible and ten the highest possible value, the likelihood of this scenario to happen is considered as a two, the impact is considered as a ten. Even though the likelihood is rather low, the impact has the highest possible value and the consequences can be very expensive for the users of this system.

4.2.4. Secure Network Communication Metamodel for smart home

A secure network communication is one of the most important requirements when speaking of security in a Cyber-Physical Systems (Figure 11). Several threats like eavesdropping, man in the middle or denial of ser- vice attacks can attack unsecure communication protocols. The smart home in this case study uses, among others, the Hypertext Transfer Protocol. This protocol is rather outdated and does not provide much security itself. Concluding, several security measures have been applied manually. A network intrusion detection system and a network intrusion prevention system have been installed to detect and directly prevent unwanted actions in the network.

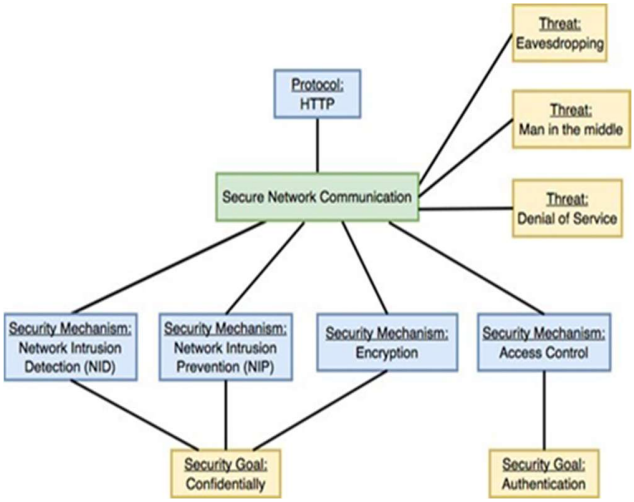

Fig. 11. Secure Network Communication Metamodel applied to case study

Additionally, access control is ensured through authentication and authorization mechanisms. Given that the Hypertext Transfer Protocol lacks encryption, posing a risk of plain- text interception by malicious intruders upon network intrusion, an encryption-decryption scheme has been implemented. It is crucial to note that the installed security mechanisms contribute to achieving various security goals such as confidentiality and authentication. The overall security of network communication is enhanced with the increased implementation of security solutions.

4.2.5. Hardware Endpoint Metamodel for smart home

In CPS, the most important hardware endpoints are Programmable Logic Controllers (sensors and actuators). The current smart home is located in California, where the temperature is very hot. Consequently, it directs some sprinklers watering the plants outside automatically (Figure 12). Next to the garden, which is the most obvious environment for that particular hard- ware endpoint, plants on a walk-on-able roof need to get watered, too. These two different environments of- fer different attack possibilities and must be protected throughout individual security mechanisms.

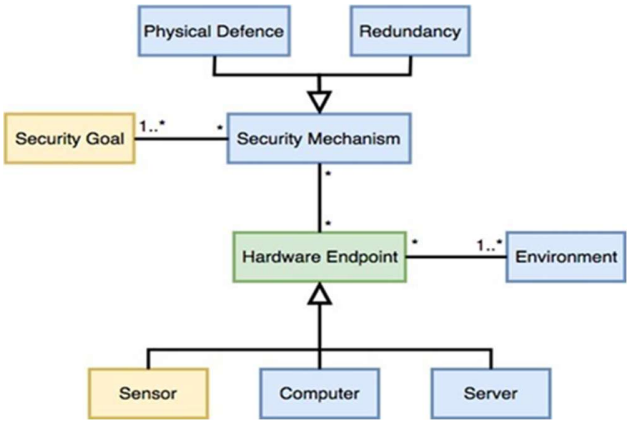

Fig. 12. Hardware Endpoint Metamodel applied to case study

Since the roof is only reachable through the in-side of the house, physical defense like fences must not be applied here. The garden, on the other hand, is reachable easily through any attacker and should be protected through fences. “The sprinklers cannot be stolen” and “The sprinklers cannot be damaged throughout malicious attackers” are two security goals realized throughout this security mechanism. It should be mentioned here, that security mechanisms for sensors and actuators are usually not worth it to be in-stalled in such small Cyber Physical Systems. The fingerprint sensor, for example, does not need a redundant backup since the likelihood that it gets damaged is rather low.

4.2.6. Sensor Communication Medium Metamodel for Smart Home

The choice of sensor communication mediums is an important step in Cyber-Physical Systems communication. This case study uses a famous one called Zig- Bee. The advantage of using ZigBee is that this protocol provides encryption schemes and authentication possibilities. Consequently, there is no need to implement these security mechanisms manually and only a Network Intrusion Detection System and a Network Intrusion Prevention System are installed as shown in Figure 13.

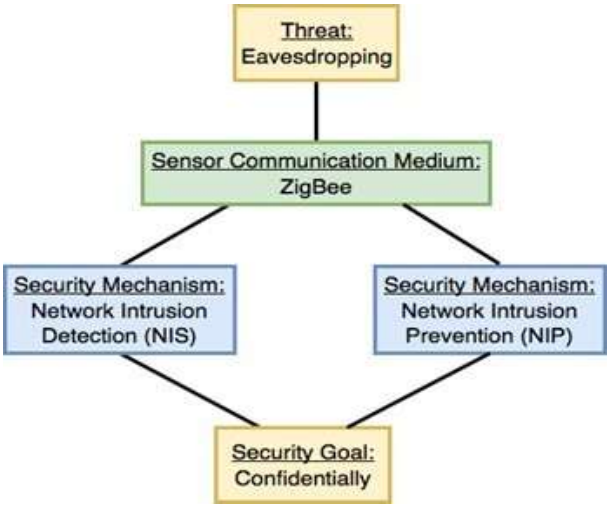

Fig. 13. Sensor Communication Medium Metamodel applied to casestudy

If the Hypertext Transfer Protocol Secure (HTTPS), which offers encryption itself, would have been used instead of the Hypertext Transfer Protocol in the Secure Network Communication Metamodel, the custom implemented cryptography schemes from above could have been dropped.

4.2.7. Risk Metamodel for Smart Home

In the initial phase of the risk assessment, the prioritization of each risk is essential. Each risk is associated with a specific threat and vulnerability, and the threat in this example aligns with the threat outlined in the Threat Metamodel above, specifically, the use of fake biometric data against a fingerprint sensor (Figure 14).

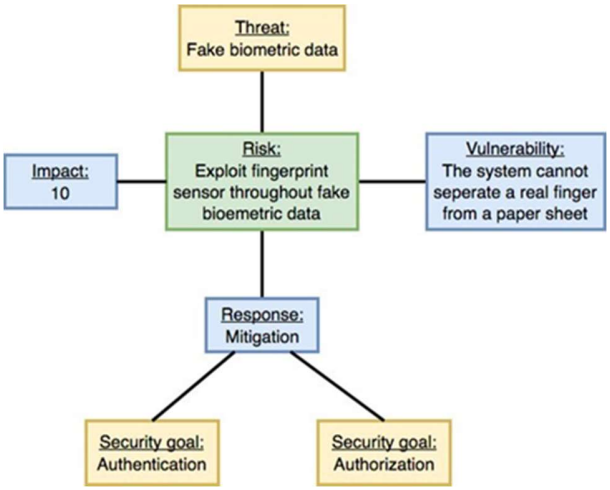

Fig. 14. Risk Metamodel applied to case study

On a scale from one to ten, where one is the lowest and ten the highest possible value, the likelihood of that threat is determined to two. The impact, on the other side, is established as ten. Concerning to the formula R = L x I, the concluding risk impact can be deduced as 20 out of 100 possible points, which is rather low but cannot be neglected. Once the total impact of the risk has been identified and compared to the others, responses can be deduced. In this case, a risk acceptance is not an opportunity since the impact of the threat is too high. The risk will be mitigated. A possible approach to prevent fake biometric data on paper- sheets is heat recognizable fingerprint sensors, which can separate between a real finger and a paper-sheet. Even though the resulting costs may be higher than expected, the security goal access control throughout authorization and authentication has become a step closer to realize.

4.2.8. Elicited Security Requirements

The examples from the case study above demonstrate how this metamodel can be applied. With the help of the proposed metamodel, we elicited several security requirements and here we show the following few security requirements:

- The system shall provide motion sensors in each window.
- The system shall provide authentication.
- The system shall provide authorization.
- The system shall provide a packet-filtering firewall
- The system shall provide a Network Intrusion Detection System.
- The system shall provide a Network Intrusion Prevention System.

- The system shall provide physical protection throughout fences
- The system shall provide heat recognizable fingerprint sensors.
- The system shall detect the impact of DoS attacks on the server from outside the system.
- The system shall prevent sniffing and monitoring traffic on the communication links of sensors.

It's important to note that the case study presented only applied one example per metamodel for demonstration purposes. However, in a rigorous security requirements engineering process, it is crucial to apply every conceivable scenario to the model to generate a comprehensive list of security requirements. The provided example has yielded ten security requirements, highlighting the effectiveness of this metamodel when applied diligently.

5. Conclusion and Discussion

The persistent challenge of security threats and vulnerabilities in cyber-physical systems integrated with industry 4.0 stems from their inherent characteristics. The heterogeneity of CPS, coupled with the prevalent use of legacy software and the introduction of a new physical dimension, creates an expansive land- scape where potential flaws can be exploited by various threats. The neglect of eliciting comprehensive security requirements in the past can be attributed to two main reasons. Firstly, there has been a prevailing assumption that CPS are inherently secure. Secondly, when security requirements have been identified, they often fell short of addressing every aspect of these complex systems. This research has outlined significant challenges related to security in cyber-physical systems within the context of Industry 4.0. Additionally, the fundamental concept of the security requirements engineering process has been explained. To help developers dealing with that process and to support organizations publishing secure systems, this paper has presented a metamodel for creating security requirements of CPS. Assets, security goals, threats, secure network communications, hardware endpoints, sensor communication mediums and risks are seven concepts which get introduced and need to be considered for a complete security requirements engineering process. For better understanding of the presented metamodel, a case study has been developed and applied to each of the seven concepts. The positive outcome of nine different security requirements validated the metamodel. This work, and especially the presented metamodel, hopefully help others to apply a serious requirements engineering process and consequently to generate a detailed list of security requirements. This endeavor, particularly the introduced metamodel, aims to assist readers in implementing a rigorous requirements engineering process, facilitating the creation of a com- prehensive list of security requirements. It is crucial to note, however, that the presented metamodel constitutes only a component within the broader requirements engineering framework. Future efforts in enhancing the security of demand the creation of additional metamodels and the incorporation of diverse perspectives into the overall process. Achieving an al- most 100% level of security necessitates continuous development, with ongoing contributions to the meta- models and an expanded scope in addressing the evolving challenges within the realm of cyber-physical systems security.

References

[1] Rehman, S.U. and Gruhn, V., 2018. An effective security requirements engineering framework for cyber-physical systems. Technologies, 6(3), p.65.

[2] A. Humayed, J. Lin, F. Li, and B. Luo, "Cyber-physical systems security—a survey," IEEE Internet of Things Journal, vol. 4, no. 6, pp. 1802–1831, 2017.

[3] M. Juma and K. Shaalan, "Cyberphysical systems in the smart city: Challenges and future trends for strategic research," in Swarm Intelligence for Resource Management in Internet of Things. Elsevier, 2020, pp. 65–85.

[4] ur Rehman, S., 2024. Enhancing Cyber-Physical Systems Security: A Comprehensive SRE Approach for Robust CPS Methodology. IJCSNS, 24(5), p.40.

[5] N. Peladarinos, D. Piromalis, V. Cheimaras, E. Tserepas, R. A. Munteanu, and P. Papageorgas, "Enhancing smart agriculture by implementing digital twins: A comprehensive review," Sen- sors, vol. 23, no. 16, p. 7128, 2023.

[6] G. Bakirtzis, B. T. Carter, C. R. Elks, and C. H. Fleming, "A model-based approach to security analysis for cyber-physical systems," in 2018 Annual IEEE International Systems Confer- ence (SysCon). IEEE, 2018, pp. 1–8.

[7] G. Bakirtzis, T. Sherburne, S. Adams, B. M. Horowitz, P. A. Beling, and C. H. Fleming, "An ontological metamodel for cyber-physical system safety, security, and resilience coengi- neering," Software and Systems Modeling, vol. 21, no. 1, pp. 113–137, 2022.

[8] M. A. U. Haq, S. U. Rehman, H. A. Alhulayyil, T. A. Alzahrani, H. S. Alsagri, and M. Faheem, "Wireless antenna sensors for biosimilar monitoring toward cyber-physical systems: A review of current trends and future prospects," IEEE Access, vol. 11, pp. 132 037–132 054, 2023.

[9] M. M. Alani and M. Alloghani, "Security challenges in the industry 4.0 era," Industry 4.0 and engineering for a sustainable future, pp. 117–136, 2019.

[10] B. Dafflon, N. Moalla, and Y. Ouzrout, "The challenges, approaches, and used techniques of cps for manufacturing in industry 4.0: A literature review," The International Journal of Advanced Manufacturing Technology, vol. 113, pp. 2395–2412, 2021.

[11] B. A. Yilma, H. Panetto, and Y. Naudet, "A meta-model of cyber-physical-social system: The cpss paradigm to sup- port human-machine collaboration in industry 4.0," in Collaborative Networks and Digital Transformation: 20th IFIP WG 5.5 Working Conference on Virtual Enterprises, PRO-VE 2019, Turin, Italy, September 23–25, 2019, Proceedings 20. Springer, 2019, pp. 11–20.

[12] T. Fitz, M. Theiler, and K. Smarsly, "A metamodel for cyber-physical systems," Advanced engineering informatics, vol. 41, p. 100930, 2019.

[13] A. Naseer, M. Tamoor, A. Khan, D. Akram, and Z. Javaid, "Occupancy detection via thermal sensors for energy consump- tion reduction," Multimedia Tools and Applications, pp. 1–14, 2023.

[14] R. Anderson and S. Fuloria, "Security economics and critical national infrastructure," in Economics of information security and privacy. Springer, 2010, pp. 55–66.

[15] M. Maidl, R. Wirtz, T. Zhao, M. Heisel, and M. Wagner, "Pattern-based modeling of cyber-physical systems for analyzing security," in Proceedings of the 24th European Conf. on Pattern Languages of Programs 2019, pp.1-10.

[16] S. Ouchani and A. Khaled, "A meta language for cyber-physical systems and threats: Application on autonomous vehicle," in 2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA). IEEE, 2019, pp. 1–8.

[17] Y. Eslami, C. Franciosi, S. Ashouri, and M. Lezoche, "A review and analysis of the characteristics of cyber-physical systems in industry 4.0," SN Computer Science, vol. 4, no. 6, p. 825, 2023.

[18] P. L. Bannerman, "Risk and risk management in software projects: A reassessment," Journal of systems and software, vol. 81, no. 12, pp. 2118–2133, 2008.

[19] M. Javaid, A. Haleem, R. P. Singh, and R. Suman, "An integrated outlook of cyber–physical systems for industry 4.0: Topical practices, architecture, and applications," Green Technologies and Sustainability, vol. 1, no. 1, p. 100001, 2023.

[20] R. W. McGrew and R. B. Vaughn, "Discovering vulnerabilities in control system human–machine interface software," Journal of Systems and Software, vol. 82, no. 4, pp. 583–589, 2009.

[21] G. McGraw, "Software security," IEEE Security & Privacy, vol. 2, no. 2, pp. 80–83, 2004.

[22] J. Greensmith and U. Aickelin, "Firewalls, intrusion detection and anti-virus scanners," Computer Science Technical Report No. [NOTTCS-TR-2005-1]. Retrieved from http://citeseerx. ist. psu. edu/viewdoc/download, 2005.

[23] C. Roberts, "Biometric attack vectors and defences," computers & security, vol. 26, no. 1, pp. 14–25, 2007.

[24] A.-S. K. Pathan, H.-W. Lee, and C. S. Hong, "Security in wire- less sensor networks: issues and challenges," in 2006 8th International Conference Advanced Communication Technology, vol. 2. IEEE, 2006, pp. 6–pp.

[25] S. Faily and I. Fléchais, "A meta-model for usable secure requirements engineering," in Proceedings of the 2010 ICSE Workshop on Software Engineering for Secure Systems, 2010, pp. 29–35.

[26] K. T. Chui, B. B. Gupta, J. Liu, V. Arya, N. Nedjah, A. Almomani, and P. Chaurasia, "A survey of internet of things and cyber-physical systems: standards, algorithms, applications, security, challenges, and future directions," Information, vol. 14, no. 7, p. 388, 2023.

[27] J. B. Awotunde, Y. J. Oguns, K. A. Amuda, N. Nigar, T. A. Adeleke, K. M. Olagunju, and S. A. Ajagbe, "Cyber- physical systems security: Analysis, opportunities, challenges, and future prospects," Blockchain for Cybersecurity in Cyber-Physical Systems, pp. 21–46, 2023.

[28] W. Stallings, Computer security principles and practice, 2015.

[29] H. Song, G. A. Fink, and S. Jeschke, Security and privacy in cyber-physical systems: foundations, principles, and applications. John Wiley & Sons, 2017.

[30] T. Miyachi, H. Narita, H. Yamada, and H. Furuta, "Myth and reality on control system security revealed by stuxnet," in SICE Annual Conference 2011. IEEE, 2011, pp. 1537–1540.

[31] J. Slay and M. Miller, "Lessons learned from the maroochy water breach," in international conference on critical infrastructure protection. Springer, 2007, pp. 73–82.

[32] M. Shahzad, M. Z. Shafiq, and A. X. Liu, "A large scale exploratory analysis of software vulnerability life cycles," in 2012 34th International Conference on Software Engineering (ICSE). IEEE, 2012, pp. 771–781.

[33] D. Pandey, U. Suman, and A. Ramani, "Security requirement engineering issues in risk management," International Journal of Computer Applications, vol. 17, no. 5, pp. 12–14, 2011.

[34] G. G. Roy, "A risk management framework for software engineering practice," in 2004 Australian Software Engineering Conference. Proceedings. IEEE, 2004, pp. 60–67.

[35] S.U. Rehman and V. Gruhn, "Security requirements engineering (sre) framework for cyber-physical systems (cps): SRE for CPS" in SoMeT, 2017, pp. 153–163.

[36] C. Gonzalez-Perez and B. Henderson-Sellers, Metamodelling for software engineering. Wiley Publishing, 2008.
[37] M. K. Jain, "Wireless sensor networks: Security issues and challenges," International Journal of Computer and Information Technology, vol. 2, no. 1, pp. 62–67, 2011.
[38] L. Sha, S. Gopalakrishnan, X. Liu, and Q. Wang, "Cyber-physical systems: A new frontier," in 2008 IEEE international conference on sensor networks, ubiquitous, and trustworthy computing (sutc 2008). IEEE, 2008, pp. 1–9.
[39] S. Myagmar, A. J. Lee, and W. Yurcik, "Threat modeling as a basis for security requirements," 2005.
[40] E. Fernandes, J. Jung, and A. Prakash, "Security analysis of emerging smart home applications," in 2016 IEEE symposium on security and privacy (SP). IEEE, 2016, pp. 636–654.

Dr. Shafiq ur Rehman received the BS/MS degree in Computer Science from Dresden University of Technology, Dresden, Germany and Ph.D. degree in Computer Science from the Department of Software Engineering, Duisburg-Essen University, Germany in 2020. He is an assistant professor at the College of Computer and Information Sciences, Imam Mohammad Ibn Saud Islamic University (IMSIU), Riyadh KSA. He also worked as a consultant (Requirements Engineer) in a well renowned international organizations in Germany. He has published several research papers in high-ranked international conferences and ISI indexed journals. He is involved in different international funded projects in the field of cyber-physical systems and cybersecurity. His research interests include AI, cyber-physical systems, cybersecurity and requirements engineering.