electronics

Article

Digital Forensics for E-IoT Devices in Smart Cities

Minju Kim [1] and Taeshik Shon [2,*]

[1] Department of Artificial Intelligence Convergence Network, Ajou University, Suwon 16499, Republic of Korea; klklkl098@ajou.ac.kr
[2] Department of Cybersecurity, Ajou University, Suwon 16499, Republic of Korea
* Correspondence: tsshon@ajou.ac.kr

Abstract: With the global expansion of urban infrastructure and development of 5G communication technology, advanced information and communications technology has been applied to power systems and the use of smart grids has increased. Smart grid systems collect energy data using Internet-of-Things (IoT) devices, such as data concentrator units (DCUs) and smart meters, to effectively manage energy. Services and functions for energy management are being incorporated into home IoT devices. In this paper, the IoT for energy management in smart cities and smart homes is referred to as the E-IoT. Systems that use the E-IoT can efficiently manage data, but they present many potential security threats, because the E-IoT devices in such homes and enterprises are networked for energy management. Therefore, in this study, to identify vulnerabilities in the E-IoT device systems, digital forensics is applied to the E-IoT device systems. E-IoT devices supplied to Korean power systems were used to build a digital forensic test bed similar to actual E-IoT environments. For digital forensics application, E-IoT data acquisition and analysis methodology was proposed. The proposed methodology consisted of three methods—network packet data analysis, hardware interface analysis, and mobile device paired with E-IoT—which were applied to a DCU, smart meter, smart plug, smart heat controller, smart microwave, and smart monitoring system. On analyzing the user and system data acquired, artifacts such as the device name and energy consumption were derived. User accounts and passwords and energy-usage logs were obtained, indicating the possibility of leakage of personal information and the vulnerabilities of E-IoT devices.

Keywords: E-IoT forensics; smart cities; digital forensics; network security; mobile forensics; hardware forensics

Citation: Kim, M.; Shon, T. Digital Forensics for E-IoT Devices in Smart Cities. *Electronics* **2023**, *12*, 3233. https://doi.org/10.3390/electronics12153233

Academic Editors: Mamoun Alazab, Umit Karabiyik and Abdelkader Ouda

Received: 23 June 2023
Revised: 17 July 2023
Accepted: 25 July 2023
Published: 26 July 2023

1. Introduction

In July 2022, the Saudi Arabian government officially announced the design of the smart city project, "The Line", as part of the Neom project [1]. The aim of Neom City is to ensure an ideal climate using artificial intelligence (AI) technology and replace fossil energy with green energy [2]. The switch to green energy has also occurred in places other than planned towns. The global increase in the use of electric vehicles, expansion of the renewable energy market, and decline of the coal industry are part of efforts to realize the decarbonization of cities [3]. Energy-related legislation and government support are being strengthened at the national level around the world. The transition from fossil energy to renewable energy has increased the use of electricity. This has resulted in changes in the electricity transmission and distribution infrastructure. The expansion of infrastructure and the development of 5G communication technology have resulted in the application of advanced information and communications technology (ICT) in power systems. The traditional power system is a centralized system that consists of one-way sequential steps from power generation and transmission to conversion and consumption. However, the smart grid with ICT comprises a ring structure with an energy management system, energy storage system (ESS), and advanced measuring infrastructure (AMI). It is more efficient than traditional power systems for managing energy because it can change the functions of each stage according to transmitted information and services.

In smart grids, energy data is collected and analyzed through IoT devices by installing sensors and communication modules at power transmission and distribution facilities. In contrast to traditional power systems, wherein energy measurements are stored in the internal storage of the device, in smart grids, energy measurements are stored to servers. Power suppliers analyze the collected data and use it for prediction and monitoring to maintain the stability of the system; for example, it is used in power demand forecasting, energy efficiency improvement, and failure prevention. Recently, in addition to IoT devices managed by power suppliers, their use for managing energy in homes has also increased. Users of smart homes monitor, control, and optimize their energy usage through the energy-management services of home IoT (hereinafter referred to as H-IoT), such as smart microwaves and smart TVs. The IoT for energy management in smart cities and smart homes, comprising devices such as data concentrator units (DCUs), smart meters, smart plugs, and smart microwaves, is referred to as E-IoT in this paper. As the E-IoT penetration rate is still lower than that of H-IoT, forensic research on H-IoT has been receiving greater attention than E-IoT. However, with the number of smart cities increases, smart-home IoT manufacturers are gradually developing H-IoT in the form of E-IoT by adding services and functions for energy management.

E-IoT systems have the advantage of being able to manage data efficiently. However, they present many potential security threats because all the devices are networked for energy management in homes and businesses [4,5]. If malicious code or hacking is attempted on one E-IoT device connected to the system, the entire system can become paralyzed. Attacks on E-IoT devices can affect the system operation of smart cities and smart homes, and the overall production activities in the city. In addition, attacks can be in the form of manipulating energy usage or stealing personal information, and such stolen information can be used for secondary attacks such as identity theft. Moreover, cyber-attacks can escalate to physical attacks if an attacker uses energy usage logs to estimate the activity time of power managers and users. Therefore, in this study, we apply digital forensics to E-IoT to analyze its vulnerabilities in advance and respond quickly to security accidents.

By applying digital forensics to E-IoT devices, we examine the possibility of vulnerability and personal information leakage. For applying digital forensics to E-IoT devices, an E-IoT test bed is built using AMI devices, home energy IoT, and home appliances. We construct a test bed similar to actual E-IoT environments to propose digital forensic methodology that can be optimally applied to E-IoT environments. In the application of this methodology, we use actual E-IoT devices. The contributions of this study are as follows:

- A test bed for applying E-IoT digital forensics was established, and methodology applicable to E-IoT was derived. For a real-life environment, DCUs and smart meters, which are AMI devices used in Korean power systems, were used.
- An E-IoT system environment was configured to establish the test bed. To investigate the E-IoT system environment, E-IoT devices were classified into three categories: (1) AMI device, (2) home-energy IoT, and (3) home appliance, and configured with an H-IoT system environment.
- For the E-IoT digital forensics, data acquisition and analysis methodology were proposed. The methodology consisted of (1) network packet data analysis, (2) hardware interface analysis, and (3) a mobile device paired with E-IoT methods.
- The methodology was applied to DCUs and smart meters, which are AMI devices; smart plugs and smart heating controllers, which comprise the home-energy IoT; and smart microwaves and smart monitoring systems, which are home appliances, for the experiments on actual E-IoT devices, and the device vulnerabilities and possibility of personal-information exposure were identified.

The rest of this paper is organized as follows. Section 2 describes the research related to smart grids and IoT. Section 3 describes the E-IoT system environment configuration and its comparison with the H-IoT system environment. Section 4 describes data acquisition methodology to be applied to E-IoT. Section 5 details the experiments on real E-IoT devices using the methodology described in Section 4. Section 6 discusses the results of such a study; and finally, Section 7 presents some concluding remarks.

2. Related Works

Haris et al. proposed a smart grid digital forensics investigation framework to support digital forensics investigations by considering the example of Stuxnet attacks [6]. Existing digital forensics frameworks and models were reviewed to identify the suitability of phases to be included in the proposed framework. In a follow-up study by Haris, a digital forensic procedure was proposed to guide investigators in performing the digital forensic investigation, especially in a smart grid environment [7]. They discussed several suitable digital forensics investigation tools and techniques to solve the problems and challenges. In this study, two cyber-attack examples were discussed, and the attack was simulated using a test bed to guide the forensic investigators based on the proposed digital forensic procedure. They presented an appropriate methodology and relevant forensic tools to ensure the integrity of the evidence during collection and analysis, which were then presented as legal evidence in court. Andrew et al. investigated the state-of-the-art ICS forensics to provide better outcomes for information gathering from the forensic analysis that can be used to improve the cyber resilience of the electricity grid [8]. Panagiotis et al. proposed the secure and private smart grid architecture [9]. It constituted an overall solution aimed at protecting SG by enhancing situational awareness, detecting timely cyberattacks, collecting appropriate forensic evidence and providing an anonymous cybersecurity information-sharing mechanism. Gonzalo et al. surveyed the existing literature related to the infrastructure and communications of the energy sector and smart grids [10]. They specifically studied the existing recommendations and models of government agencies and evaluated deep packet inspection approaches as a security tool for smart grids. Most digital forensic studies on smart grids and smart cities are based on the framework. In framework-based studies, methodologies are not presented or applied to devices because they are focused on a series of digital forensics processes. In this study, a test bed for E-IoT devices used in smart grids and smart cities is established and digital forensics is performed.

Juan et al. studied the state of the art of IoT forensic investigations and detailed the examination process for the "Xiaomi Mi Smart Sensor Set" smart home kit, while emphasizing the acquisition and analysis of the three main types of forensic evidence: (1) non-volatile memory, (2) volatile memory, and (3) network traffic [11]. However, data acquisition was limited when the latest firmware was installed. Thus, the data acquisition result differed depending on the firmware version. Jo et al. conducted a digital forensic study on an AI speaker ecosystem [12]. In Jo et al.'s study, five analysis methods were proposed by categorizing them into three forensic areas. The research by Shin et al., which was conducted as a follow-up study to that conducted by Jo et al., proposed five methods of injecting a certificate into an AI speaker to analyze the encrypted traffic between the AI speaker and the cloud [13]. The encrypted traffic of the AI speakers was analyzed through the ball grid array rework of the NAND flash memory with the certificate injection. IoT forensic research has been mainly focused on the H-IoT used in homes and companies. However, with the increase in smart grids and smart cities, services and functions for energy management have been included in the H-IoT. In this study, a digital forensics methodology is proposed and applied to the H-IoT with additional energy services, as well as E-IoT devices such as DCUs and smart meters.

3. Electric Power and Energy Related IoT for Smart Homes and Cities

With the development of smart cities, E-IoT devices, such as AMI devices, have been developed to effectively manage energy and analyze energy data. E-IoT devices transmit and manage data to servers through wired/wireless communication. In the H-IoT, home-energy IoT devices such as smart plugs and energy control technologies have been developed for energy reduction and management. Home-energy IoT can be used to manage energy in real time. Some smart home appliances can be provided with energy management services to monitor their energy usage. The E-IoT system considered here comprised AMI devices, home-energy IoT, and smart home appliances for proposing a methodology of acquiring data for E-IoT devices, and the environment with the H-IoT system was analyzed.

3.1. E-IoT and H-IoT

Figure 1 presents the composition of E-IoT and H-IoT. The H-IoT and E-IoT devices can be classified as smart home appliances, home E-IoT, and AMI devices. Smart home appliances comprise the use of IoT for user services at home. Smart home appliances include smart TVs, smart home cameras, smart microwaves, and smart humidifiers. Recently, smart-home IoT manufacturers have added services and functions for energy management to H-IoT and provided services to users through the manufacturer's platform. Figure 2 presents the Samsung SmartThings platform that manufactures smart home appliances [14]. The energy used in the smart home appliance may be checked using the mobile device platform paired with the smart home appliance. Some H-IoT devices can control as well as check energy use. These H-IoT devices are considered home-energy IoT in this study. Home-energy IoT is used to control or measure energy at home to save energy and manage energy efficiently. It comprises of smart plugs, smart switches, etc. Furthermore, home-energy IoT can also be used to control IoT devices through paired smartphones and to check energy usage. AMI devices are used to remotely measure the energy usage at home via an energy management server. AMI devices include DCUs and smart meters. Smart meters measure the energy usage of homes and send it to DCUs. The data collected in the DCU is transferred to the server, and this data is managed by the server.

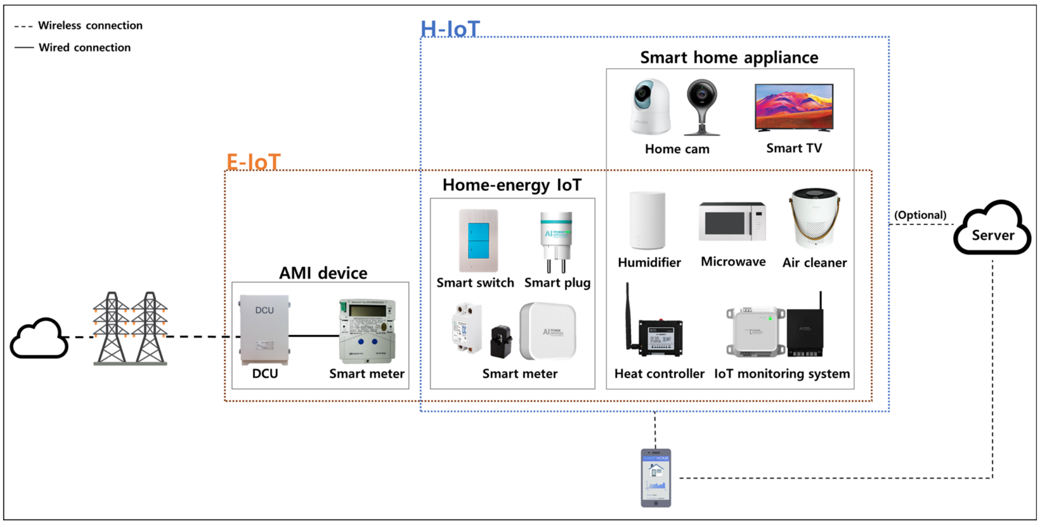
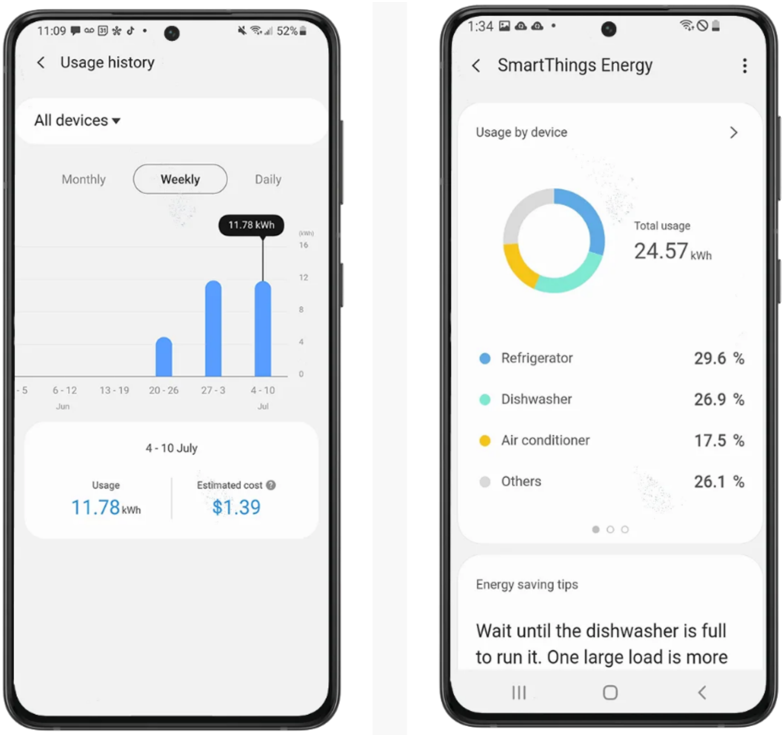


Figure 1. Configuration with categorization of E-IoT and H-IoT devices as AMI devices, home-energy IoT, and smart home appliances.

Smart home appliances and home-energy IoT are common to H-IoT and E-IoT because they provide services for users and can be used to measure energy usage. AMI devices can be categorized as E-IoT devices. Based on this configuration, the environment of the E-IoT and H-IoT systems is analyzed.

3.2. Analysis of E-IoT System Environment

Table 1 presents a comparative analysis of the environment of the E-IoT and H-IoT systems. The analysis was performed by dividing the environment according to communication, protocol, operating system (OS), hardware, and data priority.



Wait until the dishwasher is full to run it. One large load is more

Figure 2. Featured service of SmartThings Energy provided by Samsung [14].

Table 1. Environment analysis of H-IoT and E-IoT systems.

	H-IoT	E-IoT
Communication	Secure communication	Serial communication
	Prioritize high performance and response reliability	Prioritize real-time performance and response time
Protocol	Low-power protocols (e.g., Zigbee)	
	Standard protocols (e.g., IEEE 802.11, IEEE 802.15)	Long range wide area protocols and dedicated protocols (e.g., IEEE 1815.1)
Hardware	Port for boot verification and debugging	
	Short replacement cycle of 3–5 years	Long replacement cycle of more than 20 years
	USB port	Serial port
Operating system	Standard OS (e.g., Windows and Linux)	Dedicated embedded Linux OS
Data priority	Confidentiality rather than integrity and availability (user data)	Integrity and availability rather than confidentiality (system data)

3.2.1. Communication

The H-IoT exchanges user and system data when communicating with a smartphone or cloud server. Because the user data exchanged between the H-IoT and server contains personal information, the data is transmitted through the transport layer security (TLS) secure communication. To provide users with a high-quality service, the reliability of the response is important when communicating with the server, and high-performance communication is required because of the large capacity of the image or voice data transmitted.

The E-IoT transmits data through the recommended standard (RS) serial communication with a simple structure because it exchanges data of a smaller size than user data, which comprises of video and voice data. As data of a small size is exchanged, there is a relatively little response delay. In E-IoT devices, real-time responsiveness is important because it is important to store and record data over time. That is, as the real-time performance and data response are important, a communication delay is unacceptable.

3.2.2. Protocol

The H-IoT sometimes connects directly to cloud servers without the use of smartphones; however, in the majority of cases, the H-IoT pairs with smartphones. The H-IoT uses IEEE 802.15 (Bluetooth) or IEEE 802.11 (Wi-Fi) protocols to pair with smartphones, and some miniaturized H-IoT devices use low-power protocols such as Zigbee. The H-IoT may be connected via a wire or wirelessly to a personal computer (PC) or other devices through a universal serial bus (USB) or Wi-Fi. When connected to a PC via a USB, data from the IoT can be obtained from a PC and can be transmitted to an IoT device from a PC.

Some E-IoT devices can transmit and receive data using the same protocol as that used in H-IoT in homes and communicate with other IoT devices within a close range using the Zigbee protocol. One of the most significant differences between H-IoT and E-IoT is that data must be received over a wide range to send data to the server. Therefore, E-IoT devices that utilize a large area transmit and receive data using the long-range wide area (LoRa) protocol. The LoRa protocol is used to send and receive sensor data from E-IoT because of its low power and low cost. In addition, as E-IoT devices use dedicated protocols such as IEEE 1815.1, non-administrators are inaccessible and difficult to identify [15].

3.2.3. Hardware

The majority of H-IoT devices are miniaturized. Because the printed circuit board (PCB) built into the miniaturized device is small, their processors, sensors, and memory are limited. As the use of limited hardware results in a shorter replacement cycle, the H-IoT has a short replacement cycle of 3 to 5 years. Some H-IoT devices may have a joint test action group (JTAG)/universal asynchronous receiver–transmitter (UART) ports as a hardware interface [16]. The JTAG/UART port is used for normal booting or debugging during manufacturing [17]. However, as most H-IoT devices are decreasing in size, many of them have no JTAG/UART ports.

As E-IoT devices are relatively large compared to H-IoT devices, various sensors and chips can be inserted into E-IoT devices. Precise sensors are used in the E-IoT to increase the accuracy of data. E-IoT devices have a long replacement cycle of 15–20 years because only some parts can be replaced if the device fails, and replacement costs and time are high. E-IoT devices, as in the case of H-IoT devices, have JTAG/UART ports as hardware interfaces. In addition, the E-IoT has a serial port for RS communication.

3.2.4. Operating System

H-IoT devices have various OSs because they are manufactured by various manufacturers and have different functions in each device. Standard OSs such as Android and Linux are mainly used. However, the required system varies depending on the function, and thus, manufacturers sometimes develop their own OSs for each IoT device.

In contrast to H-IoT devices that require various functions to provide services to users, E-IoT devices mainly comprise the functions of energy measurement and data transmission. Due to the limited functionality requirements, they typically avoid the need for multiple OSs tailored to individual manufacturers. Because E-IoT is used by administrators, it mostly uses a dedicated embedded Linux-based OS.

3.2.5. Data Priority

The main purpose of H-IoT is to provide the service requested by users. H-IoT devices use secure communication to protect the data when transmitting service data. User data is protected to ensure data confidentiality. As H-IoT data mainly comprises user data rather than system data, ensuring data confidentiality holds greater significance than maintaining data integrity or availability.

The purpose of E-IoT is to acquire and analyze energy usage data from homes and companies. That is, energy usage, which comprises system data, is the main data. As there is little personal information in the system data, confidentiality is less important than user data in this case. Instead, the integrity and availability of data are important.

4. E-IoT Data Acquisition

For the digital forensics of E-IoT devices, data acquisition and analysis methodology was proposed. The proposed methodology consisted of a total of three methods. Three methods were used to acquire data for E-IoT digital forensics. Table 2 lists the programs used in E-IoT data acquisition methods. The first method was network packet data analysis, which acquires packets exchanged between E-IoT and servers using a network packet capture tool. Packet data acquisition of E-IoT devices is divided into network protocol analysis tools and web proxy tools according to the presence or absence of encryption.

Table 2. Program used in E-IoT data acquisition methodology.

Method	Programs	Manufacturer	Version	Usage
Network packet data analysis	Wireshark	Wireshark Foundation	3.4.0	Network protocol analyzer
	Burp Suite	PortSwigger	Professional 2021.5.2	Web proxy tool
Hardware interface analysis	PuTTy	- (open source)	0.78	Image dump in serial communication
Mobile device paired with E-IoT	FTK Imager	Exterro	4.5.0	Data structure analysis of mobile devices
	DB browser for SQLite	- (open source)	3.12.2	Database analysis on mobile device

The second method was to acquire data by analyzing hardware interfaces such as data storage chips and serial ports of E-IoT devices. It involved finding a port that can be connected to a PC among the physical hardware interfaces or to find a memory chip for chip-off. As most E-IoT devices transmit data via serial communication, PuTTy is used to dump internal data images if serial ports are found in the hardware interface.

The third method was to analyze the data stored in paired mobile devices and acquire app data related to E-IoT devices, as home-energy IoT and smart home appliances—excluding AMI devices—can be paired with mobile devices. The FTK Imager tool must be used to analyze the data structure of mobile devices. As most mobile devices have internal data in the form of databases, the DB browser for the SQLite program is used to analyze the data.

4.1. Network Packet Data Analysis

E-IoT devices communicate with servers using TLS to protect data. The collection of packet data between the E-IoT and servers is essential because device data, system data, and user-sensitive information are transmitted. In this work, we acquired and analyzed unencrypted and encrypted packets using network protocol analysis tools and web proxy tools.

The network protocol analysis tool Wireshark was used in this study to acquire packet data from E-IoT devices [18]. Wireshark is available for various Oss, such as Windows, Linux, and macOS, and can check various network protocols such as hypertext transfer protocol (HTTP) and user datagram protocol. It can also acquire various data such as ethernet and Bluetooth data. In the study, Wi-Fi generated by a PC was connected to

E-IoT devices to capture packets in the local area. Network protocol analysis tools, such as Wireshark, can acquire encrypted packets, but there is a limitation that the contents of the encrypted packets cannot be analyzed.

Web proxy tools were used to analyze unanalyzed encrypted packets on E-IoT devices. A web proxy tool is a tool that uses the man-in-the-middle technique and can capture and analyze encrypted TLS packets through proxy settings. That is, the web proxy tool acts as a proxy to debug HTTP traffic between the user's computer and the server. Typical web proxy tools include Fiddler, Charles Proxy, and Buff Suite. In this work, we acquire encrypted packets from E-IoT devices using Burp Suite, which supports TLS 1.3 [19]. Burp Suite can analyze HTTP communication in all browsers and even HTTP secure (HTTPS) communication by installing the certificate authority on the device. Burp Suite offers a choice of TLS version and encryption options, thus facilitating the capture of only the required packets.

To analyze encrypted packets of E-IoT devices, the web proxy must be trusted by installing a certificate of the web proxy tool on the E-IoT devices. However, installing certificates directly on E-IoT devices has limitations because of problems such as rework and memory capacity [20]. Instead, a certificate was installed on a smartphone paired with E-IoT to acquire and analyze packets from E-IoT devices.

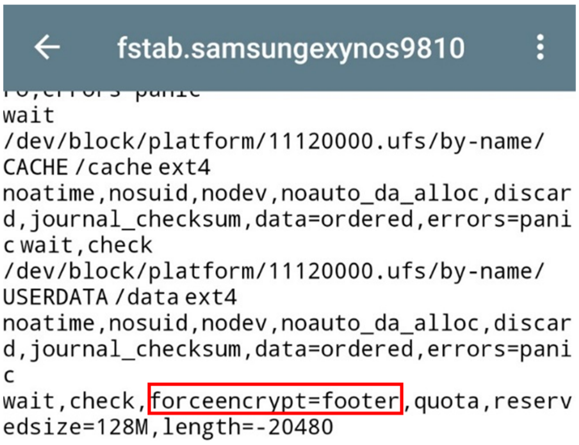
4.2. Hardware Interface Analysis

In contrast to smartphones and other devices, many E-IoT devices do not provide PC connectivity. However, it is possible to connect to a PC using interfaces such as serial ports, UART, and JTAG on a PCB that can be obtained by disassembling an E-IoT device [21]. UART/JTAG ports are used to confirm normal booting or debug E-IoT devices during manufacturing. However, for security purposes, there is a trend among most manufacturers to hide the implemented debugging port or remove the marked port. In this study, E-IoT devices were disassembled to determine whether the port exists and, if so, in what form it is implemented. If such a port was not found, the possibility of chip-off was investigated.

Chip-off is a method used when obtaining internal data at the software or hardware level is difficult. Chip-off involves physically acquiring NAND flash memory chips from a PCB and acquiring data. This method required a good understanding of various equipment and hardware. The NAND flash memory chip obtained through the chip-off may acquire data as a RAW image. However, as many E-IoT devices store data on cloud servers, it was difficult to apply this method because the NAND flash memory chip did not exist in such cases [22,23].

4.3. Mobile Device Paired with E-IoT Devices

In the process of using E-IoT devices, mobile devices may be paired with E-IoT to remotely control E-IoT devices. It is possible to obtain the data of E-IoT devices by analyzing the internal data of mobile devices paired with E-IoT devices [24]. To acquire the data on mobile devices paired with E-IoT devices, it is necessary to analyze the OS and file system of mobile devices. In this study, E-IoT devices were paired with Samsung smartphones. Samsung smartphones use the Android OS, and the majority of them use extended file system 4 (Ext4) [25,26]. To acquire data related to E-IoT from among the data on mobile devices, user data partitions, wherein user-installed apps and user data are stored, must be dumped. Administrator rights on the mobile device must be obtained to access the user data partition. In this study, the user data partition of the mobile device was dumped, but the image was encrypted, and thus, the dump image was decrypted by referring to Kim's research [27]. Kim introduced a method of decoding the full disk encryption used in Android 10 and analyzing the ext4 file system. Figure 3 presents an 'fstab' file that was analyzed to decrypt Android 10 in Kim's study, and it was decrypted by modifying 'forceencrypt=f', one of the system data of the file. The FTK Imager program was used to analyze the file storage structure of the user data partition and extract E-IoT device app data, and the data on the E-IoT device app was analyzed using the DB browser for SQLite program [28,29].



```
ro,errors=panic
wait
/dev/block/platform/11120000.ufs/by-name/
CACHE /cache ext4
noatime,nosuid,nodev,noauto_da_alloc,discar
d,journal_checksum,data=ordered,errors=pani
c wait,check
/dev/block/platform/11120000.ufs/by-name/
USERDATA /data ext4
noatime,nosuid,nodev,noauto_da_alloc,discar
d,journal_checksum,data=ordered,errors=pani
c
wait,check,forceencrypt=footer,quota,reserv
edsize=128M,length=-20480
```

Figure 3. 'fstab' files analyzed to decrypt Android 10 in Kim's study [27].

5. Digital Forensics for E-IoT

Table 3 lists the devices used in digital forensics for E-IoT. One type of AMI device, two types of home-energy IoT devices, and two types of home appliances were used. In addition, E-IoT devices were paired with Samsung smartphones and an LG PC to conduct an experiment. As a result of analyzing the E-IoT devices in advance, devices other than AMI devices were paired with mobile devices, and (low power) Wi-Fi was used. The PCB of each E-IoT was analyzed to investigate the hardware interface of the E-IoT devices. The DCU had a port for serial communication and a 256-MB K9F2G08UOC NAND flash memory chip, but no NAND flash chip or communication port was found on the other E-IoT devices. Figure 4 presents a test bed constructed using six E-IoT devices. Each device was connected to the Wi-Fi generated by a PC. Home-energy IoT and home appliance devices were wirelessly paired with mobile devices and a PC through Wi-Fi, and the AMI devices were wired to the PC through local area network (LAN) cables. Network packet data analysis and hardware interface analysis methods were applied to each E-IoT device. E-IoT paired with a mobile device was used to analyze the E-IoT data stored in the internal data of a mobile device. This section describes the significant artifacts acquired in the data collection and the analysis results for the E-IoT devices.

Table 3. Specification analysis of devices paired with E-IoT devices used in the experiment.

	AMI Device		**Home Energy IoT**		**Home Appliance**		**Paired Device**	
Manufacturer	**LoenK**	**PSTEK**	**Dawon DNS**	**Karam I&C**	**Samsung**	**Dawon DNS**	**Samsung**	**LG**
Device	DCU	Smart meter	Smart plug	Smart heat controller	Smart microwave	Smart monitoring system	Smartphone	PC
Model	-	-	PM-B540-W	KRBOS	MG23A5378CE	NM-P200-NB-N	Galaxy S9+/A32	15U590
Communication	Serial comm.	Serial comm.	Low-power Wi-Fi	Low-power Wi-Fi	Wi-Fi	Low-power Wi-Fi	Wi-Fi/LTE	Wi-Fi/LAN
Hardware interface	Serial port/ 256 MB Nand flash	X	X	X	X	X	- (Not used in this experiment)	-
Support for pairing with mobile devices	X	X	O	O	O	O	-	-

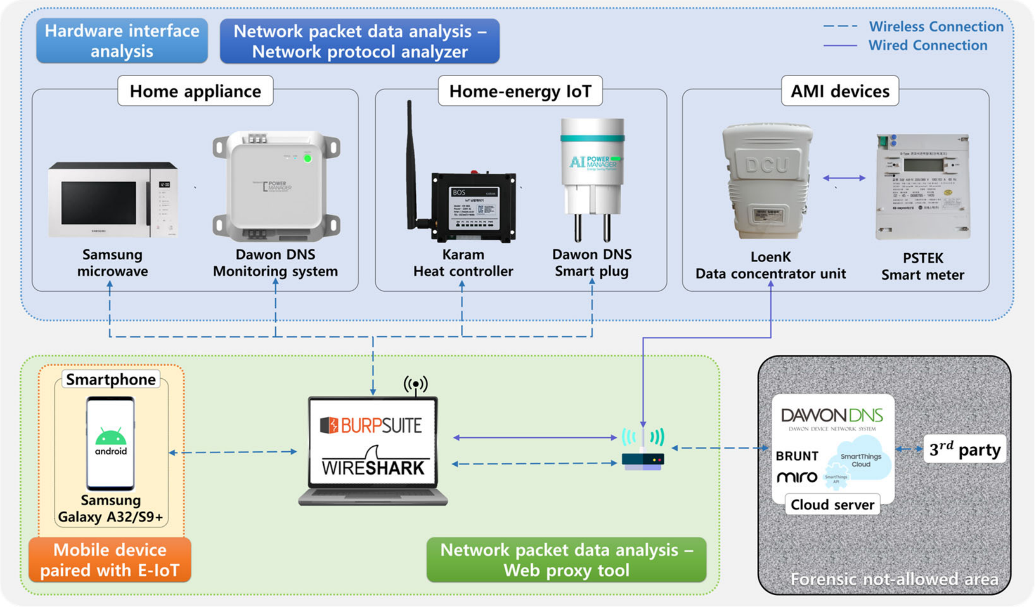


Figure 4. Test bed configuration with E-IoT devices.

5.1. Network Packet Data Analysis

5.1.1. DCU and Smart Meter

The connection of the PC with the DCU must precede the collection of network packet data. Figure 5 presents a DCU and smart meter connected to a PC based on the testbed configuration presented in Figure 4. The DCU and smart meter were connected using an RS-232 cable, and the DCU and PC were connected via a LAN cable with an access point. The data generated by the smart meter was concentrated in the DCU and stored in the server. Wireshark, a network protocol analysis tool, was used to acquire and analyze the network packet data at the DCU.

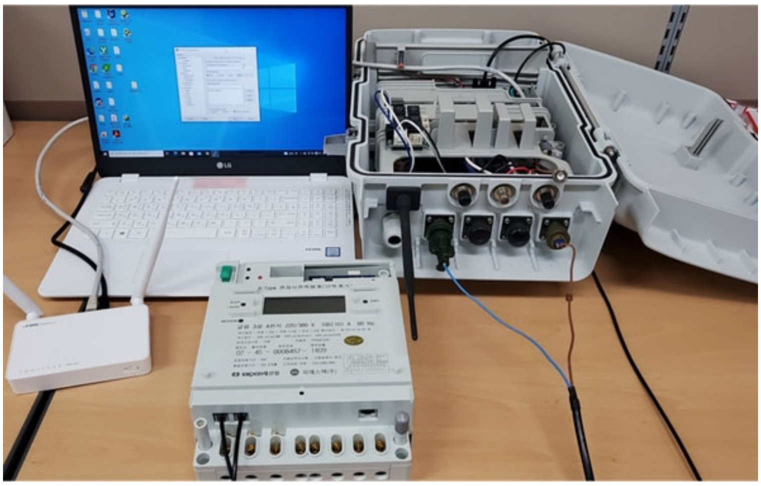
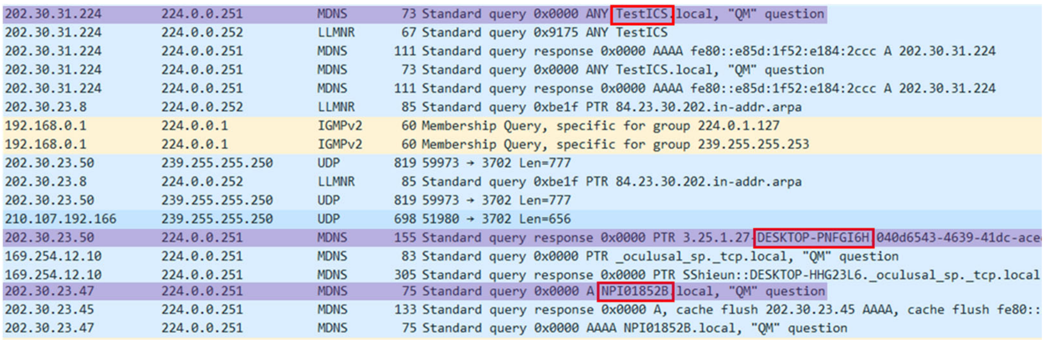


Figure 5. DCU and smart meter connected to PC based on configured test bed.

Figure 6 presents some of the packets obtained from the DCU, and Figure 7 presents a diagram of the communication between the DCU and server based on Figure 6. The DCU uses the multicast domain name system (MDNS) to send query messages around it. MDNS is a protocol used to replace DNS servers in small networks. The MDNS protocol revealed the names of the TestICS, DESKTOP-PNFGI6H, and NPI01852B devices that share the router with DCU. The DCU used a network management system (NMS) to manage communication. TestICS and DESKTOP-PNFGI6H were names of PCs that used the same router as that of the DCU. NPI01852B was an unconfirmed device. In the NPI01852B name, NPI was an abbreviation for the NMS protocol identifier, which was inferred to be the identifier of a smart meter managed by the DCU. Thus, the names of the devices sharing the router with the DCU were acquired. The communication structure of the DCU, which searches for smart meters through MDNS protocols and manages smart meters with NPI through NMS, had been confirmed using the network protocol analyzer.



```
202.30.31.224    224.0.0.251      MDNS     73 Standard query 0x0000 ANY TestICS.local, "QM" question
202.30.31.224    224.0.0.252      LLMNR    67 Standard query 0x9175 ANY TestICS
202.30.31.224    224.0.0.251      MDNS    111 Standard query response 0x0000 AAAA fe80::e85d:1f52:e184:2ccc A 202.30.31.224
202.30.31.224    224.0.0.251      MDNS     73 Standard query 0x0000 ANY TestICS.local, "QM" question
202.30.31.224    224.0.0.251      MDNS    111 Standard query response 0x0000 AAAA fe80::e85d:1f52:e184:2ccc A 202.30.31.224
202.30.23.8      224.0.0.252      LLMNR    85 Standard query 0xbe1f PTR 84.23.30.202.in-addr.arpa
192.168.0.1      224.0.0.1        IGMPv2   60 Membership Query, specific for group 224.0.1.127
192.168.0.1      224.0.0.1        IGMPv2   60 Membership Query, specific for group 239.255.255.253
202.30.23.50     239.255.255.250  UDP     819 59973 → 3702 Len=777
202.30.23.8      224.0.0.252      LLMNR    85 Standard query 0xbe1f PTR 84.23.30.202.in-addr.arpa
202.30.23.50     239.255.255.250  UDP     819 59973 → 3702 Len=777
210.107.192.166  239.255.255.250  UDP     698 51980 → 3702 Len=656
202.30.23.50     224.0.0.251      MDNS    155 Standard query response 0x0000 PTR 3.25.1.27-DESKTOP-PNFGI6H-040d6543-4639-41dc-ace
169.254.12.10    224.0.0.251      MDNS     83 Standard query 0x0000 PTR _oculusal_sp._tcp.local, "QM" question
169.254.12.10    224.0.0.251      MDNS    305 Standard query response 0x0000 PTR SShieun::DESKTOP-HHG23L6._oculusal_sp._tcp.local
202.30.23.47     224.0.0.251      MDNS     75 Standard query 0x0000 A NPI01852B.local, "QM" question
202.30.23.45     224.0.0.251      MDNS    133 Standard query response 0x0000 A, cache flush 202.30.23.45 AAAA, cache flush fe80::
202.30.23.47     224.0.0.251      MDNS     75 Standard query 0x0000 AAAA NPI01852B.local, "QM" question
```

Figure 6. Query messages sent from DCU to PCs using MDNS protocol.

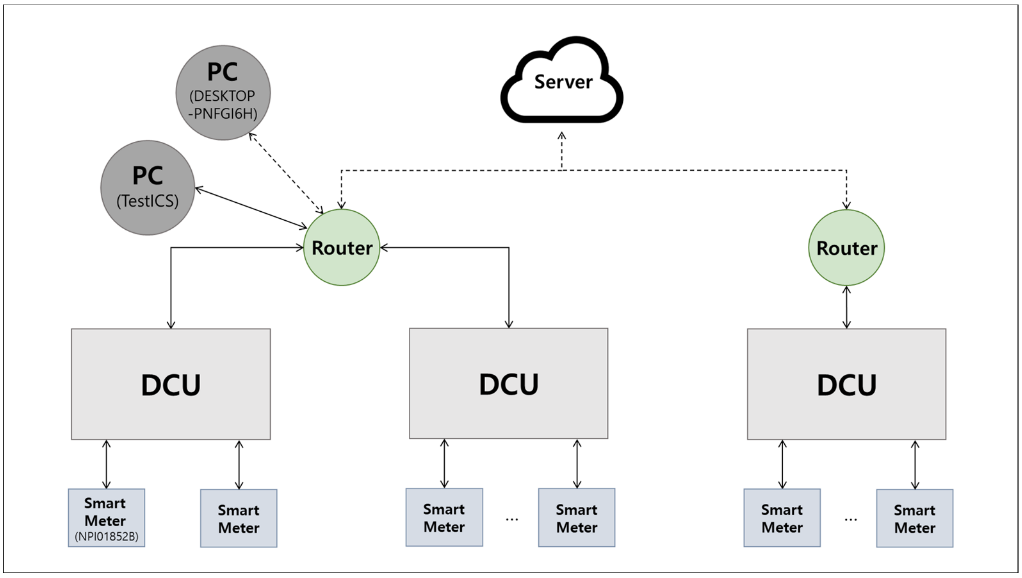
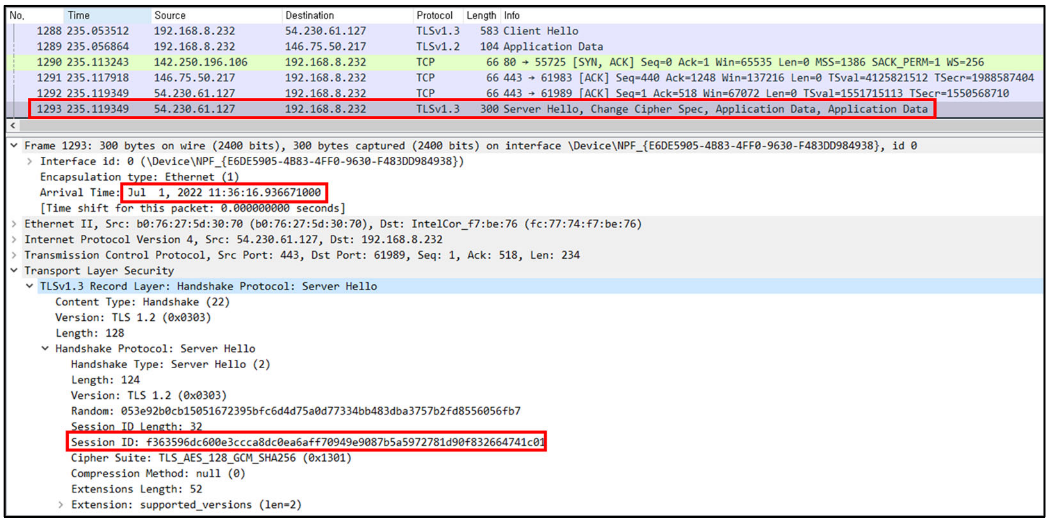


Figure 7. Schematic of AMI devices communicating with the server.

We attempted to install a certificate of Burp Suite, which was a web proxy tool, to analyze encrypted packets in the DCU. However, a certificate could not be installed on the DCU because administrator rights were required to access the DCU directory. On applying the network packet data analysis to the DCU and smart meters, the communication structure of the DCU was identified, but the encrypted packet could not be analyzed because the certificate could not be installed in the DCU. It is necessary to further study the methods of obtaining administrator rights and installing certificates.

5.1.2. Smart Microwave

The smart microwave was paired with a mobile device to remotely control and record the device. As a result of analyzing the packets acquired from the smart microwave, the majority of the packets were able to provide only simple information such as the timestamp, TLS version and Session ID, as shown in Figure 8. Therefore, the encrypted communication of the smart microwave was analyzed using the web proxy tool.

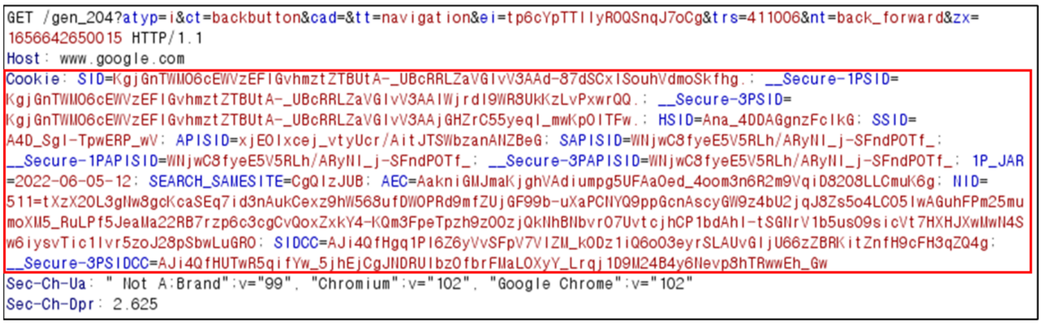


```
No.      Time        Source           Destination      Protocol  Length Info
    1288 235.053512  192.168.8.232    54.230.61.127    TLSv1.3    583 Client Hello
    1289 235.056864  192.168.8.232    146.75.50.217    TLSv1.2    104 Application Data
    1290 235.113243  142.250.196.106  192.168.8.232    TCP         66 80 → 55725 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1386 SACK_PERM=1 WS=256
    1291 235.117918  146.75.50.217    192.168.8.232    TCP         66 443 → 61983 [ACK] Seq=440 Ack=1248 Win=137216 Len=0 TSval=4125821512 TSecr=1988587404
    1292 235.119349  54.230.61.127    192.168.8.232    TCP         66 443 → 61989 [ACK] Seq=1 Ack=518 Win=67072 Len=0 TSval=1551715113 TSecr=1550568710
    1293 235.119349  54.230.61.127    192.168.8.232    TLSv1.3    300 Server Hello, Change Cipher Spec, Application Data, Application Data

Frame 1293: 300 bytes on wire (2400 bits), 300 bytes captured (2400 bits) on interface \Device\NPF_{E6DE5905-4B83-4FF0-9630-F483DD984938}, id 0
  > Interface id: 0 (\Device\NPF_{E6DE5905-4B83-4FF0-9630-F483DD984938})
    Encapsulation type: Ethernet (1)
    Arrival Time: Jul  1, 2022 11:36:16.936671000
    [Time shift for this packet: 0.000000000 seconds]
> Ethernet II, Src: b0:76:27:5d:30:70 (b0:76:27:5d:30:70), Dst: IntelCor_f7:be:76 (fc:77:74:f7:be:76)
> Internet Protocol Version 4, Src: 54.230.61.127, Dst: 192.168.8.232
> Transmission Control Protocol, Src Port: 443, Dst Port: 61989, Seq: 1, Ack: 518, Len: 234
Transport Layer Security
  TLSv1.3 Record Layer: Handshake Protocol: Server Hello
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 128
      Handshake Protocol: Server Hello
        Handshake Type: Server Hello (2)
        Length: 124
        Version: TLS 1.2 (0x0303)
        Random: 053e92b0cb15051672395bfc6d4d75a0d77334bb483dba3757b2fd8556056fb7
        Session ID Length: 32
        Session ID: f363596dc600e3ccca8dc0ea6aff70949e9087b5a5972781d90f832664741c01
        Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
        Compression Method: null (0)
        Extensions Length: 52
      > Extension: supported_versions (len=2)
```

Figure 8. Time and session ID acquired from network packets generated when the smart microwave communicates with the server.

To use Burp Suite in a smart microwave, a certificate of Burp Suite was installed on a paired smartphone. Subsequently, the encrypted traffic of the smart microwave was analyzed. Access token, cookies, and data inferred based on the amount of power consumed could be obtained. Figure 9 presents the cookies obtained from the smart microwave. Figure 10 presents some of the information obtained from the encrypted packet, and this [1656642651819000, 0, 0] data was inferred from the amount of power measured in the smart microwave. "1656642651819000" was the Unix timestamp value converted to GMT at 2:30:51 on 1 July 2022. As shown in Figure 11, we accessed the mobile platform application to check the amount of power—the date was 1 July and the amount of power was 0 Wh. Among the captured packets, the only packet with an application access time and a 0 value was the one. It was estimated to indicate the amount of power (0 Wh) measured at that time. On applying network packet data analysis to smart microwaves, simple communication information and power usage were obtained.

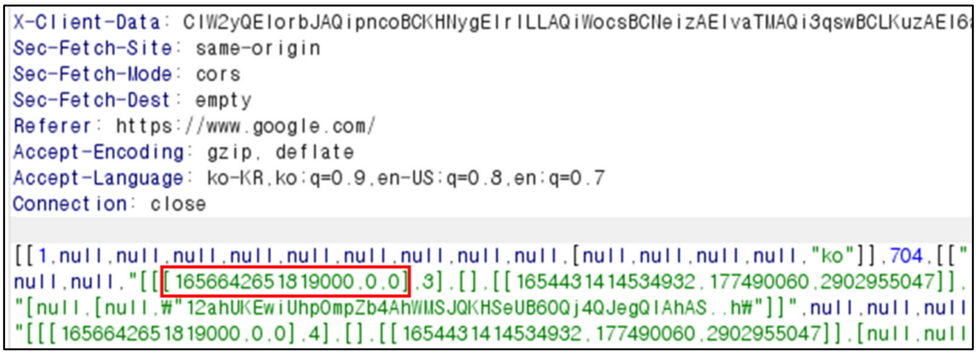


```
GET /gen_204?atyp=i&ct=backbutton&cad=&tt=navigation&ei=tp6cYpTTIlyROQSnqJ7oCg&trs=411006&nt=back_forward&zx=
165664265001 5 HTTP/1.1
Host: www.google.com
Cookie: SID=KgjGnTWMO6cEWVzEFIGvhmztZTBUtA-_UBcRRLZaVGIvV3AAd-87dSCxISouhVdmoSkfhg.: __Secure-1PSID=
KgjGnTWMO6cEWVzEFIGvhmztZTBUtA-_UBcRRLZaVGIvV3AAIWjrdI9WR8UkKzLvPxwrQQ.: __Secure-3PSID=
KgjGnTWMO6cEWVzEFIGvhmztZTBUtA-_UBcRRLZaVGIvV3AAjGHZrC55yeqI_mwKpOITFw.: HSID=Ana_4DDAGgnzFcIkG: SSID=
A4D_SgI-TpwERP_wV: APISID=xjEOIxcej_vtyUcr/AitJTSWbzanANZBeG: SAPISID=WNjwC8fyeE5V5RLh/ARyNI_j-SFndPOTf_:
__Secure-1PAPISID=WNjwC8fyeE5V5RLh/ARyNI_j-SFndPOTf_: __Secure-3PAPISID=WNjwC8fyeE5V5RLh/ARyNI_j-SFndPOTf_: 1P_JAR
=2022-06-05-12: SEARCH_SAMESITE=CgQIzJUB: AEC=AakniGMJmaKjghVAdiumpg5UFAaOed_4oom3n6R2m9VqiD8208LLCmuK6g: NID=
511=tXzX20L3gNw8gcKcaSEq7id3nAukCexz9hW568ufDWOPRd9mfZUjGF99b-uXaPCNYQ9ppGcnAscyGW9z4bU2jqJ8Zs5o4LCO5IwAGuhFPm25mu
moXM5_RuLPf5JeaMa22RB7rzp6c3cgCvQoxZxkY4-KQm3FpeTpzh9zOOzjQkNhBNbvrO7UvtcjhCP1bdAhI-tSGNrV1b5us09sicVt7HXHJXwMwN4S
w6iysvTic1Ivr5zoJ28pSbwLuGRO: SIDCC=AJi4QfHgq1PI6Z6yVvSFpV7VIZM_kODz1iQ6o03eyrSLAUvGIjU66zZBRKitZnfH9cFH3qZQ4g:
__Secure-3PSIDCC=AJi4QfHUTwR5qifYw_5jhEjCgJNDRUIbzOfbrFMaLOXyY_Lrqj1D9M24B4y6Nevp8hTRwwEh_Gw
Sec-Ch-Ua: " Not A:Brand":v="99", "Chromium":v="102", "Google Chrome":v="102"
Sec-Ch-Dpr: 2.625
```

Figure 9. Cookies acquired from network packets generated when the smart microwave communicated with the server.

5.1.3. Smart Monitoring System

On acquiring and analyzing the network packet data in the smart monitoring system using the network protocol analysis tool, it was found that the majority of the acquired packets were encrypted, and thus, only basic information such as the TLS 1.3 version and session ID could be obtained from the smart microwave. Therefore, we analyzed the network communication of smart monitoring systems using web proxy tools. Paired mobile device information, cookies, time logs, and user account emails were thus obtained. Figure 12 presents the cookies and user information obtained from the packets of the monitoring system. The user-set name and account email were acquired. In addition, the user's profile picture was obtained through the URL along with their account email ID. On applying network packet data analysis to the smart monitoring system, communication information and user information were obtained.



```
X-Client-Data: CIW2yQEIorbJAQipncoBCKHNygEIrILLAQiWocsBCNeizAEIvaTMAQi3qswBCLKuzAEI6
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://www.google.com/
Accept-Encoding: gzip, deflate
Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
Connection: close

[[1,null,null,null,null,null,null,null,null,null,[null,null,null,null,"ko"]],704,[["
null,null,"[[[1656642651819000,0,0],3],[],[[1654431414534932,177490060,2902955047]],
"[null,[null,\"12ahUKEwiUhpOmpZb4AhWMSJQKHSeUB60Qj4QJegQIAhAS..h\"]]",null,null,null
"[[[1656642651819000,0,0],4],[],[[1654431414534932,177490060,2902955047]],[null,null
```

Figure 10. Data estimated from power usage obtained from network packets generated when the smart microwave communicated with the server.

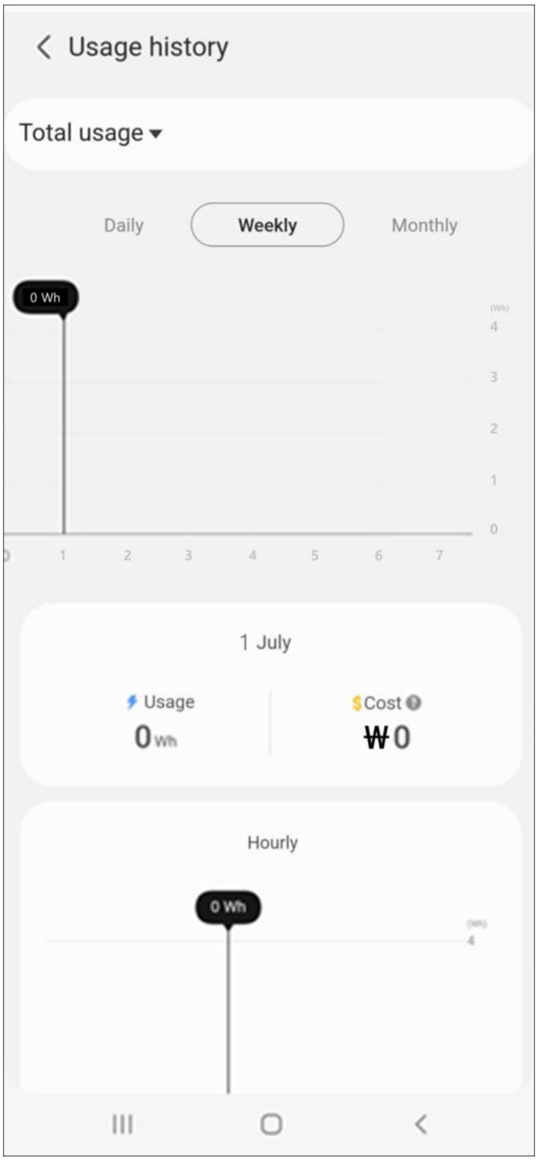
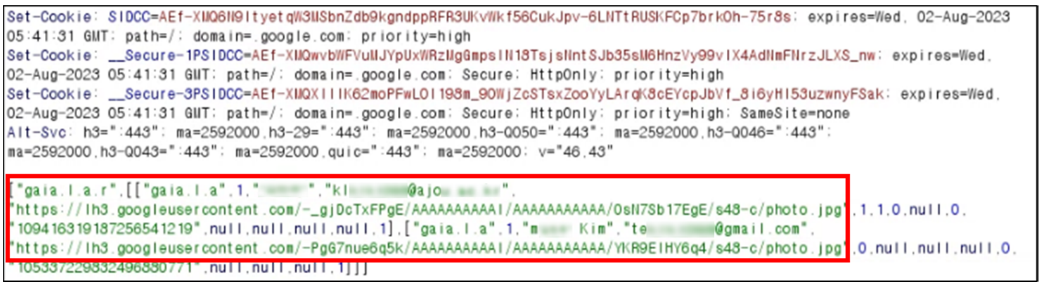


Figure 11. Mobile screen when capturing packets from smart microwave.



```
Set-Cookie: SIDCC=AEf-XMQ6N9ItyetqW3MSbnZdb9kgndppRFR3UKvWkf56CukJpv-6LNTtRUSKFCp7brkOh-75r8s; expires=Wed, 02-Aug-2023
05:41:31 GMT; path=/; domain=.google.com; priority=high
Set-Cookie: __Secure-1PSIDCC=AEf-XMQwvbWFVuMJYpUxWRzMgGmpsIN18TsjsMntSJb35sM6HnzVy99vIX4AdMmFNrzJLXS_nw; expires=Wed,
02-Aug-2023 05:41:31 GMT; path=/; domain=.google.com; Secure; HttpOnly; priority=high
Set-Cookie: __Secure-3PSIDCC=AEf-XMQXIIIK62moPFwLOI198m_90WjZcSTsxZooYyLArqK8cEYcpJbVf_8i6yHI53uzwnyFSak; expires=Wed,
02-Aug-2023 05:41:31 GMT; path=/; domain=.google.com; Secure; HttpOnly; priority=high; SameSite=none
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443";
ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43"

["gaia.l.a.r",[["gaia.l.a",1,"[redacted]","kl[redacted]@ajo[redacted]",
"https://lh3.googleusercontent.com/-_gjDcTxFPgE/AAAAAAAAAAI/AAAAAAAAAAA/OsN7Sb17EgE/s48-c/photo.jpg",1,1,0,null,0,
"109416319187256541219",null,null,null,null,1],["gaia.l.a",1,"m[redacted] Kim","te[redacted]@gmail.com",
"https://lh3.googleusercontent.com/-PgG7nue6q5k/AAAAAAAAAAI/AAAAAAAAAAA/YKR9EIHY6q4/s48-c/photo.jpg",0,null,null,null,0,
"105337229832496880771",null,null,null,1]]]
```

Figure 12. Time and user account acquired from network packets generated when the monitoring system communicates with the server.

Among the user information, the account email IDs and profile pictures required patches as an attacker could use them for committing additional crimes such as theft or a deepfake.

5.1.4. Attack Scenario for Network Packet Data Analysis

An attacker may prevent legitimate packets of E-IoT and inject malicious traffic through denial of service (DoS) attacks. The DoS attack on an E-IoT system may interfere with power services. Because power services are connected by vast systems and networks, if one system is attacked, it may affect other systems [30].

When an attacker steals packets, it is highly likely to detect the user personal information and life patterns. In addition, if an attacker manipulates the power usage of a packet and sends it to a server, users may be incorrectly charged a higher amount. Or, among the analyzed life patterns, physical attacks, such as device damage, may be made at a time when the user is not active.

5.2. Hardware Interface Analysis

5.2.1. DCU and Smart Meter

The PCBs of the DCU and smart meter were analyzed to determine whether a memory chip or port could be connected to a PC. Figure 13 presents a PCB of the DCU. A NAND flash memory chip and a port that supports various communication were found. The DCU used 256 MB "K9F2G08UOC" as a NAND flash memory chip, and RS-232 ports were found on the PCB. The DCU communicated with the PC through a serial port that was found in the DCU hardware interface analysis. Figure 14 presents the PCB of the smart meter. No serial port or flash memory chip was found on the PCB of the smart meter other than the processor. There seemed to be no separate storage because the smart meter had a low performance and sends data to the DCU.

Serial communication was performed through PuTTy, which was a terminal application. Data were output normally at the time of connection, but an administrator account was required to access the shell. A login was attempted using an ID/password (ID/PW) combination frequently used for the administrator account—i.e., root/admin. After accessing the shell, the directory of the DCU internal storage was searched. Figure 15 presents a search of the internal directory of the DCU, and it was confirmed that the DCU uses the Linux 2.6.39 version and JFFS2 and UBIFS as file systems. Data were extracted using the log storage function and the hex dump command supported by PuTTy. The internal storage of the DCU had a log file, as shown in Figure 16, and the date and time were obtained using the DCU.

On applying hardware interface analysis to the DCU, a serial port was found on the PCB and the internal storage data was dumped. No administrator account information was obtained, but an administrator account could be obtained with a frequently used combination. If the default ID/PW is not changed, it is essential to change the default login combination because an attacker can steal the device's permissions. This administrator account may be useful in future studies of network packet data analysis when installing certificates on DCUs.

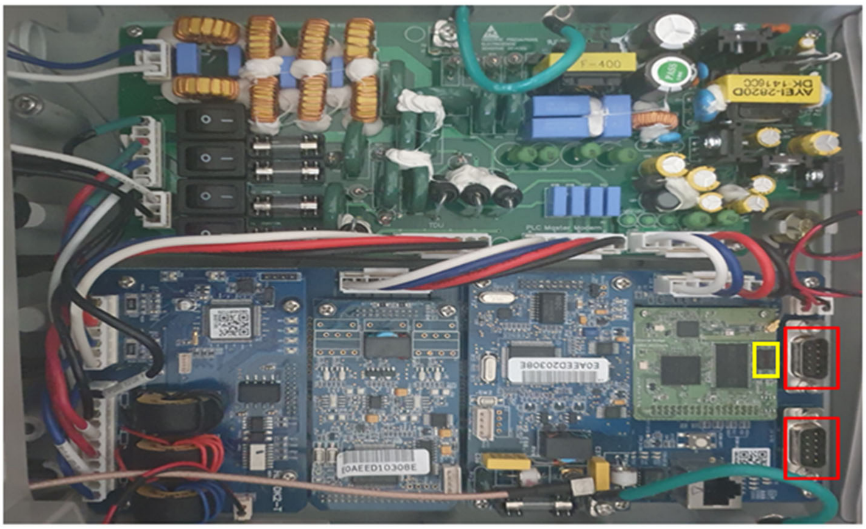


Figure 13. PCB of DCU (yellow and red squares indicate NAND flash memory chip and RS-232 serial communication port, respectively).

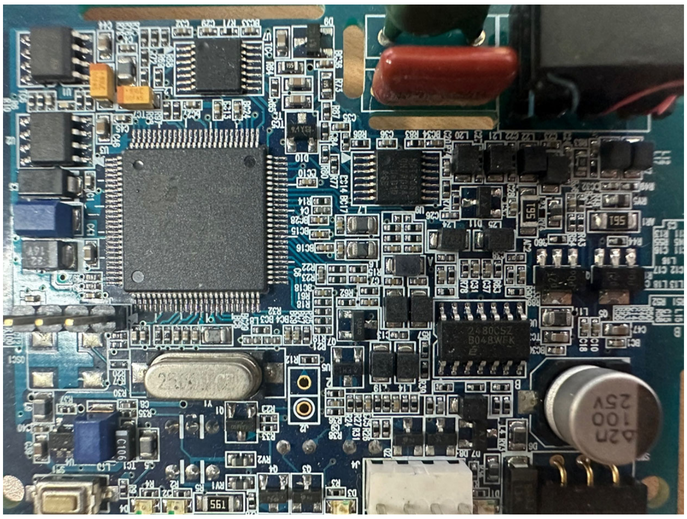
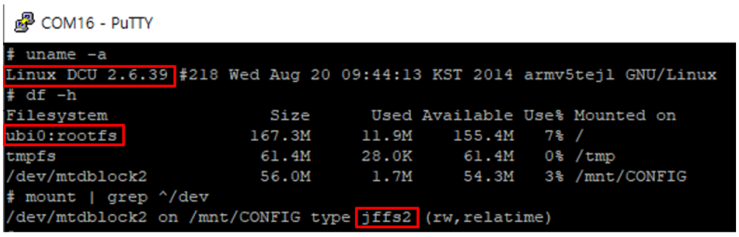
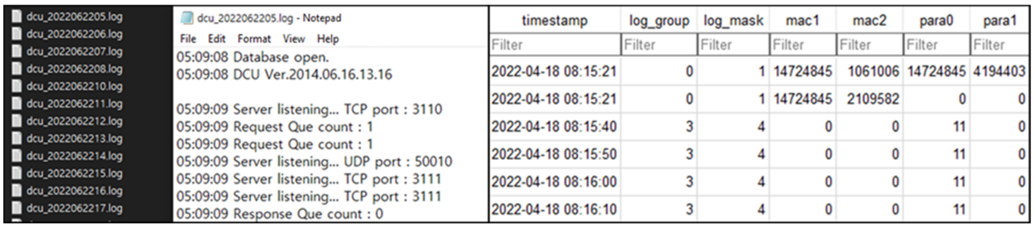


Figure 14. PCB of smart meter.



```
# uname -a
Linux DCU 2.6.39 #218 Wed Aug 20 09:44:13 KST 2014 armv5tejl GNU/Linux
# df -h
Filesystem                Size      Used Available Use% Mounted on
ubi0:rootfs             167.3M     11.9M    155.4M   7% /
tmpfs                    61.4M     28.0K     61.4M   0% /tmp
/dev/mtdblock2           56.0M      1.7M     54.3M   3% /mnt/CONFIG
# mount | grep ^/dev
/dev/mtdblock2 on /mnt/CONFIG type jffs2 (rw,relatime)
```

Figure 15. File system and OS used by DCU.



```
dcu_2022062205.log
dcu_2022062206.log
dcu_2022062207.log
dcu_2022062208.log
dcu_2022062210.log
dcu_2022062211.log
dcu_2022062212.log
dcu_2022062213.log
dcu_2022062214.log
dcu_2022062215.log
dcu_2022062216.log
dcu_2022062217.log
```

```
05:09:08 Database open.
05:09:08 DCU Ver.2014.06.16.13.16

05:09:09 Server listening... TCP port : 3110
05:09:09 Request Que count : 1
05:09:09 Request Que count : 1
05:09:09 Server listening... UDP port : 50010
05:09:09 Server listening... TCP port : 3111
05:09:09 Server listening... TCP port : 3111
05:09:09 Response Que count : 0
```

timestamp	log_group	log_mask	mac1	mac2	para0	para1
Filter	Filter	Filter	Filter	Filter	Filter	Filter
2022-04-18 08:15:21	0	1	14724845	1061006	14724845	4194403
2022-04-18 08:15:21	0	1	14724845	2109582	0	0
2022-04-18 08:15:40	3	4	0	0	11	0
2022-04-18 08:15:50	3	4	0	0	11	0
2022-04-18 08:16:00	3	4	0	0	11	0
2022-04-18 08:16:10	3	4	0	0	11	0

Figure 16. DCU usage log files obtained via DCU hardware interface analysis.

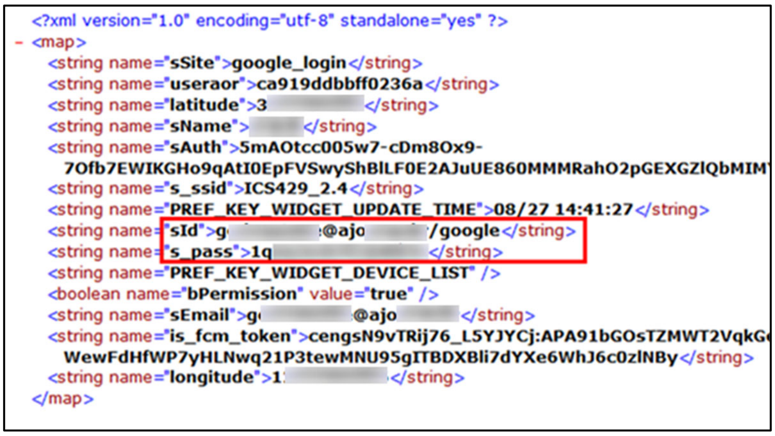
5.2.2. Attack Scenario for Hardware Interface Analysis

It is more difficult for an attacker to physically acquire E-IoT devices than to acquire network packets. However, if an attacker physically acquired an E-IoT device, it may obtain more precise log data than the network packet analysis. An attacker may replace a part of the hardware or change its access permissions, making it inaccessible to an administrator. Physical attacks can also affect higher communication layers [31].

5.3. Mobile Device Paired with E-IoT Devices

5.3.1. Smart Plug

Smart plugs use buttons or paired mobile devices to control power. Data were acquired after pairing smartphones with smart plugs. As a result of analyzing the data of the mobile device, it was confirmed that the app data of the smart plug was stored in the directory "/data/data/com.dawon.aipm/.". Figure 17 presents the username, Wi-Fi information, email ID, and PW in the "heritPreference.xml" file obtained on analyzing the directory. The PW and email ID, which are user-sensitive data, are stored in plaintext.



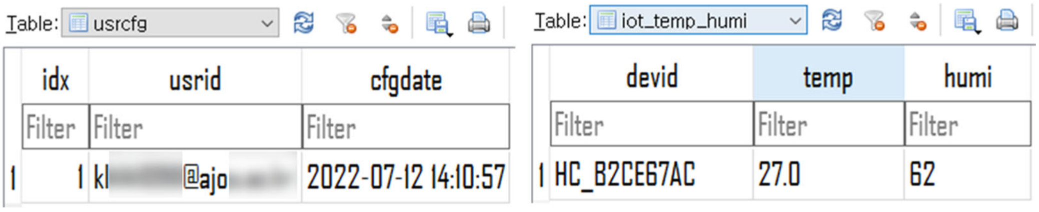
```
 <?xml version="1.0" encoding="utf-8" standalone="yes" ?>
- <map>
   <string name="sSite">google_login</string>
   <string name="useraor">ca919ddbbff0236a</string>
   <string name="latitude">3[redacted]</string>
   <string name="sName">[redacted]</string>
   <string name="sAuth">5mAOtcc005w7-cDm8Ox9-
     7Ofb7EWIKGHo9qAtI0EpFVSwyShBlLF0E2AJuUE860MMMRahO2pGEXGZlQbMIM
   <string name="s_ssid">ICS429_2.4</string>
   <string name="PREF_KEY_WIDGET_UPDATE_TIME">08/27 14:41:27</string>
   <string name="sId">g[redacted]@ajo[redacted]/google</string>
   <string name="s_pass">1q[redacted]</string>
   <string name="PREF_KEY_WIDGET_DEVICE_LIST" />
   <boolean name="bPermission" value="true" />
   <string name="sEmail">g[redacted]@ajo[redacted]</string>
   <string name="is_fcm_token">cengsN9vTRij76_L5YJYCj:APA91bGOsTZMWT2VqkG
     WewFdHfWP7yHLNwq21P3tewMNU95gITBDXBli7dYXe6WhJ6c0zlNBy</string>
   <string name="longitude">1[redacted]</string>
 </map>
```

Figure 17. User email ID and PW obtained from "heritPreference.xml" file.

On applying the mobile device paired with the E-IoT device to the smart plug, the app package data of the smart plug could be obtained. An email ID and PW were obtained by analyzing the app package of the smart plug. As the email and PW used for the login are stored in plaintext, sensitive personal information can be exposed to attackers, which can result in serious privacy issues. Therefore, PWs should be encrypted such that attackers cannot obtain them.

5.3.2. Smart Heat Controller

A smart heat controller is a smart IoT control system that controls the temperature in a room. The temperature can be controlled remotely through a paired mobile device. On analyzing the data of the paired mobile device, it was confirmed that the Garam heat controller app data was stored in the "/data/data/kr.co.karam.bos" directory. Figure 18 presents the user and energy information obtained on analyzing "database.db" file. information of the user email IDs, user registration times, room temperature, and humidity were acquired. Although there were no sensors to measure temperature and humidity on the smart heat controller itself, the temperature and humidity information measured by the thermometer paired with the heat controller were obtained.



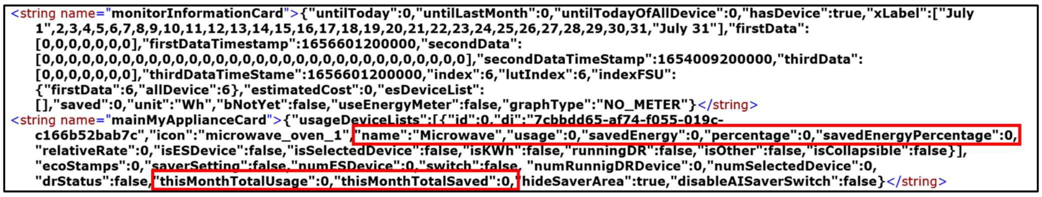
idx	usrid	cfgdate
1	kl[redacted]@ajo[redacted]	2022-07-12 14:10:57

devid	temp	humi
HC_B2CE67AC	27.0	62

Figure 18. User information (**left**) and room temperature/humidity information (**right**) obtained from "database.db" file.

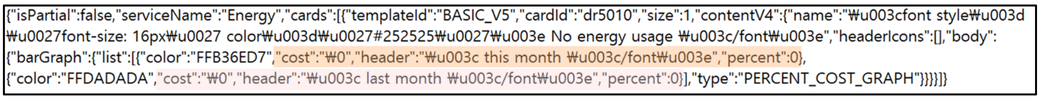
5.3.3. Smart Microwave

The smart microwave remotely controls and records usage information through a paired mobile device. On analyzing the data of the paired mobile device, it was found that the app data of the smart microwave was stored in the "/data/data/com.samsung.android.oneconnect" directory. User and energy data were obtained by analyzing the directory. Figure 19 presents the "com.samsung.android.pluginplatform.pluginbase.sdk.PluginDataStorageImpl.d94e8ce8-bf6e-4c62-b58e-3b3542ebde07.xml" file obtained from the "shared_prefs" directory. The name of the device wherein the energy was measured (Microwave) and the amount of power used (0) were recorded. The amount of power was recorded up to the total usage for the device being measured (thisMonthTotalUsage). In addition, saved energy and percent were recorded, so the previous power usage can be inferred. Figure 20 presents the "PUBLIC_DR_4c803bc6-22cb-48f5-9b53-5cb5f885bbf1.txt" file acquired from the "cache" directory. It was possible to identify the energy usage (this month) and costs (0) according to usage in this file.



```
<string name="monitorInformationCard">{"untilToday":0,"untilLastMonth":0,"untilTodayOfAllDevice":0,"hasDevice":true,"xLabel":["July
    1",2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,"July 31"],"firstData":
    [0,0,0,0,0,0,0],"firstDataTimestamp":1656601200000,"secondData":
    [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0],"secondDataTimeStamp":1654009200000,"thirdData":
    [0,0,0,0,0,0,0],"thirdDataTimeStame":1656601200000,"index":6,"lutIndex":6,"indexFSU":
    {"firstData":6,"allDevice":6},"estimatedCost":0,"esDeviceList":
    [],"saved":0,"unit":"Wh","bNotYet":false,"useEnergyMeter":false,"graphType":"NO_METER"}</string>
<string name="mainMyApplianceCard">{"usageDeviceLists":[{"id":0,"di":"7cbbdd65-af74-f055-019c-
    c166b52bab7c","icon":"microwave_oven_1","name":"Microwave","usage":0,"savedEnergy":0,"percentage":0,"savedEnergyPercentage":0,
    "relativeRate":0,"isESDevice":false,"isSelectedDevice":false,"isKWh":false,"runningDR":false,"isOther":false,"isCollapsible":false}],
    "ecoStamps":0,"saverSetting":false,"numESDevice":0,"switch":false, "numRunnigDRDevice":0,"numSelectedDevice":0,
    "drStatus":false,"thisMonthTotalUsage":0,"thisMonthTotalSaved":0,"hideSaverArea":true,"disableAISaverSwitch":false}</string>
```

Figure 19. Energy measurement devices and usage acquired from the "shared_prefs" directory.



```
{"isPartial":false,"serviceName":"Energy","cards":[{"templateId":"BASIC_V5","cardId":"dr5010","size":1,"contentV4":{"name":"₩u003cfont style₩u003d
₩u0027font-size: 16px₩u0027 color₩u003d₩u0027#252525₩u0027₩u003e No energy usage ₩u003c/font₩u003e","headerIcons":[],"body":
{"barGraph":{"list":[{"color":"FFB36ED7","cost":"₩0","header":"₩u003c this month ₩u003c/font₩u003e","percent":0},
{"color":"FFDADADA","cost":"₩0","header":"₩u003c last month ₩u003c/font₩u003e","percent":0}],"type":"PERCENT_COST_GRAPH"}}}}]}
```

Figure 20. Cost inferred based on energy usage acquired from "cache" directory.

On applying the method of the mobile device paired with the E-IoT device to the smart microwave, the app data of the smart microwave was obtained via the paired mobile device. The energy usage data was acquired by analyzing the app data. This was time-consuming because most of the data obtained from the smart microwave and smart heat controller analyzed in the experiment were stored as database files. Thus, in future works, it is necessary to develop a tool that can easily extract E-IoT-related information from database files.

5.3.4. Attack Scenario for Mobile Device Paired with E-IoT Devices

If an attacker acquires the user's email account and password from a mobile device paired with E-IoT devices, the attacker can know the user's sensitive information. Since the user may use the same or similar password in another account, additional personal information leakage may occur. In addition, card information and financial leakage may occur because it is common to store card information in a web account recently.

6. Discussion

Digital forensics was applied to E-IoT devices that can monitor, control, and manage energy in smart cities. The data obtained using digital forensics are summarized in Table A1.

Some information masked to protect privacy. To analyze the environment of the E-IoT system, the E-IoT and H-IoT systems were categorized as AMI devices, home-energy IoT, and smart home appliances. Based on the analyzed E-IoT system environment, data were acquired and analyzed through the proposed methodology. The proposed methodology consisted of (1) network packet data analysis, (2) hardware interface analysis, and (3) a mobile device paired with an E-IoT. For data collection, AMI devices such as DCUs and smart meters, home-energy IoT devices such as smart plugs and smart heat controllers, and home appliances such as smart microwaves and smart monitoring systems were used.

The network packet data analysis method uses network protocol analysis tools and web proxy tools to acquire packets exchanged between E-IoT and servers. Data such as the device name, user information, and energy usage were obtained from the DCU, smart meter, smart plug, microwave, and monitoring system. It was possible to understand the communication structure by applying network packet data analysis to DCUs and smart meters. As DCUs cannot be paired with mobile devices, in future works, it will be necessary to obtain administrator privileges and install certificates for encrypted packet analysis. Communication and user information were obtained by applying network packet data analysis to the smart monitoring system. Among the user information obtained, email IDs and profile pictures require patches because attackers can use them for crimes such as theft or deepfakes.

Hardware interface analysis identifies a port or memory chip that can be connected to a PC via a PCB of E-IoT. Among the E-IoT devices used in the study, there was a serial port on the PCB of the DCU to extract data. On analyzing the DCU dump image, the usage log was confirmed. The administrator account was unknown; however, the image dump was possible because the default ID/PW of the administrator account was unchanged. If the default is unchanged, an attacker could steal the rights of the device. With this administrator information, further studies can be conducted to obtain encrypted packet data from the network packet data analysis by installing certificates in the DCU internal directory in the future.

The method of using a mobile device paired with E-IoT can be used for acquiring only data related to E-IoT among the data of paired devices. An e-mail account and PW were obtained on applying a mobile device paired with an E-IoT device to a smart plug. The PW was stored in plaintext; it should be double-encrypted because exposure to the attacker can cause serious privacy issues. User account and energy usage information were obtained by applying a mobile device paired with an E-IoT device to a smart heat controller and microwave. Digital forensics for E-IoT obtained significant data, but also had the following three challenges:

(1) Lack of administrator rights to E-IoT devices. There was a limit to the installation of certificates for the web proxy tool in the internal storage of E-IoT devices. To install the web proxy tool certificate in the internal storage of the E-IoT device, the internal data must be accessible. However, it was difficult to access the internal data and it was difficult to install the certificate on the device because there was no administrator authority. Therefore, we analyzed encrypted packets of E-IoT by installing certificates on mobile devices paired with E-IoT. If a web proxy certificate is installed on the device, direct packets between the device and the server can be obtained instead of indirect packets between the mobile device and the server.

(2) Small PCB on some E-IoT devices. Among the devices used in the study, devices other than DCU could not be used to apply the hardware interface analysis method because ports were not available on every device. Except for the DCU and smart meter, the devices were relatively small because they were both E-IoT devices and H-IoT devices. Since the hardware of the device is miniaturized, the PCB was also small. They were combined or miniaturized to embed the processor, memory, and internal storage all on a small PCB. Identification was very difficult because the miniaturized PCB was not even marked.

(3) This was a time-consuming process. Mobile devices have been gradually developed. Many applications and data were stored in the internal storage because more capacity was available. The user data partition on a 64 GB mobile device was approximately 54 GB in size. As the size of the mobile device increased, the size of the user data partition also increased. To collect data related to E-IoT, the file storage structure of the mobile device must be analyzed in advance. Among the analyzed data, E-IoT-related app package data must be collected. E-IoT app package data should be analyzed to select meaningful artifacts. This was time consuming because it had to be analyzed individually.

7. Conclusions

With the global expansion of urban infrastructure and development of 5G technology, advanced ICT has been applied to energy systems and the use of smart grids has increased. Smart grid systems acquired energy data using IoT devices such as DCUs and smart meters to effectively manage energy. This study acquired E-IoT devices data for digital forensics to E-IoT devices used for energy management in smart cities, such as DCUs, smart plugs, and smart microwaves, and the possibility of vulnerabilities was analyzed. A test bed was established for the digital forensics of E-IoT devices. DCUs and smart meters used in Korean power systems were used to build a test bed similar to actual E-IoT environments. Data from E-IoT devices were acquired using proposed methodology. The proposed methodology consisted of three methods: (1) network packet data analysis, (2) hardware interface analysis, and (3) a mobile device paired with E-IoT. This methodology had been applied to DCUs, smart meters, plugs, heat controllers, microwaves, and monitoring systems. User data such as the device name, user account, PW, energy data—such as energy usage—and logs were obtained.

In the near future, E-IoT devices will be essential in smart homes, smart factories, and smart cities. In this study, network packet data, internal storage data, and the paired device data of E-IoT devices were analyzed. Vulnerabilities and personal information exposure were identified. Digital forensics for E-IoT devices can also be applied to devices not used in research and can be used for personal information exposure checks before E-IoT is shipped. In future work, we intend to conduct research on the installation of certificates in the internal storage of DCUs. We also intend to develop tools for analyzing database files and extracting user/system information. The E-IoT system is an environment wherein stability and reliability are important and data forensics is thus essential. Based on this study, we intend to digital forensics for E-IoT used in energy management systems and energy storage systems.

Author Contributions: Conceptualization, M.K. and T.S.; methodology, M.K. and T.S.; validation, M.K.; formal analysis, M.K.; investigation, M.K.; writing—original draft preparation, M.K.; writing—review and editing, M.K. and T.S.; project administration, T.S. All authors have read and agreed to the published version of the manuscript.

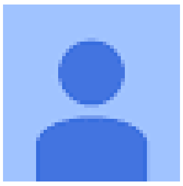
Funding: This research was supported by the Energy Cloud R&D Program through the National Research Foundation of Korea (NRF), funded by the Ministry of Science ICT (NRF-2019M3F2A1073385).

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

Table A1. Artifacts Acquired Through E-IoT Digital Forensics.

Method	E-IoT	Data	Artifact	Package
Network packet data analysis	LoenK DCU	Device information	TestICS	-
	Dawon DNS smart plug	Operating system	Linux x86_64	-
		Access time	Mon, 10 May 2021 04:34:04 GMT	-
	Samsung smart microwave	Session ID	f363596dc600e3ccca8dc0ea6aff709…	-
		TLS version	TLS 1.3	-
		Device connection	1 July 2022 11:36:16 KST, 1656642651820(Unix time)	-
		Access token	725056107548211%7C0e20c3123a9…	-
		Cookies	SID=KgjGnTWM06cEWV...	-
		Energy usage	Null (=0)	-
	Dawon DNS smart monitoring system	Smartphone information	SM-A325N	-
		Smartphone OS	Android 11	-
		User name	M**** Kim	-
		User email	te********@gmail.com	-
		Profile picture		-
Hardware interface analysis	LoenK DCU	Operating system	Linux 2.6.39	-
		File system	JFFS2, UBIFS	-
		Log	dcu_2022062205.log	-
Mobile device paired with E-IoT	Dawon DNS smart plug	User information	D****** Shin, go********@ajo*******	com.dawon.aipm/shared_prefs/heritPreference.xml
		Password	1q***********	
		Location	3*.*******, 1**.*******	
	Karam smart heat controller	User email	kl*******@ajo*******	kr.co.karams.bos/databases/database.db
		Access time	12 July 2022 14:10:57	
		Temperature and humidity	Temperature: 27.0 °C; humidity: 62%	
	Samsung smart microwave	device ID	7cbbdd65-af74-f055-019c-c166b52bab7c	com.samsung.android.oneconnect/database/Common Data.db
		Device status	Online, 7 July 2022T15:39:29.000+09:00	
		User information	J*** Lee, j**********@gmail.com	
		Energy usage	Usage: 0; Saved energy: 0	com.samsung.android.oneconnect/shared_prefs/com.samsung.android.pluginplatform.pluginbase.sdk.PluginDataStorageImpl.d94e8ce8-bf6e-4c62-b58e-3b3542ebde07.xml
		Device information	Microwave	
		Energy usage	Percent: 0, cost: 0	com.samsung.android.oneconnect/cache/PUBLIC_DR_4c853bc6-22cb-48f5-9b53-5cb5f885bbf1.txt

References

1. CNN. Future or Fantasy? Designs Unveiled for One-Building City Stretching 106 Miles in Saudi Arabia. Available online: https://edition.cnn.com/style/article/saudi-arabia-the-line-city-scli-intl/index.html (accessed on 8 March 2023).
2. Neom. The Future of Energy. Available online: https://www.neom.com/en-us/ourbusiness/sectors/energy (accessed on 8 March 2023).

3. Ardito, L.; Procaccianti, G.; Menga, G.; Morisio, M. Smart grid technologies in Europe: An overview. *Energies* **2013**, *6*, 251–281. [CrossRef]
4. Jo, W.; Kim, S.; Kim, H.; Shin, Y.; Shon, T. Automatic whitelist generation system for ethernet based in-vehicle network. *Comput. Ind.* **2022**, *142*, 103735. [CrossRef]
5. Kim, S.; Jo, W.; Shon, T. APAD: Autoencoder-based payload anomaly detection for industrial IoE. *Appl. Soft Comput.* **2020**, *88*, 106017. [CrossRef]
6. Abdullah, H.I.M.; Mustaffa, M.Z.; Rahim, F.A.; Ibrahim, Z.A.; Yusoff, Y.; Yussof, S.; Ramli, R. Smart grid digital forensics investigation framework. In Proceedings of the 2020 8th International Conference on Information Technology and Multimedia (ICIMU), Selangor, Malaysia, 24–26 August 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 200–205.
7. Abdullah, H.I.M.; Ibrahim, Z.A.; Rahim, F.A.; Fadzil, H.S.; Nizam, S.A.S.; Mustaffa, M.Z. Digital Forensics Investigation Procedures of Smart Grid Environment. *Int. J. Comput. Digit. System* **2021**, *11*, 1071–1082. [CrossRef]
8. Roberts, A. fraMework for industrial control systeMs digital forensics in the energy sector. In Proceedings of the 5th Interdisciplinary Cyber Research Conference, Tallinn, Estonia, 29 June 2019; p. 24.
9. Grammatikis, P.R.; Sarigiannidis, P.; Iturbe, E.; Rios, E.; Sarigiannidis, A.; Nikolis, O.; Ramos, F. Secure and private smart grid: The spear architecture. In Proceedings of the 2020 6th IEEE Conference on Network Softwarization (NetSoft), Ghent, Belgium, 29 June–3 July 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 450–456.
10. Parra, G.D.L.T.; Rad, P.; Choo, K.-K.R. Implementation of deep packet inspection in smart grids and industrial Internet of Things: Challenges and opportunities. *J. Netw. Comput. Appl.* **2019**, *135*, 32–46. [CrossRef]
11. Gómez, J.M.C.; Carrillo-Mondéjar, J.; Martínez, J.L.M.; García, J.N. Forensic analysis of the Xiaomi Mi Smart Sensor Set. *Forensic Sci. Int. Digit. Investig.* **2022**, *42*, 301451. [CrossRef]
12. Jo, W.; Shin, Y.; Kim, H.; Yoo, D.; Kim, D.; Kang, C.; Shon, T. Digital forensic practices and methodologies for AI speaker ecosystems. *Digit. Investig.* **2019**, *29*, S80–S93. [CrossRef]
13. Shin, Y.; Kim, H.; Kim, S.; Yoo, D.; Jo, W.; Shon, T. Certificate injection-based encrypted traffic forensics in AI speaker ecosystem. *Forensic Sci. Int. Digit. Investig.* **2020**, *33*, 301010. [CrossRef]
14. SmartThings. SmartThings Energy. Available online: https://www.smartthings.com/partners/smartthings-energy (accessed on 9 May 2023).
15. Kwon, S.; Yoo, H.; Shon, T. IEEE 1815.1-based power system security with bidirectional RNN-based network anomalous attack detection for cyber-physical system. *IEEE Access* **2020**, *8*, 77572–77586. [CrossRef]
16. Bug's Entrypoint. I Got Bored, So I Hacked My TV. Available online: https://blog.rgsilva.com/i-got-bored-so-i-hacked-my-tv/ (accessed on 1 May 2023).
17. Swaroop, K.N.; Chandu, K.; Gorrepotu, R.; Deb, S. A health monitoring system for vital signs using IoT. *Internet Things* **2019**, *5*, 116–129. [CrossRef]
18. Wireshark. Available online: https://www.wireshark.org/ (accessed on 4 April 2023).
19. PortSwigger. Available online: https://portswigger.net/burp (accessed on 4 April 2023).
20. Tawalbeh, L.A.; Muheidat, F.; Tawalbeh, M.; Quwaider, M. IoT Privacy and security: Challenges and solutions. *Appl. Sci.* **2020**, *10*, 4102. [CrossRef]
21. Samsung. RS-232 on Samsung TV's. Available online: https://www.samsung.com/us/support/troubleshooting/TSG01201603/ (accessed on 28 April 2023).
22. Ishtiaq, A.; Khan, M.U.; Ali, S.Z.; Habib, K.; Samer, S.; Hafeez, E. A review of system on chip (soc) applications in internet of things (iot) and medical. In Proceedings of the ICAME21, International Conference on Advances in Mechanical Engineering, Islamabad, Pakistan, 25 August 2021; pp. 1–10.
23. Servida, F.; Casey, E. IoT forensic challenges and opportunities for digital traces. *Digit. Investig.* **2019**, *28*, S22–S29. [CrossRef]
24. Kim, M.; Shin, Y.; Jo, W.; Shon, T. Digital forensic analysis of intelligent and smart IoT devices. *J. Supercomput.* **2023**, *79*, 973–997. [CrossRef]
25. Mathur, A.; Cao, M.; Bhattacharya, S.; Dilger, A.; Tomas, A.; Vivier, L. The new ext4 filesystem: Current status and future plans. In Proceedings of the Linux Symposium, Ottawa, ON, Canada, 27 June 2007; Volume 2, pp. 21–33.
26. Fairbanks, K.D. An analysis of Ext4 for digital forensics. *Digit. Investig.* **2012**, *9*, S118–S130. [CrossRef]
27. Kim, H.; Shin, Y.; Kim, S.; Jo, W.; Kim, M.; Shon, T. Digital Forensic Analysis to Improve User Privacy on Android. *Sensors* **2022**, *22*, 3971. [CrossRef] [PubMed]
28. Exterro. FTK Imager. Available online: https://www.exterro.com/ftk-imager (accessed on 7 March 2023).
29. DB Browser for SQLite. The Official Home of the DB Browser for SQLite. Available online: https://sqlitebrowser.org/ (accessed on 7 March 2023).

30. Procopiou, A.; Komninos, N. Current and future threats framework in smart grid domain. In Proceedings of the 2015 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER), Shenyang, China, 8–12 June 2015; IEEE: Piscataway, NJ, USA, 2015; pp. 1852–1857.
31. Andrea, I.; Chrysostomou, C.; Hadjichristofi, G. Internet of Things: Security vulnerabilities and challenges. In Proceedings of the 2015 IEEE Symposium on Computers and Communication (ISCC), Larnaca, Cyprus, 6–9 July 2015; IEEE: Piscataway, NJ, USA, 2015; pp. 180–187.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.