Sensors and Materials, Vol. 34, No. 6 (2022) 2125–2139
MYU Tokyo

S & M 2960

Function-level Access Control System for Home IoT Devices

Yuichi Hattori,[1*] Yutaka Arakawa,[2] Daichi Koike,[2]
Shigemi Ishida,[2,3] and Sozo Inoue[1]

[1]Kyushu Institute of Technology, 2-4 Hibikino, Wakamatsu-ku, Kitakyushu-shi, Fukuoka 808-0135, Japan
[2]Kyushu University, 744 Motooka, Nishi-ku, Fukuoka 819-0395, Japan
[3]116-2 Kamedanakanocho, Hakodate-shi, Hokkaido 041-8655, Japan

(Received March 23, 2022; accepted April 15, 2022)

Keywords: IoT, smart house, traffic analysis, trust, packet capture

In this paper, we propose a framework called an IoT activity tracker to ensure the safe and secure use of IoT devices around the home. The IoT activity tracker identifies the types of IoT devices and their triggering functions by traffic pattern analysis, and provides information about which IoT devices are running in the home. Also, it allows users to temporarily or permanently block the network of a particular IoT device from their smartphone if the user notices unauthorized activity of the IoT device. Furthermore, the system can be linked to sensor-based behavior recognition. For example, an IoT-based smart lock can automatically switch the communication permissions between those when the user is out and those when the user is at home depending on its status. In this paper, we report the results of a proof of concept experiment on our proposed system, which consists of a router with the proposed function and a cloud server that interfaces with users.

1. Introduction

In recent years, IoT devices have become widespread in households, and IoT devices with various functions such as remote control, lighting, door locks, and power outlets are sold and used in various situations. These devices are expected to become even more prevalent in the future; according to a survey by Japan's Ministry of Internal Affairs and Communications, the number of IoT devices worldwide in 2017 was about 27 billion and predicted to increase to 40 billion by 2020.(1) For example, well-known IoT devices used in the home include smart speakers such as Google Home and Amazon Echo. These devices are equipped with a voice user interface (VUI) that allows users to use their voice to perform various functions such as searching the Internet, operating home appliances, and playing music. Some devices are also equipped with cameras, allowing video calls with other IoT devices and smartphones. Network cameras are also readily available from home centers and mail-order sites and are being used in conjunction with smartphones and smart speakers for applications such as watching over children and crime prevention. These IoT devices are essentially designed to work with the cloud, and their functionality allows them to work with smartphones and other devices. These IoT devices are

*Corresponding author: e-mail: eidwinds@gmail.com
https://doi.org/10.18494/SAM3901

ISSN 0914-4935

connected to dedicated cloud-like servers and other systems via Wi-Fi networks in the home and provide services by collecting and analyzing the data produced by the devices. Users can access these systems from their smartphones to control their devices and view information.

Since IoT devices are designed to be connected to external networks, they pose many problems in terms of information security, and there have been incidents of them being used as a springboard for various personal information leaks and attacks. For example, a vulnerability has been discovered in a camera installed in a smart vacuum cleaner that can be used to listen in on a home, and customer information has been stolen from a casino via a smart thermometer installed in an aquarium.(2) In addition, there are websites that allow users to view and browse a list of video images of network cameras that have problems with the initial setup and configuration, meaning that they can be easily accessed from outside once the IP address is known. There has been a recent increase in attacks targeting IoT devices. For example, Zhang *et al.*, Chakraborty *et al.*, and Mao *et al.* used sounds that are inaudible to humans to access and remotely control IoT devices.(3–5)

While the proliferation of IoT devices makes our lives more convenient, it is important to consider the security of their use. Various precautions need to be taken when using IoT devices. In particular, the following three points need to be taken into account.

I. The diversity of IoT devices is so high that it is difficult to continuously update the security of all devices. New devices are being released all the time, but the rate of firmware updates is not keeping pace with that for PCs. Devices manufactured by large companies are more likely to receive consistent and regular firmware updates and support, whereas devices manufactured by smaller companies may not receive firmware updates or support due to factors such as early service termination or bankruptcy of the company itself.
II. The activity of IoT devices can be likened to a black box, often operating independently of the user's intentions regarding what data the device is sending and where. After the device has been initially connected to the network, the user often does not know which server the IoT device is connected to, what protocols they are using, or how often they are connecting to the network. More recently, as a result of incidents in Zoom video conferences, it has been discovered that network communications may be routed through certain countries.(6) Also, the route used for network communication is usually encrypted, meaning that ordinary users cannot check it.
III. Unlike PCs, users cannot install fraud detection systems, such as anti-virus software, on IoT devices.

These problems can be solved by providing controls to allow communication only for the necessary functions of the IoT device.

Therefore, in this paper, we propose a framework called the IoT activity tracker for the safe use of IoT devices around the home. The IoT activity tracker identifies the types of IoT devices and their triggering functions based on communication traffic pattern analysis, so that the user knows which IoT devices in the home are performing what kind of communication. At the same time, it allows users to easily control the communication related to the function, such as temporarily or permanently blocking it, through their smartphones. Smartphone permissions are visible and can be managed. We propose to set permissions for each smartphone app for IoT

devices in the home. We also propose a feature that allows permissions to be visualized and easily configured for each function, similarly to smartphone permission settings.

In this paper, we describe the design, developed features, and evaluation of the proposed framework. Its research contributions are as follows:

- **Helping ensure the safe and secure use of IoT devices in the home.**
  We propose a framework called an IoT activity tracker to ensure the safe and secure use of IoT devices around the home. We develop a feature allowing us to set permissions for each application, which is similar to setting the permissions on a smartphone. We also propose the access control of the proposed system by linking it with activity recognition technology (detection of home presence by sensors). For example, using a key connected to a network that can be operated via the cloud, called a smart lock, communication permissions can be automatically switched between those when the user is out and those when the user is at home depending on the status of the smart lock.
- **Evaluation of access control for proposed system.**
  We evaluate six functions on three IoT devices. We demonstrate the ability to control functions with different connection points using our proposed system.

The structure of this paper is as follows. In Sect. 2, we describe related work on IoT traffic analysis. In Sect. 3, we describe the design of the proposed system, and its evaluation is presented in Sect. 4. In Sect. 5, we discuss the proposed system. Finally, we conclude our paper in Sect. 6.

2. Related Work

2.1 Research describing end-user security and privacy concerns with smart homes

Zeng *et al.* studied end-user security and privacy concerns with smart homes.[7] They conducted interviews with 15 people living in smart homes to learn about how they used their smart homes and to understand their security- and privacy-related attitudes, expectations, and actions. On the basis of these interviews, they concluded that users are not particularly interested in the security of smart home devices. However, they claimed that creating a device information visualization system would be a potential way to increase interest in device-related security concerns for the end user. Thus, our research not only helps to detect unauthorized communication but also increases awareness among users of device-related security.

2.2 Research describing vulnerabilities of IoT communication privacy

Apthorpe *et al.* reported privacy vulnerabilities of encrypted IoT traffic.[8] By analyzing four commercially available smart home devices (Sense sleep monitor, Nest Cam indoor security camera, Wemo remote switch, Amazon Echo smart speaker), they demonstrated that the rate of network traffic can reveal user activity. This is because user behavior can be estimated using only the transmission and reception rates of encrypted traffic, as IoT devices transform real-world information into network traffic. Thus, they can warn users about potential privacy

threats. Of course, whereas it is important to protect traffic information that could enable potential attackers to estimate user behavior, it is also important to visualize activity information and report it to users for security monitoring purposes.

Dong *et al.* investigated how personal information can be leaked from network traffic generated by smart home networks.[9] They proposed a framework for device identification using the temporal relationship between packets, which identifies the device type with high accuracy. The results suggest that IoT network communications, even when protected by encryption and morphed by network gateways, pose significant challenges to user privacy.

These studies in which activity information is presented to users by analyzing the network traffic of IoT devices help to detect suspicious network communication.

2.3 IoT device identification by network traffic analysis

Although we identify a function by analyzing the network traffic of an IoT device in this study, the identification of IoT devices has been addressed in previous research. Meidan *et al.* proposed a method for IoT and non-IoT device identification using network traffic analysis with machine learning.[10] By analyzing a saved file that contains traffic information of devices connected to Wi-Fi, they identified the devices in two stages using supervised machine learning while abstracting features such as source address, destination address, and port number. In the first stage, they identified whether a device is an IoT device. In the second stage, they identified the device class from a list of registered identified IoT devices. As a result, they identified the types of IoT devices with 99.281% accuracy.

Sivanathan *et al.* proposed a method of IoT device identification in a smart city and on a campus. They set 21 IoT devices on a campus and collected traffic data for 3 weeks.[11] Then, by analyzing wide network traffic (e.g., traffic load, signaling patterns, and distribution of active and sleep times), they identified the devices using a supervised learning algorithm. As a result, they identified the types of IoT devices with 95% accuracy.

Sivanathan *et al.* developed a modular device classification architecture and used unsupervised clustering methods to identify 10 devices with an accuracy of over 94% using actual IoT device traffic.[12] They also developed a modular device classification architecture with a clustering model that identifies behavioral changes with an accuracy of over 94% for 12 devices using actual IoT device traffic.[13]

Although these studies identified devices and detected changes in behavior with a high degree of accuracy, they were not able to identify device functions. In this study, we identify the functions of devices.

2.4 Security system for IoT device using network gateway

Miettinen *et al.* proposed a system that can automatically identify the types of IoT devices connected to a network, limit the communication of vulnerable devices, and minimize damage.[14] Their proposed approach was to identify IoT devices by profiling the communication behavior specific to each type of device. Although the system controlled the communication of

vulnerable devices based on the results of device estimation, it did not control the communication based on the functions of the devices. Our proposed system controls communication at the function level of the devices.

2.5 Smartphone permissions vs smart home permissions

The management of usage resources (communications, sensors, external storage) related to smartphones is an important issue from the perspectives of privacy and security.

Currently, smartphone permissions are visible and can be managed in two different ways: by setting permissions for each app and by setting apps for each permission. There are also four types of permissions on Android devices: *all the time (location only)*, *ask every time*, *allow only while using the app*, and *don't allow*.[15] In the past, location information was obtained by applications without the user's consent, which raised privacy issues, so this type of functionality was implemented.

For a smart home, an IoT device is the equivalent of an app on a smartphone. For smart homes, as with smartphones in the past, we do not know which IoT devices are doing what. Another problem is that IoT devices may be unnecessarily communicating with third-party destinations.[16] In other words, it is necessary to control the resources used in the smart home, just as we do with smartphones today.

3. System Design

Figure 1 shows the proposed IoT activity tracker. In this research, we assume that the IoT activity tracker is used in general households and that multiple IoT devices are connected to a router either by wire or wirelessly. Because of this, we assume that the traffic information sent and received from all connected devices is collected by the router. This data is used to identify the function of each device.

We focus on the fact that IoT devices are connected to the cloud system via a home router. On the router to which all devices in the smart home are connected, we identify the functions that

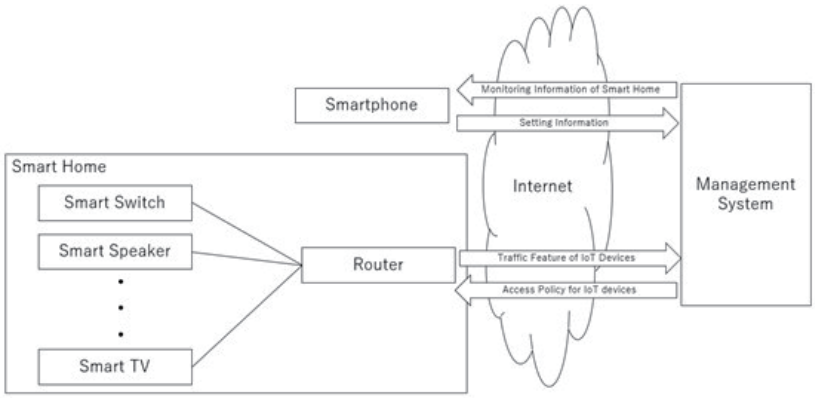

Fig. 1. Outline of proposed IoT activity tracker.

the devices invoke from the communication, and we set permissions regarding whether they can communicate. By displaying the status of the identified functions and communication packets to the user via the cloud, the user can check the status of the device at any time.

3.1 Concept of access control

We define an IoT activity tracker as a framework that allows a user to easily register their IoT devices and check their operation status. On a smartphone, a pop-up appears when installing an application, such as "This application is requesting access to a microphone." A user can also check the list of applications accessing each function from the smartphone's settings screen. In this way, there is a mechanism that allows users to use applications safely and trustingly owing to the visibility of their settings on the smartphone. Similarly, the operation of IoT devices can also be visualized similarly to apps on a smartphone, and the functions used by IoT devices and the status of communication packets can be displayed on the screen of a smartphone or another device. This allows the end user to use devices without worrying about security.

3.2 Differences from other products

There are a variety of intrusion detection systems (IDS) and intrusion prevention system (IPS) products that simply detect and block specific communication ports, destinations, and behaviors, and simple firewalls can be found in home routers, but there are no products that can block communication by IoT devices or by IoT device functions. The proposed system is also set up so that it can be configured to allow or disallow scenario-based communication and is implemented so that it can be configured on the basis of time or user action. For example, "Allow Amazon Echo to play music from 19:00 to 24:00 on weekdays but block all other music". In the future, it is envisioned that the system will be linked to sensors and human actions such as entering a room and approaching a house. A comparison of IDS/IPS, anomaly detection systems, and the proposed system is shown in Table 1. The proposed system aims to control the functions of IoT devices with a specific timing, not against known attacks or distributed denial of service (DDoS) attacks, in contrast to IDS and anomaly detection systems, and to control the functions of IoT devices from the privacy aspect.

Table 1
Comparison of IDS/IPS, anomaly detection systems, and proposed system.

	IDS/IPS	Anomaly detection	Proposed system
Access control of device function	No	No	Yes
Scenario-based access control	No	No	Yes
Access control of device	Yes	Yes	Yes
DDoS protection	Yes	Yes	No
Well-known attack protection	Yes	Partial	No
Zero-day attack protection	No	Partial	No

3.3 System architecture

The IoT activity tracker consists of an edge router and management system. Figure 2 shows an overview of the IoT activity tracker system. Edge routers are designed to be installed in a typical home and are connected to IoT devices and PCs either by wire or wirelessly. The edge router provides access control by generating an access policy based on traffic features. The management system can be operated by the user, who can set whether to allow communication for each device function. This configuration is automatically reflected in the edge router to achieve access control.

Two types of communication availability for each device function are implemented: a simple allow/block setting and a scenario with multiple conditions. Details are given in Sects. 3.6 and 3.7.

Figure 3 shows an overview of the access policy and identification model generation. The traffic features of the devices accumulated by the edge router are sent to the management system. It is envisioned that the accumulated traffic features of the edge router will be sent to the management system to be used for updating existing access policies and models as well as for building access policies and models for new IoT devices and functions.

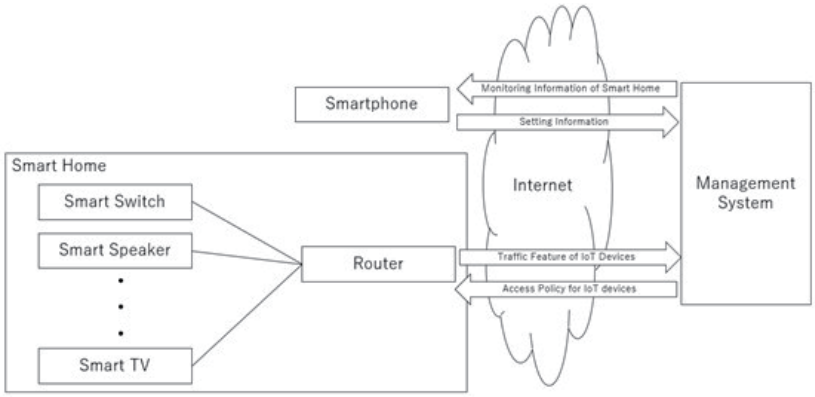

Fig. 2. Overview of IoT activity tracker system.

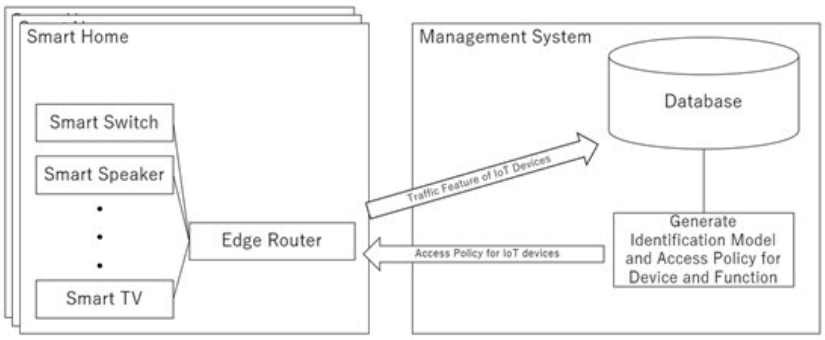

Fig. 3. Overview of access policy and identification model generation in IoT activity tracker.

3.4 Edge router

The edge router is built on the VyOS software router,[17] which is connected to IoT devices and PCs either by wire or wirelessly. Since the configuration is to be installed in a home, the global IP address of the edge router is assumed to be a dynamic IP address. The management system is generally accessed from the edge router side. The main functions communicated from the edge router to the management system are as follows:

I. Send dynamic host configuration protocol (DHCP) lease information to the management system.
II. Receive configuration information periodically from the management system.
III. Send the status of the edge router, such as the memory used, to the management system.
IV. Send the communication status to the management system.
V. Send the features of the traffic to the management system.

Function I sends information about the connected devices to the management system. This information, together with the traffic characteristics of Function V, is used to identify the devices and their functions. Function II is used to control communication on the edge router side by receiving the settings and scenarios for allowing/blocking functions set by the user from the management system. The transmission of the status such as the memory used (Function III) is mainly used to perform a health check of the edge router. The transmission of the communication status (Function IV) is used by the management system draw a graph to check whether the devices are communicating. Function V is used to access policy and identification model generation.

3.5 Management system

The management system is built as a web application and is designed to be accessed by users from their smartphones and PCs. Its main functions are as follows:

I. Edge router management
II. Connected device management
III. Scenario management
IV. Login user management

Function I is used to manage multiple edge routers that a user may have. Function II manages the devices connected to each edge router. It is possible to set communication allowing/blocking settings for each device function and to name the devices. This feature is also intended to be used for labeling devices in the future, and the names of devices can be changed manually. A screen of the management system listing the devices is shown in Fig. 4. Function III not only allows simple allowing/blocking of communication but also allows access control under specific conditions by registering scenarios such as the time of day when communication is allowed and the continuous content of user button operations. Function IV is implemented so that multiple users can manage the edge router, since it is assumed to be installed in an ordinary home where multiple people live.

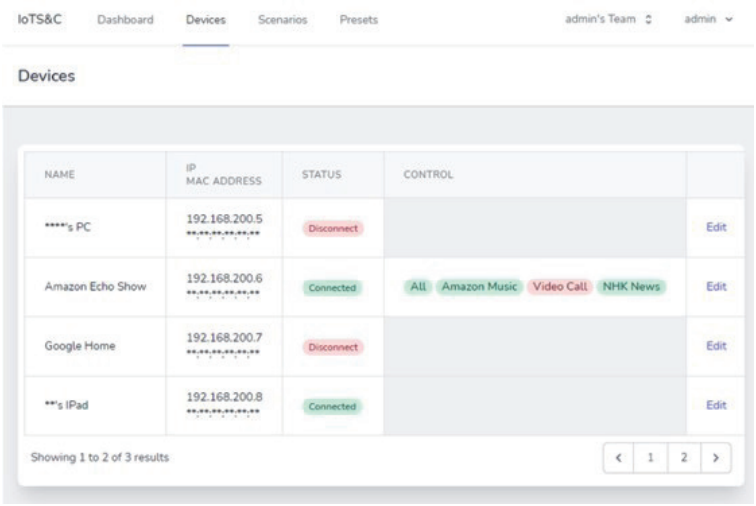

Fig. 4. (Color online) Device list screen in the management system.

3.6 Access policy for device functions

Access policies are created for each device function and to allow/deny the function. The access policy enables the allowing/blocking of destination/source communication and port numbers. The edge router receives access policies periodically from the management system and applies them as firewall rules for the software router. In the future, access policies should be automatically generated on the basis of the traffic features sent from edge routers.

3.7 Scenario-based access policy

In the IoT activity tracker, access control can be realized by registering not only simple communication availability for each function, but also time periods when communication is allowed and user's button operation on the management system as scenarios. The elements that make up a scenario are called the controls. A scenario consists of several controls. Examples of controls are as follows:

- "the user clicks button 1 on the management system"
- "10:00–19:00 on weekdays"
- "the communication of function A of IoT device 1 is blocked"

Figure 5 shows the scenario editing screen in the management system. For example, the following scenario can be defined to only allow Amazon Echo music playback communication during 10:00–11:00 on weekdays.

I. 10:00–11:00 on weekdays
II. Allow Amazon Echo's music playback feature

The following are used as controls in the current implementation.

I. Allowing/blocking the communication of functions
II. Buttons in the management system
III. Specification of the time

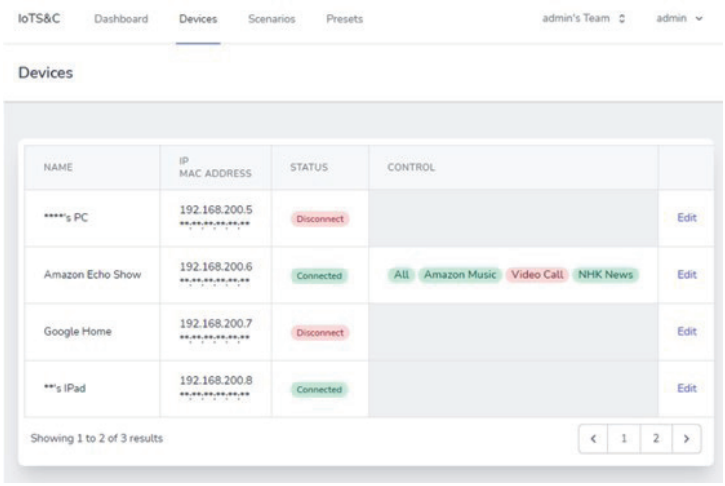

Fig. 5. (Color online) Scenario editing screen in the management system.

In addition, this function is designed with the assumption that the IoT activity tracker will work with sensors in the future to link with human actions such as entering a room or approaching a house. By registering these behaviors as one of the controls, it is possible to control communication in conjunction with sensors. This will be accomplished through communication between the management system and the sensors via an API.

3.8 Access policy and identification model sharing

In the IoT activity tracker, the features collected from the edge router are aggregated into the management system. It is envisioned that the features will be used to update existing access policies and models as well as build access policies and models for new IoT devices and functions. Even though the communication of most IoT devices is encrypted, it is not possible to conceal information such as the frequency of use of the device and the destination of communication. Collecting such information and storing it in a form that is linked to the user raises privacy concerns for the user. To eliminate this concern, the IoT activity tracker does not link the edge router to features at the stage of collection. By only linking the devices, functions, destinations of communication, and features, we ensure that no information that can be linked to a specific user is stored.

3.9 Device and function identification

Machine learning techniques are used to identify devices and functions. Details of device identification and function identification are described in Sect. 4.[18] However, we have only created models for three IoT devices with a total of 11 functions. Therefore, it is necessary to create and evaluate models for more devices and functions in the future.

4. Evaluation

For the proposed system, we developed functions related to access control except for automatic access policy generation and device and function identification. In this case, the access policy was created manually in accordance with Sect. 4.3. We then verified that the access control in the proposed system works correctly for each device function. We evaluated the accuracy of the device identification and function identification for the proposed system, and finally, we implemented access control for each function in the proposed system and verified that it works.

4.1 Device identification and function identification performances

For device identification, the accuracy was 99.1% for the three IoT devices, and for function identification, the accuracy was over 76.6% for the 11 functions, including Amazon Echo Spot, Amazon Echo Dot, and Amazon Flex.

4.2 Environment of IoT activity tracker

As a proof of concept (PoC), we built the IoT activity tracker on a virtual machine and access point. We connected Amazon Echo Show, SwitchBot Hub Mini, and SwitchBot Plug to the proposed system and built an environment to verify that certain functions can be allowed or denied from the web browser on an iPad. The system configuration is shown in Fig. 6. Since this system is different from the device used to obtain the results in Sect. 4.1, we collected the traffic information again and generated the access control policy from the collected traffic information.

4.3 Generating access policies

We collected network packets of Amazon Music, NHK News, and video call features of Amazon Echo Show and the Turn On/Off Power, Turn On/Off Audio, and Turn On/Off TV features of the SwitchBots on the edge router. We collected network packets for each function 10 times. We cut out network packets of 5 s before telling the device to act 5 s after the function was executed. Then, we counted the number of network packets per protocol [transmission control protocol (TCP) and user datagram protocol (UDP)] per source/destination port and per source/destination IP address. The domain name system (DNS) and network time protocol (NTP) were excluded because they were used by all functions. We then adopted the top TCP/UDP and destination IP address combination as the exclusion rule. However, some of the functions used the content delivery network (CDN), whose IP addresses can change each time they are used. Therefore, we obtained the fully qualified domain name (FQDN) from the IP address and the IP address range from the DNS records and used them.

4.4 Evaluation for access control

We evaluated the Amazon Music, NHK News, and video call features of Amazon Echo Show and the Turn On/Off Power, Turn On/Off Audio, and Turn On/Off TV features of the SwitchBots

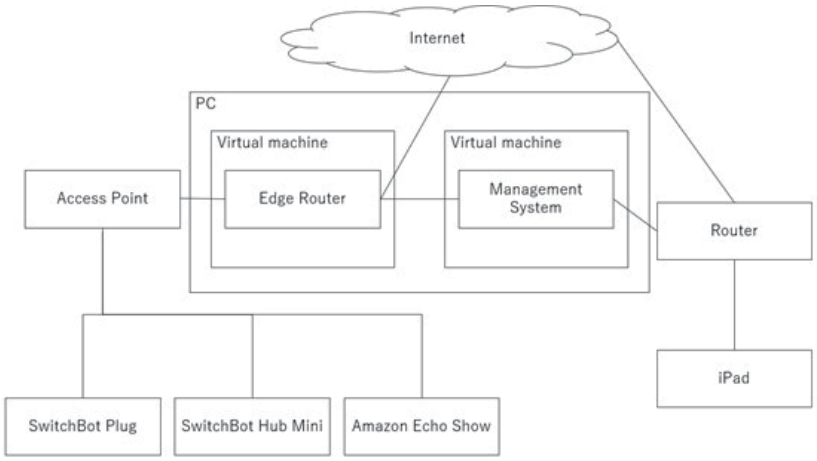

Fig. 6. System configuration.

to establish whether we could allow/deny the features. We performed two evaluations of access policies: I: whether the other features work when one feature is disabled; II: whether a time-based scenario-based policy works correctly.

As a result, we were able to disable a function by blocking the communication for any of the functions. Amazon Echo Show also confirmed that if one function was rejected, the other two functions still worked. However, SwitchBot Hub Mini even blocked other functions of the same device. These results are shown in Tables 2 and 3. To confirm the effectiveness of the scenario-based policy, we configured the Amazon Music function to stop working between 10:00 and 11:00 and confirmed that the function did only stop working during that time.

5. Discussion

5.1 Impact of IoT device updates

When IoT devices are updated, the connection point may change and control may be lost. The ability to detect firmware updates and automatically change the rules is needed in the future.

5.2 Different functions having same connection destination

The proposed system cannot control all the same connections even if they have different functions. To deal with the case of the same connections with different functions, it is necessary to discriminate not only by IP address and port, but also by communication volume and content. If the communication is not encrypted, it is possible to identify it by its content, but this is not realistic since the communication of recent IoT devices is encrypted. Of course, there are methods to check Hypertext Transfer Protocol Secure (HTTPS) communication using proxies, but they are difficult to implement because they require the installation of certificates for proxies, and so forth, imposing a heavy burden on users.

Table 2
Results of checking operation of other functions when one function is disabled (Amazon Echo Show).

Device	Disabled function	Amazon Music	NHK News	Video call
Amazon Echo Show	Amazon Music	Does not work	Works	Works
Amazon Echo Show	NHK News	Works	Does not work	Works
Amazon Echo Show	Video call	Works	Works	Does not work

Table 3
Results of checking operation of other functions when one function is disabled (SwitchBots).

Device	Disabled function	Turn on/off power	Turn on/off audio	Turn on/off TV
SwitchBot Plug	Turn on/off power	Does not work	Works	Works
SwitchBot Hub Mini	Turn on/off audio	Works	Does not work	Does not work
SwitchBot Hub Mini	Turn on/off TV	Works	Does not work	Does not work

5.3 Changes in user lifestyles

User lifestyles, and therefore use patterns of devices, change with events such as job changes and higher education. Functions with different connection points are less affected by such changes. However, when control is based on information such as time of day or the day of the week, such functions are considered to be affected. To assist the control based on information such as the time of day or the day of the week, it is necessary to use sensors or other devices to confirm room occupancy.

5.4 Control with different protocols

The SwitchBot Hub Mini is a smart remote control that uses TCP for remote command and IR spectroscopy for transmission to home appliances. For such devices, even if the first instruction is given over TCP, the encrypted communication for that part is almost the same even if the control target is different, and it is not possible to control only a specific function. Therefore, the only way to control a function is to separate the smart remote control. If the communication is not encrypted, it is possible to identify the function by the content of the communication, but this is not realistic since the communication of recent IoT devices is encrypted.

5.5 Change in destination IP

The software router configuration cannot specify the FQDN, so it must be controlled by the IP address. If the destination uses the CDN, then it is not possible to control only one IP address because the destination has multiple IP addresses. It is necessary to take measures such as to obtain the FQDN from the IP address and the IP address range from the DNS record. However, if the IoT maker changes the FQDN information, the configured IP address must also be changed. We need to update the software router configuration on a regular basis.

5.6 Who should operate this system?

Regarding the question of who should operate the proposed system, if the system is operated by an IoT manufacturer, the response may be biased, so it is preferable that a neutral organization operates the system.

6. Conclusion

In this paper, we proposed a framework called an IoT activity tracker to ensure the safe and secure use of IoT devices around the home. Also, we reported the results for the PoC of our proposed system, which consists of a router with the proposed function and a cloud server that interfaces with users. Our proposed system used access controls generated from pre-collected traffic information to allow/deny certain functions of some IoT devices. In future research, we plan to identify the called function for other IoT devices and to monitor network traffic and notify users about which function is currently being used in real time by connecting the system to a messaging application such as Slack. Also, we will implement and verify a mechanism to automatically update access policies. Additionally, we plan to identify whether the network communication is intentional by using other research techniques such as behavior recognition using Wi-Fi. Through the use of activity visualization, we hope that users will be able to use IoT devices without any security concerns.

Acknowledgments

This work was supported by JSPS KAKENHI (JP19KT0020).

References

1 ICT in Japan and the World: https://www.soumu.go.jp/johotsusintokei/whitepaper/eng/WP2018/chapter-1.pdf (accessed February 2022).
2 Robot Vacuums Suck Up Sensitive Audio in 'LidarPhone' Hack: https://threatpost.com/robot-vacuums-audio-lidarphone-hack/161421/ (accessed February 2022).
3 G. Zhang, C. Yan, X. Ji, T. Zhang, T. Zhang, and W. Xu: Proc. 2017 ACM SIGSAC Conf. Computer and Communications Security (2017). https://doi.org/10.1145/3133956.3134052
4 A. Chakraborty, M. Alam, V. Dey, A. Chattopadhyay, and D. Mukhopadhyay: arXiv preprint arXiv:1810.00069 (2018). https://arxiv.org/abs/1810.00069
5 J. Mao, S. Zhu, X. Dai, Q. Lin, and J. Liu: IEEE Internet Things J. **7** (2020) 8025. https://doi.org/10.1109/JIOT.2020.2997779
6 Zoom admits some calls were routed through China by mistake: https://techcrunch.com/2020/04/03/zoom-calls-routed-china/ (accessed February 2022).
7 E. Zeng, S. Mare, and F. Roesner: 13th Symp. Usable Privacy and Security (fSOUPSg 2017) 65–80. https://dl.acm.org/doi/10.5555/3235924.3235931
8 N. Apthorpe, D. Reisman, and N. Feamster: arXiv preprint arXiv:1705.06805 (2017). https://arxiv.org/abs/1705.06805
9 S. Dong, Z. Li, D. Tang, J. Chen, M. Sun, and K. Zhang: Proc. 15th ACM Asia Conf. Computer and Communications Security; Association for Computing Machinery (ASIA CCS '20) (New York, NY, USA) (2020) 47–59. https://doi.org/10.1145/3320269.3384732
10 Y. Meidan, M. Bohadana, A. Shabtai, J. D. Guarnizo, M. Ochoa, N. O. Tippenhauer, and Y. Elovici: Proc. Symp. Applied Computing (2017) 506–509. https://doi.org/10.1145/3019612.3019878

11 A. Sivanathan, D. Sherratt, H. H. Gharakheili, A. Radford, C. Wijenayake, A. Vishwanath, and V. Sivaraman: 2017 IEEE Conf. Computer Communications Workshops (INFOCOM WKSHPS, 2017) 559–564. https://doi.org/10.1109/INFCOMW.2017.8116438

12 A. Sivanathan, H. H. Gharakheili, and V. Sivaraman: 2019 IEEE 44th Conf. Local Computer Networks (LCN) IEEE (2019) 230–233. https://doi.org/10.1109/LCN44214.2019.8990797

13 A. Sivanathan, H. H. Gharakheili, and V. Sivaraman: IEEE Internet Things J. **7** (2020) 7295. https://doi.org/10.1109/JIOT.2020.2984030

14 M. Miettinen, S. Marchal, I. Hafeez, N. Asokan, A.-R.Sadeghi, and S. Tarkoma: 2017 IEEE 37th Int. Conf. Distributed Computing Systems (ICDCS, 2017) 2177–2184. https://doi.org/10.1109/ICDCS.2017.283

15 Change app permissions on your Android phone–Android Help: https://support.google.com/android/answer/9431959 (accessed March 2022).

16 TP-Link Deco X68 Review: A good mesh router ruined by bizarre software, https://www.xda-developers.com/tp-link-deco-x68-review/ (accessed March 2022).

17 VyOS–Open source router and firewall platform: https://vyos.io/ (accessed February 2022).

18 D. Koike, S. Ishida, and Y. Arakawa: Proc. 36th Annu. ACM Symp. Applied Computing; Association for Computing Machinery (SAC'21) (New York, NY, USA) (2021) 737–743. https://doi.org/10.1145/3412841.3441951