Intelligent Automation
& Soft Computing

Tech Science Press

DOI: 10.32604/iasc.2023.040019
Article

Design the IoT Botnet Defense Process for Cybersecurity in Smart City

Donghyun Kim[1], Seungho Jeon[2], Jiho Shin[3] and Jung Taek Seo[4,*]

[1]Department of Information Security, Gachon University, Seongnam, 13120, Korea
[2]Department of Smart Security, Gachon University, Seongnam, 13120, Korea
[3]Police Science Institute, Korean National Police University, Asan, 31539, Korea
[4]Department of Computer Engineering, Gachon University, Seongnam, 13120, Korea
*Corresponding Author: Jung Taek Seo. Email: seojt@gachon.ac.kr

Received: 28 February 2023; Accepted: 18 May 2023; Published: 11 September 2023

Abstract: The smart city comprises various infrastructures, including healthcare, transportation, manufacturing, and energy. A smart city's Internet of Things (IoT) environment constitutes a massive IoT environment encompassing numerous devices. As many devices are installed, managing security for the entire IoT device ecosystem becomes challenging, and attack vectors accessible to attackers increase. However, these devices often have low power and specifications, lacking the same security features as general Information Technology (IT) systems, making them susceptible to cyberattacks. This vulnerability is particularly concerning in smart cities, where IoT devices are connected to essential support systems such as healthcare and transportation. Disruptions can lead to significant human and property damage. One representative attack that exploits IoT device vulnerabilities is the Distributed Denial of Service (DDoS) attack by forming an IoT botnet. In a smart city environment, the formation of IoT botnets can lead to extensive denial-of-service attacks, compromising the availability of services rendered by the city. Moreover, the same IoT devices are typically employed across various infrastructures within a smart city, making them potentially vulnerable to similar attacks. This paper addresses this problem by designing a defense process to effectively respond to IoT botnet attacks in smart city environments. The proposed defense process leverages the defense techniques of the MITRE D3FEND framework to mitigate the propagation of IoT botnets and support rapid and integrated decision-making by security personnel, enabling an immediate response.

Keywords: Smart city; IoT botnet; cybersecurity

1 Introduction

Smart cities aim to achieve sustainable urban development and high quality of life by applying information and communication technologies (ICT) in urban settings [1]. Smart cities gather data through on-site sensors and the IoT to provide users with timely services in real-time. The IoT environment of a smart city constitutes a massive IoT environment encompassing numerous devices. As many devices are installed, managing security for the entire IoT device ecosystem becomes challenging, and attack vectors accessible to attackers increase [2]. Most IoT devices have low power and specifications, lacking the same security functions as general IT systems, rendering them more susceptible to cyberattacks than IT systems [3]. It has been demonstrated that IoT devices without basic security measures are vulnerable to threats due to open remote connection ports, low firmware versions, and plaintext data transmission [3]. These vulnerabilities can also apply to IoT devices installed in smart cities. Consequently, IoT devices installed in smart cities are exposed to cyber threats [4].

A smart city comprises various infrastructures, including healthcare, transportation, manufacturing, and energy. In each infrastructure, identical IoT devices are employed to deliver services, and these devices are likely to implement uniform security measures. This exposes attackers to potentially exploit the same vulnerability to attack target all IoT devices. A representative attack leveraging these weaknesses is a DDoS attack by forming an IoT botnet [5]. A smart city constitutes a large-scale IoT environment encompassing many IoT devices. The formation of IoT botnets within this massive IoT environment can precipitate extensive denial-of-service attacks, compromising the availability of services rendered by smart cities. Services within smart cities are intimately connected to fundamental support systems, such as healthcare and transportation. Consequently, disruptions in these services may result in significant human and property damages [6,7].

Although studies have proposed IoT security models, processes, and architectures, few studies target smart city environments to counter these security threats. Also, among the MITRE frameworks, few studies utilize defense specific D3FEND.

Various infrastructures, such as healthcare, transportation, manufacturing, and energy, exist in smart cities. The numerous infrastructures of smart cities comprise massive IoT environments with many IoT devices. The same defensive techniques should be applied to numerous IoT devices in smart cities. However, each infrastructure may have different levels of defense techniques due to factors such as varying security workforce capabilities and headcount. This may result in delayed decision-making to respond to IoT botnets. As IoT botnets scale, their damage becomes more significant, necessitating prompt responses. In this paper, we design a defense process that can respond to IoT botnets in a smart city environment through the MITRE framework. The process can support quick and unified decision-making by network and security personnel in each infrastructure. The contributions of this paper are:

- Threat analysis of IoT botnets in a smart city environment through the examination of existing distributed IoT botnets.
- Designing an IoT botnet defense process in a smart city environment through the MITRE framework to support quick and unified decision-making by security personnel.
- Comparative analysis of existing IoT botnet response and designed defense process.

This paper is organized as follows: Section 2 discusses related research and background, Section 3 analyzes existing IoT botnets, Section 4 designs a defense process specific to IoT botnets using the MITRE framework, Section 5 evaluates the defense process, and Section 6 concludes the paper.

2 Background and Related Work

2.1 Smart City Architecture and Components

In the study by Haque et al. [8], the smart city hierarchy was classified into four distinct types. These encompassed the layer responsible for data collection through sensors and IoT devices deployed in the field, the layer facilitating data transmission to the upper layer, the layer handling data processing and management, and finally, the layer delivering services based on the outcomes derived from the lower layer.

In the study by Jameel et al. [9], the prevailing state of modern smart cities was analyzed, and the smart city framework was divided into three types. These consisted of the application layer providing data as the top layer, the network layer connecting the bottom and top layers, and the sensory layer collecting data.

In the study by Lee et al., the main components of a smart city were identified by dividing them into major devices, systems, and networks. The cyber vulnerabilities of the identified components were closely examined to analyze possible attack scenarios and ripple effects.

Based on the analysis of the aforementioned studies, the most suitable architecture for this paper was deemed the four-layer architecture proposed by Haque et al. These layers comprise a data collection layer using field-installed sensors and IoT devices, a data transmission layer, a data processing and management layer, and a service provision layer based on the results from the lower layer. The detailed description of each layer is as follows:

- Sensing Layer: The Sensing Layer collects data through IoT devices, such as illuminance, humidity, temperature, and camera sensors. Data collection in smart cities is crucial for decision-making and automation in providing services; thus, enhancing the data collection vector improves the quality of services offered by smart cities.
- Transmission Layer: The Transmission Layer transmits data collected by sensors and IoT devices using communication technologies like Wireless Fidelity (Wi-Fi), 4G/Long-Term Evolution, and 5G.
- Data Management Layer: The Data Management Layer processes and manages collected data, performing tasks such as editing and merging to provide services. Artificial Intelligence (AI) technology can be utilized for efficient data processing, and since a large volume of data is generated from various infrastructures, adequate storage space is needed.
- Application Layer: The Application Layer delivers necessary services in various smart city infrastructures using the data processed and analyzed in the previous layer.

Fig. 1 shows the components analyzed in the research of [5,8–10], and the four layers classified by Bahalul Haque and two others.

2.2 Analysis of MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK)

The MITRE ATT&CK is a knowledge base containing information on attacker tactics and techniques derived from real-world data and accessible to everyone [11]. The MITRE ATT&CK framework provides detailed insights into cyberattacks and threat actors. It analyzes attack information from the Tactics, Techniques, and Procedures (TTP) perspective and presents it in a matrix form [12]. Moreover, ATT&CK offers information on attack tactics, techniques, and methods for detecting and mitigating these techniques. Attack modeling techniques, such as MITRE ATT&CK, deliver visual cyberattack representation options that aid decision-making for security experts and non-experts [13]. This framework categorizes attack tactics and techniques into Enterprise, Mobile, and Industrial

Control System (ICS) domains. The Enterprise domain represents attack tactics and techniques for common IT systems, including Windows, Linux, and networks. As IoT devices employ Operating Systems (OS) like embedded Linux and Windows 10 IoT, they can leverage attack information from the Enterprise domain. It comprises 14 tactics, 193 attack techniques, and 401 detailed attack techniques, making it easier to identify specific attack information. The attack tactics in the Enterprise domain can be divided into those executed before and after attacks. The tactics performed before the attack encompass all tactics from the onset of the attack, excluding Reconnaissance and Resource Development. Initial Access refers to a method for an attacker to access initial assets. Execution represents a method for an attacker to execute malware to perform malicious actions in the accessed system. Upon malware execution, tactics such as Defense evasion, Privilege escalation, and Persistence are performed. The attack can then propagate to other systems through the Lateral Movement tactic. Lastly, Impact is a tactic that damages availability and integrity, such as system destruction, service interruption, and data tampering. Table 1 describes the attack tactics featured in the MITRE ATT&CK's Enterprise domain.

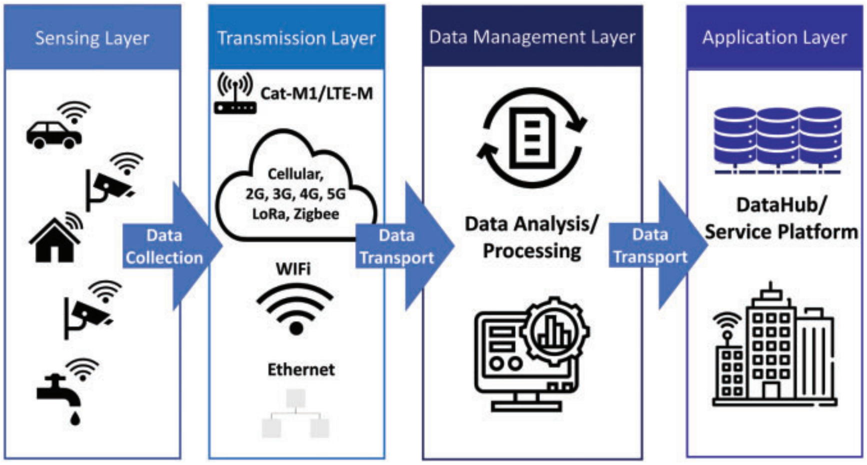

Figure 1: Smart city architecture and components

Table 1: MITRE ATT&CK tactic description

Tactic	Description
Reconnaissance	Information gathering for attack execution
Resource development	Developing resources to conduct an attack
Initial access	System initial access tactics
Execution	Malware execution tactics
Persistence	Tactics for continuing malicious behavior
Privilege escalation	Elevate the attacker's privileges for malicious behavior
Defense evasion	Tactics to evade detection of malicious behavior
Credential access	Credential theft
Discovery	Gathering intrusion system and network information
Lateral movement	Peripheral system access through network discovery

(Continued)

Table 1 (continued)

Tactic	Description
Collection	Collecting arbitrary data that attackers want
Command and control (C&C)	Perform malicious behavior through the server communication
Exfiltration	Stealing data collected and generated by the system
Impact	Manipulating, interrupting, and destroying system data

2.3 Analysis of MITRE Detection, Denial, and Disruption Framework Empowering Network Defense (D3FEND)

The MITRE D3FEND was developed in 2021 as a knowledge graph containing information about defender tactics and techniques [14]. While ATT&CK focuses on offensive strategies, D3FEND emphasizes defense, defining a set of defensive techniques that can be employed when designing and implementing security components. It aims to articulate the defense phases against cyberattacks and continues to evolve by incorporating new defensive tactics and techniques. D3FEND aligns with ATT&CK's attack tactics and techniques, supporting a comprehensive understanding of offense and defense [15]. By utilizing both frameworks in tandem, one can enhance their understanding of attack techniques and tactics and establish effective defense strategies to counteract them. This facilitates easier sharing of threat-related information within and across infrastructures and enables the coordination of defensive operations [16]. Furthermore, it simplifies user implementation by providing detailed descriptions and implementation methods for defensive technologies. Given these advantages, D3FEND can be employed for developing and optimizing integrated security strategies and processes in environments divided into various infrastructures, such as smart cities. Defensive tactics are actions to achieve specific defensive objectives and are categorized into five groups. D3FEND provides five defense tactics and 521 artifacts that can identify 177 defense techniques and attacks. Table 2 below presents MITRE D3FEND's current defensive tactics and descriptions.

Table 2: MITRE D3FEND tactic description

Tactic	Description
Model	Used to apply security engineering, vulnerability, threat, and risk analysis to digital systems
Harden	A tactic is performed before the system is activated to increase the attacker's attack cost
Detection	Identify malicious and unauthorized access to your network
Isolate	Prevent access by creating logical and physical barriers to the system
Deceive	Decoy tactics for collecting attacker information and accessing ships
Evict	Tactics to eliminate attackers from the network

2.4 Related Work

A study by Pichan et al., designed and proposed a forensic architecture capable of addressing cyberattacks on many IoT devices [17]. This research summarizes IoT device forensic challenges and defines requirements for conducting forensics. In order to tackle issues arising during forensics on numerous IoT devices, an event logging and data collection framework for IoT devices in a cloud environment is proposed. The study's scope encompasses event logging and data collection. Utilizing the IoT device forensic requirements and framework established in this study, basic parameters for IoT devices can be secured, and difficulties arising from existing heterogeneity in forensics can be overcome.

A study by Dietz et al., proposed a method to inhibit the proliferation of IoT botnets from countering large-scale cyberattacks executed through IoT botnets [18]. The suggested method prevents IoT botnet attacks by initially scanning vulnerable IoT devices and isolating them on the network through routers to which the IoT devices are connected. The proposed method is restricted to a smart home network and requires a connection to an IoT device in an access router. Nevertheless, it has the advantage of considering using heterogeneous IoT devices and utilizing Common Vulnerabilities and Exposure (CVE) for vulnerability scanning. Devices identified as vulnerable during scans are automatically quarantined by updating rules in the router's internal firewall.

A study by Mashaleh et al. introduced a methodology to prevent DDoS attacks by quickly detecting IoT botnets using machine learning [19]. This research divides IoT botnet processes into scanning, propagating, and attacking to prevent DDoS attacks. The proposed methodology involves collecting network packets, sampling to reduce data volume, and extracting features through preprocessing. Machine learning is employed by classifying the extracted features into three types of IoT botnet operations. Ultimately, the machine learning outcomes are delivered to security personnel, enabling them to quickly detect IoT network attacks and mitigate their spread.

A study by Akbar et al., matched related attack and defense techniques from the ATT&CK and D3FEND frameworks [20]. To accomplish this objective, the description texts of techniques supplied by the ATT&CK and D3FEND frameworks serve as datasets. Through Natural Language Processing (NLP), the association between attack and defense techniques is derived. This process ranks defense techniques that can counterattack techniques and presents a list to security personnel. The ranked list supports prompt decision-making, as security officers only need to select from the provided defense technique list.

In a study by Aghamohammadpour et al., a threat-hunting system is designed based on the Department of Defense Architecture Framework (DODAF). Threat hunting involves internal security personnel detecting and addressing inherent system threats before an attack occurs. This paper employs the MITRE ATT&CK and D3FEND frameworks for efficient and systematic threat hunting. It demonstrates how to configure a threat-hunting system within the DODAF framework and describes the functioning of each system component. MITRE D3FEND's five tactics are divided into Hunting Awareness and Hunting Action in the threat-hunting process. The study showcases the designed framework's applicability through actual WannaCry ransomware and Hydra malware cases.

Previous research has explored security frameworks, architectures, and methodologies for addressing attacks on IoT devices. However, these studies did not include the smart city environment within their scope or offer a method for determining a quick and unified defense technique. This paper designs an effective defense process using MITRE D3FEND to counter IoT botnets in smart cities. The standardized defense techniques of MITRE D3FEND facilitate a quick and unified response for security personnel across various infrastructures.

3 Analysis of the IoT Botnet Phase

The IoT bot scans the network, and upon discovering a vulnerable device, it initiates an intrusion process [21]. An IoT botnet refers to a network of devices infected by these bots [21]. The objectives of IoT botnets vary depending on the attacker but generally involve malicious actions such as DDoS attacks, data exfiltration, and cybercrimes like cryptocurrency mining and terrorism. Although various IoT botnets have been developed, they use similar formation processes, including device intrusion and propagation. In this section, we analyze the formation process of IoT botnets and identify possible security threats to smart cities caused by IoT botnets.

3.1 Vulnerable IoT Device Scan and Intrusion

IoT bots must compromise IoT devices to execute malicious actions desired by attackers, such as DDoS attacks. One must scan the network to identify reachable IoT devices to achieve this. Once an IoT device's accessibility is verified, various intrusion methods can be employed. Generally, IoT botnets infiltrate by performing dictionary attacks and brute-force attacks based on weak security accounts, such as default accounts. Alternatively, they exploit vulnerabilities in applications and software used by IoT devices, including buffer overflow and Remote Command Execution (RCE). IoT devices deployed in each smart city infrastructure often use identical passwords or have minor variations, making it easy for an attacker to steal account information or infiltrate if known beforehand. Moreover, the same IoT device will also possess the corresponding vulnerability if a vulnerability is discovered in commonly used software and applications.

3.2 C&C

In an IoT botnet, the C&C server is an attacker's central point to issue commands and control infected IoT devices. The C&C of an IoT botnet can be divided into a centralized structure and a Peer-to-Peer (P2P) structure [21]. The centralized structure communicates exclusively with the central server using protocols such as IRC and HTTP. In contrast, the P2P structure employs the P2P protocol, enabling peer communication rather than relying on a central server. With these characteristics, attacks in the centralized structure can be blocked by merely blocking the central server. However, blocking attacks in the P2P structure is challenging due to the absence of a central server. After the IoT bot infiltrates an IoT device, it attempts to connect to the C&C server to communicate with the attacker. If the connection to the C&C server fails, the bot may continuously try to reconnect. IoT bots that fail to connect to the C&C server will likely struggle to execute malicious actions, such as data theft and DDoS attacks. If the IoT device successfully connects to the C&C server, the attacker can install malware and issue commands for activities like DDoS attacks and information collection. Attackers can monitor the botnet's size through the C&C server and issue attack commands to IoT devices based on the size.

3.3 Propagation

Propagation is a significant characteristic of IoT botnets, enabling them to infect other devices with malware to increase their scale. Attackers prioritize expanding IoT botnets, as a larger botnet size makes it easier to achieve specific objectives and enhances its performance as an attack platform. Generally, propagation employs the same method as IoT device intrusion. The attacker continuously searches for IoT devices with the same vulnerability based on the initially infected IoT device. IoT devices installed in smart city infrastructure typically have the same security strength. Due to these characteristics, when an IoT botnet discovers and exploits a vulnerability in one IoT device within a smart city environment, it becomes highly efficient in scanning and infiltrating devices with the same vulnerability.

3.4 Attack of Action

When a large-scale IoT botnet is formed, an attacker can execute malicious actions for specific purposes. Generally, large-scale IoT botnets are created and employed for DDoS attacks, aiming at a particular server or service by transmitting massive network traffic, thus impairing availability. However, cyberattacks utilizing IoT botnets evolve, and malicious actions may vary according to trends. For example, personal information stolen through IoT botnets and videos gathered via Digital Video Record systems (DVR) can be sold on the dark web. Furthermore, with the increasing value of cryptocurrencies, large-scale IoT botnets can be leveraged for cryptocurrency mining [22,23].

3.5 IoT Botnet Threat in Smart City

It can infiltrate IoT botnet if an attacker can access the smart city's network and identify and access the installed IoT device. Attacks targeting IoT devices installed in smart city infrastructure are very advantageous to attackers. A previously deployed IoT botnet must continually seek out IoT devices with vulnerabilities pre-set by attackers. However, the IoT devices used in each infrastructure in a smart city are the same and use the same security measures. If the attack succeeds on one device, it is relatively easy to form an IoT botnet. This is because, like existing IoT botnets, the time to scan devices with the same vulnerabilities for propagation to form a large-scale botnet is drastically reduced. Furthermore, the massive IoT environment can be exploited as a powerful attack platform. This can generate massive traffic than DDoS attacks using existing IoT botnets, which can threaten the availability of services provided by smart cities.

4 Propose Defense Process

In this section, we design a defense process based on the MITRE D3FEND framework to counteract IoT botnets that infect IoT devices in smart city environments with malware. To achieve this, we extract relevant logs to identify attacks on IoT devices and associate these logs with MITRE ATT&CK's attack techniques to aid security personnel in detecting attacks. Finally, we design a defense process capable of responding to IoT botnets by integrating MITRE ATT&CK and D3FEND. At each step of the defense process, appropriate defensive techniques can be chosen using the MITRE D3FEND framework.

Logs are gathered from IoT devices installed in the smart city, and the collected logs are mapped to MITRE ATT&CK's attack techniques. ATT&CK's attack techniques, which are linked to logs, are then associated with D3FEND's defense techniques. Through this approach, the defense process can be tailored as an effective countermeasure against the attack techniques employed by IoT botnets. Fig. 2 depicts a schematic representation of the interconnection between logs, attack techniques, and countermeasure techniques.

4.1 Mapping the Log to MITRE ATT&CK

In this section, we classify the malicious action of IoT botnets analyzed in Section 3 using MITRE ATT&CK and examine the logs required to detect the categorized attack techniques. IoT devices installed in smart cities constitute a Massive IoT environment, and the data generated and collected by administrators is limited. Moreover, IoT devices are generally accessed only for management purposes. Consequently, if access-related logs, such as remote user access and Universal Serial Bus

(USB) connections, are gathered from the IoT device, an attacker's intrusion can be suspected. Based on this assumption, we consider all access to IoT devices as potential attacks. This approach enables responses to zero-day vulnerabilities without signatures. Previous research has shown that logs are generated even for zero-day attacks such as RCE [24]. Since the data generated by IoT devices is limited, attack detection is possible by predefining a threshold for logs [25].

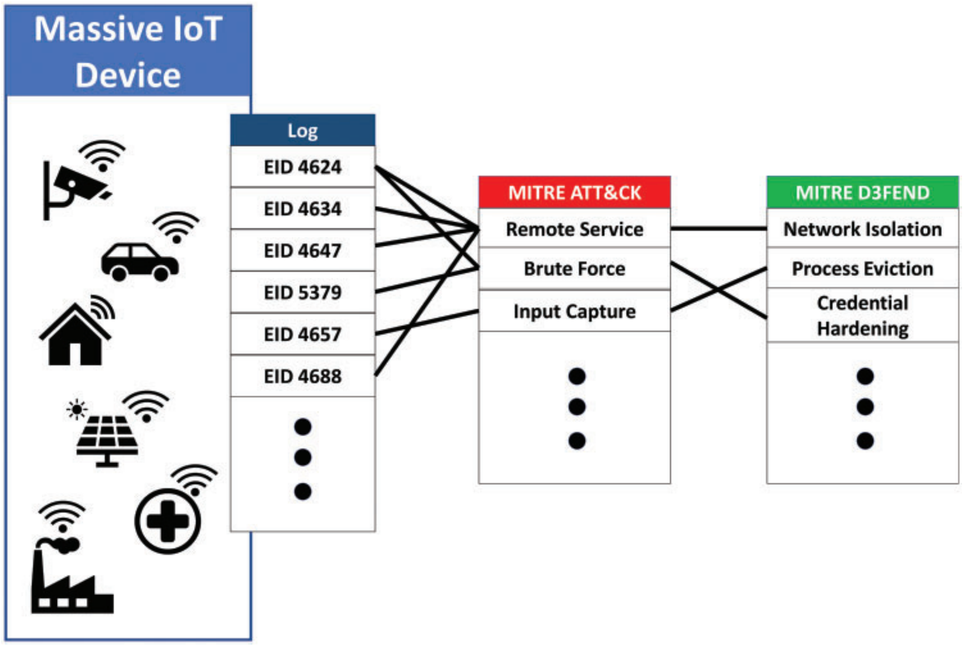

Figure 2: Mapping attack defensive techniques using logs

This paper focuses on mapping Sysmon logs available in Windows and Linux OS. Sysmon logs identify malicious or unusual activity and log how intruders and malware behave on the network [26]. When detecting an attacker's access through network data, Sysmon logs can address the challenge of detection difficulties due to issues such as encryption [27]. In this approach, the logs generated at each step of the IoT botnet can be mapped to the MITRE ATT&CK attack techniques. The rationale for mapping logs and ATT&CK attack techniques is that the log collection targets are IoT devices in a smart city. Smart city infrastructures encompass Massive IoT environments with numerous IoT devices. Additionally, due to heterogeneous hardware or software used in IoT devices, attack identification can be challenging even when data is collected [17]. Utilizing MITRE ATT&CK attack techniques can resolve this problem by simplifying attack identification in logs [28]. In a smart city's Massive IoT environment, focusing on specific events and logs rather than all logs minimizes the effect on resources such as battery life and storage capacity of IoT devices. It is recommended that security personnel from each infrastructure manually map specific events and logs to ATT&CK's attack techniques and derive a common set. The same log can be mapped to multiple attack techniques during the mapping process, but attack techniques can be distinguished based on log creation time.

4.2 Process Design with D3FEND

A smart city is a Massive IoT environment that includes various infrastructures such as medical care, transportation, energy, and manufacturing. The same defense techniques must be applied when an attack occurs on the numerous IoT devices installed in a smart city. Each infrastructure may have different defense techniques determined due to problems such as different security workforce capabilities and personnel. In this section, based on MITRE D3FEND, we design a defense process that can support the quick decision of a unified defense technique by security personnel limited to the IoT botnet. The defense process isolates IoT devices, starting with access identification. At the same time as being isolated, additional data is collected through honeypots, and so on, and when sufficient data is collected, the malware is removed. Finally, the process is terminated by identifying the cause of successful malware infection through the log and removing it. Fig. 3 shows the overall defense process designed.

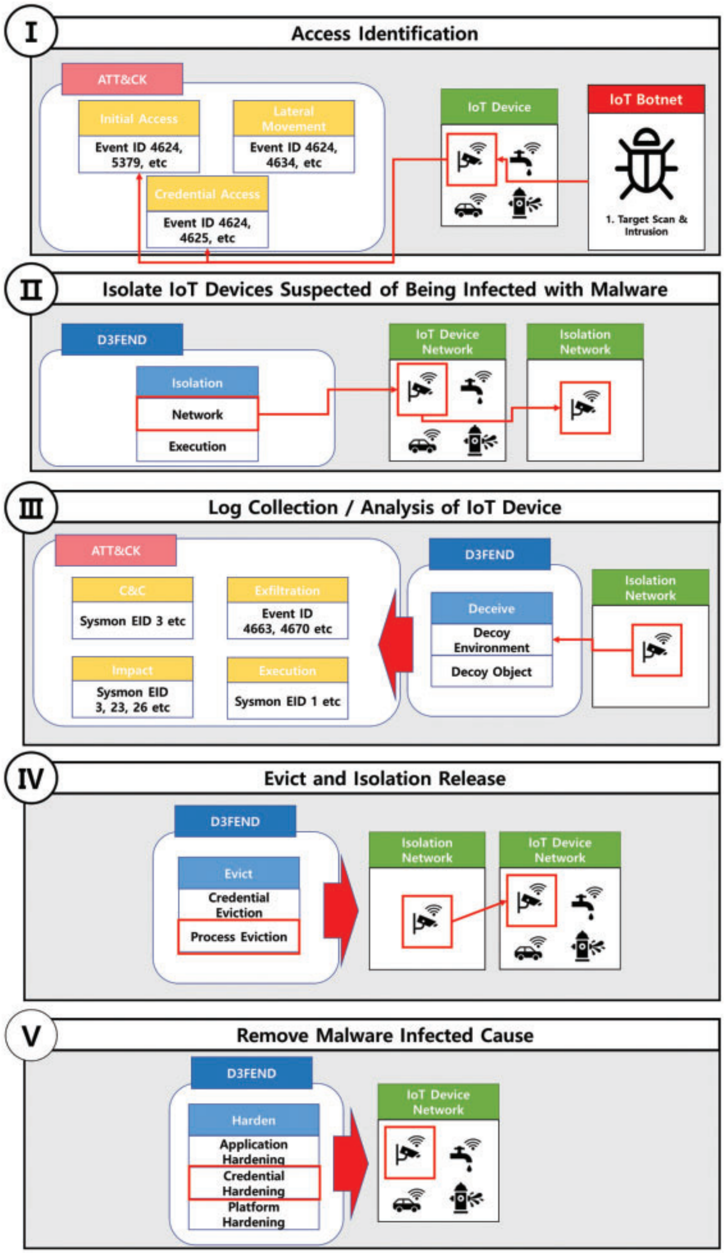

Figure 3: The flow of the designed defense process

4.2.1 Access Identification

The defense process commences by identifying the attacker's access, which can be accomplished by examining the log generated during the IoT device intrusion process [17,28,29]. Agents can be installed on IoT devices to collect logs, which should generate real-time event logs, such as Sysmon Logs. Since data generated by each IoT device in smart city infrastructures is limited, and users generally have no access, logs are not created under normal circumstances. This spares IoT devices from incurring storage capacity, memory usage, and energy consumption issues. Assuming all access to IoT devices is an attack can prevent false negatives, and a normal user's access is sufficiently identifiable in a later step.

4.2.2 Isolate IoT Device Suspected of Being Infected with Malware

The second step of the defense process isolates IoT devices suspected of being accessed by attackers. This step aims to prevent the spread of damage by halting attackers from propagating malware to other IoT devices through isolation. MITRE D3FEND's isolation comprises Network isolation and Execution isolation, which can prevent propagation, a significant characteristic of IoT botnets. Isolation facilitates additional tasks, such as collecting data and removing malware [18,30,31]. The quarantined IoT device can be released from isolation if it is identified as a normal user in a subsequent process step. Determining normal users and attackers occurs in 3 steps in the defense process. Even if the IoT device is isolated from the network, it must provide normal service to the user at this step.

4.2.3 Log Collection and Analysis of IoT Devices

Step 3 of the defense process involves monitoring isolated IoT devices for a certain period. Logs and data generated during this monitoring are collected and analyzed to identify attackers. If an attacker intrudes, they will sequentially execute attack techniques to establish an IoT botnet. Pre-selecting a threshold for logs generated during the attack process enables the distinction between normal users and attackers. The IoT botnet's attack tactics performed after intrusion include Privilege escalation, Defense evasion, Lateral movement, Impact, C&C, and Execution, as classified by MITRE ATT&CK's attack tactics. MITRE D3FEND's Deceive tactic is suitable for collecting data on these attack tactics. A honeypot technique corresponding to the Deceive tactic can effectively collect data, identify specific behaviors and variants [7,32,33], and virtually masquerade as IoT devices to collect data. Existing IoT botnets do not use Defense evasion tactics. However, the monitoring time should be specified considering Virtualization/Sandbox evasion among the Defense evasion attack techniques as the attack continues to evolve. Collecting data and logs can determine whether attackers have access and whether IoT devices are infected with malware. Moreover, it can be used to remove malware and strengthen the security of IoT devices.

4.2.4 Evict and Isolation Release

Step 4 of the defense process involves removing malicious elements from IoT devices determined to be infected by malware. Malicious elements comprise elements used for malicious actions, such as accounts created by attackers, installed malware, and tools. Malicious elements are identified and removed using the logs collected in the third step of the defense process. Among MITRE D3FEND's defense tactics, Evict removes malicious elements through countermeasures such as terminating malicious processes and locking accounts. Such malicious elements can be removed by applying Anti-virus (AV).

4.2.5 Removal Malware of Infected Cause

Step 5 of the defense process is removing the source of malware infection. The logs collected in the previous step are utilized. In the first step, the log of the attack technique used to access the IoT device can be checked. In the third step, the log of the attack technique performed to propagate to other devices can be examined. The cause of malware infection is identified through logs collected at each step. The cause of malware infection is removed by applying a defense technique corresponding to MITRE D3FEND's Harden defense tactic. For example, if a vulnerable account is the source of infection with malware, a strong defense policy is applied to the account information (Identifier/Password) to prevent a BruteForce/Dictionary Attack [34]. If software vulnerabilities cause malware infection, the cause is eliminated by updating the software to the latest version.

5 Evaluation and Analysis

This section assesses the IoT botnet defense process in the smart city environment designed in this paper. The designed process supports security personnel in smart city infrastructures to quickly determine a unified defense technique limited to IoT botnets based on MITRE D3FEND. It is challenging to verify the designed process through experiments; hence, the evaluation proceeds in two directions. The Qualitative Study compares and analyzes existing studies to evaluate whether it is possible to appropriately defend against the security threat of the IoT botnet in the smart city environment. The Case Study analyzes the attack phase of an actual IoT botnet case and assesses whether the proposed process can respond appropriately. The case study examples utilize the Mirai Botnet and the Mozi Botnet. This is a representative example of a centralized structure and a P2P structure.

5.1 Qualitative Study

This section compares the previously proposed IoT device security method with the defense process designed in this paper. For comparison, we identified four requirements from existing research and the defense process designed in this paper. Firstly, we checked whether a method to prevent propagation, the main feature of the botnet, is proposed. A total of two studies, including this paper, included the response to radio waves, the most significant characteristic of IoT botnets, in the scope of research [18]. Secondly, we checked whether the attacker suggested a method to remove the possible cause of IoT device intrusion. A total of two studies, including this paper, considered infection source removal methods to prevent the re-infection of IoT botnets [16]. Thirdly, we checked whether the heterogeneity of the IoT device is considered. Since the heterogeneity problem becomes more serious in a massive IoT environment such as a smart city, it is necessary to consider this when applying a defense process to a smart city. A total of two studies, including this paper, considered the heterogeneity problem in data collection from IoT devices [17]. We made sure to provide a variety of defense techniques. Cyberattacks have many variables, so it is necessary to consider various defense techniques applicable to one attack technique. A total of two studies, including this paper, considered these issues [16,20]. Finally, it was confirmed that defense technique decision-making was supported by users in a rapid and unified manner. It was confirmed that the research using D3FEND, including the proposed defense process, supported it. A total of three studies, including this paper, considered these issues [16,20]. However, the defense process proposed in this paper is limited to the smart city environment and the IoT botnet, so it has a limitation in that it is difficult to respond to all kinds of cyberattacks. Additionally, the manual mapping of specific events, logs, and ATT&CK performed to identify attacks is limited in that it is affected by the subjective standards of security personnel. Securing objectivity for attack identification through additional research is necessary to overcome these limitations. Table 3 compares the previously proposed IoT device security method and the defense process designed in this paper.

Table 3: A case comparison study

Category	[16]	[17]	[18]	[19]	[20]	Proposal Defense Process
Removal cause of infection	O	X	X	X	X	O
Prevention of propagating	X	X	O	X	X	O
Consider IoT heterogeneity	X	O	X	X	X	O
Offers a variety of defense techniques	O	X	X	X	O	O
Quick and unified defense technique decision support	O	X	X	X	O	O

5.2 *Case Study: Mirai Botnet*

The Mirai bot, first distributed in 2016, infected IoT devices with malware by conducting dictionary attacks through remote access protocols such as Secure Shell (SSH) or Telnet [35,36]. The infected devices continued propagating to adjacent devices to form a botnet, ultimately launching a DDoS attack that took down approximately 1,200 servers [35,36]. The Mirai bot can be considered the progenitor of currently distributing IoT bots. This is because most bots are distributed after the Mirai bot's source code is released its code. Mirai bot targets all IoT devices that utilize the Linux OS and has an open Telnet port. Initially, the Mirai bot infected IoT devices using the Linux OS. However, it has since expanded its attack targets to include multiple OS, demonstrating the potential for large-scale cyberattacks using IoT devices. The Mirai botnet formation phases are as follows:

1. Target Scan: Generate a random IP address and check for active Telnet services using ports 23 and 2323.
2. Intrusion: Execute a dictionary attack on the Telnet service based on pre-set default credentials.
3. C&C: Download and run additional malware using IoT device architecture information.
4. Propagation: Upon transmitting the infection status to the reporting server, the IoT devices scan vulnerable IoT devices on the network and propagate the malware accordingly.
5. DDoS attack: When an attack command is received via C&C, execute a DDoS attack using the received attack option.

The first step verifies whether a pre-mapped log is generated using D3FEND's detection tactic. If the log is generated, the defense process proceeds to the second step, isolating the IoT device that generated the log to another network. The third step determines whether the Mirai bot has infected the device using the collected log upon monitoring. If an infection is confirmed, proceed to the fourth step to remove the malware and lift the isolate on the network. Finally, eliminate the cause of malware infection by strengthening the account through the log identified in the first step. This defense process enables response to a Mirai bot. Security personnel in smart cities can determine techniques at isolated timing—furthermore, time to share defense techniques with other infrastructure. Table 4 below provides examples of elements utilized at each step of the designed defense process to counter the Mirai bot.

Table 4: Example of application of Mirai bot defense technique through the defense process

Defense process	Mirai Botnet Phase	Sysmon Log	MITRE ATT&CK techniques	D3FEND tactics	D3FEND technique
1	Intrusion	Event ID 3	Brute Force	Detection	Script Execution Analysis Etc.
2	C&C propagation attack	Event ID 1 Event ID 3	Ingress tool transfer Exploitation of remote services Network denial of service	Isolate	DNS allowlisting DNS denylisting broadcast domain isolation Etc.
3	C&C propagation	Event ID 1 Event ID 3 Event ID 11 Event ID 22	Brute Force Exploit public-facing application	Deceive	Connected honeypot Decoy file Decoy network resource Etc.
4	C&C propagation attack	Event ID 1 Event ID 3	Brute Force Exploit public-facing application	Evict	Process termination Account locking
5	-	Event ID 3	Brute force Exploit public-facing application	Harden	Strong password policy software

5.3 Case Study: Mozi Botnet

The Mozi bot is a botnet that uses networks such as BitTorrent to infect IoT devices, such as network gateways and digital video recorders [37,38]. Mozi reused the source code of the previously distributed Gafgyt bot [37,38]. The Mozi bot is a P2P botnet composed of nodes passing through a Distributed Hash Table (DHT). It is also difficult to track since it disguises itself as general traffic passing through DHT. In addition, Mozi bot's IoT device intrusion method can be divided into two types. If the Telnet's remote port is open, a dictionary attack is performed, and if the dictionary attack fails, it employs the vulnerability of a specific IoT device to infiltrate. If the intrusion is successful, malicious actions, such as DDoS attacks and data leakages, will be executed. The formation phases of the Mozi botnet are as follows:

1. Target Scan: Identify the attack target (IoT device) using Transmission Control Protocol (TCP) Synchronization (SYN) Reply.
2. Intrusion: Perform a dictionary attack on the telnet port or infiltrate the IoT device through HTTP command injection.
3. Load: Connects to a pre-specified server, then downloads and executes malware to perform actual malicious actions.
4. C&C: After registering the P2P network, periodically checks the P2P network to update the list of nearby nodes and the configuration file.
5. Propagation: Continuous propagation through device scanning and intrusion processes.
6. Attack: Receive an attacker's command and perform an attack based on the received command.

The first step checks whether a pre-mapped log is generated through D3FEND's detection tactic. Depending on whether the log is generated, the defense process goes to the second step, and the IoT device that generated the log is isolated to another network. If the quarantine is performed, it goes to the third step, and it is determined whether the Mozi bot is infected through the generated log. If it is determined that the Mozi bot has infected it, proceed to the fourth step to remove the malware, and release the isolate of the IoT device. Finally, remove the cause of malware infection by strengthening the account through the log identified in the first step. Mozi bot has a P2P structure, and unlike a centralized structure, it communicates with multiple devices and performs malicious actions such as radio waves and DDoS attacks. Botnets using this P2P structure can also be prevented from propagating by performing an isolation Step immediately after collecting logs. Security personnel in smart cities can determine techniques at isolated timing—furthermore, time to share defense techniques with other infrastructure. Table 5 below shows examples of logs used to counter the Mozi bot through the designed defense process, attack techniques of MITRE ATT&CK, and defense techniques of D3FEND.

Table 5: Example of application of Mozi bot defense technique through defense process

Defense process	Mozi Botnet phase	Sysmon log	MITRE ATT&CK technique	D3FEND tactic	D3FEND technique
1	Intrusion	Event ID 3	Brute force Exploitation of remote services	Detection	Remote terminal session detection Etc.

(Continued)

Table 5 (continued)

Defense process	Mozi Botnet phase	Sysmon log	MITRE ATT&CK technique	D3FEND tactic	D3FEND technique
2	Load C&C Propagation	Event ID 1 Event ID 3	Ingress tool transfer Exploitation of remote services Network denial of service	Isolate	DNS allowlisting DNS denylisting broadcast domain isolation Etc.
3	Load C&C propagation	Event ID 1 Event ID 3 Event ID 8 Event ID 11 Event ID 22	Brute force Exploit public-facing application	Deceive	Connected honeypot Decoy file Decoy network resource Etc.
4	C&C propagation attack	Event ID 1 Event ID 3	Brute Force Exploit public-facing application	Evict	Process termination Account locking
5	-	Event ID 3	Brute force Exploit public-facing application	Harden	Strong password policy software Software update

6 Conclusion

The same IoT devices will likely be employed in each smart city's infrastructure, and the same security measures will be implemented to provide a single service. This commonality may create potential vulnerabilities that attackers can exploit, emphasizing the need for robust and adaptive security strategies to protect smart city infrastructures. This paper designs a defense process to effectively respond to IoT botnet attacks that may arise due to these characteristics of smart cities. Previous research on IoT botnet defense has not considered the smart city environment and does not support rapid and integrated decision-making by security personnel. Furthermore, prior research has yet to utilize D3FEND to address IoT botnets. In this paper, to specialize in IoT botnets, we analyzed existing IoT botnets and designed the defense process through the defense techniques of D3FEND. The propagation of IoT botnets can be mitigated by using designed defense processes. In addition, even if an IoT botnet attack occurs in various smart city infrastructures, the defense process supports rapid and unified decision-making, enabling an immediate response. However, the proposed defense process is limited to IoT botnets. The process of mapping specific events, logs, and ATT&CK may be influenced by the subjective standards of security personnel, resulting in potential inaccuracies. In future research, we aim to employ machine learning technology to automatically map specific events and logs of IoT devices installed in smart cities to ATT&CK attack techniques and automate defense technique decisions for each attack technique. By doing so, we hope to contribute to the cyber safety of smart cities and the future urban landscape.

Acknowledgement: This study was revised and supplemented from a paper presented at the 6th International Symposium on Mobile Internet Security (MobiSec' 22) conference.

Funding Statement: This work was supported by Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korea government (MSIT) (No. 2021-0-00493, 5G Massive Next Generation Cyber Attack Deception Technology Development, 60%) & this work was supported by Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korea government (MSIT) (No. 2021-0-01806, Development of Security by Design and Security Management Technology in Smart Factory, 30%) & this work was supported by the Gachon University Research Fund of 2023 (GCU-202106330001%, 10%).

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

References

[1] Y. Lim, J. Edelenbos and A. Gianoli, "Dynamics in the governance of smart cities: Insights from South Korean smart cities," *International Journal of Urban Sciences*, vol. 27, no. 1, pp. 183–205, 2023.

[2] R. Kitchin and M. Dodge, "The (in)security of smart cities: Vulnerabilities, risks, mitigation, and prevention," *Smart Cities and Innovative Urban Technologies*, vol. 26, no. 2, pp. 47–65, 2020.

[3] C. Kolias, A. Stavrou, J. Voas, I. Bojanova and R. Kuhn, "Learning Internet-of-Things security 'Hands-on'," *IEEE Security & Privacy*, vol. 14, no. 1, pp. 37–46, 2016.

[4] Y. Mehmood, F. Ahmad, I. Yaqoob, A. Adnane, M. Imran *et al.,* "Internet-of-Things-based smart cities: Recent advances and challenges," *IEEE Communications Magazine*, vol. 55, no. 9, pp. 16–24, 2017.

[5] J. Lee, J. Kim and J. Seo, "Cyber attack scenarios on smart city and their ripple effects," in *Proc. 2019 Int. Conf. on Platform Technology and Service (PlatCon)*, Jeju, Korea (South), pp. 1–5, 2019.

[6] S. K. Gupta, S. Vanjale, S. Rasal and M. Vanjale, "Securing IoT devices in smart city environments," in *Proc. of 2020 Int. Conf. on Emerging Smart Computing and Informatics (ESCI)*, Pune, India, pp. 119–123, 2020.

[7] S. S. Chakkaravarthy, D. Sangeetha, M. V. Cruz, V. Vaidehi and B. Raman, "Design of intrusion detection honeypot using social leopard algorithm to detect IoT ransomware attacks," *IEEE Access*, vol. 8, pp. 169944–169956, 2020.

[8] A. K. M. Haque, B. Bhushan and G. Dhiman, "Conceptualizing smart city applications: Requirements, architecture, security issues, and emerging trends," *Expert Systems*, vol. 39, no. 5, pp. 1–23, 2022.

[9] T. Jameel, R. Ali and S. Ali, "Security in modern smart cities: An information technology perspective," in *Proc. 2019 2nd Int. Conf. on Communication, Computing and Digital Systems (C-CODE)*, Islamabad, Pakistan, pp. 293–298, 2019.

[10] M. M. Rashid, J. Kamruzzaman, M. M. Hassan, T. Imam and S. Gordon, "Cyberattacks detection in IoT-based smart city applications using machine learning techniques," *International Journal of Environmental Research and Public Health*, vol. 17, no. 24, pp. 9347, 2020.

[11] The MITRE Corporation, "MITRE ATT&CK," The MITRE Corporation, 2016. [Online]. Available: https://attack.mitre.org/

[12] K. Kim, Y. Shin, J. Lee and K. Lee, "Automatically attributing mobile threat actors by vectorized ATT&CK matrix and paired indicator," *Sensors*, vol. 21, no. 19, pp. 6522, 2021.

[13] H. S. Lallie, K. Debattista and J. Bal, "An empirical evaluation of the effectiveness of attack graphs and fault trees in cyber-attack perception," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 5, pp. 1110–1122, 2017.

[14] The MITRE Corporation, "MITRE D3FEND," The MITRE Corporation, 2021. [Online]. Available: https://d3fend.mitre.org/

[15] R. Kumar, R. Kela, S. Singh and R. Trujillo-Rasua, "Apt attacks on industrial control systems: A tale of three incidents," *International Journal of Critical Infrastructure Protection*, vol. 37, pp. 100521, 2022.

[16] A. Aghamohammadpour, E. Mahdipour and I. Attarzadeh, "Architecting threat hunting system based on the DODAF framework," *The Journal of Supercomputing*, vol. 79, no. 4, pp. 4215–4242, 2023.

[17] A. Pichan, M. Lazarescu and S. T. Soh, "A logging model for enabling digital forensics in iot, in an inter-connected iot, cloud eco-systems," in *Proc. of 2020 Fourth World Conf. on Smart Trends in Systems, Security and Sustainability (WorldS4)*, London, UK, pp. 478–483, 2020.

[18] C. Dietz, R. L. Castro, J. Steinberger, C. Wilczak, M. Antzek *et al.,* "IoT-botnet detection and isolation by access routers," in *Proc. of 2018 9th Int. Conf. on the Network of the Future (NOF)*, Poznan, Poland, pp. 88–95, 2018.

[19] A. S. Mashaleh, N. F. B. Ibrahim, M. Alauthman and A. Almomani, "A proposed framework for early detection IoT botnet," in *Proc. of 2022 Int. Arab Conf. on Information Technology (ACIT)*, Abu Dhabi, United Arab Emirates, pp. 1–7, 2022.

[20] K. A. Akbar, S. M. Halim, Y. Hu, A. Singhal, L. Khan *et al.,* "Knowledge mining in cybersecurity: From attack to defense," in *Proc. of Data and Applications Security and Privacy XXXVI: 36th Annual IFIP WG 11.3 Conf.*, Newark, NJ, USA, pp. 110–122, 2022.

[21] S. Dange and M. Chatterjee, "IoT botnet: The largest threat to the IoT network," in *Proc. of Data Communication and Networks*, Singapore, pp. 137–157, 2019.

[22] C. U. O. Kumar and P. R. K. S. Bhama, "Detecting and confronting flash attacks from IoT botnets," *The Journal of Supercomputing*, vol. 75, no. 12, pp. 8312–8338, 2019.

[23] A. Borys, A. Kamruzzaman, H. N. Thakur, J. C. Brickley, M. L. Ali *et al.,* "An evaluation of IoT DDoS cryptojacking malware and Mirai botnet," in *Proc. of 2022 IEEE World AI IoT Congress (AIIoT)*, Seattle, WA, USA, pp. 725–729, 2022.

[24] C. Smiliotopoulos, K. Barmpatsalou and G. Kambourakis, "Revisiting the detection of lateral movement through Sysmon," *Applied Sciences*, vol. 12, no. 15, pp. 7746, 2021.

[25] S. Eswaran, A. Srinivasan and P. Honnavalli, "A threshold-based, real-time analysis in early detection of endpoint anomalies using SIEM expertise," *Network Security*, vol. 2021, no. 4, pp. 7–16, 2021.

[26] Microsoft, "Sysmon-windows sysinternals microsoft docs," 2023.

[27] V. Mavroeidis and A. Jøsang, "Data-driven threat hunting using sysmon," in *Proc. of the 2nd Int. Conf. on Cryptography, Security and Privacy*, New York, NY, USA, pp. 82–88, 2018.

[28] C. Liu, A. Singhal and D. Wijesekera, "Forensic analysis of advanced persistent threat attacks in cloud environments," in *Proc. of Advances in Digital Forensics XVI: 16th IFIP WG 11.9 Int. Conf.*, New Delhi, India, pp. 161–180, 2020.

[29] M. S. Gaur, S. Kumar, N. K. Gaur and P. S. Sharma, "Persuasive factors and weakness for security vulnerabilities in big IOT data in healthcare solution," in *Proc. of 3rd Int. Conf. on Computational & Experimental Methods in Mechanical Engineering (ICCEMME)*, Uttar Pradesh, India, pp. 012046, 2021.

[30] F. Hategekimana, T. J. Whitaker, M. J. H. Pantho and C. Bobda, "IoT device security through dynamic hardware isolation with cloud-based update," *Journal of Systems Architecture*, vol. 109, pp. 101827, 2020.

[31] T. Manish, "Mitigating threats in IoT network using device isolation," M.S. Dissertation, Aalto University, Finland, 2018.

[32] R. Vishwakarma and A. K. Jain, "A honeypot with machine learning based detection framework for defending IoT based botnet DDoS attacks," in *Proc. of 2019 3rd Int. Conf. on Trends in Electronics and Informatics (ICOEI)*, Tirunelveli, India, pp. 1019–1024, 2019.

[33] Y. M. P. Pa, S. Suzuki, K. Yoshioka, T. Matsumoto, T. Kasama *et al.,* "IoTPOT: A novel honeypot for revealing current IoT threats," *Journal of Information Processing*, vol. 24, no. 3, pp. 522–533, 2016.

[34] C. Frank, C. Nance, S. Jarocki and W. E. Pauli, "Protecting IoT from Mirai botnets; IoT device hardening," *Journal of Information Systems Applied Research*, vol. 11, no. 2, pp. 33–44, 2018.

[35] J. A. Jerkins, "Motivating a market or regulatory solution to IoT insecurity with the Mirai botnet code," in *Proc. of 2017 IEEE 7th Annual Computing and Communication Workshop and Conf. (CCWC)*, Las Vegas, NV, USA, pp. 1–5, 2017.

[36] H. Sinanović and S. Mrdovic, "Analysis of Mirai malicious software," in *Proc. of 2017 25th Int. Conf. on Software, Telecommunications and Computer Networks (SoftCOM)*, Split, Croatia, pp. 1–5, 2017.

[37] T. F. Tu, J. W. Qin, H. Zhang, M. Chen, T. Xu *et al.,* "A comprehensive study of Mozi botnet," *International Journal of Intelligent Systems*, vol. 37, no. 10, pp. 6877–6908, 2022.

[38] J. Sahota and N. Vlajic, "Mozi IoT malware and its botnets: From theory to real-world observations," in *Proc. of 2021 Int. Conf. on Computational Science and Computational Intelligence (CSCI)*, Las Vegas, NV, USA, pp. 698–703, 2021.