Computers, Materials & Continua

Tech Science Press

Doi:10.32604/cmc.2025.063687

ARTICLE

A Common Architecture-Based Smart Home Tools and Applications Forensics for Scalable Investigations

Sungbum Kim[1], Gwangsik Lee[2], Jian Song[2], Insoo Lee[2] and Taeshik Shon[3,*]

[1]Department of AI Convergence Network, Ajou University, Suwon, 16499, Republic of Korea
[2]Forensic Science Investigation Department, Supreme Prosecutors' Office 157, Seoul, 02435, Republic of Korea
[3]Department of Cyber Security, Ajou University, Suwon, 16499, Republic of Korea

*Corresponding Author: Taeshik Shon. Email: tsshon@ajou.ac.kr

Received: 21 January 2025; Accepted: 21 February 2025; Published: 26 March 2025

ABSTRACT: The smart home platform integrates with Internet of Things (IoT) devices, smartphones, and cloud servers, enabling seamless and convenient services. It gathers and manages extensive user data, including personal information, device operations, and patterns of user behavior. Such data plays an essential role in criminal investigations, highlighting the growing importance of specialized smart home forensics. Given the rapid advancement in smart home software and hardware technologies, many companies are introducing new devices and services that expand the market. Consequently, scalable and platform-specific forensic research is necessary to support efficient digital investigations across diverse smart home ecosystems. This study thoroughly examines the core components and structures of smart homes, proposing a generalized architecture that represents various operational environments. A three-stage smart home forensics framework is introduced: (1) analyzing application functions to infer relevant data, (2) extracting and processing data from interconnected devices, and (3) identifying data valuable for investigative purposes. The framework's applicability is validated using testbeds from Samsung SmartThings and Xiaomi Mi Home platforms, offering practical insights for real-world forensic applications. The results demonstrate that the proposed forensic framework effectively acquires and classifies relevant digital evidence in smart home platforms, confirming its practical applicability in smart home forensic investigations.

KEYWORDS: Digital forensic; forensic framework; internet of things; smart home; smart home platform

1 Introduction

Advances in software and hardware technologies have made factories, vehicles, homes, and infrastructure increasingly smart [1]. As a result, companies and countries are focusing on research and development in areas such as networks, devices, and cybersecurity to expand smart industries [2,3]. In the smart home industry, appliance manufacturers, mobile carriers, and construction companies are increasingly investing in smart home solutions, while numerous companies are introducing IoT devices through both proprietary and third-party platforms.

As smart home services expand, IoT devices generate and store vast amounts of data. This data is stored both within the devices and on cloud servers of smart home platforms, and it includes sensitive user information such as phone numbers, emails, and home addresses, as well as logs and timestamps that track user behavior. From a forensic perspective, this data plays a crucial role in identifying suspects and providing evidence of criminal activities. For example, if an intruder unlawfully enters a residence, sensor activation

records can confirm the exact time of the intrusion. Even if the perpetrator attempts to tamper with evidence by damaging a smart camera, forensic techniques can restore and recover the stored footage. Additionally, cloud forensics can help retrieve video data stored in the smart home platform's cloud.

Investigation agencies and research institutes have been conducting studies on data acquisition and analysis using various smart home IoT devices such as home cameras, AI speakers, smart plugs, and smartphones to broaden the scope of digital investigations [4–6]. However, due to the continuous development and application of new IoT technologies, it is difficult to apply existing research directly. Moreover, since smart homes are built on diverse platforms, studies that focus solely on the forensic analysis of individual devices have limitations in real-world investigations.

IoT devices consist of various software and hardware components, generating and storing different types of data depending on their functions. Furthermore, the complex interconnections among IoT devices lead to distributed data storage. These challenges make it difficult to develop a standardized forensic framework for IoT environments [7–9]. In most smart home setups, platforms such as Amazon Alexa and Google Home are used by consumers, providing common components like security products (e.g., smart cameras and door locks) and domestic appliances (e.g., smart refrigerators and washing machines).

Traditional methods that focus on isolated devices are increasingly inadequate for addressing the evolving complexity of smart home environments. Therefore, scalable and adaptable research frameworks are essential to integrate and analyze data across diverse IoT ecosystems effectively. In this study, we propose a layer-based architecture that represents smart home structures using common components to overcome the limitations of current smart home IoT forensics. This layered smart home architecture can be applied to actual IoT environments during investigations, allowing for efficient identification of complex interconnections. Based on this architecture, we also propose a smart home forensic framework that analyzes the functions of IoT devices to infer the types of generated data, acquires the actual data, and classifies it according to its characteristics. By inferring the data, investigators can pinpoint the target IoT device to extract the artifacts needed for a specific event. Classifying data based on its characteristics further enables rapid identification of necessary evidence corresponding to different types of crimes. We validate the proposed framework using the Samsung SmartThings and Xiaomi Mi Home platforms.

The contributions of this study are as follows: 1) It classifies meaningful elements from a digital forensics perspective by identifying components common to smart home ecosystems. 2) It derives a common structure for smart homes in the form of a layered architecture based on these components, thereby laying the foundation for smart home forensics. 3) It proposes a forensic framework applicable to general smart home environments. The framework infers the data generated in a smart home and extracts it from actual devices, classifying the artifacts into device use data, user data, and smart home environment identification data, which facilitates subsequent investigations. 4) It demonstrates a method for utilizing the extracted artifacts through data inference and extraction on the Samsung SmartThings and Xiaomi Mi Home platforms, confirming the framework's applicability in a general smart home setting.

The remainder of this paper is organized as follows. Section 2 describes smart home components and structures, Section 3 reviews smart home forensic research, Section 4 explains the common structure of smart homes based on these components, Section 5 presents the forensic framework for smart home environments, Section 6 verifies the framework through forensic analysis on the Samsung SmartThings and Xiaomi Mi Home platforms, Section 7 discusses the study, and Section 8 concludes the paper.

2 Background

The concept of a smart home emerged as users began utilizing a wide range of IoT devices to access various services within their homes. Several researchers have proposed frameworks or models to perform smart home forensics [10,11]. In the context of smart home forensics, it is important to identify the components constituting the smart home environment. Smart homes generally follow the same structure as the one depicted in Fig. 1. IoT devices are interconnected seamlessly to offer diverse services, enabling users to control and manage them both within and outside their homes. These devices communicate with devices and cloud servers through various network protocols for smart home services. Devices can be connected wirelessly, such as via Wi-Fi, as well as through wired connections like Ethernet. In addition, devices such as sensors are connected using low-power wireless communication such as Bluetooth, ZigBee, and Z-wave. These connected IoT devices generate a wide range of data, which is stored in the devices' internal storage and on cloud servers. Data stored on cloud servers can be used to remotely control and manage apps installed on management devices such as smartphones and tablets. This section describes the components constituting the smart home environment.

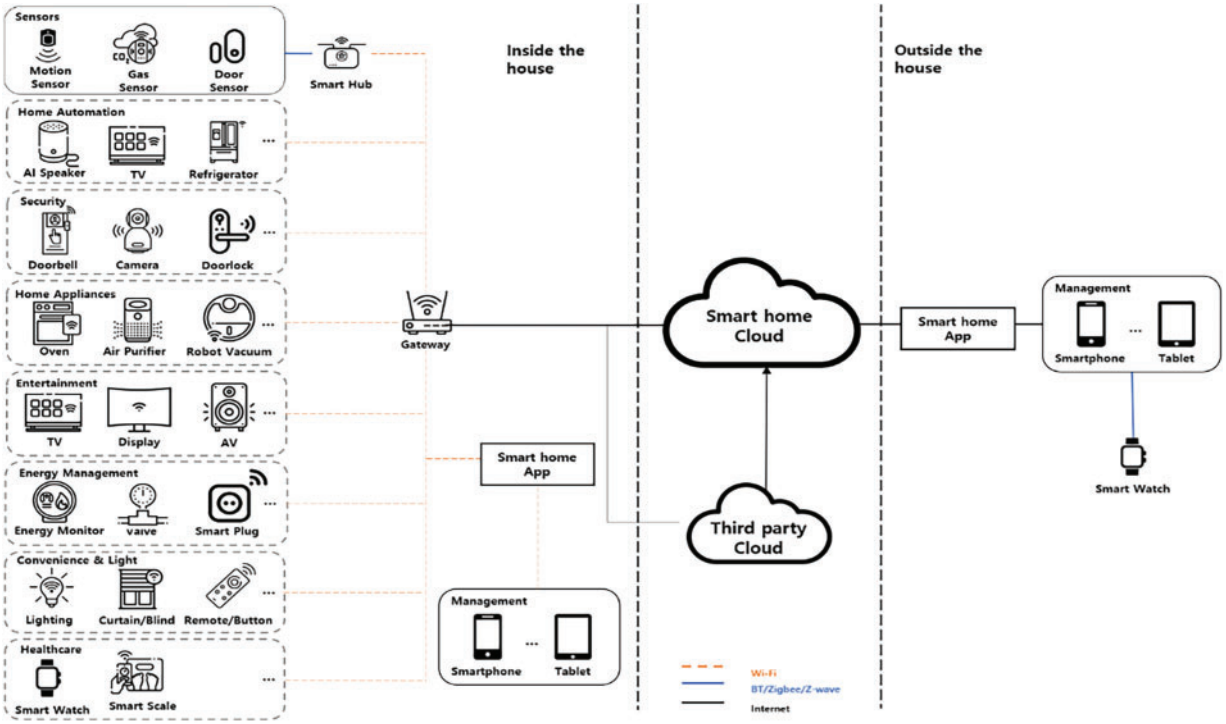


Figure 1: Structure of smart home ecosystem

Smart home IoT devices represent the most basic form of smart home construction. These devices are created by embedding hardware (HW) and software (SW) components—such as a central processing unit (CPU) and an operating system (OS)—into conventional household appliances like washing machines, televisions, and speakers, while adding additional functionalities. Moreover, they enable new services through devices not typically found in homes, such as crime prevention sensors and smart meters.

These devices offer specialized functionalities, communicate with cloud servers, and can be controlled and managed via smartphone apps. In addition, some devices are designed to control other smart home devices.

Companies and users classify smart home services based on functionality. Consequently, users choose and install the IoT devices required to access their desired smart home services. For example, home cameras and crime prevention sensors are purchased and utilized for residential security. Thus, IoT devices are categorized according to the services they provide, which facilitates the inference of the type of data they generate.

To manage the growing number of IoT devices and services, smart home platforms have emerged, enabling users to control their devices efficiently. Currently, major companies are developing a range of devices and technologies to establish dominance within the smart home ecosystem, while small and medium-sized companies collaborate with these giants to enhance compatibility and market their IoT devices. Although most platforms offer similar services, subtle variations and distinctions exist among them. Identifying these commonalities and differences is important from a forensic perspective.

Cloud servers play a crucial role by integrating, managing, and controlling smart home applications while facilitating scalable home configurations through software development kits (SDKs) and application programming interfaces (APIs). As a result, a wide variety of data is stored on these servers. In particular, many miniaturized and integrated IoT devices rely on cloud servers due to their limited internal storage. Consequently, forensic investigations in smart home environments may employ methods such as packet analysis to infer data stored on cloud servers.

Smart homes comprise various components that exchange data using a range of communication protocols. While protocols such as Ethernet and Wi-Fi are commonly used, low-power alternatives like Bluetooth and Z-wave are also available. In addition, management applications installed on devices such as smartphones and tablets control these components, and hubs and gateways facilitate sensor connectivity. The protocols and devices involved in these interactions are significant for forensic analysis, as they help reveal the overall communication structure among components.

3 Related Works

The smart home environment stores data generated by IoT devices and provides services to users based on that data. Since this data originates in residential areas, it holds significant forensic value. Consequently, various forensic studies have been conducted on IoT devices and smartphones. For instance, Castelo Gómez et al. conducted a forensic study on smart home kits—comprising hubs and sensors—by acquiring data from Xiaomi Mi smart sensor sets and linked smartphones, thereby obtaining several smart home artifacts from related applications [12]. Similarly, Boucheraud et al. undertook forensic research in IoT environments based on crime scenarios. They configured a home IoT environment using smart bulbs, cameras, sensors, scales, and wearable devices in addition to home automation devices such as AI speakers, Raspberry Pis, and hubs. Their analysis involved logical extraction via APIs and Android Debug Bridge (ADB) as well as physical extraction using Joint Test Action Group (JTAG) and Chip-Off techniques [13]. Li et al. proposed a forensic process centered on physical extraction techniques for IoT devices, utilizing 3D printers and pogo pins to connect to interfaces such as JTAG and Universal Serial Bus (USB), and evaluated five different data acquisition methods [14]. In another study, Kim et al. performed data acquisition and analysis on smartphone applications linked to IoT devices by connecting Google Nest, SmartThings, and Kasa Cam to corresponding apps, and successfully extracted voice command information, phone data, and smart home device information [15]. Iqbal et al. conducted a forensic analysis on five types of smart plugs, analyzing data from connected smartphones and examining communication packets using Wireshark. Hutchinson et al. studied the August Smart Doorbell Pro and August Smart Lock Pro by linking both routed and isolated smartphones to these devices; they collected network traffic via Wireshark and extracted user data, location data, and doorbell camera images through smartphone analysis with administrative rights [16]. Furthermore,

Kim et al. proposed a digital forensic methodology focusing on wallpads—smart home management devices with displays. They built a testbed using wallpads from Samsung, Kocom, and Commax, and extracted and analyzed network packets, disk images, and files using both logical and physical acquisition techniques. Their work successfully identified user-related information and multimedia files stored on these devices [17]. Additionally, Youn et al. conducted a forensic study on the Echo Show 2nd, an AI speaker with a display, extracting and analyzing data to propose a smart display digital forensics framework [18]. Although most smart home forensic studies to date have concentrated on individual IoT devices and smartphones—such as AI speakers and smartwatches [19–22]—and have provided detailed methodologies for analyzing device-generated data, they remain largely device-centric. These studies lack a standardized forensic framework that can be applied across different smart home ecosystems. Moreover, most users interact with smart home environments through integrated platforms rather than through individual IoT devices. While existing research offers valuable forensic methodologies, it does not fully address the challenges posed by smart home platforms, which serve as central hubs for device management and user interaction. This gap underscores the need for a comprehensive forensic framework that encompasses both individual IoT devices and platform-level interactions. Therefore, this study proposes a common architecture for smart homes along with a forensic framework that is applicable to general smart home environments. To validate the proposed framework, we establish a platform-level testbed that mirrors real-world smart home usage, ensuring a more holistic and applicable forensic methodology.

4 Smart Home Common Architecture

For forensic frameworks applicable to modern smart home environments, it is crucial to identify common components and structural elements. Smart homes operate primarily through the Internet of Things (IoT), where IoT devices contain key forensic elements such as cameras, memory, and operating systems (OS). These devices generate different types of data depending on their product family, even when they offer similar services. These services are integrated and managed by centralized platforms, each of which varies in its supported devices and services based on the company that operates it. Platforms are interconnected via cloud servers, providing compatibility and management services through APIs, software development kits (SDKs), and smart home applications. The smart home ecosystem relies on various wired and wireless communication technologies and is primarily controlled via management devices such as smartphones and tablets. Given this complexity, the core components of a smart home can be categorized into five main layers: cloud servers, platforms, services, IoT devices, and device components. In this study, we propose a common smart home architecture based on a layered model. The designed architecture consists of five layers, as illustrated in Fig. 2, where communication and management functions are implemented vertically across all layers. For instance, AI speakers comprise device components such as microphones and speakers, along with hardware/software elements like CPUs, memory, and OS. As integral components of smart home ecosystems, they facilitate centralized control and automation. At the service layer, AI speakers provide home automation functionalities that vary based on the smart home platform they are integrated with. If the platform belongs to a home appliance manufacturer, it may support a broader range of home appliances, whereas IT-driven platforms may emphasize IT service integrations. The smart home platform communicates with cloud servers via applications, enabling remote control and device management. New devices can be linked through APIs and SDKs at the cloud layer. Additionally, smart home systems are typically managed via smartphones and tablets, while communication protocols such as Ethernet, 4G, and Wi-Fi facilitate connectivity at each stage.

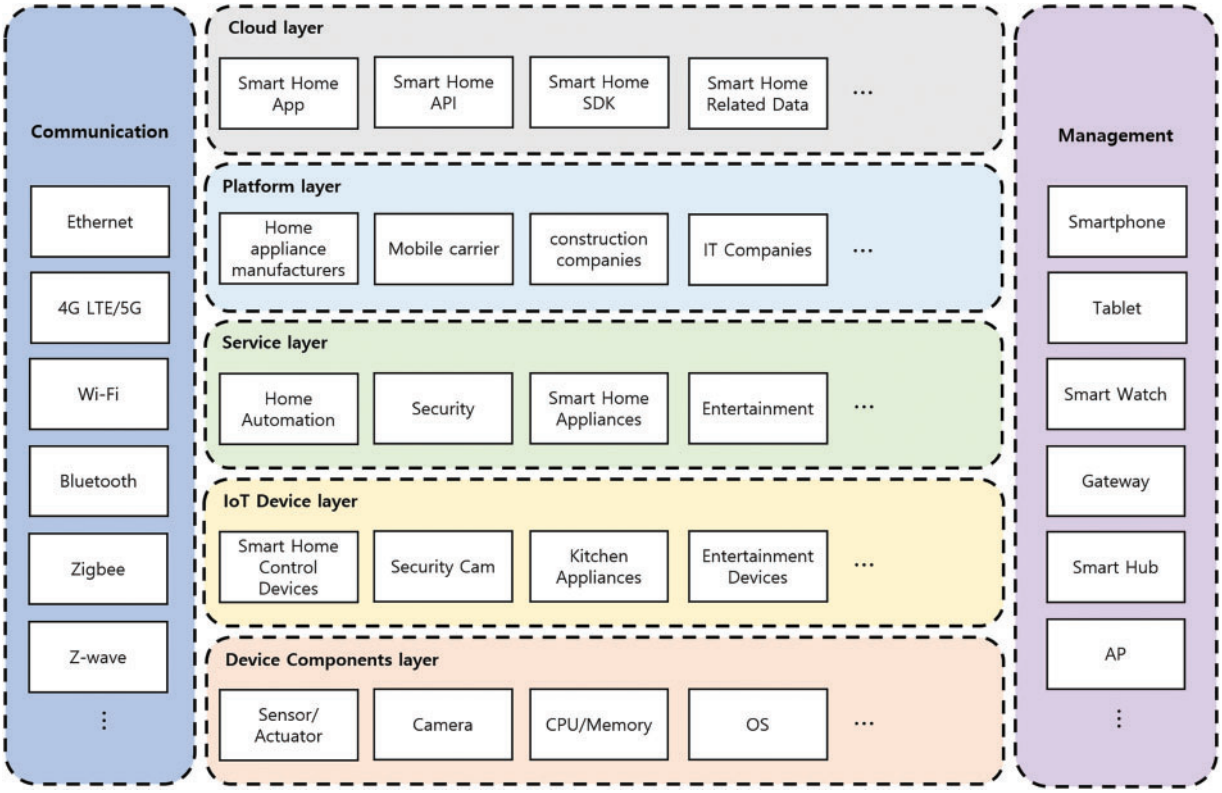


Figure 2: Smart home common architecture

The cloud layer, located at the top, is a key element in smart home operations and functions based on the smart home's cloud server. This layer comprises smart home applications, SDKs, APIs, and data related to smart home services. The platform layer encompasses smart home platforms provided by companies such as home appliance manufacturers and mobile carriers. These platforms deliver smart home services by integrating their own and third-party services and devices through cloud servers. The service layer consists of a variety of offerings provided by the platform, including home automation, crime prevention and security, and smart home appliance services. The IoT device layer includes the actual IoT devices that enable these services. Various devices are used for different purposes; for example, AI speakers and hubs support home automation, while smart door locks, doorbells, and smart home cameras cater to security services. The device components layer refers to the internal parts of smart home IoT devices, including hardware such as sensors, actuators, cameras, and CPUs, as well as software elements like operating systems. Data stored on these devices can be inferred from the components that constitute them. In addition to these five layers, the architecture incorporates elements for interlayer communication and smart home management. Communication between layers and devices utilizes low-power protocols such as Bluetooth, Zigbee, and Z-Wave, as well as Ethernet, 4G/5G, and Wi-Fi. Moreover, management is facilitated through devices such as smartphones, tablets, hubs, and gateways. The seamless interaction between these layers and components enables smart home platforms to provide platform-specific services. This common architecture encapsulates the shared elements of smart homes and is adaptable to the unique characteristics of various smart home platforms. Consequently, it can be applied across different smart home systems and scaled to accommodate newly released smart home technologies.

5 Forensic Analysis Framework for Smart Home Ecosystem

The common architecture includes most components of the smart home environment. And we propose a framework for smart home forensics using smart home environment information derived from the common architecture (see Fig. 3). The forensic framework consists of three stages, as shown in Fig. 4: 1) functional analysis-based data inference, 2) real-world device-based data identification, and 3) data identification available for criminal investigation. App service analysis is performed to infer data in the smart home environment. Smart homes can generally be controlled and managed through platform apps installed on management devices such as smartphones. Therefore, it is possible to infer data generated through common functions of IoT devices and platforms via app analysis. By inferring data, it is possible to narrow the scope of analysis by selecting the target device, which can help conduct an efficient forensic investigation. Second, the data to be analyzed is extracted and examined. Smart home data can exist in cloud servers, management devices, or in-device storage, and this stage identifies where the inferred data is stored. Finally, the identified data are classified according to their characteristics. Data types can be classified into device use data, user data, and smart home environment identification data, and these data types vary depending on the event.

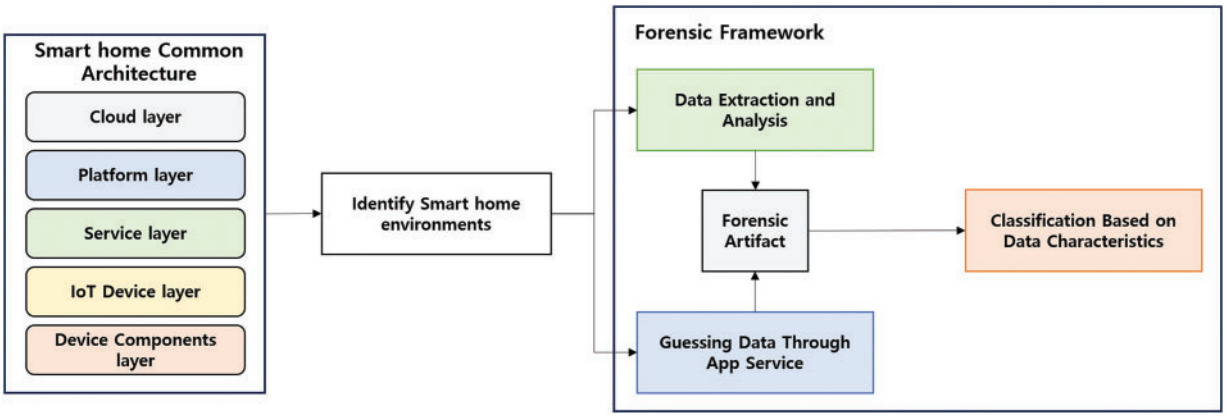


Figure 3: Smart home forensics diagram

5.1 Stage 1: Guessing Data through APP Service Analysis

In general, the smart home environment is managed and controlled through a smartphone application. IoT devices are linked to cloud servers using smartphones to communicate smart home-related data and provide services. Although some sensors are limited to low-power wireless communication, all IoT devices transmit and receive data via cloud servers and Wi-Fi, as they communicate with servers through hubs in conjunction with smart hubs. Therefore, because most smart home services are provided based on the functions of smartphone applications, it is possible to identify these services and device functions through smartphone app function analysis, which in turn allows for data inference. Although various devices may be present at an investigation site, extracting and analyzing data from all devices is often impractical due to numerous restrictions. Consequently, inferring the stored data forms the basis for selecting a target device for data extraction. For example, in a residential intrusion incident, the analysis may focus on devices such as home cameras—inferring that they store images of outsiders—rather than on devices like smart TVs and AI speakers.

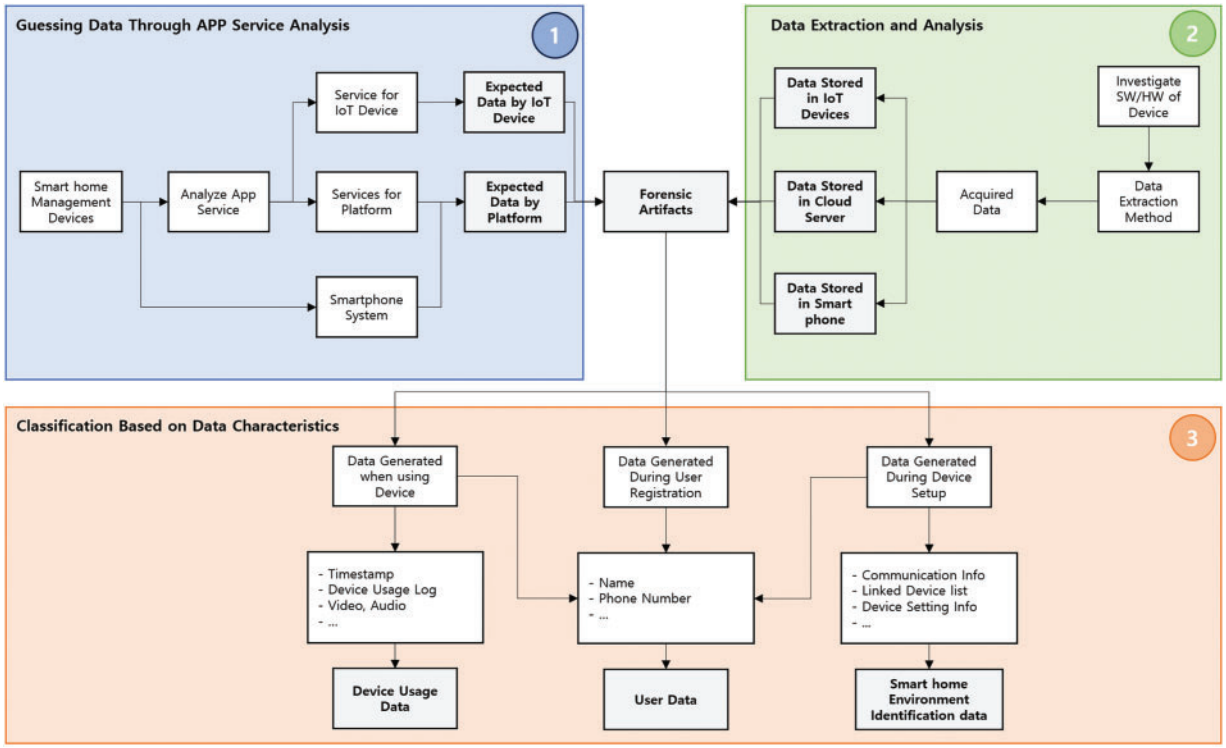


Figure 4: Forensics analysis framework based on smart home platform common architecture (Stage 1 derives the expected data, while Stage 2 extracts the actual acquired data. The actual data predicted through the expected data is integrated as forensic artifacts.)

Identification data in the smart home platform may be composed of two types: expected data for each device and common expected data for the platform. The expected data for each device is data generated to provide unique functions for each service and device, and the expected data varies depending on the device's function. Platform-common expected data is data generated throughout the component through platform-specific functions, and the expected data has different characteristics depending on platform-common functions and management device systems. For data in a management device system, expected data can be identified through various smartphone analysis studies. Therefore, it is possible to derive common expected data for each device and platform through smart home application function analysis.

5.2 Stage 2: Data Extraction and Analysis

The data inferred through functional analysis is validated by applying specific device-targeted data acquisition methods, allowing us to pinpoint the storage location, which can be classified as device, cloud, or management device. When data resides on a device, it is extracted using methods tailored to that device after comprehensive software and hardware analysis; extraction is feasible if internal storage is present, and techniques include logical extraction—via a direct connection between the IoT device and a PC—and physical extraction using Universal Asynchronous Receiver-Transmitter (UART), JTAG, or Chip-off methods. When data is stored in the cloud, it is identified through analysis of device-to-cloud communication packets, which requires that the device supports Wi-Fi and that packets can be captured using a PC's mobile hotspot function. For management devices, typically smartphones, established forensic data acquisition methods are employed, and once data is retrieved, further extraction is conducted through a detailed analysis of the application data stored on the management device.

5.3 Stage 3: Classification Based on Data Characteristics

Smart home data can be composed of three types based on data characteristics through functional analysis and data identified through actual devices. Device usage data' is data that can identify the alibi of the person who used the device through the device usage log. The 'smart home environment identification data' can identify the configuration of the smart home environment, and more data can be obtained through other acquisition methods using the data. The 'smart home environment identification data' includes communication information, device specification information, device identification information, and a list of linked devices.

6 Case Studies for Forensics Analysis of Smart Home Platforms

To validate the proposed forensic framework, we established a smart home platform test bed and conducted a comprehensive forensic analysis. The smart home platform is configured as illustrated in Fig. 5, and the test bed was designed accordingly. The configurations of the Samsung SmartThings and Xiaomi Mi Home test beds used in the experiment are detailed in Table 1. For management devices, we employed a routed Samsung Galaxy S9+ running Android 10. These test beds acquire artifacts through data inference and extraction and develop methods for utilizing these artifacts in scenarios similar to those encountered in the home of a suspect in a fugitive murder case.

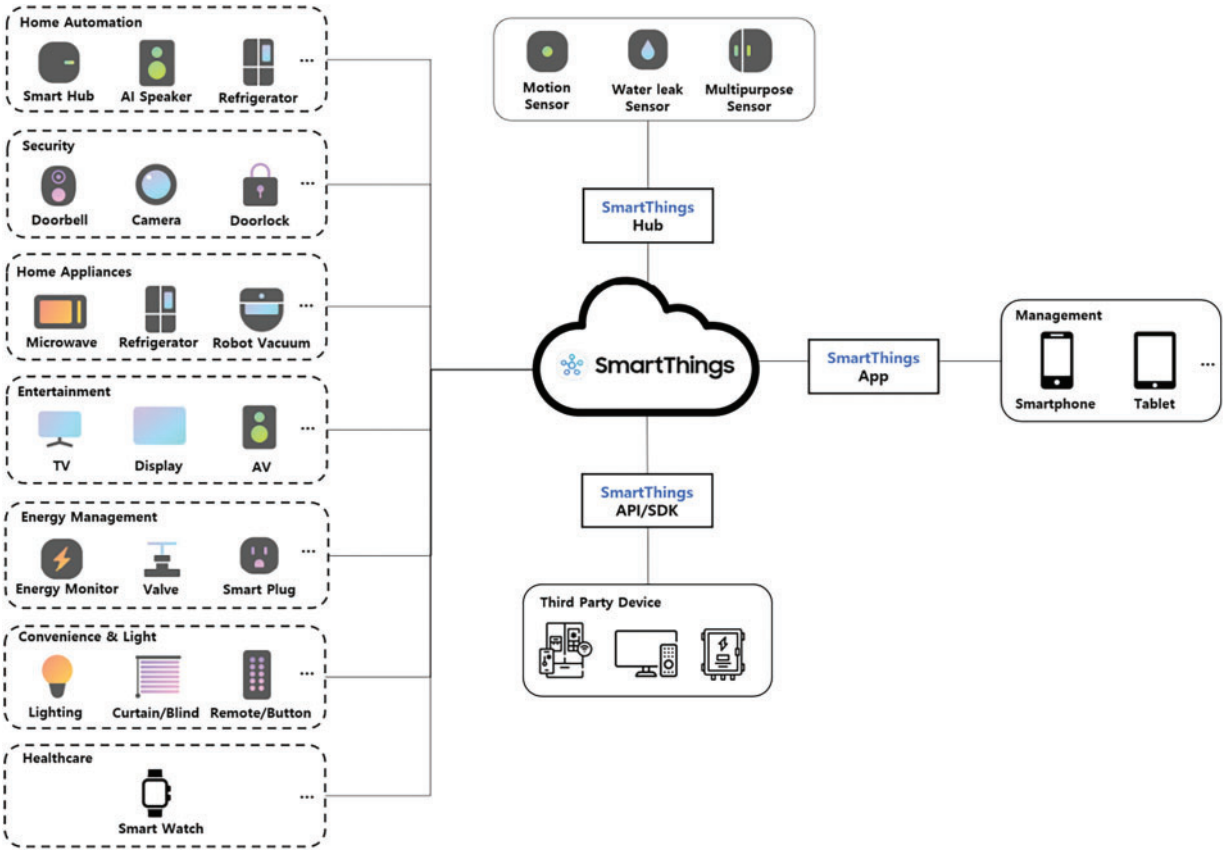


Figure 5: Example of samsung smartthings platform configuration

Table 1: Device type and model name of IoT device used in the experiment

Smart home platform	Device	Model
Samsung SmartThings	AI speaker	sm-v310
	Smart hub	IOT-V3P03
	Door sensor	IOT-MPP03
	Motion sensor	IOT-MTP03
	Smart button	IOT-BTP03
	Doorlock	ECK-300
	Robot vacuum	VR30T80313W
	Smart plug	PM-B550E-W
	Air monitor	ACM-B1M0S
	Smart watch	PM-B550E-W
	Smart tag	EI-T5300BBEGKR
	Smart desk lamp	MT428D21K
	IP camera	MJSXJ09CM
Xiaomi Mi Home	Robot vacuum	Xiaomi Dreame Robot vacuum F9
	Smart TV	L55M5-5ASP
	Air purifier	AC-M16-SC
	Smart watch	SYB01

6.1 Samsung SmartThings

6.1.1 Guessing Data through APP Service Analysis

Through analysis of smart home app functions, we can identify the services provided by smart home devices and infer the expected data based on these functions. For example, with SmartThings, the entire smart home environment is controlled via the "SmartThings" application, which in turn allows us to determine the functions of linked devices. Fig. 6 shows the main feature tab of the Galaxy Home Mini, an AI speaker, revealing the available functions of Samsung AI speakers. These speakers offer features such as alarms, timers, reminders, and music playback. Additionally, the setup function indicates that network information—such as Wi-Fi MAC addresses—is stored along with details on the AI speaker's location, user preferences, and user accounts. As illustrated in Table 2, the inferred stored data may reside on the device itself, cloud servers, or smartphones, a finding that can be confirmed through actual data analysis.

6.1.2 Data Extraction and Analysis

The data expected earlier can be divided into three types of storage: internal storage of the device, cloud server, and management device (smartphone). Accordingly, data acquisition was performed by targeting each data store.

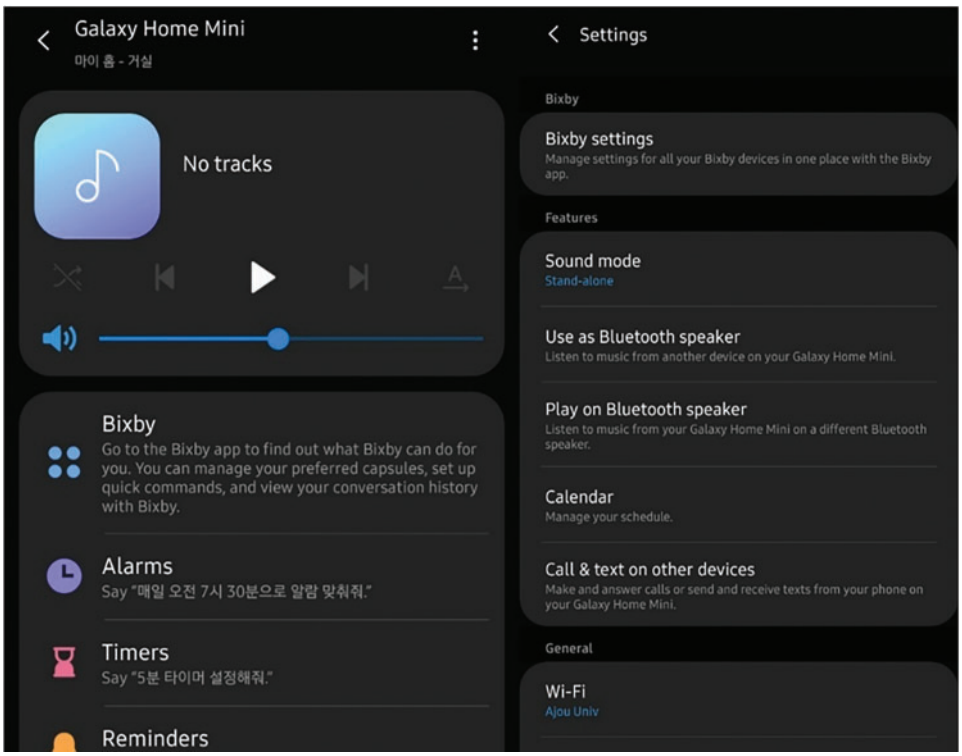


Figure 6: Galaxy home mini function of samsung smartthings smartphones

Table 2: Expected data according to SmartThings IoT device type

Device	Expected data
AI speaker	Setup info, Voice history, Alarm/timer/reminder info, Linked third-party info, Network info
Smart hub	Device on/off info, A List of devices linked to the smart hub
Door sensor	Real-time temperature info, Door open history info
Motion sensor	Motion detection record info, Temperature info
Smart button	Usage history, Settings info
Doorlock	Lock status info, door lock operation record
Robot vacuum	Scheduled cleaning settings info, cleaning history
Smart plug	Energy consumption, device usage records
Air monitor	Co2, temperature and humidity info by time zone
Smart watch	User health info
Smart tag	location info, recording instrument location
Smart Desk lamp	usage history, settings info

Data in Device Storage

To perform data acquisition inside IoT devices, it is necessary to first verify the presence or absence of storage inside the device through device specification analysis. Through device specification analysis, devices with internal storage are AI speakers, smart hubs, robot vacuum cleaners, air monitors, and smartwatches. For AI speakers, 4 GB Nand Flash memory (KLM4G1FETE-B041, 153ball) was identified, and data were acquired through chip-off as shown in Fig. 7. The separated chip could extract dump images after connecting to a PC through a flash memory reader. The dump image was mounted on Linux to identify the partition and extract the image. Because of the mount, a dump image and partition of 3.7 GiB capacity could be identified as shown in Fig. 8. In addition, as shown in Fig. 9, it is estimated that the 16th partition, known as the user partition, is based on the examination of the partition using FTK Imager.

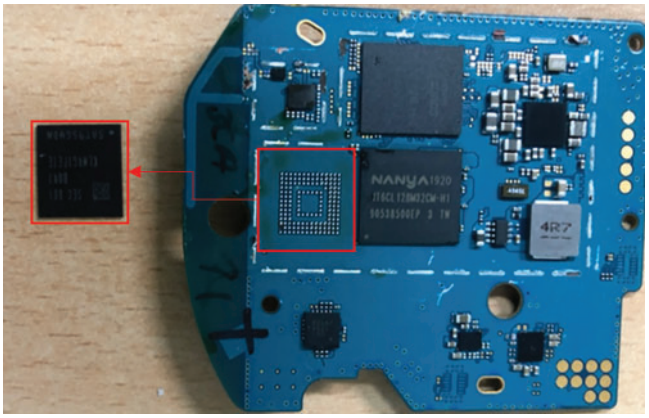


Figure 7: Nand flash memory in galaxy home mini PCB

```
Disk /dev/sdb: 3.7 GiB, 3909091328 bytes, 7634944 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: gpt
Disk identifier: 52444E41-494F-2044-4D4D-43204449534B

Device       Start     End Sectors  Size Type
/dev/sdb1     8192    9215    1024  512K Microsoft basic data
/dev/sdb2     9216   65535   56320 27.5M Microsoft basic data
/dev/sdb3    65536   81919   16384    8M Microsoft basic data
/dev/sdb4    81920  122879   40960   20M Microsoft basic data
/dev/sdb5   122880  139263   16384    8M Microsoft basic data
/dev/sdb6   139264  155647   16384    8M Microsoft basic data
/dev/sdb7   155648  163839    8192    4M Microsoft basic data
/dev/sdb8   163840  196607   32768   16M Microsoft basic data
/dev/sdb9   196608  229375   32768   16M Microsoft basic data
/dev/sdb10  229376  782335  552960  270M Microsoft basic data
/dev/sdb11  782336 1105919  323584  158M Microsoft basic data
/dev/sdb12 1105920 1146879   40960   20M Microsoft basic data
/dev/sdb13 1146880 1148927    2048    1M Microsoft basic data
/dev/sdb14 1148928 1159167   10240    5M Microsoft basic data
/dev/sdb15 1159168 1179647   20480   10M Microsoft basic data
/dev/sdb16 1179648 4956159 3776512  1.8G Microsoft basic data
/dev/sdb17 4956160 7630847 2674688  1.3G Microsoft basic data
/dev/sdb18 7630848 7631359     512  256K Microsoft basic data
```

Figure 8: Mounted galaxy home mini dump image

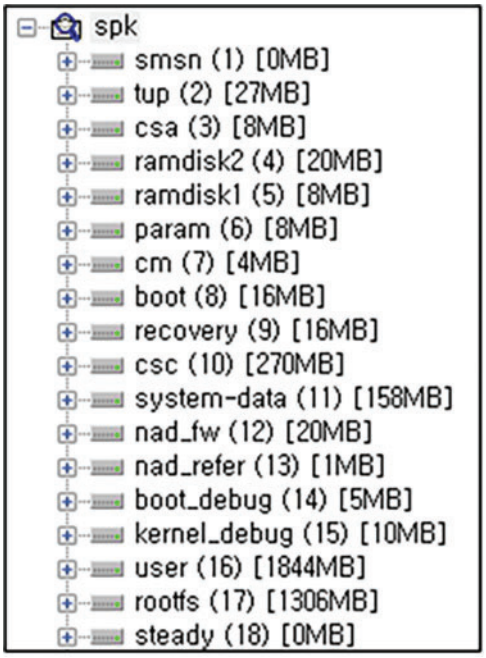


Figure 9: Galaxy home mini partition list (FTK Imager)

Multiple artifacts can be obtained from the database file stored in the AI speaker dump image. For instance, as shown in Fig. 10, the 'device_table' in 'sc.db' currently holds a list of smart home-linked devices. Additionally, the 'Unique_table' in 'cloud_pdm.db' stores the login ID used to link the account, as illustrated in Fig. 11; this login ID is typically an email address. It was also confirmed that device setting information—including the user's name, date of birth, and timer settings—is stored.

	id	name	groupid	type	vid	mnmn	version	nick	color
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	3077adc2-670f-46ed-8de4-f55b26e5f4d0		cf4b8f85-eaab-4575-b95f-aa74888f30f6	oic.wk.d	NULL	NULL	NULL	Multipurpose Sensor	
2	43b8f6d1-7abd-4318-a13d-68d66402fead	허브 Hub	cf4b8f85-eaab-4575-b95f-aa74888f30f6	x.com.st.d.hub	NULL	NU	Hub	허브	
3	2d9f184b-157c-4edd-8fbb-339ce309d00b		cf4b8f85-eaab-4575-b95f-aa74888f30f6	oic.wk.d	NULL	NULL	NULL	Motion Sensor	
4	f988b56f-9e3f-430b-8138-011b4cebd5b2		cf4b8f85-eaab-4575-b95f-aa74888f30f6	oic.wk.d	NULL			C2O Door Lock	
5	b8183fe4-4d82-f400-c746-32dfb068073e	LED Stand	cf4b8f85-eaab-4575-b95f-aa74888f30f6	oic.d.light	NULL	Smart LED Light		스마트 LED 스탠드	
6	347f8387-ea5e-dc3c-de00-8c4aedbb7788	Galaxy Home Mini (HWYZ)	cf4b8f85-eaab-4575-b95f-aa74888f30f6	oic.d.networkaudio	NULL			Galaxy Home Mini (HWYZ)	
7	58505373-c309-4662-a257-61fd386094ce		cf4b8f85-eaab-4575-b95f-aa74888f30f6	oic.wk.d	NULL	NULL	NULL	Button	
8	0601f7e5-a779-4a2b-bb7f-8baf0a9ca625	78e36d05ba01	cf4b8f85-eaab-4575-b95f-aa74888f30f6	oic.d.smartplug	NULL	NULL	NULL	78e36d05ba01	
9	59c2a831-1520-4004-b2d9-09140800fae2	SmartTag	b0994a8b-3dc8-437b-90ed-c9efdab8cb48	x.com.st.d.tag	NULL	Robot cleaner		SmartTag	
10	1a4ed374-6748-e1b1-7288-48658841bded	[robot vacuum] Samsung	cf4b8f85-eaab-4575-b95f-aa74888f30f6	oic.d.robotcleaner	NULL			로봇청소기	

Figure 10: 'Device_table' table in 'home/owner/apps_rw/com.samsung.lux-st-service/data/sc.db' (accessed on 1 February 2025)

For robot vacuum cleaners, 4 GB Nand Flash memory of the same model as AI speakers were identified, and dump images were similarly extracted using chip-off. In the robot vacuum cleaner image, cleaning records including cleaning start timestamps were stored in the 'History table' of 'history_new3.db' as shown in Fig. 12. In addition, information on the reservation cleaning time set by the user was stored.

	key	val	resv
	Filter	Filter	Filter
1	guid	k1w71jf2ba	
2	login_id	ics.smarthome.iot@gmail.com	
3	account_id	1	

Figure 11: 'Unique_table' table in 'home/owner/apps_rw/com.samsung.tizen.samsung-cloud/data/.cloud_pdm.db' (accessed on 1 February 2025)

	id	start_time	utc_time	clean_type	suction	area	elapsed_time	error	success_info	fail_info	area_count	cleaning_option	is_uploaded
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	1	1665054290	1665054305	7	0	BLOB	0	58	NULL	NULL	NULL	2	1
2	2	1665055218	1665055371	1	2	BLOB	2	58	NULL	[Room]	BLOB	2	1
3	3	1665055526	1665055543	1	0	BLOB	0	58	NULL	[Room][Room 2][Room 3]	BLOB	2	1
4	4	1665056996	1665057014	1	2	BLOB	0	58	NULL	[Room][Room 2][Room 3]	BLOB	2	1

Figure 12: 'History' table in '/home/owner/apps_rw/org.tizen.ocfd/data/history/history_new3.db' (accessed on 1 February 2025)

For smart hubs, the same model, 4 GB Nand Flash memory, could be identified and the image dumped, but internal data could not be verified because of disk encryption through LUKS, as shown in Fig. 13. In addition, for air monitors, Nand Flash memory was identified as a result of printed circuit board (PCB) analysis, but internal extraction was infeasible owing to the absence of a reader capable of reading the memory, and for smartwatches, Nand Flash memory could not be identified.

```
0000000 4C 55 4B 53 BA BE 00 01-61 65 73 00 00 00 00 00 LUKS°¾··aes·····
0000010 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0000020 00 00 00 00 00 00 00 00-78 74 73 2D 70 6C 61 69 ········xts-plai
0000030 6E 36 34 00 00 00 00 00-00 00 00 00 00 00 00 00 n64·············
0000040 00 00 00 00 00 00 00 00-73 68 61 32 35 36 00 00 ········sha256··
```

Figure 13: Hub V3 partition disk encryption for samsung smartthings

Cloud Server

Most smart home IoT devices communicate with cloud servers via Wi-Fi, allowing communication packets between the wall pad and the cloud to be captured using a PC's mobile hotspot function. Since these packets exchange information related to device usage and user data, it is possible to infer the data stored on the cloud server, which may be useful for future warrant issuance screening. However, the contents of packets from AI speakers remain unknown because most are encrypted with TLS, as shown in Fig. 14, and the same applies to other devices.

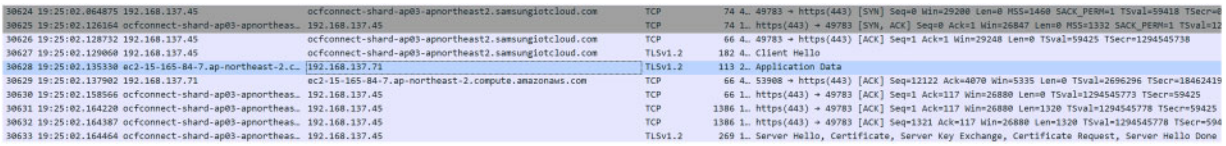


Figure 14: Packets generated when using AI speakers

Smartphone

Given that all IoT devices are managed through a dedicated application, it is evident that a smartphone stores a wealth of related information. In our experiment, the smartphone was pre-rooted, and its dump image was acquired via ADB. Within the application's data directory, several database files were identified. For example, the devices table in CloudDb.db contains a list of interconnected devices, as illustrated in Fig. 15. Additionally, the Messages table in NotificationDb.db logs system notifications and timestamps—for instance, hub connection messages and cleaning start/end events, as shown in Fig. 16. Furthermore, the smartphone retains user personal information linked to SmartThings, as well as device-specific settings and network information.

deviceName	nick	permission	modelId	deviceType	mnmnType
Filter	Filter	Filter	Filter	Filter	Filter
SmartThings v3 Hub	허브	1	x.com.st.d.hub&SmartThings@SmartThin…	x.com.st.d.hub	2
motion-temp-battery	Motion Sensor	1	x.com.st.d.sensor.motion&SmartThingsCo…	x.com.st.d.sensor.motion	2
	Multipurpose Sensor	1	x.com.st.d.sensor.multifunction&SmartThi…	oic.wk.d	2
one-button-temp-battery	Button	1	x.com.st.d.button&SmartThingsCommunit…	x.com.st.d.button	2
dawon-switch-power-energy-prod-0908	78e36d05ba01	1	oic.d.smartplug&DawonDNS@dawon-…	oic.d.smartplug	2
LED Stand	스마트 LED 스탠드	1	oic.d.light&SmartThings@SmartThings-…	oic.d.light	2
lock-battery	C2O Door Lock	1	oic.d.smartlock&SmartThingsCommunity…	oic.d.smartlock	2
SmartTag	SmartTag	1	x.com.st.d.tag&Samsung Electronics@IM-…	x.com.st.d.tag	2
Galaxy Home Mini (HWYZ)	Galaxy Home Mini (HWYZ)	1	oic.d.networkaudio&Samsung …	oic.d.networkaudio	5
[robot vacuum] Samsung	로봇청소기	1	oic.d.robotcleaner&Samsung …	oic.d.robotcleaner	3
air-monitor-v1-20201123-2-nr	에어모니터	1	x.com.st.d.airqualitysensor&SmartThings…	x.com.st.d.airqualitysensor	2
dawon-switch-power-energy-prod-0908	78e36d05ba01	1	oic.d.smartplug&DawonDNS@dawon-…	oic.d.smartplug	2

Hub

Smart LED Light

Robot cleaner

Air monitor

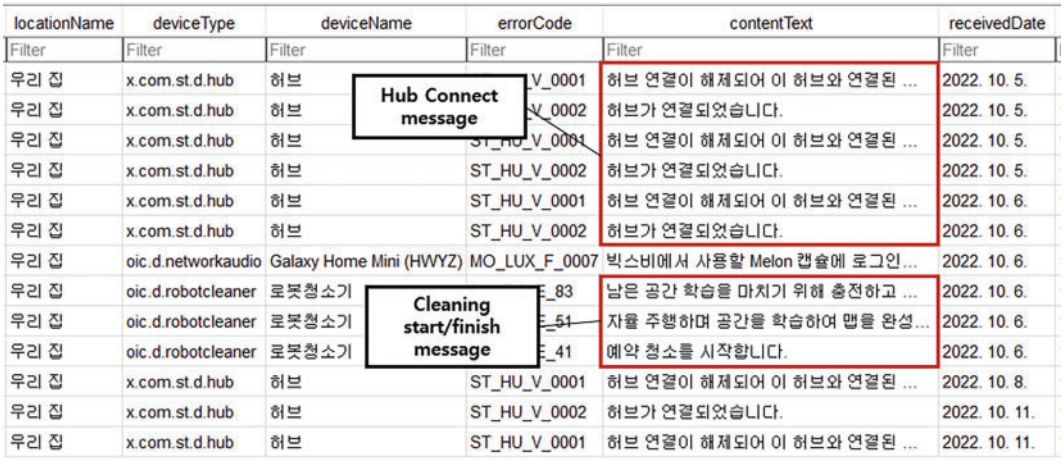
Figure 15: 'devices' table in 'data/com.samsung.android.oneconnect/databases/CloudDb.db' (accessed on 1 February 2025)

6.1.3 Classification Based on Data Characteristics

Acquired data have different utilization methods depending on their characteristics. The data can be broadly divided into three categories: device usage data, user data, and smart home environment identification data. Device usage data reveal the behavior of the device user, user data confirm the identity of the user, and smart home environment identification data clarify the overall configuration of the smart home. Accordingly, in this section, we demonstrate how data utilization methods can be derived for various crime scenarios based on these characteristics.

In this scenario, an in-house murder in a two-person household is investigated using a pre-configured Samsung SmartThings smart home environment to track the alibi of a housemate, who is the prime suspect. The suspect claims he was outside the home at the time of the crime. Prior analysis of the smart home architecture identified the components available within a residence. Since the smart home environment connects various IoT devices—such as AI speakers, TVs, and sensors—via a central gateway, identifying

these components is a crucial first step in the investigation. Accordingly, the investigator secured the AI speaker, robot vacuum cleaner, smart hub, smart button, and the tablet used as a management device linked to SmartThings at the scene.



locationName	deviceType	deviceName	errorCode	contentText	receivedDate
Filter	Filter	Filter	Filter	Filter	Filter
우리 집	x.com.st.d.hub	허브	V_0001	허브 연결이 해제되어 이 허브와 연결된 ...	2022. 10. 5.
우리 집	x.com.st.d.hub	허브	V_0002	허브가 연결되었습니다.	2022. 10. 5.
우리 집	x.com.st.d.hub	허브	ST_HU_V_0001	허브 연결이 해제되어 이 허브와 연결된 ...	2022. 10. 5.
우리 집	x.com.st.d.hub	허브	ST_HU_V_0002	허브가 연결되었습니다.	2022. 10. 5.
우리 집	x.com.st.d.hub	허브	ST_HU_V_0001	허브 연결이 해제되어 이 허브와 연결된 ...	2022. 10. 6.
우리 집	x.com.st.d.hub	허브	ST_HU_V_0002	허브가 연결되었습니다.	2022. 10. 6.
우리 집	oic.d.networkaudio	Galaxy Home Mini (HWYZ)	MO_LUX_F_0007	빅스비에서 사용할 Melon 캡슐에 로그인...	2022. 10. 6.
우리 집	oic.d.robotcleaner	로봇청소기	_83	남은 공간 학습을 마치기 위해 충전하고 ...	2022. 10. 6.
우리 집	oic.d.robotcleaner	로봇청소기	_51	자율 주행하며 공간을 학습하여 맵을 완성...	2022. 10. 6.
우리 집	oic.d.robotcleaner	로봇청소기	_41	예약 청소를 시작합니다.	2022. 10. 6.
우리 집	x.com.st.d.hub	허브	ST_HU_V_0001	허브 연결이 해제되어 이 허브와 연결된 ...	2022. 10. 8.
우리 집	x.com.st.d.hub	허브	ST_HU_V_0002	허브가 연결되었습니다.	2022. 10. 11.
우리 집	x.com.st.d.hub	허브	ST_HU_V_0001	허브 연결이 해제되어 이 허브와 연결된 ...	2022. 10. 11.

Figure 16: 'Messages' table in 'Data/com.samsung.android.oneconnect/databases/NotificationDb.db' (accessed on 1 February 2025)

The components of the smart home environment contain different types of data depending on the platform, service, and IoT device. A functional analysis of the smart home can predict what data are stored, thereby narrowing the range of devices targeted during data acquisition and accommodating even the latest IoT devices. In this investigation, functional analysis of IoT devices linked with Samsung SmartThings was performed to derive expected data; as a result, data acquisition efforts focused on the AI speakers and robot vacuum cleaners. Investigators extracted and analyzed NAND flash memory from both devices using chip-off techniques and corroborated expected findings by analyzing data from a confiscated smartphone application.

As noted above, the acquired data fall into three categories—device usage data, user data, and smart home environment identification data—with each type serving distinct investigative purposes. In this case, where verifying the suspect's alibi is paramount, device usage data are crucial. The investigator inferred that the suspect was at home at the time of the crime by examining cleaning timestamps and reservation settings from the robot vacuum cleaner. Additionally, system notification logs from the tablet controlling the smart home confirmed that both the smart hub and the robot vacuum cleaner generated notifications at the relevant times. Moreover, user data—such as account details, name, and date of birth—retrieved from the AI speakers were used to assess the possibility of accomplices. Finally, by collecting a list of interconnected devices (i.e., smart home environment identification data) from the AI speakers, investigators confirmed the potential for additional evidence from smart lighting and security sensors like Table 3.

Table 3: Devices and data used in the investigation (scenario)

IoT device	Device usage data	Smart home environment identification data	User data
AI speaker	–	Linked device list	User account, name and date of birth
Robot vacuum	Cleaning timestamp, schedule setting time, system notification message	–	–
Smart hub	System notification message	–	–
Smart Button	–	–	–

6.2 Xiaomi Mi Home

6.2.1 Guessing Data through APP Service Analysis

Xiaomi Mi Home also infers expected data based on the functional analysis of the smart home app. For Xiaomi, the entire smart home environment is managed through the "Mi Home" app. Fig. 17 shows the main function tab of the IP camera. In addition to its primary video recording function, the IP camera offers features such as person detection and the replay of previous monitoring records. In this way, the stored data can be inferred, as shown in Table 4. This data may reside on the device, in cloud servers, or on smartphones, which can be confirmed through actual data analysis.

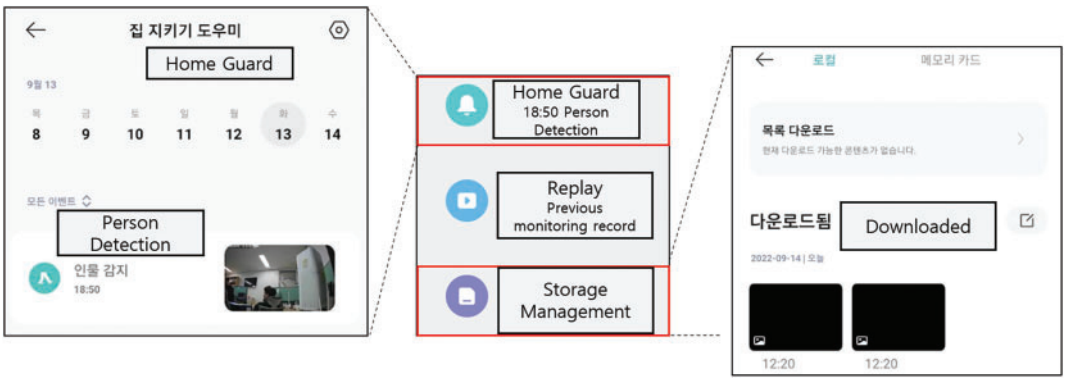


Figure 17: IP camera function in Xiaomi Mi Home app

6.2.2 Data Extraction and Analysis

Data Stored on the Device

Based on device specification analysis, it was determined that devices with internal storage—such as IP cameras and smart TVs—can store data locally. For an IP camera, which saves images on an SD card, data extraction is performed using an SD card reader. When connected to a PC, this reader revealed several JPEG and MP4 files (see Fig. 18). The analysis further showed that the IP camera automatically records a video every minute, storing both thumbnail (.jpeg) and video (.mp4) files.

Table 4: Expected data according to Xiaomi Mi home IoT device type

Device	Expected data
IP camera	Recorded video, person detection record, device settings
Robot vacuum	cleaning record, area cleaned
Smart TV	TV usage history, third-party app information
Air purifier	PM2.5, temperature, humidity
Smart watch	user information

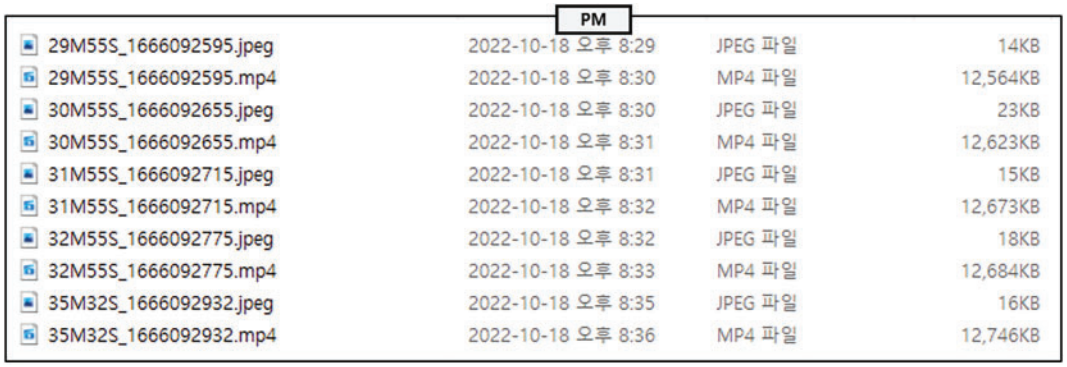


Figure 18: Multimedia files (JPEG, MP4) stored on the IP camera memory card

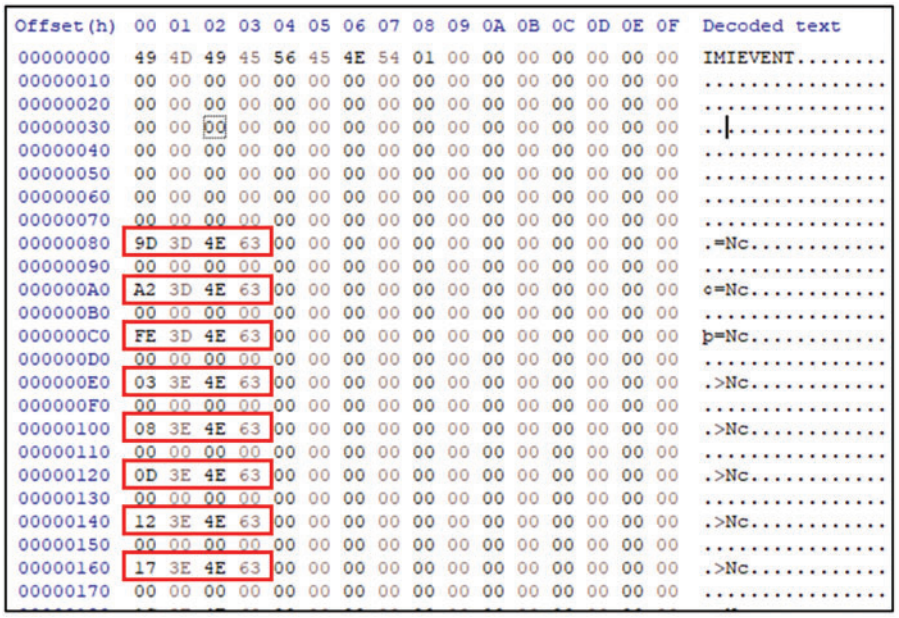
Furthermore, because of analyzing the '/MIJIA_RECORD_MOTION/2022101814/motion_record_msg' file in the SD card directory with Hex Editor, it was confirmed that the time stamp when a person was detected was saved in little-endian as shown in Fig. 19. For smart TVs, UART pin and Nand Flash memory could be identified, however, data acquisition was infeasible owing to technical limitations.

Cloud Server

Similar to other IoT devices, Xiaomi Mi Home's IoT devices communicate with the cloud server via Wi-Fi. Accordingly, communication packets between each device and the cloud server were acquired through packet capture. However, similar to Samsung SmartThings, there were some packets encrypted with TLS, and there was no meaningful data in other packets.

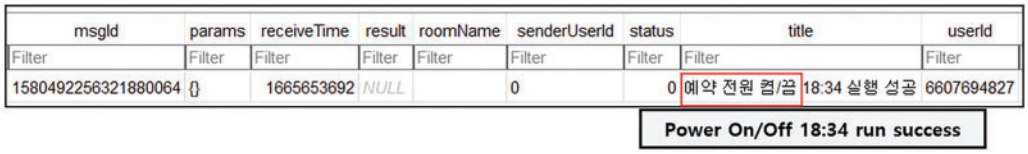
Smartphone

The smartphone used in the experiment targeting the Xiaomi platform was pre-rooted, and its dump image was acquired via ADB. Several database files were found within the smartphone's app data. For instance, in cn_6607694827_typelist_v2.db, user IDs, device notification messages, and timestamps are stored, as shown in Fig. 20.



Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	49	4D	49	45	56	45	4E	54	01	00	00	00	00	00	00	00	IMIEVENT.....
00000010	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000030	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000040	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000050	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000060	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000070	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000080	9D	3D	4E	63	00	00	00	00	00	00	00	00	00	00	00	00	.=Nc.....
00000090	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000000A0	A2	3D	4E	63	00	00	00	00	00	00	00	00	00	00	00	00	¢=Nc.....
000000B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000000C0	FE	3D	4E	63	00	00	00	00	00	00	00	00	00	00	00	00	þ=Nc.....
000000D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000000E0	03	3E	4E	63	00	00	00	00	00	00	00	00	00	00	00	00	.>Nc.....
000000F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000100	08	3E	4E	63	00	00	00	00	00	00	00	00	00	00	00	00	.>Nc.....
00000110	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000120	0D	3E	4E	63	00	00	00	00	00	00	00	00	00	00	00	00	.>Nc.....
00000130	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000140	12	3E	4E	63	00	00	00	00	00	00	00	00	00	00	00	00	.>Nc.....
00000150	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000160	17	3E	4E	63	00	00	00	00	00	00	00	00	00	00	00	00	.>Nc.....
00000170	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....

Figure 19: IP camera people detection timestamp



msgId	params	receiveTime	result	roomName	senderUserId	status	title	userId
Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1580492256321880064	{}	1665653692	NULL		0	0	예약 전원 켬/끔 18:34 실행 성공	6607694827

Power On/Off 18:34 run success

Figure 20: DB file (cn_6607694827_typelist_v2.db) stored in IP camera memory card

6.2.3 Classification Based on Data Characteristics

For the Xiaomi Mi Home, artifacts were previously obtained from both IP cameras and management devices. However, due to technical limitations, data extraction from devices other than the IP camera was not feasible. In the case of the IP camera, videos and photos were stored on the SD card, and people detection timestamps were recorded. Since this information is generated through device usage, it is classified as device usage data as shown in Table 5 . This data is critical because it can help establish the alibi of an individual involved in a case. For example, in a house invasion, the automatically recorded video can capture the intruder's face, clothing, and body type, while the people detection timestamp indicates the exact time the intruder entered the house.

Table 5: Devices and data used in the investigation (scenario)

IoT device	Device usage data	Smart home environment identification data	User data
IP camera	Timestamp, Multimedia file (jpeg, mp4)	–	–

7 Discussion

In this study, we proposed an architecture that represents the smart home environment from a forensic perspective, based on its constituent components. The architecture is organized into five layers—cloud, platform, service, IoT device, and device component—each representing a common element within the smart home ecosystem. This comprehensive architecture not only encapsulates all smart home components but also serves as a foundational model for forensic research, as it aligns with the overall structure of smart homes. Moreover, our proposed architecture is extendable, allowing for the incorporation of new devices, services, and platforms as they emerge.

Based on this common architecture, we developed a forensic framework comprising three parts. In the function analysis-based smart home data inference phase, a functional analysis of the smart home application identifies the capabilities supported by IoT devices and the specific features of each platform. For instance, Samsung and Xiaomi operate through the SmartThings and Mi Home apps, respectively, both of which enable remote control of interconnected devices. This analysis allows us to infer the anticipated data from these devices and platforms, aiding in the planning and targeting of specific devices during the forensic readiness stage.

The inferred data may be stored in the cloud, within management systems, or in the internal storage of IoT devices—each requiring different data acquisition methods for extraction. When data resides in a device's internal storage, techniques such as extracting data from NAND flash memory or SD cards can be employed. In our study, data extraction from Samsung and Xiaomi devices allowed us to identify user information and lists of linked devices. Although additional artifacts might be recovered through file system recovery of deleted files, data extraction was not feasible from other devices (for example, the Samsung Smart Hub, due to disk encryption, or small devices like smart plugs and smart tags, due to limited storage), and data from devices such as the Xiaomi Smart TV could not be acquired because of technical constraints. While numerous studies have addressed data acquisition methods, evolving IoT devices necessitate new methodologies and further research into the latest smart home technologies.

If data is stored in the cloud, its verification can be achieved by analyzing the packets exchanged between the IoT device and the cloud server. In our study, packet analysis was limited by TLS encryption, and unencrypted packets did not reveal meaningful data. However, in some cases, artifacts extracted from packet analysis have supported warrant review. For example, if a certificate can be injected into the device, tools like Burp Suite can decrypt TLS packets, enabling data extraction via replay attacks. These security constraints often restrict data acquisition, and as security measures evolve, continuous research into new acquisition techniques is essential.

When data is stored in a smartphone app, extraction is accomplished by analyzing data on smartphones linked with Samsung and Xiaomi applications. Our research confirmed that a significant amount of app data is stored on these devices; however, obtaining smartphones from a home environment can be challenging. Nonetheless, smartphones can provide critical information from IoT devices that lack onboard storage, such as sensors and door locks, making them invaluable evidence when available.

Finally, the data derived through these methods are utilized differently depending on the type of crime. Accordingly, we categorized the data into three types: device usage data, user data, and smart home environment data. Device usage data can help establish a suspect's alibi, user data assists in identifying both victims and suspects, and smart home environment data enables investigators to accurately assess the configuration of the smart home, thereby facilitating more efficient investigations.

8 Conclusion

Owing to advances in software and hardware technology, a wide range of IoT devices are being released. In particular, improvements in hardware—such as enhanced sensing technology—enable devices to collect diverse data and deliver higher-quality services. Consequently, not only are traditional home appliances being converted into IoT devices, but entirely new devices are also being developed to provide users with convenient functionalities at home.

Accordingly, smart home vendors are expanding the smart home environment through dedicated platforms. These smart homes deliver customized services by communicating with cloud servers via IoT devices. As these devices continuously generate and store various types of data, numerous forensic studies have been conducted on smart home systems. However, with the emergence of the latest devices and the expanding scope of smart homes, scalable forensic research is increasingly required.

In this study, we identified the components and structures of smart homes to develop a forensic method suitable for this evolving environment, and based on this, we derived a common smart home architecture. The common architecture is composed of five layers—cloud, platform, service, IoT device, and device components—each representing a fundamental element of the smart home environment. Building on this common architecture, we proposed a forensic framework for smart home environments.

The forensic framework comprises three steps: predictive data inference, actual data acquisition, and data identification for criminal investigations. In our study, Samsung and Xiaomi smart home test beds were established to verify the forensic framework. Expected data within the smart home were identified through functional analysis of the smart home apps, and some of this data was obtained and validated using the Samsung and Xiaomi test beds. We acquired various data from the devices, including user information and lists of connected devices. These data can serve not only as direct evidence, depending on their characteristics, but also as clues for obtaining additional information through further analysis. Subsequently, the identified data were classified into three categories: device usage data, smart home environment identification data, and user data.

The classification of smart home components and the common architecture established in this study incorporates the fundamental elements of smart home environments, enabling their collective application during investigations. This study is of great significance in the field of smart home digital forensics. Moreover, when investigators examine smart home IoT devices in the field, the proposed framework can serve as a valuable reference and provide key evidence by tracking data collection, analysis, and user behavior.

In future work, we plan to analyze Matter—the emerging smart home standard—and conduct further research to enhance our proposed smart home common model, ultimately deriving a more scalable smart home framework.

Acknowledgement: This work was supported by Supreme Prosecutors' Office of the Republic of Korea.

Funding Statement: This research received no external funding.

Author Contributions: Sungbum Kim: Methodology: Investigation, Formal analysis, Writing—original draft. Gwangsik Lee: Writing—review & editing, Validation. Jian Song: Writing—review & editing, Validation. Insoo Lee: Writing—review & editing, Validation. Taeshik Shon: Conceptualization, Writing—review & editing, Resources, Supervision, Validation. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: No new dataset was generated for this study, and the analysis was conducted based on publicly available literature and existing data.

Ethics Approval: All authors certify that they have no affiliations with or involvement in any organization or entity with any financial interest or non-financial interest in the subject matter or materials discussed in this manuscript.

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

References

1. Mehta A, Verma RK. QoS-aware edge server placement for collaborative predictive maintenance in industrial Internet of Things. J Supercomput. 2024;80(13):19324–50. doi:10.1007/s11227-024-06210-w.
2. Kebande VR. Industrial Internet of Things (IIoT) forensics: the forgotten concept in the race towards Industry 4.0. Forensic Sci Int Rep. 2022;5:100257. doi:10.1016/j.fsir.2022.100257.
3. Douiba M, Benkirane S, Guezzaz A, Azrour M. An improved anomaly detection model for IoT security using decision tree and gradient boosting. J Supercomput. 2023;79(3):3392–411. doi:10.1007/s11227-022-04783-y.
4. Torabi S, Bou-Harb E, Assi C, Debbabi M. A scalable platform for enabling the forensic investigation of exploited IoT devices and their generated unsolicited activities. Forensic Sci Int Digit Investig. 2020;32(4):300922. doi:10.1016/j.fsidi.2020.300922.
5. Iqbal A, Olegard J, Ghimire R, Jamshir S, Shalaginov A. Smart home forensics: an exploratory study on smart plug forensic analysis. In: 2020 IEEE International Conference on Big Data (Big Data); 2020 Dec 10–13; Atlanta, GA, USA: IEEE; 2020. p. 2283–90. doi:10.1109/bigdata50022.2020.9378183.
6. Salamh FE. A forensic analysis of home automation devices (FAHAD) model: Kasa smart light bulb and eufy floodlight camera as case studies. Int J Cyber Forensics Adv Threat Investig. 2021;1(1–3):18–26. doi:10.46386/ijcfati.
7. Abdel-Fattah F, Fayyad S, Heyari AM, Al-Zoubi H. A survey of Internet of Things (IoT) forensics frameworks and challenges. In: 2023 International Conference on Information Technology (ICIT); 2023 Aug 9–10; Amman, Jordan: IEEE; 2023. p. 373–7. doi:10.1109/ICIT58056.2023.10226103.
8. Alam MN, Kabir MS. Forensics in the internet of things: application specific investigation model, challenges and future directions. In: 2023 4th International Conference for Emerging Technology (INCET); 2023; Belgaum, India. p. 1–6.
9. Stoyanova M, Nikoloudakis Y, Panagiotakis S, Pallis E, Markakis EK. A survey on the Internet of Things (IoT) forensics: challenges, approaches, and open issues. IEEE Commun Surv Tutor. 2020;22(2):1191–221. doi:10.1109/COMST.2019.2962586.
10. Kim J, Park J, Lee S. An improved IoT forensic model to identify interconnectivity between things. Forensic Sci Int Digit Investig. 2023;44:301499. doi:10.1016/j.fsidi.2022.301499.
11. Sathwara S, Dutta N, Pricop E. IoT Forensic A digital investigation framework for IoT systems. In: 2018 10th International Conference on Electronics, Computers and Artificial Intelligence (ECAI); 2018 Jun 28–30; Iasi, Romania: IEEE; 2018. p. 1–4. doi:10.1109/ECAI.2018.8679017.
12. Castelo Gómez JM, Carrillo-Mondéjar J, Martínez Martínez JL, Navarro García J. Forensic analysis of the xiaomi mi smart sensor set. Forensic Sci Int Digit Investig. 2022;42–43:301451. doi:10.1016/j.fsidi.2022.301451.
13. Bouchaud F, Vantroys T, Grimaud G. Forensic analysis of IoT ecosystem. In: 2021 8th International Conference on Future Internet of Things and Cloud (FiCloud); 2021 Aug 23–25; Rome, Italy: IEEE; 2021. p. 115–22. doi:10.1109/ficloud49777.2021.00024.
14. Li Z, Amer W, Ruessler G, Garcia M, Liu X. A common but flexible method for IoT device forensics. In: 2021 IEEE Global Communications Conference (GLOBECOM); 2021 Dec 7–11; Madrid, Spain: IEEE; 2021. p. 1–7. doi:10.1109/GLOBECOM46510.2021.9685986.
15. Kim S, Park M, Lee S, Kim J. Smart home forensics—data analysis of IoT devices. Electronics. 2020;9(8):1215. doi:10.3390/electronics9081215.
16. Hutchinson S, Karabiyik U. Forensic analysis of the August smart device ecosystem. In: 2020 International Symposium on Networks, Computers and Communications (ISNCC); 2020 Oct 20–22; Montreal, QC, Canada: IEEE; 2020. p. 1–7. doi:10.1109/isncc49221.2020.9297346.
17. Kim S, Bang J, Shon T. Forensic analysis for cybersecurity of smart home environments with smart wallpads. Electronics. 2024;13(14):2827. doi:10.3390/electronics13142827.

18. Youn MA, Lim Y, Seo K, Chung H, Lee S. Forensic analysis for AI speaker with display Echo Show 2nd generation as a case study. Forensic Sci Int Digit Investig. 2021;38:301130. doi:10.1016/j.fsidi.2021.301130.
19. Kim M, Shin Y, Jo W, Shon T. Digital forensic analysis of intelligent and smart IoT devices. J Supercomput. 2023;79(1):973–97. doi:10.1007/s11227-022-04639-5.
20. Kim S, Jo W, Lee J, Shon T. AI-enabled device digital forensics for smart cities. J Supercomput. 2022;78(2):3029–44. doi:10.1007/s11227-021-03992-1.
21. Li S, Choo KKR, Sun Q, Buchanan WJ, Cao J. IoT forensics: amazon echo as a use case. IEEE Internet Things J. 2019;6(4):6487–97. doi:10.1109/JIOT.2019.2906946.
22. Servida F, Casey E. IoT forensic challenges and opportunities for digital traces. Digit Investig. 2019;28(3):S22–9. doi:10.1016/j.diin.2019.01.012.