Computers, Materials & Continua
DOI: 10.32604/cmc.2022.028495
Article

Tech Science Press

Novel Architecture of Security Orchestration, Automation and Response in Internet of Blended Environment

Minkyung Lee[1], Julian Jang-Jaccard[2] and Jin Kwak[3,*]

[1]ISAA Lab, Department of Cyber Security, Ajou University, Suwon, 16499, Korea
[2]Department of Computer Science and Information Technology, Massey University, Auckland, 0745, New Zealand
[3]Department of Cyber Security, Ajou University, Suwon, 16499, Korea
*Corresponding Author: Jin Kwak. Email: security@ajou.ac.kr
Received: 10 February 2022; Accepted: 23 March 2022

Abstract: New technologies that take advantage of the emergence of massive Internet of Things (IoT) and a hyper-connected network environment have rapidly increased in recent years. These technologies are used in diverse environments, such as smart factories, digital healthcare, and smart grids, with increased security concerns. We intend to operate Security Orchestration, Automation and Response (SOAR) in various environments through new concept definitions as the need to detect and respond automatically to rapidly increasing security incidents without the intervention of security personnel has emerged. To facilitate the understanding of the security concern involved in this newly emerging area, we offer the definition of Internet of Blended Environment (IoBE) where various convergence environments are interconnected and the data analyzed in automation. We define Blended Threat (BT) as a security threat that exploits security vulnerabilities through various attack surfaces in the IoBE. We propose a novel SOAR-CUBE architecture to respond to security incidents with minimal human intervention by automating the BT response process. The Security Orchestration, Automation, and Response (SOAR) part of our architecture is used to link heterogeneous security technologies and the threat intelligence function that collects threat data and performs a correlation analysis of the data. SOAR is operated under Collaborative Units of Blended Environment (CUBE) which facilitates dynamic exchanges of data according to the environment applied to the IoBE by distributing and deploying security technologies for each BT type and dynamically combining them according to the cyber kill chain stage to minimize the damage and respond efficiently to BT.

Keywords: Blended threat (BT); collaborative units for blended environment (CUBE); internet of blended environment (IoBE); security orchestration, automation and response (SOAR)

This work is licensed under a Creative Commons Attribution 4.0 International License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

1 Introduction

According to the World Economic Forum, Information and Communication Technology (ICT), such as artificial intelligence, big data, and Internet of Things (IoT) in the fourth industrial revolution has advanced to convergence technology of nanotechnology, biotechnology, information technology, and cognitive science, maximizing the connectivity between various technologies [1]. For example, with the emergence of massive IoT, a hyper-connected network environment has emerged which connects millions of devices at a high density. An evolution to a hyper-connected society is underway, where data generation, collection, and sharing activities occur ceaselessly for people, objects, and spaces using the Internet as a medium [2]. Furthermore, various convergence environments, such as smart factories, smart buildings, and cooperative intelligent transport systems (C-ITS) have emerged. Internet technology (IT) is combined and applied in these environments to connect each other producing complex services and data [3,4]. New advanced security threats exploiting various security vulnerabilities in different architecture services used in these new environments have been found [5,6]. A variety of response technologies cyberattacks utilizing conventional Instruction Prevention Systems (IPS) and Security Information and Events Management (SIEM) have been offered to respond to such advanced security threats [7–12]. However, the need to detect and respond automatically to these new types of cyberattacks without the intervention of security personnel has emerged by integrating various existing security technologies cyberattacks. However, the concern over the management of the various types of log data produced from heterogeneous security technologies and the operations of effective security response mechanisms on different architectures has been raised [13]. This research possesses various contributions in the future environment such as IoBE:

- First, it has prepared for the blended environment by analyzing massive IoT and various convergence environments.
- Second, the variety of attack surfaces has been explored in IoBE by analyzing attack surfaces in the environment.
- Third, future environment such as IoBE has been explored by defining and analyzing the environment where various convergence environments are connected.
- Finally, countermeasure has explored how to respond to numerous security incidents in IoBE including various convergence by analyzing SOAR and proposing SOAR-CUBE.

In this paper, we propose a security orchestration, automation and, response with collaborative units of blended environment (SOAR-CUBE) architecture to respond to newly emerging security threats rapidly and efficiently. In Section 2, we analyze massive IoT, a hyper-connected network environment, and analyze SOAR that automates the response process of various security threats. In Section 3, we define a number of terms used in the new environment, namely Internet of Blended Environment (IoBE) and Blended Threat (BT). Section 4 newly proposes a SOAR-CUBE architecture that can be applied to a complex environment by integrating heterogeneous security technologies to respond to BT efficiently in IoBE, and Section 5 provides the conclusion.

2 Basic Definitions

In this section, we describe the definitions of massive IoT as millions of devices are all connected at a high density and the definitions of SOAR as automation processes of various threats to counter security incidents with minimal human intervention. They have already been defined by Gartner.

2.1 Massive IoT

Massive IoT refers to a hyper-connected network environment, in which millions of devices are all connected at a high density. The emergency of the massive IoT has been brought through the development of low-power wide-area (LPWA) network technology (e.g., Sigfox and LoRa) that facilitates broad communication with the devices using low-power consumption which enabled a large-scale IoT connected within a specific range. Tab. 1 shows the key requirements for the construction of massive IoT in terms of key requirements and descriptions [14].

Table 1: Key requirements for massive IoT

Key Requirement	Description
Long battery life	Devices are often battery-powered, and expensive to replace after deployment
Strong coverage	Networks must penetrate deep indoors and underground for many use cases, such as mining
Low cost	Affordable device and low operational cost necessary to create a business case with high volumes
Scale & density	Networks must easily scale to handle a huge of devices as use cases grow
Performance flexibility	Networks must be able to handle multiple applications with different performance requirements (e.g., "latency" and "throughput")

Tab. 2 illustrates different environments where massive IoT applications are deployed and the descriptions of how the massive IoT applications are used in each environment.

Table 2: The environment of massive IoT applications

Environment	Description
Utilities	Smart metering, smart grid management
Transport & logistics	Asset tracking, fleet management
Industrial	Process monitoring and optimization
Smart cities	Smart lighting, waste disposal, parking
Smart buildings	Home automation, smart hearing, alarms (security, smoke detectors)

With the recent progress and advancement in the IT, various environments have been increasingly combined, for example, smart factories integrated within a smart building. With the increasing combination of different environments for massive IoT applications—call it a convergence environment, it is expected that the architecture and platform that house the combination of massive IoT-applied environments will become complex. In addition, the number of sensors and data- processing capacity have been growing with the continuous development of IoT devices and technology. They are evolving into intelligent smart sensors as the data processing and analysis functions are combined [15]. However, malicious attacks or unintended information breaches can occur while collecting and processing the data produced in various convergence environments. This is due to an increase in the processing amount of data from massive IoT devices. There is also a concern that cyberattacks will become highly advanced because of an increase in the processing capacity of IoT devices and reduction in the processing costs [16]. The advancement of new types of networks (e.g., 5G, LPWA, and wireless

networks) which connect to the architectures and devices of massive IoT is becoming diverse. This new style of connection in the new convergence environments is expected to massively expand the attack surfaces where the security threats can occur.

2.2 Security Orchestration, Automation and Response

In recent years, many companies have been adopting various security technologies, such as anti-virus software, firewalls, and intrusion detection systems [17], and implementing SIEM to detect security threats by managing and analyzing various produced logs. However, according to the 2020 Cyber Resilient Organization report from IBM, 51% of companies had no computer security incident response plan across the organization, and 53% responded that the time required for detecting and responding to cyberattacks was increasing [18]. Furthermore, according to Baker Hosteller, security experts required at least 104 days for detecting, analyzing, and notifying attacks in 2020, as opposed to 87 days before that year [19]. The frequency of security incidents occurring in organizations and companies as well as the time required for detecting, analyzing, and responding to security incidents are on the rise because the manpower and time are required to perform integrated management and analysis of heterogeneous solutions [18]. With the requirement for automation, Gartner introduced the concept of SOAR. According to Gartner, SOAR automates response processes of various threats to respond to security incidents with minimal human intervention. It is a security automation platform that helps employees to respond to advanced security threats according to the standardized work process when an incident that requires human intervention occurs. For such automated responses to security incidents, SOAR consists of Security Orchestration and Automation (SOA), Security Incident Response Platform (SIRP), and Threat Intelligence Platform (TIP) [20], which are described as follows:

- Security Orchestration and Automation (SOA): Data generated from heterogeneous security solutions are collected and the workflows between the security solutions are automated to identify monotonous and/or repetitive tasks of the security response team and reduce the time consumed on security incident response work.
- Security Incident Response Platform (SIRP): By automating the security threat response processes, tasks are assigned and managed according to the processes predetermined by the internal security incident response policy for each incident type when a security incident occurs.
- Threat Intelligence Platform (TIP): Information on threat elements is provided in association with the company's existing security systems or response solutions by performing correlation analysis on threat data collected in real-time from various sources to support the analysis work of the security threats occurring in the organization. This increases the proactive responsiveness of the security personnel.

Studies are underway on the need for SOAR to receive threat element information and facilitate the automation of security threat response systems through correlation analyses of data between heterogeneous security tools. However, there is a lack of studies on the development of a model for practically applying and managing the SOAR in convergence environments. Islam et al. [21] proposed a hierarchical architecture model consisting of (i) security tools, (ii) integration, (iii) data processing, (iv) semantic, (v) orchestration, and (vi) user interface layer to design a SOAR platform. They verified an automated incident response process by automatically integrating security technologies. However, they did not offer a comprehensive study conducted on TIP for collecting threat data and performing correlation analysis. Zheng et al. proposed security automation and orchestration framework for continuous monitoring and automatic patches of security of heterogeneous devices for reasons such

as the complexity of patch application caused by an increase in attack surfaces of massive IoT [22]. Their study requires further research in various domains, such as authentication and network security focusing on IoT system security. In addition, many companies are developing security products, as listed in Tab. 3 [23–26]. These SOAR technologies are insufficient in that they do not provide all the key functions for SOA, SIRP, and TIP, and studies on SOAR applicable to complex environments. To fill these research gaps, we propose an architecture that can efficiently apply SOAR in various environments connected with IT.

Table 3: Analysis of key functions of related works about SOAR

Related works / Key functions		[21]	[22]	[23]	[24]	[25]	[26]
SOA	Standardization of heterogeneous data		✓		✓		
	Integrating security tools	✓	✓	✓	✓	✓	✓
		✓					
	Analysis of workflow	✓		✓		✓	
SIRP	Providing the viewpoint of human intervention			✓		✓	✓
	Process automation	✓		✓	✓	✓	✓
	Response in a complex environment						
	Detecting false positive and false negative		✓				
TIP	Determination of additional threat analysis				✓		
	Threat data sharing		✓		✓		
	Threat data analysis	✓	✓		✓		

3 New Definitions

In this section, we provide the definitions of Internet of Blended Environment (IoBE) as an environment where smart factories, digital healthcare, smart grids, etc. are interconnected for efficient analysis of the complexly connected convergence environment. Blended Threat (BT) is one in which various security threats are combined throughout the vulnerable surface where security attacks can occur in IoBE. We provide a comprehensive analysis of different attack surfaces raised from each environment in IoBE along with the types of security threats raised from BT. We also define Collaborative Units of Blended Environment (CUBE) to indicate a dynamic combination of possible BT and response technologies on IoBE.

3.1 Internet of Blended Environment (IoBE)

In a convergence environment a variety of ITs, such as sensing, networking, big data, artificial intelligence (AI), and cloud are fused [27]. In such a convergence environment, the threat prone attack surfaces are on the rise because of the emergence of massive IoT. Various studies have been underway to find effective responses on these attack surfaces to prevent and respond to data corruption and forgery in the processes of the data life cycle, such as data collection, processing, and storage [28,29]. However, convergence environments, such as digital healthcare and smart grid, can be connected to each other. For example, the energy waste can be tracked through an energy consumption pattern analysis of an entire city. This is perfomred by analyzing the data from the energy management system

that monitors the energy consumption of the smart grids and the data from the power consumption monitoring system of smart buildings. In this case, various convergence environments can become very complex as each connected environment becomes more diverse.

The convergence environments, in which IoBE can be constructed, include smart factories, smart grids, and digital healthcare, as described in Tab. 4.

Table 4: Applicable area in IoBE

Environment	Description	Components of environment
Smart factory	A factory that has optimal product production processes through automation and inter-device collaboration based on ICT-based intelligent systems, logical connections for communication between heterogeneous protocols, and data analysis of sensors/equipment/facilities [30]	Distributed control system (DCS), programmable logic controller (PLC), remote terminal unit (RTU), data acquisition system (DAQ), supervisory control and data acquisition (SCADA), human-machine interface (HMI), factory energy management system (FEMS), etc.
Smart grid	A power grid that maximizes the energy consumption efficiency by monitoring and managing electricity transportation from all households by using ICT to satisfy the electricity demand of end-users [31]	Energy management system (EMS), advanced metering infrastructure (AMI), smart metering system, meter data management system (MDMS), in home display (IHD), etc.
Digital healthcare	An environment that promotes and creates values for investments in better healthcare and medical care based on the real-time collection and sophisticated analysis of data and information from all social activities as well as data regarded as health data in medical systems [32]	Electronic medical records (EMR), electric health record (EHR), personal health account (PHA), population health systems, electronic prescription, medical device data systems, software as a medical device (SaMD), wireless medical device, telemedicine, picture archiving communication system (PACS), laboratory information system (LIS), etc.

(Continued)

Table 4: Continued

Environment	Description	Components of environment
Smart building	It is a building that emerged based on the convergence of construction and ICT, and it incorporates energy-saving and eco-friendly functions that are added in a form of applying the intelligent automation concept to early period buildings. It facilitates optimal working environment and efficient management through optimal building management and pleasant office environment, etc. [33]	Video surveillance systems (VSS), closed-circuit television (CCTV), access control systems, lighting control systems, heating, ventilation and air conditioning (HVAC), fire alarm systems, integrated building management system (IBMS), etc.
C-ITS	It is a smart traffic system for sharing information and providing traffic safety services through real-time vehicle-to-vehicle and vehicle-to-road data exchanges. It is a traffic-safety-oriented system that enables proactive responses in unanticipated situations by providing real-time traffic services [34]	Eco-driving, traffic safety monitoring technique based V2X, bird-eye view, follow-me service, smart tolling system, etc.

Consequently, the data communication in the convergence environment is expected to become more complex for collecting, processing, and storing data. Fig. 1 illustrates how IoBE can interact with various convergence environments for the process of the data lifecycle. The flow of the data in IoBE is as follows:

1. Data acquisition: It refers to the process of collecting data generated from systems, such as digital healthcare, smart factory and smart grid. In data acquisition, various types of data are collected through different domains and paths, such as Digital Imaging and Communications in Medicine (DICOM) which communicates digital images of medical devices in digital healthcare.
2. Data storage: It is the process of storing the collected data at a data center. Note that data are stored in various formats.
3. Data processing: It involves processing the stored data and includes a process of converting raw data into high-level information required by services or systems. Through a process of forming and analyzing the relationships between different data, new data that can be used by the services or systems within the IoBE are created.
4. Data archive: It is the process that facilitates quick retrieval of data through the creation of metadata to consider the long-term retention of the collected and processed data.
5. Data dissemination: It is the process of disseminating or sending data to users through user interfaces. It can be used in application services, such as medical treatment and statistical analysis.

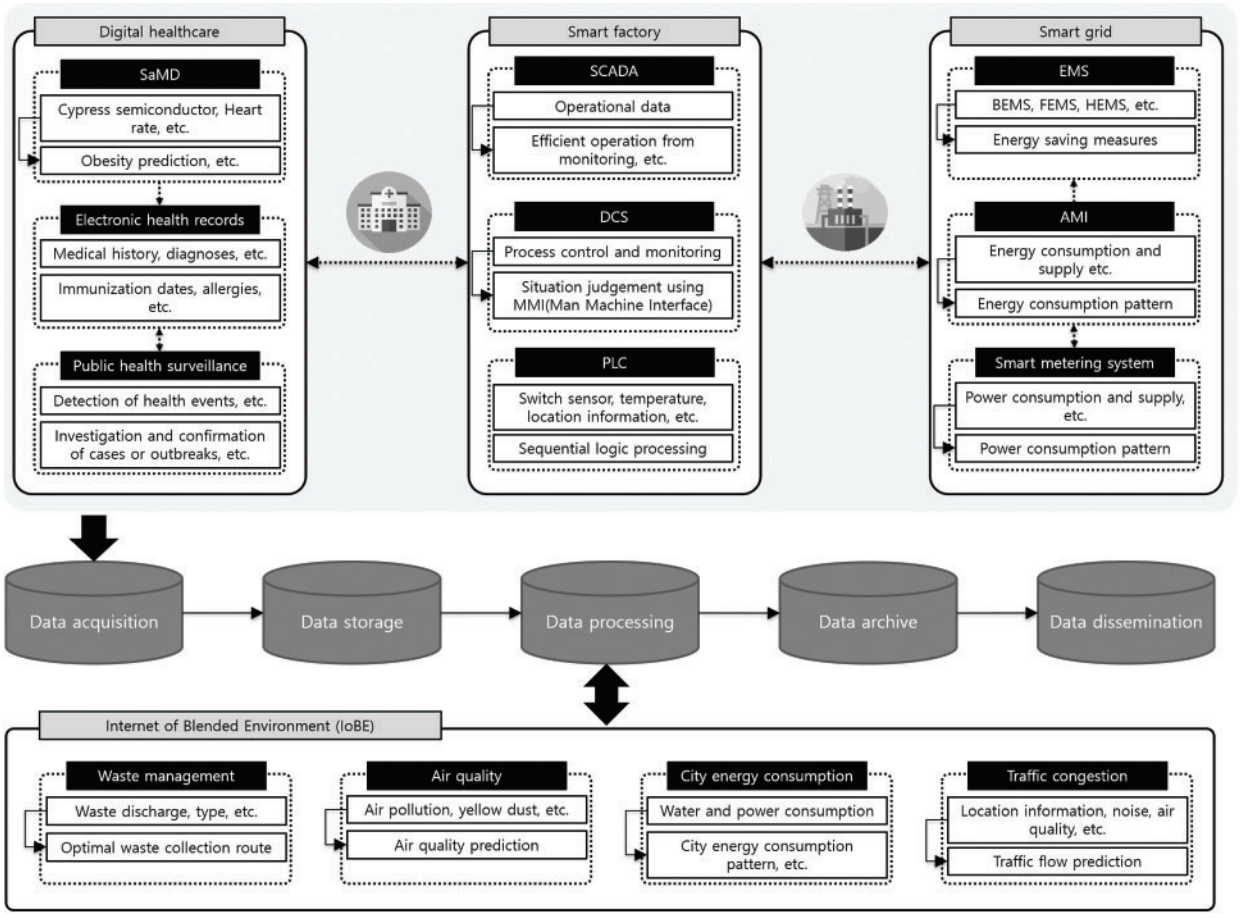

Figure 1: IoBE as an environment where a variety of IT such as sensing, networking, big data, AI, and cloud are blended

The IoBE can create a smart city environment. Furthermore, based on the technological advancement in the future, it is expected that the connections between smart cities in the IoBE will facilitate the creation of a broader smart society and smart nation.

3.2 Blended Threat (BT)

The addition of new environments to various convergence environments constiituting an IoBE is expected to cause complex security threats that exploit security vulnerabilities existing in the numerous components of the IoBE, such as device architectures, network protocols, and platforms [2,35]. Therefore, an analysis is required for the attack surfaces where security threats can be found in IoBE. Tabs. 5–9 below provide comprehensive analysis of the attack surfaces that can cause security vulnerabilities in each convergence environment of IoBE.

Table 5: Examples of attack surface in smart factory

Attack surface	Security threats	Description
Physical access	Physical damage	Devices are damaged through physical access by unauthorized persons in the factory [36,37]
	Data tampering	Normal operation settings and codes are modified using software vulnerabilities through physical interface access [36,37]
	Data breach	Work process data are acquired through mirroring based on unauthorized physical access to devices in the factory [36,37]
	Malfunction & interruption	Operation-stopping function is executed after accessing PLC through a brute force attack [36,37]
Industrial control system	Malfunction & interruption	Malfunction of the factory is triggered through SCADA after installing unauthorized software that contains malicious codes on mobile devices [37]
Factory control network	Data tampering	Modification of data such as PLC and DCS through buffer overflow attacks based on unauthorized access to the work-process network [37]
	Data breach	Stealing of processing data through RTU access using the wireless network of work processes [37]
	Malfunction & interruption	Paralysis of network resources through malicious code infection of embedded OS based on unauthorized access to the wireless network of work processes [37]
	Malicious code infection	Infection of malicious codes, such as Mirai botnet through the wireless network [37]
Factory work domain	Malfunction & interruption	Disruption through network attacks by installing unauthorized software containing malware such as worms on a work PC [38]
	Malicious code infection	Infection of ransomware in OWS, using Server Message Block (SMB) vulnerabilities after infecting a work PC with ransomware [39]
Supply chain	Data tampering	Work-process data are modified by sending modified packets to DCS after infiltrating EWS and HMI through unauthorized remote access

(Continued)

Table 5: Continued

Attack surface	Security threats	Description
	Data breach	Recipes stored in the production equipment are leaked through a USB during maintenance and repair work [37]
	Malfunction & interruption	Malfunction of equipment and control systems is triggered by infecting SCADA with a USB infected by malicious code during maintenance and repair work [37]
	Malicious code infection	A Word file attached in an e-mail of the manufacturer is executed on OWS to infect with ransomware [37]
Personnel and aging equipment	Data breach	The stored work process data are acquired by acquiring disposed equipment
	Malfunction & interruption	Service is stopped due to work overload on the MES constructed with low-end hardware
	Malicious code infection	OWS allowing Internet access is infected with malware through a visit to a phishing site

Table 6: Examples of attack surface in smart grid

Attack surface	Security threats	Description
Advanced metering infrastructure (AMI)	Data breach	Packet data are leaked through attacks such as sniffing based on AMI network access by an unauthorized person [40]
	Data tampering	AMI data are modified through man-in-the-middle attack between smart meters, AMI headend, and third-party providers [41]
	Malfunction & interruption	A large-scale power outage is triggered by manipulating smart meters or paralyzing systems through DoS attacks for major components of AMI [40]
	Malicious code infection	Malware infection using vulnerabilities of smart meters [42]
ESS	Data breach & tampering	Data are leaked and modified through man-in-the-middle attacks in the communication linkage section of ESS, DSC (Distribution substation controller), etc. [43]
	Malfunction & interruption	Malfunction and interruption through the transmission of unauthorized control commands to the ESS [44]

(Continued)

Table 6: Continued

Attack surface	Security threats	Description
EV charging system	Data breach & tampering	Data are leaked and modified through man-in-the-middle attacks in the interface communication section between the EV communication module and charging station [45]
EMS	Data breach	Breach of major information such as information related to the energy use in the system [46]
	Data tampering	Monetary damage through modification of power usage data in the EMS [47]
	Malfunction & interruption	Paralysis of system resources through DoS attack on EMS [47]
	Malicious code infection	A malicious site is connected through forged IP packets in the process of requesting a service to the supplier [47]

Table 7: Examples of attack surface in digital healthcare

Attack surface	Security threats	Description
Medical devices	Physical damage	Medical devices are damaged through physical access by an unauthorized person [48]
	Data tampering	Specific data in firmware are modified and injected into a medical device by acquiring the firmware through a debug port [48,49]
	Data breach	Data such as encryption keys are leaked through an attack when an encryption algorithm is executed for information sent from the medical device [48]
	Malfunction & interruption	Malfunction of a medical device is triggered by interfering with data detection based on a spoofing attack on a sensor, to which the authentication system is not applied [48]
	Malicious code infection	Malware infection through a USB port [48]
Medical information system	Data breach & tampering	Leakage and modification of medical data through access to the administrator account by an unauthorized person [49,50]
	Malicious code infection	Malware infection through vulnerabilities of an application linked to the medical information system [51]

(Continued)

Table 7: Continued

Attack surface	Security threats	Description
Digital healthcare network	Data tampering	Manipulation of medical information through modification of packet data between the medical information system server and clients [49]
	Data breach	Leakage of data such as personal information through collection of packets sent using the DICOM (Digital imaging and communications in medicine) protocols based on sniffing attack [50]
	Malfunction & interruption	Paralysis of medical information system through DoS attacks, such as resource exhaustion in the internal and external networks of the hospital [51]

Table 8: Examples of attack surface in smart building

Attack surface	Security threats	Description
CCTV system	Physical damage	CCTV is damaged through physical access by an unauthorized person
	Data breach	Image data are leaked through a stolen administrator account and man-in-the-middle attack [52]
	Data tampering	Image data are deleted through a stolen administrator account [52]
	Malfunction & interruption	Remote code is executed through a vulnerability attack in the CCTV terminals to use them for DDoS attacks [53]
	Malicious code infection	Malware infection through USB ports and Web interfaces [54]
Access control system	Malfunction & interruption	Remote control and interruption of the system through a stolen administrator account in the entrance control system [55]
	Unauthorized person's access	An entrance card is duplicated through data breach of the entrance card using RFID vulnerabilities [55]
HVAC	Data tampering	Remote control of smart thermometer through unauthorized access in the remote system [56]
	Data breach	Data breach through the HVAC supplier system [56]

(Continued)

Table 8: Continued

Attack surface	Security threats	Description
	Malfunction & interruption	Malfunction and interruption of HVAC through the access of an unauthorized person in the remote system [56]
Fire alarm system	Malfunction & interruption	Malfunction and interruption of fire alarm through the access of an unauthorized person in the remote system [57]
IBMS	Data tampering	Building control data are modified to abnormal data through a man-in-the-middle attack, etc. in the building network [58,59]
	Malicious code infection	Malware infection through vulnerability attack in the integrated management system [60]
	Malfunction & interruption	System malfunction in the building through a stolen administrator account of the integrated management system [58]

Table 9: Examples of attack surface in C-ITS

Attack surface	Security threats	Description
Physical access	Data breach	Leakage of data through physical stealing of hardware interface (JTAG, OBD-II) [61]
	Data tampering	Modified firmware is injected into a vehicle through a debug port
	Malfunction & interruption	Remote control of a vehicle through OCU access using OBD-II vulnerabilities [62]
Supply chain	Data breach	Leakage of data such as personal information through unauthorized access to OEM server, cloud server, etc. [63]
	Data tampering	Data modification for system diagnostic data [64]
	Malfunction & interruption	Incapacitation of vehicle updates related to safety through DoS attack on the back-end server [65]
	Malicious code infection	Ransomware infection using vulnerabilities in networks and operating systems in the supply chain [65]
Traffic control system	Data breach	Interception of data such as sensor identification data and commands, using vulnerabilities of the wireless network [66]

(Continued)

Table 9: Continued

Attack surface	Security threats	Description
	Data tampering	Firmware modification using vulnerabilities of the wireless vehicle detection system, etc. [66]
	Malfunction & interruption	Traffic signal control based on access to the signal control system by an unauthorized person [66,67]
	Malicious code infection	Ransomware infection through a phishing mail, etc. in the traffic control system [68]
V2X communication	Data tampering	Unauthorized opening and closing of a vehicle, using vulnerabilities in the wireless network [69]
	Malfunction & interruption	Malfunction of service using vulnerabilities in wireless protocols between the smart car gateway and the in-vehicle devices [70]
	Malicious code infection	Vehicle location tracking and vehicle stealing through the installation of a malicious app on the user's smartphone [69]

As attack surfaces in each convergence environment increase, additional attack surfaces may occur. As such, the complexity of security threats that currently threaten the society may also increase. The security threats are expected to increase because various components will become even more complex as new environments are added and connected to other environments in the IoBE. Furthermore, even for the same type of security threats, such as Distributed Denial of Service (DDoS) attacks and malware infection, attacks may occur through different attack surfaces and vulnerabilities depending on the environment [71]. Therefore, the BT in our context refers to the security threats that occur as various security threats are converged and combined through attack surfaces in an IoBE, as shown in Fig. 2.

Attack scenarios can be caused by blending security threats that may occur because of the connection relationship between each component in the IoBE, as shown in Tab. 10.

Table 10: Attack scenario using BT in IoBE

No	Description
1	HAN/NAN server infiltration through known vulnerabilities of protocols and end-points in the smart grid
2	Remote control of FEMS through industrial AP access of an unauthorized device
3	FEMS energy consumption forgery of smart factory or infiltration into a digital healthcare server
4	Data-stealing through vulnerabilities of the DICOM protocols
5	EMR data tampering through CT/MRI image data modification

To respond to BT, a response measure is required based on the vulnerability analysis of each component, and an analysis of the attack surfaces where cyberattacks may occur is required through the analysis of the connection relationship between the components.

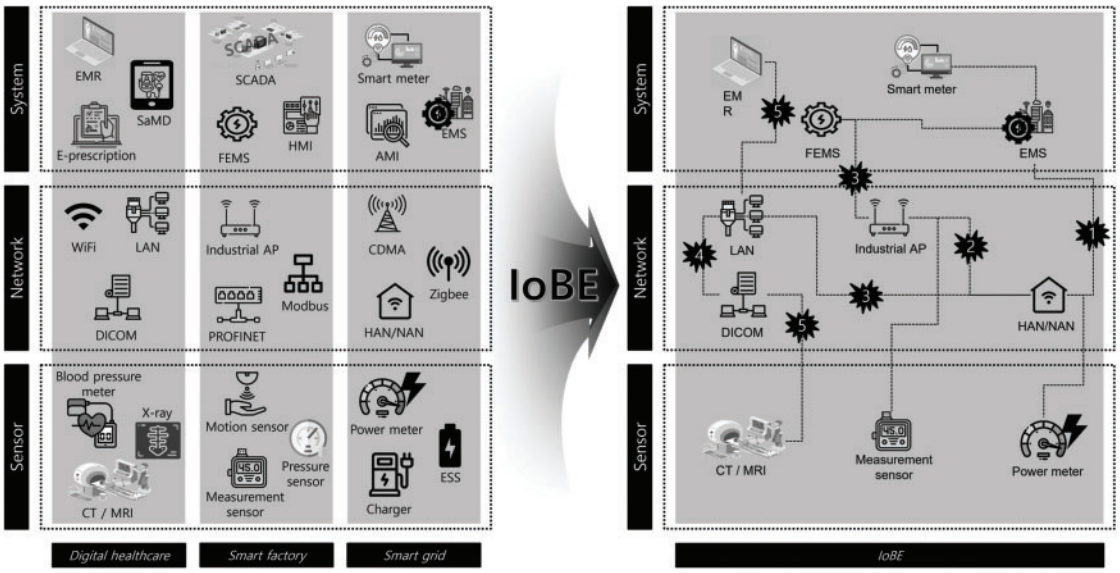

Figure 2: Blended threat in IoBE

3.3 Collaborative Units of Blended Environment (CUBE)

The data in IoBE are generated in complex environments and transmitted through multiple domains through different paths. Therefore, security threats are different for different components, such as the wireless LAN and edge network sections, and the security level required to respond to these threats is also different [72–74]. Furthermore, because new environments are combined in IoBE, the security technologies used in various environments are diverse. Therefore, automatic detection and response to cyberattacks is required to minimize the damage casued by a BT. We define a pair of security threat and response technology for each security threat as a unit to provide distributed deployment of existing security technologies for efficient responses. Although there is no security technology corresponding to the recent intelligent security threats, mitigation method has been designed to minimize damage in the event of a security threat. It can define a pair of security threat and response technology including mitigation methods for each security threats. In addition, several such units can be dynamically combined as collaborative units to respond flexibly to different BTs. In short, CUBE can be considered as a dynamic combination of possible security threats and response technologies in IoBE. The CUBE defined to respond to BT is shown in Fig. 3.

- Unit: It is a pair of security threats and mitigation technology for each security threat. For example, the response technologies include malicious mail pattern-based spam-mail blocking and unidentified-sender blocking for a security threat that disseminates e-mails such as phishing e-mails containing malicious code, for example, a worm and virus to induce the execution by users [75].
- Collaborative Units: It refers to a dynamic combination of mitigation technologies according to the cyber kill chain, which is a stage where cyber-attack occurs. The cyber kill chain stage is an attack chain, which is a path that the attacker takes to infiltrate the system to incapacitate the attacking target [76]. By modeling a BT, it is possible to appropriately mitigate appropriately to the security threat at each stage based on the hierarchical structure of the complex security threats.

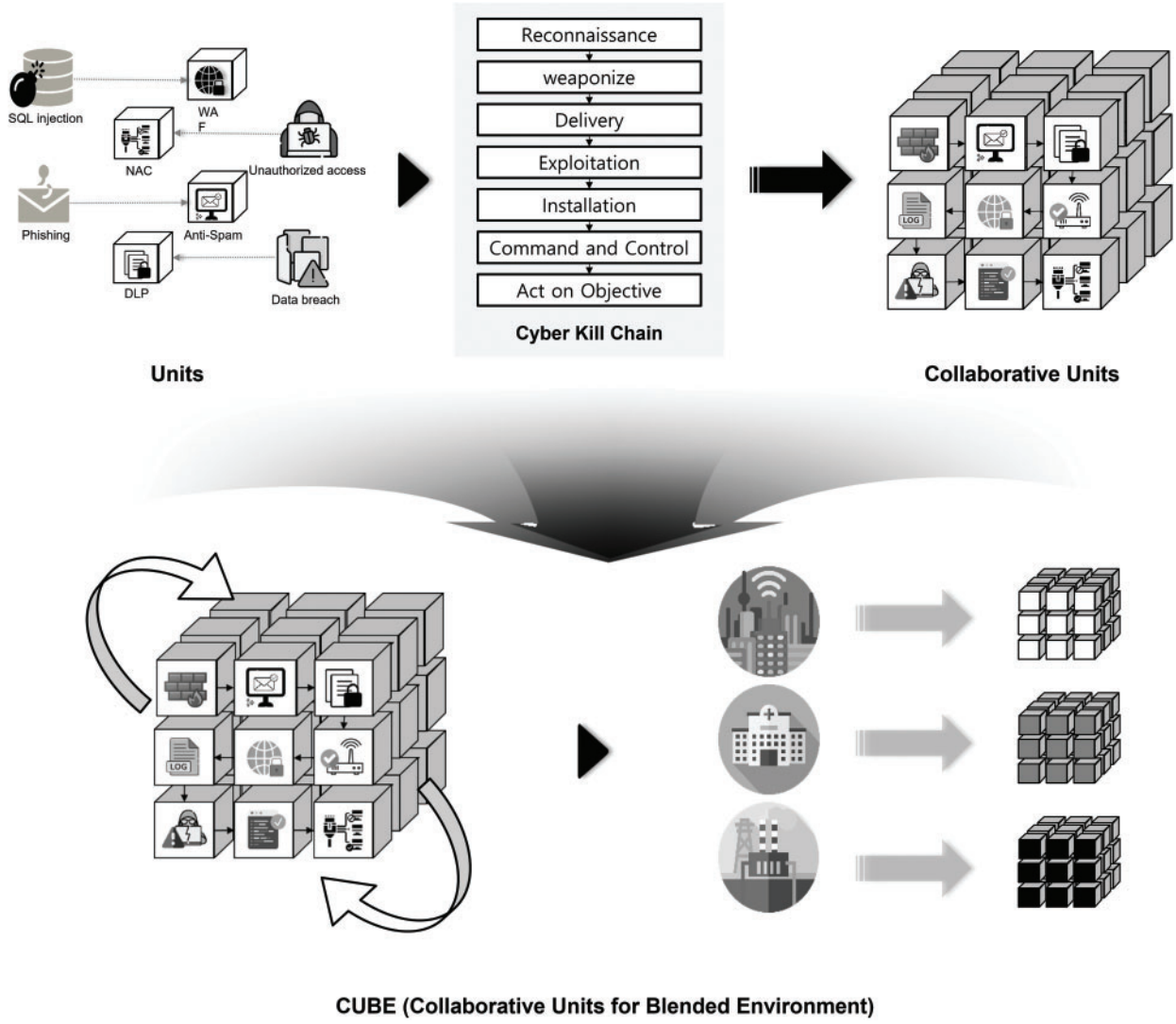

Figure 3: Definition of CUBE

- Collaborative Units for Blended Environment: It refers to a dynamic combination of possible security threats and mitigation technologies in IoBE. It can change dynamically according to different security policies and response systems in the IoBE, which is the attack target of a blended attack.

3.4 Security Orchestration and Response with Collaborative Units of Blended Environment

In this paper, we define SOAR-CUBE as an architecture that applies CUBE to SOAR. SOAR-CUBE consists of the followings components.

- Threat Intelligence Platform with Collaborative Units of Blended Environment (TIP-CUBE): This platform collects threat data based on blended attacks occurring in the IoBE and analyzes the data correlations. Therefore, the attack information such as the origin can be identified by backtracking the occurrence path of the BT through the correlations between the data.

Furthermore, the cyber-attack response time can be minimized through the BT by predicting vectors that may occur based on the linkage with existing security solutions that are used in the IoBE, i.e., the environment in which SOAR-CUBE is operated. For example, it is possible to predict BT through system connectivity within the IoBE by analyzing the components constituting the IoBE and threat intelligence to analyze security vulnerabilities that may occur in these components. In addition, a unit which comprises a pair of security threats and a mitigation technology for each security threat can be built based on the predicted BT and mitigation technologies operated by organizations or companies.

- Security Orchestration and Automation with Collaborative Units of Blended Environment (SOA-CUBE): This is the security orchestration and automation technology in CUBE. Because various security technologies corresponding to BT are dynamically combined and used in the CUBE, collaboration and linkage between various tools are required. The linkage between heterogeneous security tools is facilitated through workflow modeling that links different inputs and outputs between security tools such as security solutions and response technologies and dynamic playbook creation that informs the human intervention point based on a response system composed with a series of logics for cyber-attack response [77,78].
- Security Incident Response Platform with Collaborative Units of Blended Environment (SIRP-CUBE): This component is an automation technology of the response system in the event of cyberattacks and security incidents, such as blended attacks in an IoBE. In other words, this technology automates the mitigation technology in CUBE, which is defined as a dynamic combination of security threats and mitigation technologies. The automation of response systems can be achieved through the development of BT-type classification techniques and blended attack detection and response techniques for efficient responses through minimal human intervention in millions of security incidents occurring in various manners.

4 Conceptual Architecture

Fig. 4 illustrates the architecture of the SOAR-CUBE and the terms and components used in the architecture is described in Tab. 11. The illustration as to how SOAR-CUBE detects and responds to different BT follows.

Table 11: Components of SOAR-CUBE architecture

Environment	Description
Attacker	People who cyber attack through the attack surface on target
Database	Collection of event and log data that are structured, integrated, and managed from SOAR-CUBE
TIP-CUBE	Threat intelligence platform for responding blended threat in IoBE
SOA-CUBE	Security orchestration and automation for responding to the blended threats in IoBE
SIRP-CUBE	Security incident response platform for responding blended threat in IoBE

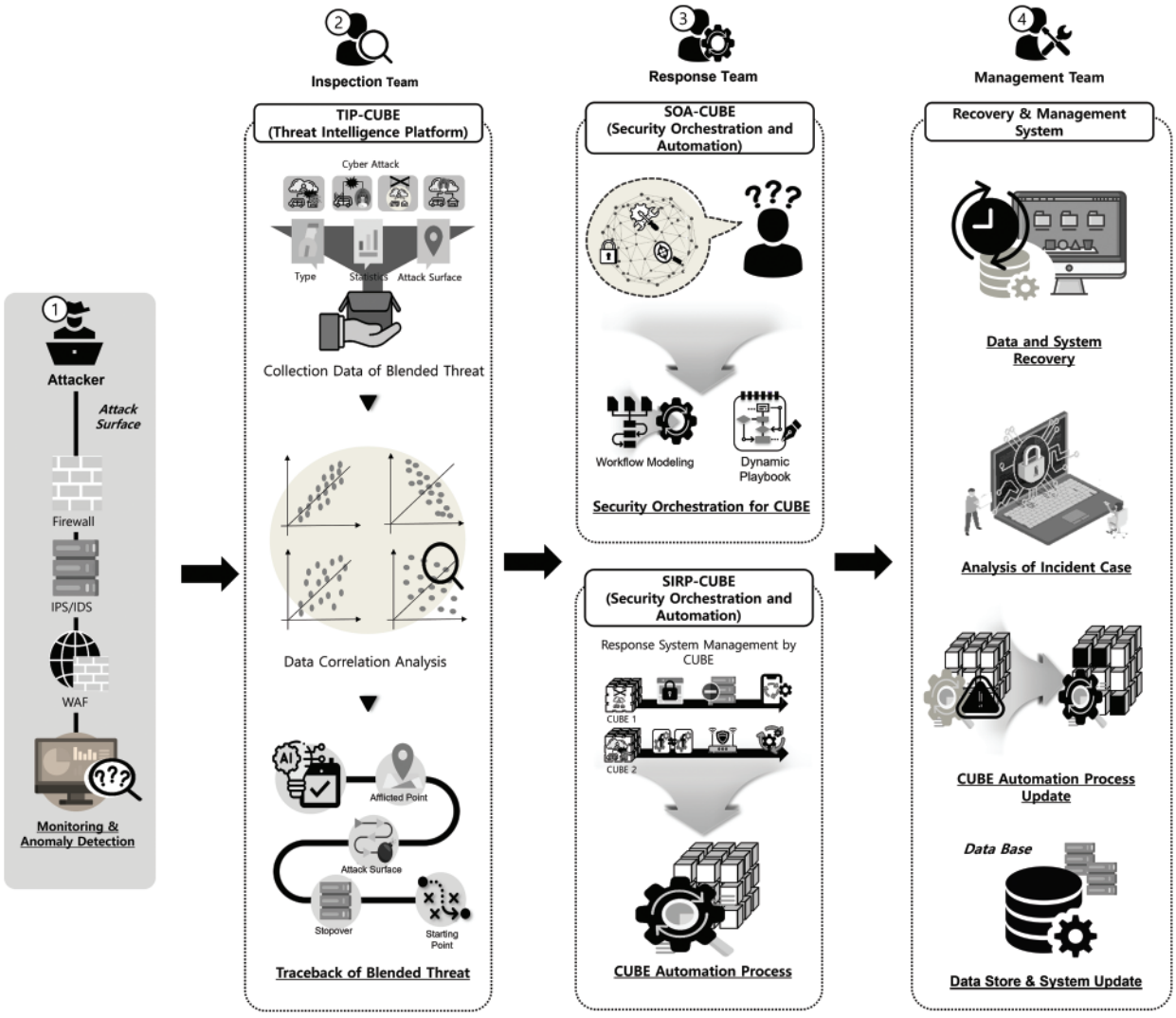

Figure 4: A conceptual architecture for SOAR-CUBE

4.1 Monitoring & Anomaly Detection (Step 1)

In this step, the attacker attempts to penetrate the SOAR-CUBE architecture-applied environment through various attack surfaces in the IoBE. The anomalies are detected using the security devices designed in advance through this process. The attack patterns mainly used in cyberattacks are defined in advance to block the attacker based on these patterns. If the attacker cannot be blocked in advance (e.g., because the blended attack bypasses the pre-defined patterns), the anomaly is detected through the analysis of data, such as security events and logs generated by security technologies constructed in the IoBE. Existing IPS/IDS or SIEM can be used in this step.

4.2 Inspection Team (Step 2)

This step is performed by the inspection team if an anomaly is detected in Step 1. The attack data produced through TIP are collected, and the threat types are classified based on the collected

data. Furthermore, the attack data can be comparatively analyzed with the open threat data of the Open Source Intelligence(OSINT) to define the intrusion indicators in advance or identify the attack patterns. If the attack pattern is difficult to be identified owing to an unknown or intelligent attack, the BT attack path can be deduced through correlation analysis of the log data in the IoBE system. In addition, no BT is detected or analyzed in the CUBE, the inspection team can generate a CUBE considering the BT based on the analysis performed by other companies or organizations through threat intelligence.

4.3 Response Team (Step 3)

This step is for protecting the assets in the IoBE via the response team after the BT analysis of Step 2 performed by the inspection team. It includes SOA-CUBE and SIRP-CUBE. The process of creating the security technology's workflow and the dynamic playbook is undergone according to the cyber-kill chain stage and attack type of the BT detected through SOA-CUBE. In SOA-CUBE, the orchestration that connects each input/output of security technology for inter-operation is required before the occurrence of the BT. Afterward, the automated response is performed according to the cyber kill chain stage via SIRP-CUBE. It includes the process of automating the simple and repetitive response according to the response system based on the dynamic playbook. Because each component environment in the IoBE is operated based on different policies, the response system can change dynamically depending on the environment applied in SIRP-CUBE.

4.4 Management Team (Step 4)

This step is for performing the maintenance and repair of SOAR-CUBE. It includes the process of recovering the damaged system and data after responding to a blended attack. In the maintenance-and-repair step, the log data generated in the SOAR-CUBE architecture are analyzed and managed to identify similar types of BT in the future. Furthermore, if the response to a blended attack is managed, it will be possible to respond more efficiently when the same attack occurs again. In this step, refactoring and geometry management are performed, including performance improvement and error correction for the existing SOAR-CUBE architecture.

5 Conclusion

Recently, various devices such as control equipment and medical devices, have been connected to networks in convergence environments. Furthermore, new platforms have been developed; this has opened up large and new attack surfaces. Different convergence environments can be interconnected to provide new services and platforms. As various convergence environments have emerged and have been connected to each other, the complexity of the attack surfaces where security threats can occur has increased. To address this security issue, we first offered the definition of IoBE as an environment in which various convergence environments are interconnected. We also defined a BT as a security threat that uses multiple security vulnerabilities through various attack surfaces in the IoBE. As the surfaces exposed to BT in the IoBE have increased, the frequency of security incidents in organizations and companies has also increased. Furthermore, manpower and time are required for integrated management and analysis of heterogeneous security solutions, thus, increasing the time consumed in detecting, analyzing, and responding to the security incidents after their occurrence. Therefore, we proposed a new concept called CUBE, which facilitates dynamic changes according to the environment applied to the IoBE by distributing and deploying security technologies for each

BT type and dynamically combining them according to the cyber kill chain stage to minimize the damage and respond efficiently to a BT.

We also proposed a SOAR-CUBE architecture to respond to security incidents with minimal human intervention by automating the BT response process. It can be used to perform modeling of a workflow that links heterogeneous security technologies and threat intelligence function that collects threat data and performs a correlation analysis of the data. Furthermore, it facilitates efficient responses to complex BTs through security orchestration, automation function, and response automation function based on the dynamic playbook creation. In the future, we plan to further study the prediction of complexly-connected data-communication paths through service and system predictions in the future environment and investigate complex attack surfaces, where cyberattacks such as data corruption and forgery, can occur in the data life cycle. Furthermore, we plan to incorporate and standardize the input-output data created or used in different security technologies (for example, firewall andIPS) to interlock them. In conclusion, we will simulate our proposed architecture in IoBE and verify that it will be efficient and accurate.

Funding Statement: This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. 2021R1A2C2011391) and was supported by the Ajou University research fund.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] World Economic Forum, "The forth industrial revolution: What it means, how to respond," 2016. [Online]. Available: https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/.

[2] H. Hejazi, H. Rajab, T. Cinkler and L. Lengyel, "Survey of platforms for massive IoT," in *2018 IEEE Int. Conf. on Future IoT Technologies*, Eger, Hungary, pp. 1–8, 2018.

[3] K. Zhang, J. Ni, K. Yang, X. Liang, J. Ren *et al.,* "Security and privacy in smart city applications: Challenges and solutions," *IEEE Communications Magazine*, vol. 55, no. 1, pp. 122–129, 2017.

[4] M. Alenezi and M. Zarour, "On the relationship between software complexity and security," *International Journal of Software Engineering & Applications*, vol. 11, no. 1, pp. 51–60, 2020.

[5] Y. Mirsky, T. Mahelr, I. Shelef and Y. Elovici, "CT-GAN: Malicious tampering of 3D medical imagery using deep learning," in *28th USENIX Security Symp.*, Berkeley, USA, pp. 461–478, 2018.

[6] M. Westerlund, "The emergence of deepfake technology: A review," *Technology Innovation Management Review*, vol. 9, no. 11, pp. 39–52, 2019.

[7] C. S. Kruse, B. Smith, H. Vanderlinden and A. Nealand, "Security techniques of the electronic health records," *Journal of Medical Systems*, vol. 41, no. 127, pp. 52, 2017.

[8] J. M. Hamamreh, H. M. Furqan and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1773–1828, 2019.

[9] Y. Wu, A. Khisti, C. Xiao, G. Caire, K. K. Wong *et al.,* "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 4, pp. 679–695, 2018.

[10] W. Lian, Z. Li, C. Guo, Z. Wei and X. Peng, "FRChain: A blockchain-based flow-rules-oriented data forwarding security scheme in SDN," *KSII Transactions on Internet and Information Systems*, vol. 15, no. 1, pp. 264–283, 2021.

[11] W. Zhang, Y. Wu, H. Xiong and Z. Qin, "Accountable attribute-based encryption with public auditing and user revocation in the personal health record system," *KSII Transactions on Internet and Information Systems*, vol. 15, no. 1, pp. 302–321, 2021.
[12] H. Jung, H. Jo and H. Lee, "UDP-based active scan for IoT security (UAIS)," *KSII Transactions on Internet and Information Systems*, vol. 15, no. 1, pp. 20–34, 2021.
[13] J. Kinyua and L. Awuah, "AI/ML in security orchestration, automation and response: Future research directions," *Intelligent Automation & Soft Computing*, vol. 28, no. 2, pp. 527–545, 2021.
[14] Northstream, "Massive IoT: Different technologies for different needs," 2017. [Online]. Available: http://mb.cision.com/Public/13353/2297600/ab77b7d4dc2b9cfa.pdf.
[15] F. Guo, F. R. Yu, H. Zhang, X. Li, H. Ji *et al.,* "Enabling massive IoT toward 6G: A comprehensive survey," *IEEE Internet of Things Journal*, vol. 8, no. 15, pp. 11897–11915, 2021.
[16] W. U. Khan, J. Liu, F. Jameel, M. T. R. Khan, S. H. Ahmed *et al.,* "Secure backscatter communications in multi-cell NOMA networks: Enabling link security for massive IoT," in *IEEE Conf. on Computer Communications Workshops*, Toronto, Canada, pp. 213–218, 2020.
[17] G. E. Avina, S. P. Gordon, R. S. Kittinger, L. Kiran and I. K. McCann, "Tailoring of cyber security technology adoption practices for operational adoption in complex organizations," 2017. [Online]. Available: https://www.osti.gov/biblio/1596209-tailoring-cyber-security-technology-adoption-practices-operational-adoption-complex-organizations.
[18] IBM, "Cyber resilient organization report 2020," 2020. [Online]. Available: https://www.ibm.com/security/digital-assets/soar/cyber-resilient-organization-report/#/.
[19] BakerHostetler, "BakerHostetler 2021 data security incident response report–disruption and transformation," 2021. [Online]. Available: https://www.bakerlaw.com/press/bakerhostetler-2021-data-security-incident-response-report-security-disruption-and-transformation.
[20] Gatner, "Market guide for security orchestration, automation and response solutions," 2020. [Online]. Available: https://www.gartner.com/en/documents/3990720/market-guide-for-security-orchestration-automation-and-r.
[21] C. Islam, M. A. Babar and S. Nepal, "A multi-vocal review of security orchestration," *ACM Computing Surveys*, vol. 52, no. 2, pp. 1–45, 2020.
[22] Y. Zheng, A. Pal, S. Abuadbba, S. R. Pokhrel and S. Nepal, "Towards IoT security automation and orchestration," in *2020 Second IEEE Int. Conf. on Trust, Privacy and Security in Intelligent Systems and Applications*, Atlanta, GA, USA, pp. 55–63, 2020.
[23] AhnLab, "AhnLab sefinity AIR," 2021. [Online]. Available: https://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?seq=29982.
[24] SecuLayer, "eyeCloudXOAR," 2021. [Online]. Available: https://www.seculayer.com/solutions/eyecloudxoar/.
[25] Fireeye, "SOAR with FireEye helix: Reduce security risk with security operations, automation and reporting," 2019. [Online]. Available: https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/helix/ds-fe-helix-soar.pdf.
[26] IBM, "IBM security SOAR platform," 2021. [Online]. Available: https://www.ibm.com/kr-ko/qradar/security-qradar-soar.
[27] C. M. Lee and H. Chang, "A study on security strategy in ICT convergence environment," *The Journal of Supercomputing*, vol. 70, no. 1, pp. 211–223, 2014.
[28] A. Sinaeepourfard, J. Garcia, X. Masip-Bruin, E. Marin-Tordera, X. Yin *et al.,* "A data lifecycle model for smart cities," in *2016 Int. Conf. on Information and Communication Technology Convergence*, Jeju, Korea, pp. 400–405, 2016.
[29] H. Daki, A. E. Hannani, A. Aqqal, A. Haidine and A. Dahbi, "Big data management in smart grid: Concepts, requirements and implementation," *Journal of Big Data*, vol. 4, no. 13, pp. 1344, 2017.
[30] B. Chen, J. Wan, L. Shu, P. Li, M. Mukherjee *et al.,* "Smart factory of industry 4.0: Key technologies, application case, and challenges," *IEEE Access*, vol. 6, pp. 6505–6519, 2017.

[31] UNECE, "Overview of activities and players in smart grids," 2015. [Online]. Available: https://unece.org/fileadmin/DAM/energy/se/pdfs/geee/News/Smart_Grids_Overview_05-19-15.pdf.
[32] WHO, "WHO guideline: Recommendations on digital interventions for health system strengthening," 2019. [Online]. Available: http://apps.who.int/iris/bitstream/handle/10665/311941/9789241550505-eng.pdf?ua=1.
[33] A. Ghaffarianhoseini, U. Beradi, H. AlWaer, S. Chang, E. Halawa *et al.,* "What is an intelligent building? Analysis of recent interpretations from an international perspective," *Architectural Science Review*, vol. 59, no. 5, pp. 338–357, 2015.
[34] European Union, A European strategy on cooperative intelligent transport systems, a milestone towards cooperative, connected and automated mobility, 2016. [Online]. Available: http://aei.pitt.edu/96134/.
[35] A. K. Alharam and W. Elmedany, "Complexity of cyber security architecture for IoT healthcare industry: A comparative study," in *5th Int. Conf. on Future Internet of Things and Cloud Workshops*, Prague, Czech Republic, pp. 246–250, 2017.
[36] Trend Micro, "Rogue robots: Testing the limits of an industrial robot's security," 2017. [Online]. Available: https://documents.trendmicro.com/assets/wp/wp-industrial-robot-security.pdf.
[37] N. Tuptuk and S. Hailes, "Security of smart manufacturing systems," *Journal of Manufacturing Systems*, vol. 47, pp. 93–106, 2018.
[38] O. Yousuf and R. N. Mir, "A survey on the internet of things security: State-of-art, architecture, issues and countermeasures," *Information and Computer Security*, vol. 27, no. 2, pp. 292–323, 2019.
[39] E. C. Thompson, "Vulnerability management," in *Designing a HIPAA-Compliant Security Operations Center*. Berkeley, CA, USA: Apress, pp. 65–92, 2020. [Online]. Available at: https://doi.org/10.1007/978-1-4842-5608-4_4.
[40] D. Grochocki, J. H. Huh, R. Berthier, R. Bobba, W. H. Sanders *et al.,* "AMI threats, intrusion detection requirements and deployment recommendations," in *IEEE Third Int. Conf. on Smart Grid Communications*, Tainan, Taiwan, pp. 395–400, 2012.
[41] A. Anwar, A. N. Mahmood and Z. Tari, "Identification of vulnerable node clusters against false data injection attack in an AMI based smart grid," *Information Systems*, vol. 53, no. 1, pp. 201–212, 2015.
[42] Y. Guo, C. Ten, S. Hu and W. W. Weaver, "Preventive maintenance for advanced metering infrastructure against malware propagation," *IEEE Transactions on Smart Grid*, vol. 7, no. 3, pp. 1314–1328, 2016.
[43] N. Kharlamova, S. Hashemi and C. Træholt, "Data-driven approaches for cyber defense of battery energy storage systems," *Energy and AI*, vol. 5, no. 4, pp. 100095–100103, 2021.
[44] J. Sun, P. Li and C. Wang, "Optimise transient control against DoS attacks on ESS by input convex neural networks in a game," *Sustainable Energy, Grids and Networks*, vol. 28, pp. 100535–100547, 2021.
[45] T. Nasr, S. Torabi, E. B. Harb, C. Fachkha and C. Assi, "Power jacking your station: In-depth security analysis of electric vehicle charging station management system," *Computer & Security*, vol. 112, no. 6, pp. 102511, 2022.
[46] A. Tang, S. Sethumadhavan and S. Stolfo, "CLKscrew: Exposing the perils of security-oblivious energy management," in *26th USENIX Security Symp.*, Vancouver, BC, Canada, pp. 1057–1074, 2017.
[47] P. Zhao, Z. Cao, D. D. Zeng, C. Gu, Z. Wang *et al.,* "Cyber-Resilient multi-energy management for complex systems," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 3, pp. 2144–2159, 2021.
[48] M. Khera, "Think like a hacker: Insights on the latest attack vectors (and security controls) for medical device applications," *Journal of Diabetes Science and Technology*, vol. 11, no. 2, pp. 207–212, 2017.
[49] A. K. Pandey, A. I. Khan, Y. B. Abushark, M. M. Alam, A. Agrawal *et al.,* "Key issues in healthcare data integrity: Analysis and recommendations," *IEEE Access*, vol. 8, pp. 40612–40628, 2020.
[50] A. H. Seh, M. Zarour, M. Alenezi, A. K. Sarkar, A. Agrawal *et al.,* "Healthcare data breaches: Insights and implications," *Healthcare*, vol. 8, no. 2, pp. 133, 2020.
[51] S. Oh, Y. Seo, E. Lee and Y. Kim, "A comprehensive survey on security and privacy for electronic health data," *Emerging Technologies in Health Informatics and Management*, vol. 18, pp. 1, 2021.
[52] S. Hong and S. Jeong, "The analysis of CCTV hacking and security countermeasure technologies: Survey," *Journal of Convergence for Information Technology*, vol. 8, no. 6, pp. 129–134, 2018.

[53] Y. Lee, N. Baik, C. Kim and C. Yang, "Study of detection method for spoofed IP against DDoS attacks," *Personal and Ubiquitous Computing*, vol. 22, no. 1, pp. 35–44, 2018.
[54] M. Shobana and S. Rathi, "IoT malware: An analysis of IoT device hijacking," *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, vol. 3, no. 5, pp. 653–662, 2018.
[55] V. Kharchenko, Y. Ponochovnyi, A. M. Q. Abdulmunem and A. Boyarchuk, "Security and availability models for smart building automation systems," *International Journal of Computing*, vol. 16, no. 4, pp. 194–202, 2017.
[56] M. Elnour, N. Meskin, K. Khan and R. Jain, "Application of data-driven attack detection framework for secure operation in smart buildings," *Sustainable Cities and Society*, vol. 69, pp. 102816–102831, 2021.
[57] H. Shin, J. Noh, D. Kim and Y. Kim, "The system that cried wolf: Sensor security analysis of wide-area smoke detectors for critical infrastructure," *ACM Transactions on Privacy and Security*, vol. 23, no. 15, pp. 1–32, 2020.
[58] R. Chan, F. Tan, U. Teo and B. Kow, "Vulnerability assessment of building management systems," in *Critical Infrastructure Protection XIV*. Cham, Switzerland: Springer, pp. 209–220, 2020. [Online]. Available at: https://doi.org/10.1007/978-3-030-62840-6_10.
[59] A. Sheikh, V. Kamuni, A. Patil, S. Wagh and N. Singh, "Cyber attack and fault identification of HVAC system in building management systems," in *Int. Conf. on Power and Energy Systems*, Perth, WA, Australia, pp. 1–6, 2019.
[60] D. Meyer, J. Haase, M. Eckert and B. Klauer, "New attack vectors for building automation and IoT," in *Annual Conf. of Industrial Electronics Society*, Beijing, China, pp. 8126–8131, 2017.
[61] F. Majéric, B. Gonzalvo and L. Bossuet, "JTAG fault injection attack," *IEEE Embedded Systems Letters*, vol. 10, no. 3, pp. 65–68, 2018.
[62] T. U. Kang, H. M. Song, S. Jeong and H. K. Kim, "Automated reverse engineering and attack for CAN using OBD-II," in *IEEE 88th Vehicular Technology Conf.*, Chicago, IL, USA, pp. 1–7, 2018.
[63] Y. T. Lee, W. Enck, H. Chen, H. Vijayakumar, N. Li *et al.,* "Polyscope: Multi-policy access control analysis to compute authorized attack operations in android systems," in *USENIX Security Symp.*, pp. 2579–2596, 2021. [Online]. Available at: https://www.usenix.org/conference/usenixsecurity21/presentation/lee-yu-tsung.
[64] S. PatweEmail and S. Phansalkar, "Blockchain-enabled IoT security in automotive supply chain," *Sustainability*, vol. 13, no. 24, pp. 13646–13668, 2021.
[65] A. Y. Ofori and C. Boachie, "Malware attack predictive analytics in a cyber supply chain context using machine learning," in *Int. Conf. on Cyber Security and Internet of Things*, Accra, Ghana, pp. 66–73, 2019.
[66] I. Pekaric, C. Sauerwein, S. Haselwanter and M. Felderer, "A taxonomy of attack mechanisms in the automotive domain," *Computer Standards & Interfaces*, vol. 7, no. 4, pp. 103539–103553, 2021.
[67] Q. A. Chen, Y. Yin, Y. Feng, Z. M. Mao and H. X. Liu, "Exposing congestion attack on emerging connected vehicle based traffic signal control," in *Network and Distributed System Security (NDSS) Symp.*, San Diego, CA, USA, pp. 1–15, 2018.
[68] M. A. Branquinho, Ransomware in industrial control systems. What comes after wannacry and petya global attacks?. in *Safety and Security Engineering VII*. Southampton, UK: WIT Press, pp. 329–334, 2018. [Online]. Available at: https://www.witpress.com/elibrary/wit-transactions-on-the-built-environment/174/36526.
[69] A. Ghosal and M. Contri, "Security issues and challenges in V2X: A survey," *Computer Networks*, vol. 169, no. 12, pp. 107093–107112, 2020.
[70] N. Lyamin, D. Kleyko, Q. Delooz and A. Vinel, "Real-time jamming DoS detection in safety-critical V2V C-ITS using data mining," *IEEE Communications Letters*, vol. 23, no. 3, pp. 442–445, 2019.
[71] B. Tushir, Y. Dalal, B. Dezfouli and Y. Liu, "A quantitative study of DDoS and E-DDoS attacks on WiFi smart home devices," *IEEE Internet of Things Journal*, vol. 8, no. 8, pp. 6282–6292, 2021.
[72] W. Chen, S. Xiao, L. Liu, X. Jiang and Z. Tang, "A DDoS attacks traceback scheme for SDN-based smart city," *Computers & Electrical Engineering*, vol. 81, pp. 106503–106514, 2020.

[73] R. Mahajan and S. Zafar, "DDoS attacks impact on data transfer in IoT-manet-based e-healthcare for tackling COVID-19," *Data Analytics and Management*, vol. 54, pp. 301–309, 2021.
[74] S. Lee, A. Abdullah, N. Jhanjhi and S. Kok, "Classification of botnet attacks in IoT smart factory using honeypot combined with machine learning," *PeerJ Computer Science*, vol. 7, no. 6, pp. 350–372, 2021.
[75] D. Xiao and M. Jiang, "Malicious mail filtering and tracing system based on KNN and improved LSTM algorithm," in *IEEE Int. Conf. on Dependable, Autonomic and Secure Computing, Int. Conf. on Pervasive Intelligence and Computing, Int. Conf. on Cloud and Big Data Computing, Int. Conf. on Cyber Science and Technology Congress*, Calgary, AB, Canada, pp. 222–229, 2020.
[76] P. N. Baharami, A. Dehghantanha, T. Dargahi, R. M. Parizi and K. K. R. Choo, "Cyber kill chain-based taxonomy of advanced persistent threat actors: Analogy of tactics, techniques, and procedures," *Journal of Information Processing Systems*, vol. 15, no. 4, pp. 865–889, 2019.
[77] S. Luo and M. B. Salem, "Orchestration of software-defined security services," in *IEEE Int. Conf. on Communications Workshops*, Kuala, Lumpur, Malaysia, pp. 436–441, 2016.
[78] C. Onwubiko and K. Ouazzane, "SOTER: A playbook for cybersecurity incident management," *IEEE Transactions on Engineering Management*, pp. 1–21, 2020. [Online]. Available at: https://doi.org/10.1109/TEM.2020.2979832.

Appendix A: A list of abbreviations

Tab. 12 is a list of abbreviations and the description of it inthe paper.

Table 12: A list of abbreviations

Abbreviations	Description
AMI	Advanced Metering Infrastructure
AI	Artificial Intelligence
AP	Access Point
BT	Blended Threat
CCTV	Closed-Circuit Television
C-ITS	Cooperative Intelligent Transport Systems
CT/MRI	Computed Tomography/Magnetic Resonance Imaging
CUBE	Collaborative Units for Blended Environment
DAQ	Data Acquisition System
DCS	Distributed Control System
DICOM	Digital Imaging and Communications in Medicine
DDoS	Distributed Denial of Service
DoS	Denial of Service
DSC	Distribution Substation Controller
EHR	Electric Health Record
EMR	Electronic Medical Records
EMS	Energy Management System
ESS	Energy Storage System
EV	Electron Volt
FEMS	Factory Energy Management System
HAN/NAN	Home Area Network/Neighborhood Area Network
HMI	Human-Machine Interface
HVAC	Heating, Ventilation and Air Conditioning

(Continued)

Table 12: Continued

Abbreviations	Description
IBMS	Integrated Building Management System
ICT	Information and Communication Technology
IDS	Instruction Detection Systems
IHD	In Home Display
IoBE	Internet of Blended Environment
IoT	Internet of Things
IPS	Instruction Prevention Systems
IT	Internet Technology
JTAG	Joint Test Action Group
LAN	Local Area Network
LIS	Laboratory Information System
LPWA	Low-Power Wide-Area
MDMS	Meter Data Management System
MES	Manufacturing Execution System
OBD	On-Board Diagnostics
OCU	On-Board Connectivity Unit
OEM	Original Equipment Manufacture
OSINT	Open Source Intelligence
OWS	Operator Workstation
PACS	Picture Archiving Communication System
PHA	Personal Health Account
PLC	Programmable Logic Controller
RFID	Radio-Frequency Identification
RTU	Remote Terminal Unit
SaMD	Software as a Medical Device
SCADA	Supervisory Control and Data Acquisition
SIEM	Security Information and Events Management
SIRP	Security Incident Response Platform
SMB	Sever Message Block
SOA	Security Orchestration and Automation
SOAR	Security Orchestration, Automation and Response
SIRP-CUBE	Security Incident Response Platform with Collaborative Units for Blended Environment
SOAR-CUBE	Security Orchestration, Automation and Response with Collaborative Units of Blended Environment
TIP	Threat Intelligence Platform
USB	Universal Serial Bus
V2X	Vehicle to Everything
VSS	Video Surveillance System