Internet of Things 22 (2023) 100766

Contents lists available at ScienceDirect

Internet of Things

journal homepage: www.elsevier.com/locate/iot

Research article

Threat modeling in smart firefighting systems: Aligning MITRE ATT&CK matrix and NIST security controls

Shahzaib Zahid [a], Muhammad Shoaib Mazhar [a], Syed Ghazanfar Abbas [a], Zahid Hanif [a], Sadaf Hina [b,*], Ghalib A. Shah [a,1]

[a] Al-Khwarizmi Institute of Computer Science (KICS), University of Engineering and Technology (UET) Lahore, Lahore 54000, Pakistan
[b] University of Salford, Prestwood Rd Salford Manchester M5 4WT, United Kingdom

ARTICLE INFO

Keywords:
Threat modeling
Smart industrial system
Cyber–Physical System (CPS)
Smart firefighting system
NIST controls
IoT
IIoT

ABSTRACT

Industrial automation technologies are envisioned as multi-device systems that are constantly interacting with one another and with enterprise systems. In these industrial systems, the industrial internet of things (IIoT) significantly improves system efficiency, scalability, ease of control, and monitoring. These benefits have been achieved at the cost of greater security risks, thus making the system vulnerable to cyberattacks. Historically, industrial networks and systems lacked security features like authentication and encryption due to intended isolation over the Internet. Lately, remote access to these IIoT systems has made an attempt of holistic security alarmingly critical. In this research paper, a threat modeling framework for smart cyber–physical system (CPS) is proposed to get insight of the potential security risks. To carry out this research, the smart firefighting use case based on the MITRE ATT&CK matrix was investigated. The matrix analysis provided structure for attacks detection and mitigation, while system requirement collection (SRC) was applied to gather generic assets' information related to hardware, software and network. With the help of SRC and MITRE ATT&CK, a threat list for the smart firefighting system was generated. Conclusively, the generated threat list was mapped on the national institute of standards and technology (NIST) security and privacy controls. The results show that these mapped controls can be well-utilized for protection and mitigation of threats in smart firefighting system. In future, critical cyber–physical systems can be modeled upon use case specific threats and can be secured by utilizing the presented framework.

1. Introduction

Cyber–Physical System (CPS) is an integral part of smart industrial systems like smart grids [1], smart homes [2], smart factories [3], smart cities [4] and many more. CPS is a group of networked systems that can monitor and manage IoT operations and real-world devices [5]. CPS can assess their cyber–physical adapt by using basic components such as sensors, aggregators, and actuators, as they enable them to control and affect the physical world. CPS is capable of utilizing real-time computing to adjust the run-time of systems' processes, as well as their flexibility. Indeed, CPS is found in a wide range of systems as shown in Fig. 1, including power transmission, communication, agricultural, environmental, and military systems. CPS combines computation with physical components to produce behaviors that are represented in the system's cyber and physical components. Sensors play a critical

* Corresponding author.
E-mail addresses: shahzaibzahid82@gmail.com, shah.zaib@technogenics.io (S. Zahid), shoaib.mazhar@kics.edu.pk (M.S. Mazhar), ghazanfar.abbas@kics.edu.pk (S.G. Abbas), zahid.hanif@kics.edu.pk (Z. Hanif), s.hina@salford.ac.uk (S. Hina), ghalib@kics.edu.pk (G.A. Shah).
[1] Senior Member, IEEE.

https://doi.org/10.1016/j.iot.2023.100766
Received 1 December 2022; Received in revised form 20 March 2023; Accepted 21 March 2023
Available online 5 April 2023

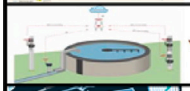
Naming	Classification	Description
 Smart House	Industrial-Consumer IoT	• Control Smart Devices • Homeowner Security & Comfort
 Oil Refinery	Industrial-Transportation IoT	• Naphta, Gasoline, Diesel • Asphalt, Petroleum, Fuel, Oil
 Smart Grid	Industrial IoT	• Smart Efficient Energy • Energy Control & Management
 Water Treatment	Industrial-Consumer IoT	• Improved Water Quality • Overcome Contamination & Undesirable Components
 Medical Devices	Medical-Wearable IoT	• Improved Patients Life • Enhanced Medical Treatment • Remote Patient Monitoring
 SCADA	Industrial IoT	• Control & Monitor Telecoms. • Control & Monitor Industries
 Smart Cars	Industrial-Transportation IoT	• Echo Friendly • Enhanced Driver Experience • Advanced Safety Features
 Supply Chains	Industrial-Transportation IoT	• Real-Time Delivery Source/Destination • Less Delays & Echo Friendly

Fig. 1. Contemporary CPS classification [9].

role in the efficiency of these systems [6] as they generate large amount of complex data. The sensor data is analyzed by CPS and utilized for remedial actions [7]. The Internet of things (IoT) exposes significant flaws in existing CPS, encountered due to lack of security-by-design notion in sensors and network devices. IoT depicts plenty of new issues and challenges that require an integrated approach to security and privacy than the conventional information systems [8].

Despite numerous advantages, CPS is vulnerable to a range of physical and cyber security threats, attacks, and constraints [10]. The sensitivity of the system is a result of its diverse structure, reliance on private and sensitive data, and extensive implementation. Consequently, even little system intrusions can have a significant impact on the functioning of security controls [9]. Notably, non-strategic actions could result in an excessively large network overhead, especially in terms of latency. In light of this, frequent upgrades for operating systems and software programs, vulnerability patching and custom configurations should be implemented to minimize/mitigate zero-day vulnerabilities [11].

The rapid adoption of IoT devices has resulted in a significant rise in security concerns [12]. Due to crucial security-by-design flaws in IoT devices, hackers can easily gain control and use them for malicious purposes, compromising their availability and data transmission [13]. According to a report, total active connections of IoT are expected to reach 30.9 billion worldwide from 2010 to 2025 [14]. According to the 2021 Unit 42 IoT threat report, a study conducted on 1.2 million IoT devices suggests that 57% of them are susceptible to assaults of medium or high intensity, and 41% of attacks make use of hardware flaws when these devices are connected to the internet [15]. Moreover, according to Kaspersky's research report, in the first half of 2021, 1.5 billion cyberattacks on IoT devices have been documented [16]. In order to effectively minimize the possible risks, threats, and assaults to IoT devices prior to deployment in a real-time environment, it is essential to identify these attacks throughout the design phase.

Due to their frequent reliance on IoT technologies and associated networks for operation, smart cyber–physical systems (CPS) are increasingly becoming the target of cyberattacks. Previously, upstream security predicted that there will be 6.3 million reported cyberattacks against autonomous cars in 2020, with a 99 percent increase from 2019 [17]. A report by ABI research claimed that the global smart cities market was expected to reach $158 billion by 2022, with security being a key concern for smart city stakeholders [18]. According to Irdeto, 82% of smart healthcare organizations have experienced a cyber attack on their IoT devices, and 30% of those attacks resulted in compromised end-user data [19]. Another report by the department of energy found that the potential cost of a successful cyber attack on the U.S. power grid could reach $1 trillion [20]. A survey by Accenture claimed that over the previous three years, the cost of global cybercrimes to enterprises had escalated by 50%, with the average cost of a cyberattack expected to be $13 million by 2020 [21]. Overall, the cyberattacks on smart CPS are a growing threat that organizations need to take seriously. It is essential to implement robust cybersecurity measures, including access controls, encryption, and intrusion detection systems, to mitigate the risk of cyberattacks on smart CPS.

The COVID-19 pandemic has enhanced remote access to industrial control systems, expanding the attack surface for cybercriminals. There was a 30% rise in remote access to industrial control systems during the COVID-19 pandemic, according to a report by the industrial control systems cyber emergency response team (ICS-CERT). According to a report by the FBI, the number of cyber attacks

on critical infrastructure increased by 50% during the COVID-19 pandemic [22]. The use case of this research is smart firefighting CPS [23] where most of the data is collected remotely. Smart firefighting CPS relies on a variety of interconnected components and systems, such as sensors, actuators, and control systems, which interact with one another and with central command centers across networks. Any cyberattack on these systems could jeopardize their functionality, posing a risk of fatalities, resources' loss, and interference with emergency response operations. Moreover, smart firefighting CPS frequently manage private and sensitive information, like building plans, occupancy information, and important infrastructure details. A successful cyber attack on these systems could lead to the theft or exposure of this data, which could be used for nefarious purposes such as planning terrorist attacks or other criminal activities. Furthermore, smart firefighting CPS often rely on other critical infrastructure systems, such as power grids and communication networks. A cyber attack on these systems would cause cascading failures that could further compromise the safety and effectiveness of smart firefighting CPS.

A threat model identifies possible system flaws that an attacker could exploit to gain access to the system. A technique for identifying threats during the early stages of the system design process is known as threat modeling, which can easily prevent the issues as discussed earlier [24]. It also assists in the implementation of effective security measures in response to detected threats, thereby assisting in threat mitigation. In this research work, a cyber security framework is proposed that maps threats of MITRE ATT&CK Matrix [25] related to smart firefighting CPS on NIST security and privacy controls [26]. Security requirement collection (SRC) is designed to gather detailed information of CPS under consideration. SRC provides information about the security goals, endpoint hardware identification, sensor data communication, asset identification, and network communication assets used in the CPS of smart firefighting. This study used MITRE ATT&CK Matrix and SRC to generate the possible threat list of smart firefighting systems. Next, it utilized the project of the center of threat-informed defense (CTID) [27] to map the threats list on NIST security and privacy control requirements.

The allocation of functions between cyber and physical components can vary in different firefighting CPS. In some systems, the emphasis may be on the physical components, with the cyber components playing a supporting role, while in others, the cyber components may be more central. For example, some firefighting CPS may use physical sensors and devices to detect and respond to fire, with the cyber components serving to monitor and control these devices remotely. In such systems, the emphasis is on the physical components, and the cyber components serve to enhance the physical capabilities. In contrast, other firefighting CPS may lay a greater emphasis on cyber components, such as predictive modeling and artificial intelligence, to identify and predict fire spread before it happens. In these systems, the physical components may serve to confirm and respond to the predictions made by the cyber components. Overall, the allocation of functions between cyber and physical components in firefighting CPS depends on various factors, including the specific application, the available technology, and the desired level of automation and control. It is important for the designers and users of firefighting CPS to carefully consider these factors and balance the roles of the cyber and physical components to achieve the desired outcomes [28]. The proposed model threat list also vary according to the technology being used in smart firefighting system. In this research, generic smart firefighting CPS includes all technologies and applications as described in Section 3. Major contributions of this research are :

1. Addressing the mitigation tactics and techniques of MITRE ATT&CK.
2. Providing a system requirement collection (SRC) mechanism to gather detailed asset information of any CPS.
3. Generating threat list for CPS under observation, with the help of MITRE ATT&CK and SRC.
4. Mapping threats related to smart firefighting system on NIST security and privacy controls.
5. Providing threat mitigation using NIST security and privacy controls.

The rest of the sections of this research paper are arranged as follows. Section 2 describes the literature survey of various existing threat modeling frameworks. Section 3 represents the system model of smart firefighting CPS. Section 4 discusses the proposed methodology for threat modeling based on the MITRE ATT&CK matrix and NIST security and privacy controls. Section 5 elaborates on the results of the proposed methodology and compares them to previous results. Finally, in Section 6, the paper concludes the research work and provides future directions for further research in this area. Overall, the paper presents a comprehensive approach to threat modeling in smart firefighting CPS, which can be useful for designers and developers of such systems to improve their security and resilience.

2. Literature survey

The CIA triad, or confidentiality, integrity, and availability, is a model to impose information security policies within an organization [29]. Threat modeling is a methodology that identifies possible threats during the early phases of system design process, CIA and operations, executed by the organization [30]. Many threat modeling existing techniques like STRIDE, PASTA, etc. are summarized in [31], that experts, researchers, and professionals utilize to assess threats to systems, processes, and even human resources. The possible ways that an attacker may breach a system are determined using a threat modeling technique. Various mitigation solutions are put out to protect underlying systems from the detected vulnerabilities and related identified threats.

Smart cyber–physical systems (CPS) face a range of threats and exploits that can compromise their security and functionality. The Stuxnet worm is among the most well-known instances of a cyberattack on a CPS. The worm was specially developed to attack the programmable logic controllers (PLCs) used in an Iranian nuclear plant and caused physical damage to the centrifuges employed in the facility. Stuxnet took advantage of a number of flaws in the facility's Windows operating system and Siemens control software [32]. Another illustration of a cyberattack on CPS is the Mirai botnet. In 2016, Mirai launched a distributed denial-of-service (DDoS) attack against the DNS provider Dyn using compromised Internet of things (IoT) gadgets like home routers and

surveillance cameras. Several websites' activities were interfered with and there were widespread internet outages as a result of the attack [33]. Triton is a form of virus that attacks the safety systems used in industrial control systems (ICS). The malware, found in 2017, was used to assault a Saudi Arabian petrochemical company. Triton was built to interfere with the facility's safety systems, which resulted in a disastrous failure [34].

The BlueKeep vulnerability is a critical vulnerability in the remote desktop protocol (RDP), used in Windows operating systems. A remote code execution vulnerability, found in 2019, can let an attacker take control of a vulnerable system without human intervention. This flaw provides an access to a CPS, where an attacker could use it to take over control and harm the resources [35]. The SolarWinds supply chain attack is another recent example of a sophisticated cyber-attack that affected several organizations worldwide. The SolarWinds orion programme, used to manage IT infrastructure, was the focus of the attack. Injecting malware into the program allowed the attackers to access systems and sensitive data. Despite the fact that this attack did not particularly target a CPS, it shows how crucial it is to secure the supply chain for the hardware and software parts of CPS [36]. In 2017, the NotPetya ransomware attack, having its origins in Ukraine, spread globally and impacted numerous companies. The attack took use of loopholes in the Windows operating system and deployed a Petya ransomware version. For a number of businesses and organizations, including those in the shipping, pharmaceutical, and logistics sectors, NotPetya resulted in major disruptions and monetary losses [37].

Dragonfly 2.0 was a cyber-espionage campaign that targeted several energy companies worldwide between 2015 and 2018. The attackers gained access to the ICS utilized by these businesses using spear-phishing and other methods, gathering private data about infrastructure and operations [38]. Malware known as Trisis especially targeted the Triconex safety instrumented system (SIS) used in the oil and gas sector and other ICS safety systems. This malware was also used against a Saudi Arabian petrochemical facility with an intention to manipulate the facility's safety systems and had the potential to cause a catastrophic disaster [39]. The Wi-Fi protected access II (WPA2) protocol, which is used to secure Wi-Fi networks, has a significant vulnerability, found in 2017, called KRACK. An attacker might be able to intercept and decrypt Wi-Fi traffic using this vulnerability. This could enable an attacker to intercept and alter data sent between the various parts of the system in a CPS that uses Wi-Fi for communication [40].

These examples demonstrate the wide variety of dangers and weaknesses that smart CPS must constantly monitor and mitigate. To secure the CPS from cyberattacks, enterprises must put strong security measures in place, including network segmentation, access control, and routine patching.

Wang et al. [41] investigated dangers and enhanced data security of smart city systems, and presented a strategy of threat modeling. This method takes both technical and commercial activities into account. This method first identified hundreds of elements from system design, networks, operating systems, database schemas, encryption methods, security policies, business processes, and corporate data to assess vulnerabilities to smart city systems. Later, the suggested technique was applied by the Hardware, Intelligence, Software, Policies, and Operation (HiSPO) approach to determine threat factors based on the chosen attributes. The calculated threat factors were thoroughly assessed and mitigation strategies were provided to boost the system's overall security.

Khan et al. [42] provided thorough threat modeling structure for cyber–physical systems based on STRIDE (CPS). This CPS utilized technology that could react in real-time environment, by integrating the physical and digital worlds. The study's main contribution was defining a systematic technique that could be used to the STRIDE approach's successful characteristic modeling-specific threats. Threat modeling against an actual lab-based synchronous islanding testbed, such as a smart grid CPS system, was used for analysis. In this research, STRIDE risks to system components were mapped using data flow diagrams (DFD) (comprised of entity, data flow, data store, and process). The STRIDE technique, at the component level, was utilized to increase the system's effectiveness. The output of STRIDE was fed to risk analysis processes to establish the most critical threats and mitigation measures.

Marksteiner et al. [43] developed an approach tailored for smart grids that integrated risk assessment and threat modeling to produce a comprehensive list of security criteria. A smart grid massively interconnects ICT-enhanced sensors and actuators for the distribution of electricity from producers to consumers. This inter-connectivity exposes the grid to several threats. A threat modeling method was utilized in this study to protect the low-voltage smart grid architecture by taking into account vulnerabilities at the architectural, protocol, and device levels. Following a risk assessment, mitigating strategies were put up to boost the low-voltage smart grid system's security. Various threat modeling techniques such as DFD based STRIDE and cyber-attack scenarios were incorporated to achieve the desired goal.

Kavallieratos et al. [44] undertook an investigation of the threats to the smart home ecosystem, where the distribution of IoT devices expanded the attack surface. Potential threats that target both the physical elements of a smart home environment and the data flows between them were found and examined using the STRIDE threat analysis approach. In order to effectively assess risks, the STRIDE-identified features were employed in the topology generator for smart home networks, and the malware propagation graph-based model. The findings were useful in studying the connections between states that are changing dynamically as well as the spread of malware infections in the ecosystem of smart homes.

In 2020, Abbas et al. [45] proposed a threat modeling strategy to evaluate and counteract botnet assaults on a smart home system. IoT devices were used in smart home systems, which broadens the attack surface for criminals. Attackers seized control of IoT devices and employed them in hostile operations like assaults using botnets. By creating data flow diagrams (DFD) and process flow diagrams (PFD), the suggested method was able to identify the development-level and application-level dangers in the smart home system (SHS). After botnet attack risks were discovered, mitigation strategies were incorporated to reduce the usage of unnecessary services, implementing implicit jailbreak, embedding firewall rules for auditing, encryption of traffic along with other relevant countermeasures.

Cho et al. [46] proposed a threat modeling technique for smart greenhouse to identify attacks and mitigation strategies for increasing threats to smart farming. The malign threats can directly and adversely damage crops and harm human safety. By creating

an attack tree, all possible threats in the smart farm were analyzed. To find cyber threats and strengthen system design, STRIDE threat modeling approach was applied to the smart greenhouse. As a result, 126 threats were derived and 4 types of attack trees were created, which generated more clear and systematic threat classification of smart greenhouse.

Later in 2021, Vaccari et al. [47] proposed a threat modeling approach for identification and mitigation of cyber-threats that cause phishing attacks on IoT-based smart systems. The increase in vulnerable IoT devices has lured attackers for targeting these devices through phishing attacks to take full control for post-exploitation. In this research, IoT-based use cases included smart autonomous vehicles and smart home systems. In order to reveal all potential dangers that might result in a phishing attack, the planned work was completed by applying STRIDE threat modeling technique to both situations. After risks were identified, mitigation strategies for both the smart autonomous vehicle system and the smart home system were suggested including implementation of data validation using message authentication codes, firmware updates etc.

Vakhter at el.[48] investigated the security of miniature wireless biomedical devices (MWBDs). The threat modeling procedure for MWBDs was thoroughly defined by the researchers. The use of STRIDE and DREAD threat modeling approaches was suggested for a domain-specific qualitative/quantitative threat model. To determine an assault's likelihood and effect, the model included pertinent attack attributes. A risk matrix technique was utilized to evaluate the risk for each attack attribute. Users and a wide variety of MWBDs were the main focus of the study activity. So, several kinds of MWBDs were subjected to the threat model.

Jeong et al. [49] proposed a design and communication algorithm of smart firefighting helmet used for transmission of voice and video between the firefighters. In this work, no separate radio operations were required for communication. These proposed devices enhanced the response time of communication at the disaster site.

Above research studies show that rapid growth of IoT not only brings the smartness into systems but also escalates vulnerabilities and attack vectors. The goal of this study is to identify hazards in a specific use case of a smart firefighting system and offer sensible CPS mitigation methods. The foundation of a smart firefighting system is the creation, storage, exchange, analysis, and integration of data from several databases and sensor networks. Due to the limited resources of sensors, the computing capacity of computers, and the combination of wireless communication technologies, smart firefighting systems have evolved from traditional systems to intelligent ones. The ultimate objective is to connect subsystems into an enterprise system of systems to provide complete access to the information that is accessible. However, the enterprise system should be secured against these threats. Different threat modeling mechanism have been described earlier for threat modeling, but this research focuses on threat modeling for a smart firefighting CPS using NIST security and privacy controls. The aim is to identify potential vulnerabilities, threats, and attack vectors including hostile threats, human error, structural failure, misconfigurations, privacy breaches and exploitation. Based on the threat model, this study intends to provides a mechanism for not only identifying potential attacks, but also proposes strategies for mitigation of these attacks.

3. System model

This research study analyzes the use case of smart firefighting system [50]. In smart firefighting, applications can be categorized and decomposed into services, networking, and sensor components. Section 3.1 provides the information about services required by different teams of firefighters and IoT technologies used by them. Smart firefighters interact with various applications while performing their assigned roles. Section 3.2 elaborates on the IoT sensors used by various firefighters. Section 3.3 describes the integration of sensors on firefighter suit and connection with various technologies. Similarly, Section 3.4 focuses on the software applications, databases, and different building systems. Section 3.5 describes various prediction and analytical models used by firefighters. While communication and networking technologies are discussed in this section. Although, focus of this research is on cyber world of firefighting but these IoT applications are connected with firefighters' physical equipment.

Utilizing the strength of new information, communication, sensor, and simulation technologies to significantly improve situational awareness, prediction models, and decision-making, smart firefighting has become significant use case of this study. There are a variety of commercial devices being utilized in several application areas of smart firefighting as a result of the miniature sensors, the power of computers, and the combination of wireless communication technologies. Smart firefighting provides a framework to

- integrates and aggregates a lot of data from several source databases and sensor networks.
- process, analyze, and predict using the collected information.
- disseminate the results and provide targeted decision-making to communities, fire departments, incident command systems (ICS), and firefighters.

In this system, a temporary wireless network is created by the high speed vehicle networking system, which connects different personnel and systems. This networking system is also used in other smart CPS, like autonomous cars and smart transportation systems [51]. Autonomous vehicles use high-speed vehicle networking systems to facilitate the communication between vehicle's various sensors, actuators, and control systems. This communication network enables the vehicle to sense their environment, make decisions based on the data it receives, and operate safely and efficiently. Various sensor technologies are deployed at the personal protective equipment (PPE) level, mobility level, and stationary level. With the help of these sensors, the situation on the fire ground is thoroughly and precisely assessed. Throughout the process, a wireless network connection is made to the sensor network.

Real-time information from the sensor network, video streaming cameras, and smart equipment is transmitted to the incident commander (IC), This is utilized to make operational plan decisions and give orders to firefighters on the fire scene. Text, audio, and video are the three available forms for sensor-related data. The IC uses special analysis tools like situational awareness for firefighters (SAFIRE) which has been used in a variety of CPS applications, including industrial control systems, smart grids, and

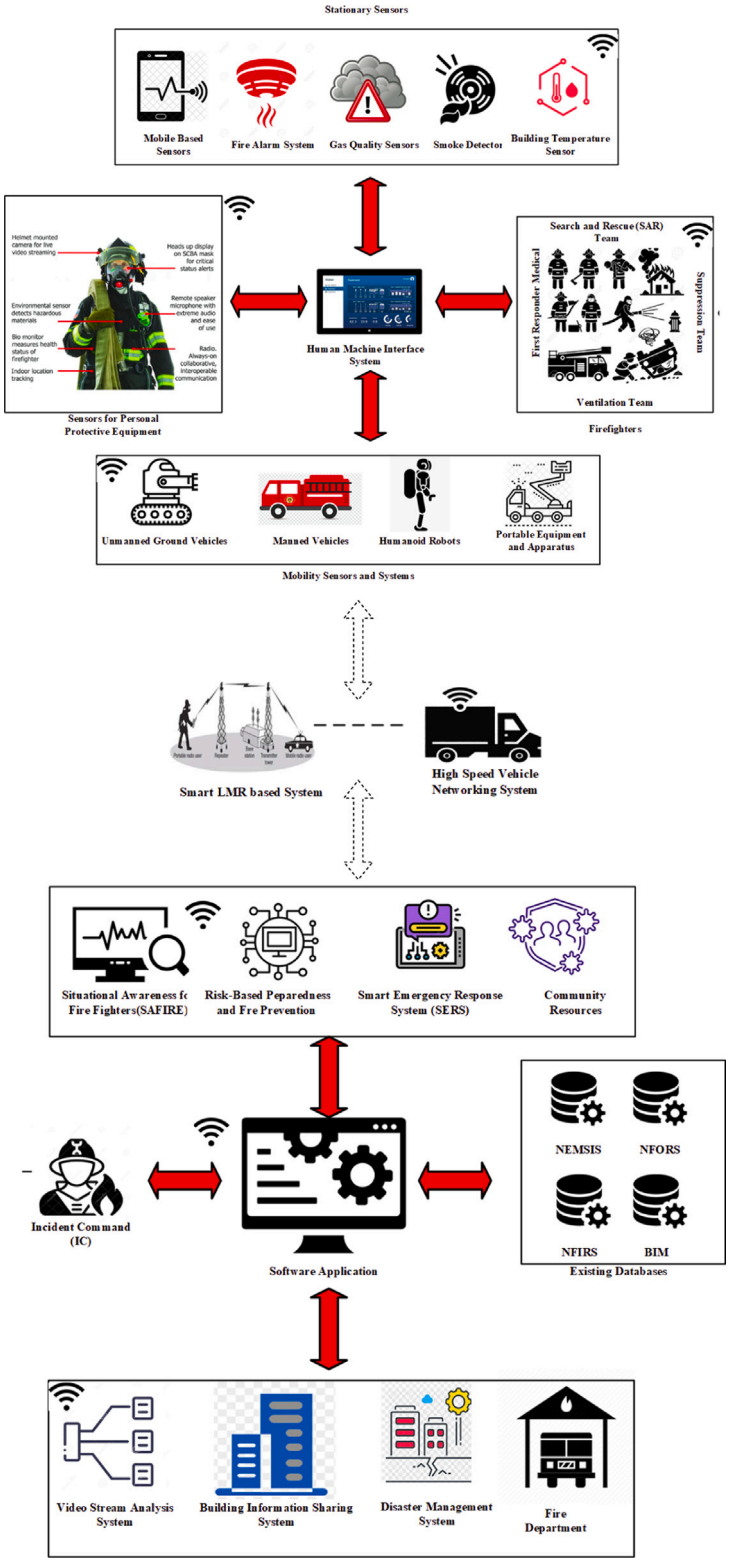


Fig. 2. System model.

autonomous vehicles [52]. The national renewable energy laboratory (NREL) in the United States, for instance, has developed a smart grid testbed using SAFIRE that enables researchers to assess the functionality and security of advanced grid technology in a practical setting, including risk-based preparedness for sensor-related fire prevention, smart emergency response systems (SERS), and analytic tools to convert the real-time data into useful information.

Smart emergency response systems (SERS) [53] are a crucial part of cyber–physical systems (CPS). SERS are intended to improve emergency responders' abilities by giving access to real-time situational awareness, communication, and decision-making support. Examples of emergency responders include firefighters, police officers, and paramedics. SERS usually combine communication networks, decision support systems, and a variety of sensors, including cameras, microphones, and environmental sensors. Information concerning the emergency situation, such as the location and size of a fire or the presence of hazardous materials, can be detected and transmitted by the sensors. Responders can share information and plan their actions in real-time, thanks to communication networks, and decision support systems can aid them in selecting the best course of action depending on the facts at hand. Based on this information, the operational plan is set, modified and communicated in real-time. These computational tools have access to various data repositories of current and previous fire incidents.

There are several uses for the model's outputs and predictions. When a fire is predicted to spread, for example, the outputs and projections are communicated immediately to the fire crew or to other local services like the closest hospitals. The model can be combined with a smoke-generation model and a weather model to estimate the potential impact on the neighborhood, if it indicates that the fire may progress into a section of a structure where dangerous substances are known to be kept. In order to facilitate planning for a potential evacuation and the care of patients, information can be gathered and delivered immediately to law enforcement organizations and neighborhood health and care facilities. Most of the time, real-time 3D visualization of the fire ground, equipment, and personnel is driven by model outputs and forecasts. Before giving any orders to employees, the IC utilizes the application software and visualization system to track the development of the fire event and to assess the probable effects of decisions and actions. Additionally, the visualization is recorded for upcoming analysis, learning opportunities, and training.

3.1. Firefighters

Firefighters operate in teams of 2,4,6 and 8. Firefighters are assigned different roles and duties in the operation. Depending upon the roles, firefighters are supplied with different equipment and operate different systems. The person designated as the incident commander (IC) is in charge of all parts of an emergency response, including the formulation of incident objectives, administration of all incident activities, application of resources, and oversight of all responders. Priorities are established, incident response teams are organized, and the overall incident action plan is defined by the incident commander.

The primary task of the search and rescue (SAR) unit is to locate victims and crew during the operation. SAR ensures the pursuit and provision of aid to people who are in distress or imminent danger. The fire suppression team is responsible for tactics used to suppress fire during any operation. Firefighting efforts require different techniques, equipment, and training from the more familiar firefighting structure for different areas. The process includes installing water hoses and supplies in interior parts of the building, monitoring the pressure, and providing all necessary equipment to the crew to suppress the fire. Different types of vehicles are involved if the place is out of reach of firefighters. All the information gathered from sources is sent to IC, and decision-making is performed for the operation. The ventilation team is a critical part of structural firefighting tactics. It diligently works to expel heat and smoke from a burning structure, enabling the firefighters to locate people who may be trapped, tackle the fire more safely and easily, and keep an eye on the fire transition system to identify those who have crossed flash-over criteria. By using the emergency medical services (EMS) system, emergency medical responders (EMRs) offer essential patients instant access to life-saving care. While waiting for further EMS services to arrive, EMRs can offer urgent life-saving actions with their knowledge and expertise gained through the training. In order to evaluate the physical state of the firefighters, they also keep an eye on the personal alert safety system (PASS), also known as the automated distress signal unit (ADSU).

3.2. Sensors

The idea of smart firefighting" is based on gathering crucial information and processing it for use in decision-making. Sensors are the major source of information generation. Fig. 2 shows various sensors involved in the smart firefighting system.

Sensors in the personal protective equipment (PPE) are the ones used on clothing and equipment carried by the firefighters. These were frequently used during COVID-19 pandemic activities [54]. PPE includes a self-contained breathing apparatus and a water hose system, increasing firefighters' mobility and allowing them to penetrate the fire's structure considerably deeper than was previously feasible. The firemen can identify hot spots through smoke, darkness, or heat-permeable barriers, with the use of thermal imaging cameras (TICs). The use of ventilation or handheld thermal imaging camera is the norm in firefighting systems. For firefighters, a gas dosimeter system (GDS) is used to track their total exposure to toxins inside the building. Firefighters' mobility and an auditory transmission are detected by the personal alert safety system (PASS) gadget. It acts as a sensor device to ascertain motionless state of a firefighter for an excessive amount of time. Fire transition sensor system is used for monitoring the flashover conditions, and physiological monitoring system is used to monitor the real-time conditions of the firefighters, like skin temperature.

Sensors built inside or carried by firefighting equipment and gear are the only mobility sensors and systems that are available. The use of mobile apparatus and equipment, such as land vehicles, watercraft, aircraft, satellites, and robotic systems, in firefighting and emergency response, is made possible by these sensors and the distributed networks they are connected to. These sensors' data, which is frequently time-sensitive, may be used to quantify exposure to risks, identify their presence, and keep track of the firefighters'

physiological conditions. Furthermore, before firemen even start their reaction, fixed sensors are placed on the dedicated spots. To repair and stabilize the building and the surrounding environment, these sensors work in tandem with firemen, firefighter-carried sensors, building systems, and building occupants. Smoke detectors, gas quality sensors, temperature sensors for buildings, fire alarm systems, heating, ventilation, and air conditioning (HVAC) systems, as well as portable sensors carried by the general public, are examples of stationary sensors used in smart firefighting.

Firefighters employ a lot of modern sensors, and as many of them are connected online, they are open to hacking attacks. In 2014, a cyberattack on a German steel plant disrupted control systems, as it prevented a blast furnace from properly shutting down, resulting in serious damage to the facility [34]. Similar to this, a cyberattack in 2017, directed against the Ukrainian power infrastructure resulted in extensive outages [55]. Attackers can utilize the sensors as a doorway to access other systems, including the national emergency response system or the communication systems used by the firefighters, if they manage to get access to the sensors. This might seriously affect national security as it could make it more difficult for the government to respond to crises.

3.3. Integration

Integrating sensor data with software analytic tools is necessary to process the information gathered from sensors within or across the architectural levels. Standardized grammar semantics and networking protocols are used to cover the conceptual material. Wireless communications are also included. For the purpose of modeling, programming, control, and communications, information models and database standards are used in different fields to represent concepts. In smart firefighting, sensors are integrated with analytical tools which consolidate the sensors' data from various databases and different building information systems. Building information sharing system is related to the department of buildings (DOB) [56]. This system keeps the record of building inspection reports, which provide necessary information that help in decision-making in case of an incident. Video stream analysis system, analyzes live videos captured by the TIC installed on the firefighters' PPE and cameras placed on the drones to make other required decisions and execute real-time face identification of the survivors in the field. High-quality information management systems for emergency preparedness, response, recovery, and resilience-building are made available to everyone via disaster management systems. This system offers the public a way to report emergencies through open short messaging service (SMS).

3.4. Software application

Incident commander needs a software application which collects information from various systems and models at one point. First responders make a lot of decisions in the moment when getting ready for, traveling to, and leaving fire events. This calls for comprehensive and current knowledge of the incident's location, risks to people and resources, accessible emergency resources, and local environmental conditions. Systems that offer this information aid emergency personnel in deciding the best course of action to safeguard human life while limiting hazard to and damage to resources. Information from fire related databases is also provided to incident command system as National Fire Incident Reporting System (NFIRS), National EMS Information System (NEMSIS) and National Fire Operations Reporting System (NFORS). These databases help the incident commander in decision-making if a similar incident occurs. Similar to this, detailed information regarding event features, resource capabilities, and site characteristics should be observed, recorded, and stored in order to provide an accurate assessment of the efficacy of equipment, tactics, and resources. Fig. 2 shows that the software application accessed by IC gathers the information from the various analytical tools, databases, sensor network and risk-based prediction models.

Many high-profile cyberattacks have recently occurred on government institutions, including the SolarWinds breach in 2020 that had an effect on a number of federal agencies [57] and the colonial pipeline ransomware assault in 2021 that resulted in fuel shortages in the southeast of the United States [58]. It is crucial that these systems are made secure against cyberattacks due to the sensitive nature of the data held in NFIRS, NEMSIS, and NFORS. The strong cybersecurity measures should be adopted by government organizations.

3.5. Model-based predictions and decision-making

The IC plans an initial strategy for suppression, rescue, and alerting the required local services, such as hospitals, as soon as there is a fire. It does this by using the information and technology that are already available. IC is also linked with fire department to demand more resources and firefighters. Before arriving at the fire ground, duties of all teams are predominantly assigned along the measures individuals should use when they get there. The incident commander will deploy various sensor technologies and put up a temporary wireless network after the equipment and staff have arrived in order to acquire a thorough and precise evaluation of the situation. Throughout the whole incident, the sensors and network continue to function as needed. The IC receives the streaming, real-time data and utilizes computational tools to create a new operating plan and give fresh orders to the firemen.

The IC develops and executes many computer simulations of fire propagation, smoke production, structure integrity, evacuation, suppression, ventilation, climatic conditions, air and water supply, tenability, and resource allocation in order to update the operational plan. Each of these models retrieves data from the repository and sensors, combines, processes, and analyzes that data, and then outputs predictions or conclusions for other models to utilize as input and for the IC to use for decision-making. Fig. 2 shows situational awareness for firefighters (SAFIRE) using the sensor network and multimedia data collection for creating the situational awareness of the incident.

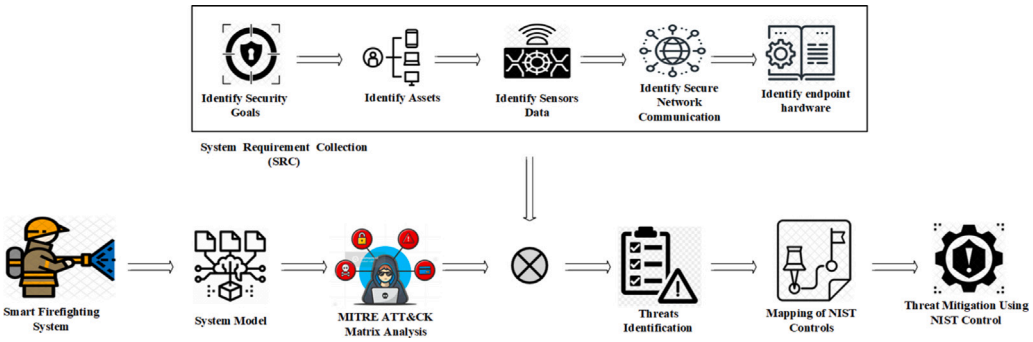


Fig. 3. Proposed methodology for threat modeling of smart firefighting CPS.

An incident storage database is created and Ebox installed outside the building is accessed to gather the building information. A frost & sullivan report projected that the worldwide smart building market will develop at an average rate of 17.6% from 2017 to 2022, demonstrating that the use of smart building technology is growing. The prevalence of smart buildings is expected to increase the number of cyberattacks directed at them. Also, according to a survey conducted by NTT Security, building automation systems (BAS) used in smart buildings were among the most hacked systems. According to a study, the average number of BAS attacks increased by 224% between 2017 and 2018.

Risk-based preparedness and fire prevention generates the firecast based decision-making according to the information gathered. Firecast is a machine learning algorithm which operates on the incident information to predict the best prevention techniques after risk assessment. Smart emergency response system (SERS) enables the location and assistance of each other during a disaster for both the survivors and the emergency workers. Models, outputs, and forecasts are automatically updated when new real-time data is gathered by the software programs. Forecasts of the developing situation are also helpful to other entities with significant firefighting duties, such as the police and hospitals.

4. Methodology

The proposed framework is a unique threat modeling mechanism for a smart industrial system. The research study used smart firefighting CPS use case for threat modeling, as described in Section 3. This framework is dependent on the MITRE ATT&CK matrix and system requirement collection (SRC) for identification of possible threats to smart firefighting. First, MITRE ATT&CK matrix analysis provides structure of attacks detection and mitigation. SRC gathers generic assets' information related to hardware, software and network layers. Then, a threat list is generated for smart firefighting system with the help of SRC and MITRE ATT&CK. Finally, mapping of threat list on NIST security and privacy controls is done using project of center for threat-informed defense (CTID) [59]. These mapped controls are utilized for mitigation of threats in smart firefighting system. See Fig. 3 for proposed methodology.

4.1. MITRE ATT&CK matrix analysis

MITRE ATT&CK [25] stands for MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK). It is a globally available knowledge-base about adversarial tactics and approaches based on actual observations. This framework is a regulated a model and knowledge foundation for cyber-adversary conduct, representing different stages of adversarial attacks' life cycle and the platforms they often use to target systems. There are two major components, tactics and techniques. Tactics are the objectives of an attacker, and techniques are the method by which the attacker achieves the tactical goals. Tactics and techniques are arranged as rows and columns of MITRE ATT&CK matrix. There are 14 tactics and 218 major techniques listed in MITRE ATT&CK matrix. Primarily, there are three categories of MITRE ATT&CK. ATT&CK for enterprise focuses on adversarial behavior in the enterprise system also covering cloud environments, Windows OS, and Mac OS, ATT&CK for mobile focuses on aggressive conduct, while the ATT&CK for enterprise matrix includes pre-ATT&CK, which focuses on "pre-exploit" hostile behavior.

In the ATT&CK matrix, mitigations are security concepts and a collection of instruments that stop a group of methods or sub-techniques from being effectively applied to a system or in an organization. Analysis of these mitigations, for different techniques, offers deep understanding of attack and help to identify the suitable security controls from NIST security and privacy controls. With deep analysis of the use case, possible attacks are identified in MITRE ATT&CK matrix for smart industrial system of smart firefighting. Mitigations of these attacks are analyzed to find prevention strategies and how attacks are linked with mitigations.

4.2. System requirement collection

System requirement collection (SRC) is a mechanism to configure the vulnerabilities caused by the components' varied nature and heterogeneity in order to devise a secured system. SRC and MITRE ATT&CK analysis generate the threats list for smart firefighting systems. SRC consists of six steps, including the identification of security goals, assets, sensor data, secure network communication, endpoint hardware and threats. These threats are reviewed in MITRE ATT&CK matrix and their techniques and mitigations are further analyzed.

4.2.1. Identify security goals

The required security decisions for the smart systems are developed by combining business objectives and long-term goals. This is accomplished by determining the security objectives, such as confidentiality, integrity, availability, non-repudiation, and authentication. These are considered as the most crucial security goals for any business organization and CPS.

4.2.2. Identify assets

Assets often include employees, software, hardware, sensors, and other items of any value to the organization. Therefore, the aim of this activity is to identify all the assets engaged in the smart CPS. The assessment of organizational and environmental assets is another component of this process. The asset list often includes information about people, data, networks, sensors, and physical components.

4.2.3. Identify sensors data

Sensors are used for communication of the system with the external environment. Data from the sensor is generated when sensors become functional. Sensor data is received using different technologies, like programmable logic controller (PLC), supervisory control and data acquisition (SCADA) system and application programming interface (API). A few higher-level sensors assist the central data cloud for data broadcasting. Protocols like Machine-to-Machine (M2M) are used to communicate with these sensors. Different sensors use different mediums for communication and technological interventions.

4.2.4. Identify secure network communication

This activity's goal involves network analysis. It is necessary to have a highly secure network and protocols that are used for communication on this network. The majority of devices in a smart CPS communicate on wireless network, and the system must have efficient authentication techniques for devices present in the network. Different devices use distinct networks and need secure communication network protocols to be deployed.

4.2.5. Identify endpoint hardware

It is critically advised to use only hardware with authorized endpoints. Hardware used in smart firefighting systems can be a sensor, vehicles, fire machinery, and other smart devices used in this cyber–physical system. Individuals must be informed about the vulnerabilities these devices can create, if not handled properly. Here, authorization means verifying the protocols of fire systems and standards testing for all hardware devices before including them in smart systems.

4.3. Threats identification

This activity's objective is to identify vulnerabilities in the autonomous cyber–physical system. CPS can be divided into three layers and threats in each layer should be identified. Software layer includes all software application systems running in the CPS. Network layer focuses on the network devices and protocols used for communication. Whereas, physical layer includes the hardware system and end-point devices. All these layers have been briefly discussed in SRC list, which highlights all major components of a smart firefighting system. MITRE ATT&CK matrix is later analyzed for identification of possible attacks on these components. With the help of MITRE ATT&CK matrix and SRC, a threat list is generated for smart firefighting CPS.

4.4. Mapping of NIST controls

In threat identification, various attacks from the MITRE ATT&CK have been studied. It is necessary to understand and determine the security approaches and innovations that may be used to prevent these attacks from being executed. For each technique or sub-technique of attack, mitigations are examined to find appropriate NIST security and privacy controls. For each security control, determine if it is aligned with the intent of the mitigation under review and if it is relevant to the technique or sub-technique under review. Once this candidate list of security controls has been identified, it is further reviewed, analyzed, and tailored in line with the control mapping scoping decisions to fully determine matches to techniques and/or sub-techniques of attacks. When this is completed, the security control selection is finalized, and the mapping is created for these attacks.

4.5. Threat mitigation using NIST control

Once the threats are mapped to specific NIST controls, the implementation of these controls in the organization or on CPS will automatically mitigate not only the specific threats but also safeguard personnel, property, and organizational activities. Additionally, the controls put in place will guarantee ongoing defense against a variety of risks and dangers, such as hostile assaults, mistakes made by people, natural disasters, structural flaws, foreign intelligence entities, and privacy problems. The controls are often adaptable, salable, and used as part of an organization-wide risk management strategy.

5. Results and evaluation

5.1. System Requirements Collection (SRC)

5.1.1. Security goals in smart firefighting CPS

In smart firefighting CPS, like every other system, CIA rules are major security objectives. In general, some security objectives are listed below.

- Confidentiality: The most important aspect of the security objectives is confidentiality. classified and personal information relevant to the smart firefighting system and its users, at any level, must not be disclosed to any unauthorized entity.
- Integrity: The accuracy of the system is intrinsically linked to data. The efficiency of smart firefighting systems is based on data and information used within the linked systems for decision-making. As a result, its integrity is critical. Any undesired modification of data can result in a disastrous situation, causing misleading results as an output from one component and used as an input for another component of the smart firefighting system. Integrity ensures that data in the system has not been tampered with by a malicious entity.
- Authorization: In a smart firefighting system, authorization defines the accessibility or user/client permissions connected to resources through a security measure. When accessing data and resources, a strong authorization system must be used.
- Role-based access control: Different authorized users should have distinct functions in intelligent systems. The amount of access to the system's range of diverse applications, databases, and networking devices is specified by these roles. In order to indicate the assigned responsibility of providers, the system maintains track of the access control list. Profile information, a port, a network channel, a login ID, and a badge number of firefighters can help to maintain the role-based authorization for the smart firefighting system.
- Robustness: The smart firefighting system should include a backup of alternative servers, sensing devices, power supplies, and other crucial systems to deliver a prompt reaction if any breakdown happens.
- Availability of data: The smart firefighting system must have ready access to requested data when it is required. Therefore, it is important that all systems and databases should be resilient to failures and responsive all the time.
- Contractual integrity: A written contractual definition should be followed by third-party hardware, software, and network vendors involved in the smart firefighting system. Moreover, any firefighting department cannot include devices without approval from the national fire protection association (NFPA).

5.1.2. Assets in smart firefighting CPS

The goal of this activity was to identify all the assets involved in a smart firefighting system. Assets in the smart firefighting system are categorized into three types of categories namely; software layer, network layer, and physical layer as shown in Fig. 2. Different software, hardware, and network components along with the use case description are available in Section 3 of the system model.

5.1.3. Sensors data in smart firefighting CPS

The sensors of smart firefighting system are categorized into three types as shown in Fig. 2. Sensors for personal protective equipment are the sensors attached to firefighters' clothing and devices. Mobility sensors are attached to mobile devices for data gathering. Stationary sensors are deployed in a building through which the firefighting system interacts and make useful decisions. To get data from the real-world world, sensor communication employs a variety of methods. For secure communication in a smart firefighting system, we identified wireless devices connected through IEEE 802.11-based communication protocol. Details about these sensors can be accessed from the research roadmap for smart firefighting [50].

5.1.4. Secure network communication in smart firefighting CPS

Discovery of secure network communication mechanism was the main objective of this section. The majority of devices in a smart firefighting system communicate wirelessly and the network should handle authentication in their network. Different devices use various types of networks and need secure communication network protocols to be deployed. DTLS, TLS, IPsec, and HIP-DEX are all significant security protocols to be deployed. Various remote and data communication technologies and diverse network types are used in smart firefighting systems for secure communication.

5.1.5. Endpoint hardware in smart firefighting CPS

In smart firefighting system, endpoint devices include sensors, PPEs of firefighters, IC applications software, and wireless devices among others. Fig. 2 shows the structure of smart firefighting system and outlines about the endpoint hardware. Details can be studied in, Section 3 of system model, with use case description, and research roadmap for smart firefighting system [50].

5.2. Threats identification in smart firefighting CPS

SRC provided the holistic overview of the smart firefighting CPS on application layers, physical layers and network layers. When major components and technologies were identified, MITRE ATT&CK analysis helped to generate the list of possible threats to the system. With the help of SRC and MITRE ATT&CK, a threat list was generated which is shown in Table 1, Table 2, and Table 3.

Table 1
Threat list for smart firefighting system.

Threat ID	Threat name	Threat description
T1001.003	Protocol Impersonation	Command and control communications are obscured by the attacker within the smart firefighting environment like high-Speed Vehicle Networking Systems, Remote Data Communication, and Wi-Fi Drones to make it more difficult to detect.
T1003.003	NTDS	Attacker focus on active databases in smart systems. He tries to exploit active directories vulnerabilities by copying or creating a replica. These directories include Event Database, Incident Storage and Archival Database, BIM Database, NFIRS, N-FORS in order to steal credential information, as well as obtain other information about domain members such as devices, users, and access rights.
T1003.005	Cached Domain Credentials	Attackers try to get access to smart firefighting systems' cached domain passwords, which are intended to authenticate users in the case that a domain controller is down.
T1003.008	OS Credential Dumping	Attacker uses brute force to try many password combinations on the OS dumps in different smart firefighting system components. This is done offline, so there are no traces left behind.
T1005	Data from Local System	Attacker searches through local components of smart firefighting like Stationary Sensors, Mobility Sensors and Systems, Sensors for Personal Protective Equipments or local databases as Event Database, Incident Storage and High-Speedatabase, BIM Database, which can leads to leakage of important data and become threads of attacks.
T1011	Exfiltration Over Other Network Medium	Attackers tries to steal information through the remote communication channel or other networking modes of the intelligent firefighting system.
T1020.001	Traffic Duplication	Traffic mirroring can be used by attackers to automate data intrusions using the vulnerable communications infrastructure of smart firefighting.
T1021	Remote Services	In the smart firefighting system, attackers utilize legitimate accounts to get access to the service and then carry out activities as the users who are currently signed in.
T1021.003	Distributed Component Object Model	The distributed component object paradigm allows for the use of legitimate accounts by adversaries to communicate with distant machines like drones and remotely operated vehicles. The opponent might then utilize the smart firefighting system's functionality as the user who is now signed in.
T1036	Masquerading	In order to look trustworthy or innocuous to users and security mechanisms in the intelligent firefighting system, attackers may try to modify the properties of their artifacts.
T1040	Network Sniffing	Adversaries may sniff network traffic of a firefighting enterprise to get details about the environment, along with any authentication information transmitted through the connection.
T1046	Network Service Scanning	In the smart firefighting system, attackers try to get a description of the operations that are functioning on remote servers, including those that might be open to software and hardware attack.
T1048	Exfiltration Over Alternative Protocol	Data leakage through a protocol other than the one used by the current command and control channel is a method used by attackers to steal information. The central server of smart firefighting is accessed from and to different network locations.
T1055.004	Asynchronous Procedure Call	Through the execution of malicious codes in the address space of a different live process, attackers introduce harmful code. using the concurrent procedure call queue in a smart firefighting system to get around process-based protections and perhaps escalate permissions.
T1071	Application Layer Protocol	Application layer protocols are used by attackers to connect in order to bypass network filtering and detection by merging into the current traffic of smart firefighting systems.
T1071.004	DNS	In order to bypass detection and network filtering, attackers' communication is dependent on the DNS application layer protocol which helps them to hide with normal traffic of the system.
T1087	Account Discovery	Attacker tries to get information about accounts of firefighters like First Responder, and Incident Commander on a system and within an environment of smart firefighting. Based on this information, adversaries try to launch attacks on the systems and smart equipment.
T1087.004	Cloud Account	A hacker attempts to obtain information on cloud accounts that smart firefighting companies have built and set up for users, remote access, applications, or the management of resources inside cloud computing.
T1090	Proxy	To prevent direct connections to their smart firefighting infrastructure, attackers may apply a connection proxy to divert network traffic between systems like sensors, databases, and systems and applications or to function as a middleman for communication links to a command and control server.
T1098	Account Manipulation	Adversaries manipulate accounts of firefighters to maintain access to firefighting systems.
T1098.001	Additional Cloud Credentials	To sustain permanent access to victim accounts and instances in the context of smart firefighting, attackers apply adversary-controlled privileges to a cloud server.
T1102.002	Bidirectional Communication	Adversaries use existing, legitimate external Web services for two-way communication via breached system in the smart firefighting over the Web services channel.
T1110	Brute Force	When credentials are forgotten or when the smart firefighting system includes password hashes, attackers utilize brute force methods to access systems.
T1110.002	Password Cracking	When credential material like password hashes are discovered, attackers may utilize password cracking to try and retrieve usable credentials, such as plain-text passwords.
T1110.004	Credential Stuffing	Through credential overlap, attackers gain access to the targeted domains of smart firefighting by using credentials stolen from penetration dumps of unconnected accounts.
T1119	Automated Collection	An attacker can utilize automated approaches to obtain internal data from a smart firefighting system after they have gained access to a system or network.
T1134	Access Token Manipulation	Adversaries modify access tokens to operate as a firefighter who has the access to firefighting systems to carry out deeds and get around access restrictions.
T1134.003	Make and Impersonate Token	Adversaries may modify access tokens in smart firefighting environment to conduct operations and get around access barriers by operating under a different user or security management context.
T1136	Create Account	Adversaries create an account to maintain access to victim firefighting systems.

Table 2
Threat list for smart firefighting system.

Threat ID	Threat name	Threat description
T1187	Forced Authentication	Adversaries may gather credential material of systems involved in smart firefighting by commanding or compelling a user to instantly supply authentication data via a technique they can eavesdrop on.
T1190	Exploit Public-Facing Application	Through the use of software, data, or orders, adversaries may try to exploit a flaw in a smart firefighting system's Internet-facing computer or program in order to trigger unwanted or unexpected activity.
T1195.003	Compromise Hardware Supply Chain	In order to compromise data or a system, attackers modify hardware elements like as sensors and intelligent equipment in smart firefighting systems.
T1203	Exploitation for Client Execution	Software weaknesses exist in client systems, including firefighters, which might be exploited by attackers to execute malware. The software has vulnerabilities as a result of unsecured development methods, which might lead to unanticipated behavior and impact the whole smart firefighting system.
T1204.002	User Execution: Malicious File	In a smart firefighting system, data is shared from various sources to a central point that is accessible to everyone on the team. Attackers use these types of files for the execution of malicious code on any point and because of the enterprise nature of the system, attackers can gain access to the complete system.
T1210	Exploitation of Remote Services	Once within a network of smart firefighting which consists of different types depending upon the nature of operations. Attackers use remote services to get illegal access to smart firefighting systems.
T1211	Exploitation for Defense Evasion	In order to surpass security measures, attackers target the applications of smart firefighting systems to find vulnerabilities. So, one can exploit these vulnerabilities and get unauthorized access.
T1212	Exploitation for Credential Access	The attacker used collected passwords from dump files and other resources. Then attackers find the vulnerability in applications of smart firefighting systems including sensors, BIM, and SAFIRE. Then, exploits these programming flaws using passwords and executes code that he wants on the system.
T1213	Data from Information Repositories	Adversaries may leverage information repositories like Event Database, Incident Storage and Archival Database, BIM Database, NFIRS, N-FORS to mine valuable information in smart firefighting environment. By exploitation, attacker has direct access to information.
T1485	Data Destruction	In order to prevent access to the smart firefighting system's platforms, applications, and shared network, attackers delete data and files on particular systems or in huge quantities on a network.
hline T1486	Data Encrypted for Impact	For the purpose of interfering with the availability of the system and network assets, the attackers apply data encryption techniques on databases and network communication to halt the system.
T1491	Defacement	Attacker changes the visual content of real-time sensors and other information to firefighters and other administration.
T1491.001	Internal Defacement	This could involve making changes to user-facing systems such application systems, HMI systems, and visualization systems, along with changing the desktop background.
T1491.002	External Defacement	In an effort to communicate with users within an organization, coerce them, or in any other way mislead them, an enemy may vandalize systems outside of smart firefighting.
T1495	Firmware Corruption	Attacker damages or erase the data on the flash memory of Video Stream Analysis System, Building Information Modeling, Building Management System, Analytical Tool System BIOS of or other firmware in devices attached to a system of firefighting in order to disable them or prevent them from booting.
T1498	Network Denial of Service	To hinder or stop the user of the smart firefighting system from accessing particular resources, attackers use Network Denial of Service (DoS) attacks.
T1498.001	Direct Network Flood	By delivering a large amount of network traffic directly to intelligent firefighting systems, attackers try to induce a denial of service (DoS) which compromises the system.
T1499	Endpoint Denial of Service	Endpoint Denial of Service (DoS) attacks can be carried out by attackers to impede or completely stop the provision of services to users of smart firefighting systems.
T1499.003	Application Exhaustion Flood	In order to execute DoS through web-based applications and services of smart firefighting systems, attackers target resource-intensive components of online apps such as Google Earth Visualization System, MapPLUTO, Fire Department, and Community Resources.
T1499.004	Application or System Exploitation	Attacker exploit software vulnerabilities and cause a DoS attack. It may result in a system or program crashing, denying access to authorized users of the smart firefighting system.
T1505.002	Transport Agent	In smart firefighting, attackers may take use of servers' authorized adaptable development features to get everlasting access to systems.
T1528	Steal Application Access Token	Adversaries are able to get privileges to access distant systems and resources of smart firefighting systems by stealing user application access tokens which are for authorized users.
T1542.001	System Firmware	Adversaries may modify system firmware of devices and sensors to persist on systems of smart firefighting to perform or assist in malicious activity.
T1543	Create or Modify System Process	In order to maintain persistence within the smart firefighting system, attackers may design or alter system-level programs that regularly execute harmful payloads.
T1546.008	Event Triggered Execution: Accessibility Features	Through the execution of harmful content that is sparked by smart firefighting systems' accessible capabilities, attackers build resilience and increase privileges.
T1548	Abuse Elevation Control Mechanism	An attacker circumvent the built-in control measures to get more access to databases and smart firefighting software.
T1552.003	Bash History	Attackers look for unsecured stored passwords by searching the bash command history on infected computers.

5.3. Mapping of NIST controls for smart firefighting CPS

This study used project of center for threat-informed defense (CTID) for mapping the threats list on NIST security and privacy controls 800-53 rev 5 [59]. CTID is a private research and development organization which is funded and operated by MITRE Engenuity. CTID mission is to deploy a threat informed defense system globally. Fig. 4 shows the technique of mapping for threats on respective attacks.

Table 3
Threat list for smart firefighting system.

Threat ID	Threat name	Threat description
T1550.001	Application Access Token	Acquisition of application access certificates by attackers, allows them to access restricted accounts, data, or services on distant smart firefighting systems without going through the standard authentication mechanism.
T1552	Unsecured Credentials	Adversaries may scan hacked networks to locate and seize credential information that was not securely stored by the smart firefighting system.
T1552.005	Cloud Instance Metadata API	Insecurely stored credentials are sought after by criminals that scan hacked smart firefighting systems. These passwords might be lost or kept in a variety of places on an enterprise system.
T1553	Subvert Trust Controls	A smart firefighting system's security measures that either notify users of suspicious activities or forbid the execution of suspicious applications might be undermined by attackers.
T1554	Compromise Client Software Binary	Adversaries modify client software like application system, Visualization System, SAFIRE, SERS, and Analytical Tool System binaries to create enduring exposure to smart firefighting systems. Through these systems, firefighters and other user get access to complete enterprise system.
T1556	Modify Authentication Process	In order to acquire user credentials or permit unauthorized access to accounts, attackers may change the smart firefighting system's authentication techniques and procedures.
T1556.001	Domain Controller Authentication	In order to get beyond standard authentication procedures and get access to accounts in a smart firefighting environment, attackers patch the authentication process on a domain controller.
T1557	Adversary-in-the-Middle	Attackers use the adversary-in-the-middle (AiTM) approach to place themselves in the center of two or more networked devices engaged in smart firefighting in order to enable additional behaviors like network sniffing or transmitted data manipulation.
T1557.002	ARP Cache Poisoning	Attackers target the cache of various applications and systems to perform the man-in-the-middle attack in smart firefighting system.
T1560	Archive Collected Data,	Data from the smart firefighting system that is acquired before exfiltration will be compressed and encrypted by an attacker. Attacker may simply transfer data across the network while hiding his identity thanks to compression and encryption.
T1562.004	Disable or Modify System Firewall	Attackers may alter or disable system firewalls in order to get around restrictions on network usage. The smart firefighting system's rules may be added, deleted, or modified, as well as the entire process might be disabled.
T1563	Remote Service Session Hijacking	In order to move laterally in the firefighting environment, attackers take control of already running sessions with distant services.
T1565	Data Manipulation	In order to skew external results or conceal activities, attackers change, remove, or otherwise alter data in the Event Database, Incident Storage and Archival Database, BIM Database, NFIRS, or N-FORS. In a smart firefighting setting, enemies may try to influence decision-making, organizational understanding, or business processes by manipulating data.
T1565.001	Stored Data Manipulation	To influence external outcomes or conceal the behavior of the firemen, attackers may edit, remove, or otherwise alter data.
T1565.003	Runtime Data Manipulation	Adversaries may modify systems in order to manipulate runtime data from Sensors and System as it is accessed and displayed to an end user of the smart firefighting system.
T1566	Phishing	Phishing emails are one-way, attackers try to enter victim systems. involved in the smart firefighting.
T1569	System Services	By engaging with or making services either locally or remotely, adversaries may take advantage of system services or daemons in smart firefighting to run commands or programs that can execute malicious material.
T1573	Encrypted Channel	In a smart firefighting setting, attackers may use a recognized encryption method to masquerade command and control communications rather than depending on any built-in security features which are offered by a communication protocol.
T1574	Hijack Execution Flow	By controlling the way smart firefighting application systems run programs or firmware executes the tasks, attackers can carry out their own malicious payloads.
T1574.005	Executable Installer File Permissions Weakness	Attackers utilize installers in firefighting enterprises to execute certain programs as part of their functionality or to carry out other tasks, but they may also use these installers to deploy their own malicious payloads.
T1599.001	Network Address Translation Traversal	By hacking perimeter network devices like Wi-Fi drones, High Speed Vehicle Networking Systems, and network communication channels, adversaries can cross network borders. An attacker may be able to get around constraints on traffic routing in a firefighting environment that ordinarily divide trusted and untrusted networks by compromising these devices.
T1602	Data from Configuration Repository	The configuration repositories may be used by attackers to get information about controlled devices. Management systems employ configuration archives to setup, organize, and control information on distant smart firefighting system services.
T1546.009	AppCert DLLs	By executing malicious material that is prompted by AppCert DLLs loaded into processes, attackers establish persistence and/or raise privileges, which results in the event-triggered execution of assaults against smart firefighting systems.

NIST Security control framework mappings to MITRE ATT&CK are included in the repository together with available resources and literature. With the help of these mappings, businesses may analyze the extent to which existing security controls are effective against threats that are detailed in the ATT&CK knowledge base. They also lay the groundwork for incorporating threat data from the ATT&CK into the risk management procedures. Table 4 shows the mapping of threat list on NIST controls.

5.4. Threat mitigation in smart firefighting CPS

With a careful and strategic mechanism, the mapping of the threat list on NIST security and privacy controls was successfully completed. The process for mapping a threat list on NIST security and privacy controls involves various steps. First step was the

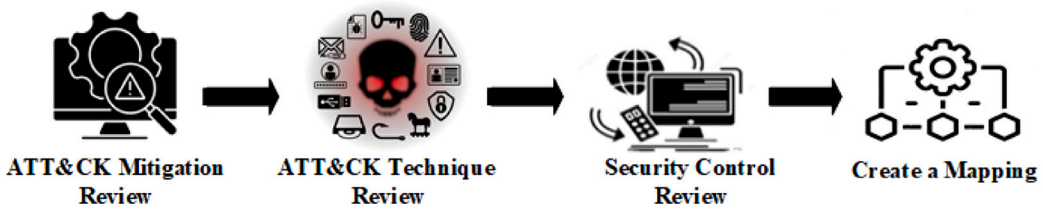


Fig. 4. Center for threat-informed defense (CTID) technique.

identification of threat list generated with help of SRC and Mitre ATT&CK framework. Then, the next step was to identify the NIST security and privacy controls relevant to the threats related to smart firefighting CPS. This research has relied on the comprehensive and widely recognized guidelines and security controls provided by [60]. Once the relevant NIST controls have been identified, the next step was to map the threat list to the corresponding NIST controls. This involves identifying the controls that address the specific threat and mapping them accordingly. Then, CITD technique is used to generate the mapping as shown in Fig. 4 where mitigations for certain tasks are reviewed to find out objective and technique related to that specific attack. Then, the attackers' tactics to obtain their objective and techniques used are analyzed. Finally, these mitigation techniques are analyzed in line with NIST security controls and the mapping is created.

When the mapped controls are implemented in the organization or on the cyber–physical system, they automatically mitigate the specific threats and protect the organizational operations and assets. As was already established, businesses and industrial CPS must regularly deal with a variety of dangers and hazards, including hostile assaults, employee mistakes, natural calamities, structural problems, foreign intelligence elements, and privacy issues. These are the ongoing dangers to businesses and intelligent industrial CPS. A crucial part of an organization-wide strategy to manage risk is played by the security and privacy measures, which are adaptable and customized. The table of threats and NIST controls mapping shows that multiple controls can be mapped against each attack. These multiple controls provide advanced security against specific attacks.

T1040-network sniffing is a network monitoring and retrieval technique that involves continuous monitoring and retrieving of all data packets that pass through the network. This attack is mitigated by applying encryption of all sensitive information and multi-factor authentication on all wired/wireless communication. On the other hand, T1040 is mitigated by AC-17, AC-18, AC-19, IA-2, IA-5, SC-4, SC-8, SI-4, SI-7 security controls. T1110-brute force is used by an attacker to gain access to systems when passwords are unknown or when password hashes are obtained. This attack is mitigated by setting account login policies to observe failed login attempts, multi-factor authentication, password policies and user account management. Implementation of these techniques and policies is a difficult task. After mapping T1110 to NIST controls, these types of attacks are mitigated by AC-3, CM-2, IA-2, IA-5, SI-4 controls.

6. Conclusion

For cyber-security professionals, the ever-changing state of the cyber threats landscape makes cyber-attacks a critical issue to address. The smart industrial sector is a large contributor to this challenge, as most smart facilities encompass internet-connected devices that are potentially vulnerable to attacks. The effects of cyber-attacks are severe and difficult to reverse after systems get hacked. Finding and removing the dangers in the system before they are implemented is one technique to protect the weaknesses of dispersed IoT devices in a smart industrial system. To achieve the objective, a threat-modeling technique was suggested in this study in an effort to detect and reduce possible dangers in the smart cyber–physical system. The proposed work was carried out by applying a threat modeling approach on the use case of smart firefighting CPS. This framework utilized the MITRE ATT&CK matrix and system requirement collection (SRC) for the identification of possible threats in smart firefighting CPS. First, MITRE ATT&CK matrix analysis provided the structure of attack detection and mitigation. SRC gathered generic assets information related to hardware, software, and network layers. Then, a threat list was generated for smart firefighting system with the help of SRC and MITRE ATT&CK. Finally, the mapping of the threat list on NIST security and privacy controls was carried out using the project of the center for threat-informed defense (CTID). These mapped controls can be utilized for the mitigation of threats in smart firefighting systems. This research study has significant theoretical and practical implications for security practitioners, network communication officers and other personnel responsible for security posture of any smart cyber–physical system. In future, the framework can be employed to secure more smart industrial systems.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

Table 4
Mapping of threat list on NIST controls.

Threat ID	Mapped controls	Threat ID	Mapped controls
T1001.003	AC-4, CM-2, SC-7, SI-4	T1491	AC-3, CM-2, CP-7, CP-9, SI-4, SI-7
T1003.003	AC-3, CM-2, CM-5, CP-9, IA-2, IA-5, SI-4, SI-7	T1491.001	AC-3, CM-2, CP-7, CP-9, SI-4, SI-7
T1003.005	AC-3, AC-4, CM-2, CM-5, IA-2, IA-4, IA-5, SI-4	T1491.002	AC-3, CM-2, CP-7, CP-9, SI-4, SI-7
T1005	AC-3, CM-12, CP-9, SI-4	T1495	AC-3, CM-5, IA-2, RA-9, SI-7
T1011	AC-18,SI-4	T1498	AC-3, AC-4, SC-7
T1020.001	AC-17, AC-18, AC-19, AC-4, CA-3, CM-2, SC-4, SC-7, SC-8, SI-4, SI-7	T1498.001	AC-3,AC-4,SC-7
T1021	AC-17, AC-3, CM-5, IA-2, IA-5, SI-4	T1499	AC-3, AC-4, SC-7, SI-4
T1021.003	AC-17, AC-3, AC-4, CM-2, CM-5, IA-2, SC-3, SC-7, SI-4	T1499.003	AC-3,AC-4,SC-7,SC-4
T1036	AC-3, CM-2, SI-4, SI-7	T1499.004	AC-3, AC-4, SC-7, SI-4
T1040	AC-17, AC-18, AC-19, IA-2, IA-5, SC-4, SC-8, SI-4, SI-7	T1505.002	AC-3, CM-2, CM-5, IA-2, SI-4, SI-7
T1046	AC-4, CM-2, SC-7, SI-4, SI-4	T1528	AC-10, AC-3, AC-4, CM-2, CM-5, IA-2, IA-4, IA-5, SI-4
T1048	AC-3, AC-4, CA-3, CM-2, SA-9, SC-7, SI-4	T1542.001	AC-3, CM-5, IA-2, RA-9, SI-7
T1055.004	SC-7,SC-4	T1543	AC-17,AC-3,CM-2,CM-5,IA-2,IA-4,SI-4,SI-7
T1071	AC-4, CM-2, SC-7, SI-4	T1546.008	SI-4, SI-7
T1071.004	AC-3, AC-4, CM-2, SC-7, SI-4	T1548	AC-3, CM-2, CM-5, IA-2, SI-4, SI-7
T1087	SI-4	T1550.001	AC-17, AC-19, CM-2, IA-2, IA-4, SC-8, SI-4, SI-7
T1087.004	AC-3,AC-4,CM-5,IA-2,IA-5,SC-7,SI-4,SI-7	T1552	AC-17, AC-18, AC-19, AC-3, AC-4, CM-2, CM-5, IA-2, IA-3, IA-4, IA-5, SC-4, SC-7, SI-4, SI-7
T1090	AC-3, AC-4, CM-2, SC-7, SC-8, SI-4	T1552.003	SI-4
T1098	AC-3, AC-4, CM-5, IA-2, SC-7, SI-4	T1552.005	AC-3, AC-5, IA-3, IA-4, SC-7, SI-4
T1098.001	AC-3, AC-4, CM-5, IA-2,IA-5, SC-7, SI-4, SI-7	T1553	CM-2, CM-5, RA-9, SI-4, SI-7
T1102.002	AC-4,CM-2,SC-7,SI-4	T1554	CM-2,SI-7
T1110	AC-3,CM-2,IA-2,IA-5,SI-4	T1556	AC-3, CM-2, CM-5, IA-2, IA-5, SI-4, SI-7
T1110.002	AC-3, CM-2, IA-2, IA-4, IA-5, SI-4	T1556.001	AC-3, CM-5, IA-2, IA-5, SI-4, SI-7
T1110.004	AC-3, CM-2, IA-2, IA-5, SI-4	T1557	AC-17, AC-18, AC-19, AC-3, AC-4, CM-2, SC-4, SC-7, SC-8, SI-4,SI-7
T1003.008	AC-3, CM-2, CM-5, IA-2, IA-5, SI-4	T1557.002	AC-17,AC-18,AC-19, AC-3, AC-4, CM-2, SC-4, SC-7, SC-8, SI-4, SI-7
T1119	AC-17, AC-18, AC-19, CM-2, CP-6, CP-7, CP-9, SC-4, SI-4, SI-7	T1560	SC-7, SI-4
T1134	AC-3,CM-5, IA-2	T1562.004	AC-3, CM-2, CM-5, IA-2, SI-4, SI-7
T1134.003	AC-3, CM-5, IA-2	T1563	AC-17, AC-3, AC-4, CM-2, CM-5, IA-2, IA-4, IA-6, SC-7, SI-4
T1136	AC-3,AC-4,CM-5,IA-2,IA-5,SC-7,SI-4,SI-7	T1565	AC-17, AC-18, AC-19, AC-3, AC-4, CM-2, CP-6, CP-7, CP-9, SC-4, SC-7, SI-4, SI-7
T1187	AC-3, AC-4, CM-2, SC-7, SI-4	T1565.001	AC-17, AC-18, AC-19, AC-3, CM-2, CP-6, CP-7, CP-9, SC-4, SC-7, SI-4, SI-7
T1190	AC-3, AC-4, CA-2, CM-5, IA-2, SC-2, SC-3, SC-7, SI-4, SI-7	T1565.003	AC-3, AC-4, CP-9, SC-4, SC-7, SI-4
T1195.003	CM-5,RA-9,SI-7	T1566	AC-4, CM-2, SC-7, SI-4
T1203	AC-4, SC-2, SC-3, SC-7, SI-4, SI-7	T1569	AC-3, CM-2, CM-5, IA-2, SI-4, SI-7
T1204.002	AC-4, CM-2, SC-7, SI-4, SI-7	T1573	AC-4, CM-2, SC-7, SI-4
T1210	AC-3, AC-4, CA-2, CM-2, CM-5, IA-2, SC-2, SC-3, SC-7, SI-4, SI-5, SI-7	T1574	AC-3, AC-4, CM-2, CM-5, IA-2, SI-4, SI-7
T1211	AC-4, CM-2, SC-2, SC-3, SC-7, SI-4, SI-5, SI-7	T1574.005	AC-3, AC-4, CM-2, CM-5, IA-2, SI-4
T1212	AC-4, CM-2, SC-2, SC-3, SC-7, SI-4, SI-7	T1599.001	AC-3, AC-4, CM-2, CM-5, IA-2, IA-5, SC-7, SI-4, SI-7
T1213	AC-17, AC-3, AC-4, CM-2, CM-5, IA-2, IA-4, SI-4, SI-7	T1602	AC-17, AC-18, AC-19, AC-3, AC-4, CM-2, IA-3, IA-4, SC-3, SC-4, SC-7, SC-8, SI-4, SI-7
T1485	AC-3, CM-2, CP-7, CP-9, SI-4, SI-4	T1546.009	SI-7, CM-2
T1486	AC-3, CM-2, CP-6, CP-7, CP-9, SI-4, SI-7		

Acknowledgement

The research work was supported by the research lab funded by National Center for Cyber Security (NCCS), Pakistan.

References

[1] O.M. Butt, M. Zulqarnain, T.M. Butt, Recent advancement in smart grid technology: Future prospects in the electrical power network, Ain Shams Eng. J. 12 (1) (2021) 687–695.
[2] R.K. Radha, Flexible smart home design: Case study to design future smart home prototypes, Ain Shams Eng. J. 13 (1) (2022) 101513.
[3] S.M.M. Sajadieh, Y.H. Son, S.D. Noh, A conceptual definition and future directions of urban smart factory for sustainable manufacturing, Sustainability 14 (3) (2022) 1221.

[4] A. of Science of South Africa, et al., The Smart City Initiatives in South Africa and Paving a Way to Support Cities to Address Frontier Issues Using New and Emerging Technologies, Academy of Science of South Africa (ASSAf), 2020.
[5] J. Lee, B. Bagheri, H.-A. Kao, A cyber-physical systems architecture for industry 4.0-based manufacturing systems, Manuf. Lett. 3 (2015) 18–23.
[6] M. Javaid, A. Haleem, R.P. Singh, S. Rab, R. Suman, Significance of sensors for industry 4.0: roles, capabilities, and applications, Sensors Int. 2 (2021) 100110.
[7] H. Singh, Big data, industry 4.0 and cyber-physical systems integration: A smart industry context, Mater. Today Proc. 46 (2021) 157–162.
[8] A. Tandon, Survey of security issues in cyber-physical systems, in: Machine Learning, Advances in Computing, Renewable Energy and Communication, Springer, 2022, pp. 347–357.
[9] J.-P.A. Yaacoub, O. Salman, H.N. Noura, N. Kaaniche, A. Chehab, M. Malli, Cyber-physical systems security: Limitations, issues and future trends, Microprocess. Microsyst. 77 (2020) 103201.
[10] T. Berger, P. Engzell, Industrial automation and intergenerational income mobility in the United States, Soc. Sci. Res. (2022) 102686.
[11] D.A. Sepúlveda Estay, A system dynamics, epidemiological approach for high-level cyber-resilience to zero-day vulnerabilities, J. Simul. (2021) 1–16.
[12] Y. Xiao, Y. Jia, C. Liu, X. Cheng, J. Yu, W. Lv, Edge computing security: State of the art and challenges, Proc. IEEE 107 (8) (2019) 1608–1631.
[13] Y. Al-Hadhrami, F.K. Hussain, DDoS attacks in IoT networks: a comprehensive systematic literature review, World Wide Web 24 (3) (2021) 971–1001.
[14] R. Al Attar, J. Al-Nemri, A. Homsi, A. Qusef, Risk assessment for emerging domains (IoT, cloud computing, and AI), in: 2021 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology, JEEIT, IEEE, 2021, pp. 120–127.
[15] C. Itodo, S. Varlioglu, N. Elsayed, Digital forensics and incident response (DFIR) challenges in IoT platforms, in: 2021 4th International Conference on Information and Computer Technologies, ICICT, IEEE, 2021, pp. 199–203.
[16] M.S. Mazhar, Y. Saleem, A. Almogren, J. Arshad, M.H. Jaffery, A.U. Rehman, M. Shafiq, H. Hamam, Forensic analysis on internet of things (IoT) device using machine-to-machine (M2M) framework, Electronics 11 (7) (2022) 1126.
[17] E. Aliwa, O. Rana, C. Perera, P. Burnap, Cyberattacks and countermeasures for in-vehicle networks, ACM Comput. Surv. 54 (1) (2021) 1–37.
[18] E. Ismagilova, L. Hughes, N.P. Rana, Y.K. Dwivedi, Security, privacy and risks within smart cities: Literature review and development of a smart city interaction framework, Inform. Syst. Front. (2020) 1–22.
[19] E. Anthi, Detecting and Defending Against Cyber Attacks in a Smart Home Internet of Things Ecosystem (Ph.D. thesis), Cardiff University, 2022.
[20] J.E. Sullivan, D. Kamensky, How cyber-attacks in Ukraine show the vulnerability of the US power grid, Electr. J. 30 (3) (2017) 30–35.
[21] H. Krasner, The cost of poor software quality in the US: A 2020 report, in: Proc. Consortium Inf. Softw. QualityTM (CISQTM), 2021.
[22] H. Saleous, M. Ismail, S.H. AlDaajeh, N. Madathil, S. Alrabaee, K.-K.R. Choo, N. Al-Qirim, COVID-19 pandemic and the cyberthreat landscape: Research challenges and opportunities, Digit. Commun. Netw. (2022).
[23] D.P. Bliss, F.O. Vice President, Creating the research roadmap for smart fire fighting, NIST Special Publ. 1191 (2015) 1–247.
[24] J. Simonjan, S. Taurer, B. Dieber, A generalized threat model for visual sensor networks, Sensors 20 (13) (2020) 3629.
[25] MITRE ATT&CK®, 2022, URL https://attack.mitre.org/. (Accessed 9 February 2022).
[26] J.T. Force, Security and Privacy Controls for Information Systems and Organizations, Tech. rep., National Institute of Standards and Technology, 2017.
[27] M.R. Rahman, L. Williams, An investigation of security controls and MITRE ATT\&CK techniques, 2022, arXiv preprint arXiv:2211.06500.
[28] C.-H. Wang, H.-N. Dai, C.-Y. Lee, T.-H. Chang, Cyber-physical systems for fire safety: a review, Fire Technol. 55 (3) (2019) 999–1021.
[29] J.V.D. Ham, Toward a better understanding of "cybersecurity", Digit. Threats Res. Pract. 2 (3) (2021) 1–3.
[30] A. Schaad, D. Binder, Ml-supported identification and prioritization of threats in the ovvl threat modelling tool, in: IFIP Annual Conference on Data and Applications Security and Privacy, Springer, 2020, pp. 274–285.
[31] N. Shevchenko, T.A. Chick, P. O'Riordan, T.P. Scanlon, C. Woody, Threat Modeling: a Summary of Available Methods, Tech. rep., Carnegie Mellon University Software Engineering Institute Pittsburgh United, 2018.
[32] B. Bakić, M. Milić, I. Antović, D. Savić, T. Stojanović, 10 Years since stuxnet: What have we learned from this mysterious computer software worm? in: 2021 25th International Conference on Information Technology, IT, IEEE, 2021, pp. 1–4.
[33] M.M. Salim, S. Rathore, J.H. Park, Distributed denial of service attacks and its defenses in IoT: a survey, J. Supercomput. 76 (2020) 5320–5363.
[34] T. Alladi, V. Chamola, S. Zeadally, Industrial control systems: Cyberattack trends and countermeasures, Comput. Commun. 155 (2020) 1–8.
[35] O. Valea, C. Oprişa, Towards pentesting automation using the metasploit framework, in: 2020 IEEE 16th International Conference on Intelligent Computer Communication and Processing, ICCP, IEEE, 2020, pp. 171–178.
[36] R. Alkhadra, J. Abuzaid, M. AlShammari, N. Mohammad, Solar winds hack: In-depth analysis and countermeasures, in: 2021 12th International Conference on Computing Communication and Networking Technologies, ICCCNT, IEEE, 2021, pp. 1–7.
[37] S. Furnell, D. Emm, The ABC of ransomware protection, Comput. Fraud Secur. 2017 (10) (2017) 5–11.
[38] C. Kaura, N. Sindhwani, A. Chaudhary, Analysing the impact of cyber-threat to ICS and SCADA systems, in: 2022 International Mobile and Embedded Technology Conference, MECON, IEEE, 2022, pp. 466–470.
[39] T. Miller, A. Staves, S. Maesschalck, M. Sturdee, B. Green, Looking back to look forward: Lessons learnt from cyber-attacks on industrial control systems, Int. J. Crit. Infrastruct. Prot. 35 (2021) 100464.
[40] M. Alhamry, W. Elmedany, Exploring Wi-Fi WPA2 KRACK vulnerability: A review paper, in: 2022 International Conference on Data Analytics for Business and Industry, ICDABI, IEEE, 2022, pp. 766–772.
[41] P. Wang, A. Ali, W. Kelly, Data security and threat modeling for smart city infrastructure, in: 2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications, SSIC, IEEE, 2015, pp. 1–6.
[42] R. Khan, K. McLaughlin, D. Laverty, S. Sezer, STRIDE-based threat modeling for cyber-physical systems, in: 2017 IEEE PES Innovative Smart Grid Technologies Conference Europe, ISGT-Europe, IEEE, 2017, pp. 1–6.
[43] S. Marksteiner, H. Vallant, K. Nahrgang, Cyber security requirements engineering for low-voltage distribution smart grid architectures using threat modeling, J. Inform. Secur. Appl. 49 (2019) 102389.
[44] G. Kavallieratos, N. Chowdhury, S. Katsikas, V. Gkioulos, S. Wolthusen, Threat analysis for smart homes, Future Internet 11 (10) (2019) 207.
[45] S.G. Abbas, S. Zahid, F. Hussain, G.A. Shah, M. Husnain, A threat modelling approach to analyze and mitigate botnet attacks in smart home use case, in: 2020 IEEE 14th International Conference on Big Data Science and Engineering, BigDataSE, IEEE, 2020, pp. 122–129.
[46] S.-H. Cho, D.-S. Kang, M.-S. Kang, H.-S. Kim, J.-W. Bae, C.-I. Lee, H.-B. Ji, Y.-H. Won, H.-K. Hong, K. Kim, A study on threat modeling in smart greenhouses, J. Inform. Secur. Cybercrimes Res. 3 (1) (2020) 1–12.
[47] S.G. Abbas, I. Vaccari, F. Hussain, S. Zahid, U.U. Fayyaz, G.A. Shah, T. Bakhshi, E. Cambiaso, Identifying and mitigating phishing attack threats in IoT use cases using a threat modelling approach, Sensors 21 (14) (2021) 4816.
[48] V. Vakhter, B. Soysal, P. Schaumont, U. Guler, Security for emerging miniaturized wireless biomedical devices: Threat modeling with application to case studies, 2021, arXiv preprint arXiv:2105.05937.
[49] S.-S. Jeong, et al., A study on A smart firefighting helmet capable of video/audio transmission based on the firefighting standard disaster system, Turkish J. Comput. Math. Educ. (TURCOMAT) 12 (6) (2021) 493–497.
[50] A.P. Hamins, N.P. Bryner, A.W. Jones, G.H. Koepke, et al., Research roadmap for smart fire fighting, 2015.
[51] P. Rani, R. Sharma, Intelligent transportation system for internet of vehicles based vehicular networks for smart cities, Comput. Electr. Eng. 105 (2023) 108543.

[52] Y. Zhang, W. Deng, K. Huang, C. Yang, False data injection attack testbed of industrial cyber-physical systems of process industry and a detection application, in: 2021 IEEE International Conference on Recent Advances in Systems Science and Engineering, RASSE, IEEE, 2021, pp. 1–7.
[53] T. Peng, W. Ke, Urban fire emergency management based on big data intelligent processing system and Internet of Things, Optik 273 (2023) 170433.
[54] M. Holland, D.J. Zaloga, C.S. Friderici, COVID-19 Personal Protective Equipment (PPE) for the emergency physician, Vis. J. Emerg. Med. 19 (2020) 100740.
[55] D.E. Whitehead, K. Owens, D. Gammel, J. Smith, Ukraine cyber-induced power outage: Analysis and practical mitigation strategies, in: 2017 70th Annual Conference for Protective Relay Engineers, CPRE, IEEE, 2017, pp. 1–8.
[56] J. Zhu, G. Wright, J. Wang, X. Wang, A critical review of the integration of geographic information system and building information modelling at the data level, ISPRS Int. J. Geo-Inf. 7 (2) (2018) 66.
[57] N. Jones, Guilty of hiding a data breach, Netw. Secur. 2023 (2) (2023).
[58] C. Bronk, N. Jones, Cyber cases: The PICCA framework for documenting geopolitically relevant cyber action, J. Strateg. Secur. 16 (1) (2023) 5.
[59] J. Baker, Security control mappings: A bridge to threat-informed defense, 2022, https://medium.com/mitre-engenuity/security-control-mappings-a-bridge-to-threat-informed-defense-2e42a074f64a. (Accessed 9 February 2022).
[60] K. Dempsey, G. Witte, D. Rike, Summary of NIST SP 800-53, Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations, Tech. rep., National Institute of Standards and Technology, 2014.