Reinforcement of IoT Open Platform Security using PUF-based Device Authentication

Byoungkoo Kim, Seungyong Yoon and Yousung Kang
Cryptographic Engineering Research Section, Cyber Security Research Division
Electronics and Telecommunications Research Institute (ETRI)
Daejeon, Korea
{bkkim05, syyoon, youskang}@etri.re.kr

2022 13th International Conference on Information and Communication Technology Convergence (ICTC) | 978-1-6654-9939-2/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICTC55196.2022.9952998

***Abstract*—Recently, as the use of Internet of Things (IoT) devices has expanded, security issues have emerged. As a solution to the IoT security problem, PUF (Physical Unclonable Function) technology has been proposed, and research on key generation or device authentication using it has been actively conducted. In this paper, we propose a method to apply PUF-based device authentication technology to the Open Connectivity Foundation (OCF) open platform. The proposed method can greatly improve the security level of IoT open platform by utilizing PUF technology.**

Keywords—Device Authentication, PUF, IoT Open Platform

I. INTRODUCTION

Recently, IoT devices have been widely used in various fields. However, as various applications and services are widely provided and spread in the IoT environment, security issues are emerging. Because most IoT devices have power and resource limitations, it is difficult to apply existing security solutions such as vaccines and firewalls as they are. Therefore, many studies are being conducted to safely protect IoT devices from various security threats and vulnerabilities. PUF technology is attracting attention as a basic element of security to solve the security problems faced by such IoT devices. PUF is a technology that utilizes the unique characteristics of each device, and it is fundamentally impossible to duplicate even a device made with the same manufacturing process. In other words, since there is no need to inject the key externally or store it in memory, it can provide a very secure, lightweight and cost-effective method, which is suitable for IoT device authentication. However, although research on PUF-based authentication technology to solve IoT security problems is being actively conducted, attempts to solve security problems by applying PUF technology to IoT standard open platforms are insufficient. Therefore, when the above PUF technology is utilized, it can be of great help in strengthening the security of the existing IoT platform, which is attempting to switch to an open infrastructure-based integrated service ecosystem that considers mutual compatibility and scalability[1]. Above all, the proposed method that overcomes the limitations of existing PUF-based authentication technologies and complies with standards is expected to make the IoT environment more secure.

This paper proposes a method to strengthen IoT open platform security using PUF-based device authentication method. This paper is organized as follows: Section II briefly presents the current status of IoT open platform and PUF. Section III describes a design of the proposed scheme and explains how the proposed scheme enhances IoT open platform security. Section IV presents the prototype to which the proposed scheme will be applied. Lastly, Section V presents the conclusion.

II. BACKGROUND

A. PUF technology

The PUF has a structure that generates response (R), which is the only output to the input called challenge (C)[2]. Therefore, it can be modeled as a function representing the input-output relationship. The device is the input set challenge C = {C1, C2, …, Cn} for the set of outputs response R = {R1, R2, …, Rn} = PUF (C1, C2, …, Cn) can be extracted from PUF, and all challenge-response pairs, CRPs = {(C1, R1), (C2, R2), …, (Cn, Rn)} can be obtained. Secret key generation and device authentication are performed using these CRPs information. PUFs can be divided into two categories: weak PUFs and strong PUFs. Weak PUF typically has no or fixed challenge and has a limited response. Therefore, it is mainly used for secret key or identity generation. Strong PUF can acquire many CRPs. Since it is difficult to predict the response to a random challenge, it is often used for device authentication.

B. OCF Iotivity

The OCF defines a standard specification that can connect and control IoT devices[3]. It builds an architecture that guarantees interoperability between IoT devices and presents a model for managing resources. The standard specification consists of core, resource type device, bridging, and security. In addition, OCF has developed and provided IoTivity, an open source software framework for IoT.

III. PROPOSED SCHEME

A. Design of PUF-based Device Authentication Platform

The device authentication method using PUF technology on the OCF Iotivity open platform described above is presented, and Fig. 1 shows a schematic diagram of the overall application. As shown in the figure, the IoT device has a separate PUF device and provides PSK and public key-based device authentication using the PUF value. This PUF-based device authentication method follows the procedure of the Iotivity-Lite version of the OCF lightweight platform. In addition, such a device authentication method is preferentially applied to the device authentication process (OTM) performed in the onboarding process of the OCF standard and the device authentication process in the cloud registration process. Here, the Iotivity-Lite version is a lightweight platform of the OCF standard and follows the same OCF standard specification with only a difference in the implementation method for applying a lightweight device. This PUF-based device authentication method is performed through the interaction between IoT devices, OCF Cloud, and Mediator/OTGC, which are components of the OCF Iotivity open platform. The following describes schematic

design details for each component to provide the above function.

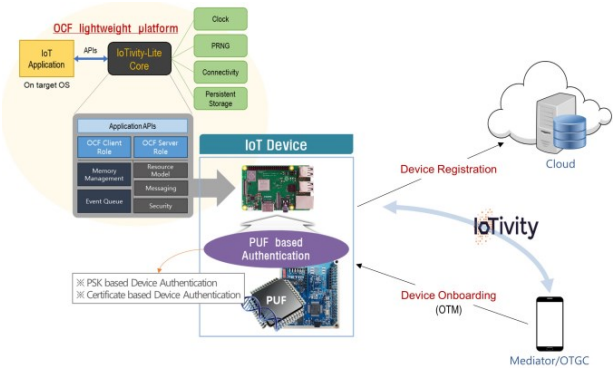

Fig. 1. Overall concept of PUF-based IoT device authentication on OCF

First, the IoT device basically operates as an OCF resource server and has a structure as shown in Fig. 2. As shown in the figure, an IoT device basically has a resource device according to the service it provides, and a control module and application module that control it. In addition, in order to manage resource information according to the OCF standard, it has an Iotivity Resource Module using the Iotivity-Lite library. Above all, a PUF device for providing a PUF-based device authentication technique is mounted, and a PUF I/O module for extracting and managing a PUF value from the corresponding PUF device is provided. Here, the PUF I/O Module utilizes the device authentication-related functions of the Iotivity-Lite library to provide a device authentication method in the OCF standard procedure.

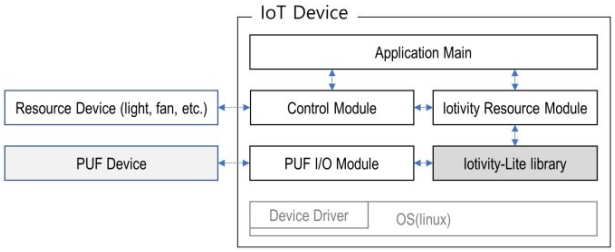

Fig. 2. The structure of IoT device

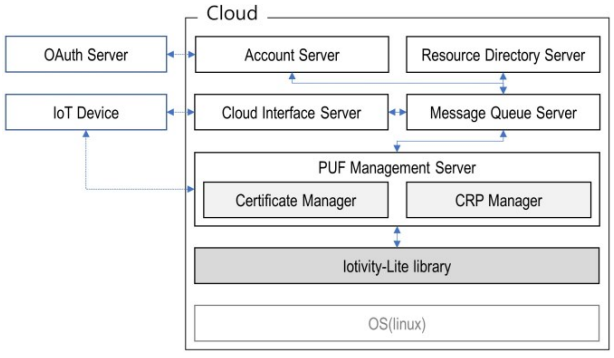

Fig. 3. The structure of OCF Cloud

Next, Fig. 3 briefly shows the structure of OCF Cloud for remote service provision. OCF Cloud has Account Server, Resource Directory Server, Cloud Interface Server, Message Queue Server, and OAuth Server as defined in the existing OCF standard. Additionally, the PUF Management Server is a module for providing PUF-based device authentication, and includes a Certificate Manager for public key-based device authentication and a CRP Manager for PSK-based device authentication. This utilizes the device authentication related functions of the Iotivity-Lite library to provide a device authentication method in the OCF standard procedure, like the above IoT device.

Finally, Fig. 4 briefly shows the structure of Mediator/OTGC (Onboarding Tool & Generic Client). It is basically loaded with a GUI module for controlling the service as a user device. In addition, the Mediator Module performs a function of registering itself and its own device to the cloud through interworking with the OAuth Module and the Onboarding Module. Here, the Onboarding Module performs the ownership acquisition procedure for the IoT device according to the existing OCF standard, but has an additional mechanism for providing a PUF-based device authentication technique.

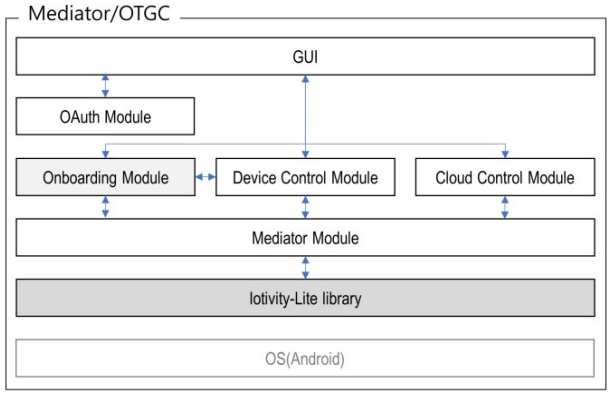

Fig. 4. The structure of meidator/OTGC

As described above, the IoT device, OCF Cloud, and Mediator/OTGC use the Iotivity-Lite library provided by the OCF standard to basically provide device authentication and other services according to the OCF standard procedure. Therefore, the device authentication technique using PUF on the OCF Iotivity open platform has a mechanism that can be performed while maximally complying with the OCF standard.

B. PUF-based IoT Device Authentication Mechanism

The PUF-based device authentication technique through the interaction between the IoT device, OCF Cloud, and Mediator/OTGC, which are components of the OCF Iotivity open platform described above, is applied to the device ownership acquisition process (OTM) performed in the onboarding of the OCF standard and device authentication in the device registration process to the OCF Cloud. Here, the OTM process for acquiring device ownership can be applied to both the PSK-based authentication method and the public key-based authentication method, and the device registration process to OCF Cloud is applied only to the public key-based authentication method. This is because, in the case of OCF Cloud, only the certificate-based device authentication method is provided according to the OCF standard specification. The proposed PUF-based IoT device authentication method shows that the PUF technology is sufficiently applicable to the global standard-based IoT open platform. It operates based on the OCF Iotivity standard, a representative IoT standardization organization, and uses

PUF technology in a form suitable for the onboarding procedure and the registration procedure to the OCF Cloud provided by the OCF security specification, thereby fundamentally blocking the exposure of the authentication key while blocking the existing standard. It provides an IoT device authentication method that can ensure compatibility and interoperability with technology. Above all, these PUF-based device authentication methods have the advantage that they can be applied to the IoT open platform without major modifications.

C. *Security Enhancement of IoTivity*

The proposed PUF-based IoT device authentication provides a scheme to strengthen security level by applying the OCF IoTivity open platform. The IoT device executes the OTM during the onboarding sequence. Utilizing PUF technology to run OTM makes it safer and more convenient to take ownership of a device. This is because, like *Random PIN Based OTM*, the process in which the user directly intervenes to input a *PIN* number can be omitted. In addition, after registering IoT devices in the OCF Cloud, device authentication is essential to provide services. The security can be improved through the certificate generation and authentication process using PUF rather than the traditional certificate-based authentication method. This is because the private key is not stored in non-volatile memory (NVM) such as flash memory, and whenever necessary in real time, a key is generated and used through PUF and immediately deleted. Fig. 5 shows the PUF-based certificate-based authentication method proposed in this paper.

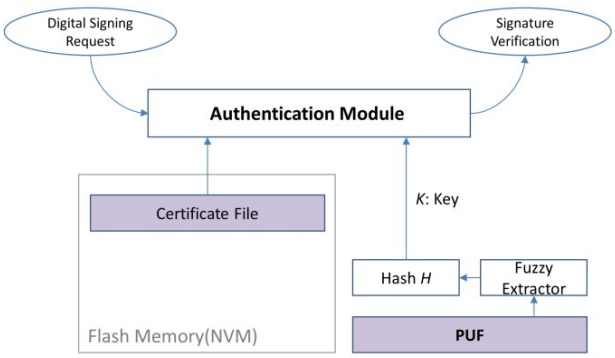

Fig. 5. Proposed cetificate-based authentication using PUF

IV. Implementation

To verify the proposed mechanism, a PUF-based IoT device authentication platform applicable to the OCF Iotivity standard was implemented. Fig. 6 shows an IoT device prototype. As shown in the figure, IoT devices basically operate on a commercial Raspberry Pi 3 Model B, and a self-made board called a *Kidden Board* is used as a peripheral device. Next, OCF Cloud for remote service provision used a general Linux server system based on Ubuntu. Finally, Mediator/OTGC provides a screen for PUF-based device authentication and a device registration screen to the cloud separately as shown in Fig. 7. In the figure, the upper three screens briefly show the PSK-based device authentication process using PUF. In addition, the cloud-based device control and monitoring service functions using LED bulbs were tested to check whether the normal operation was performed in the OCF standard specification.

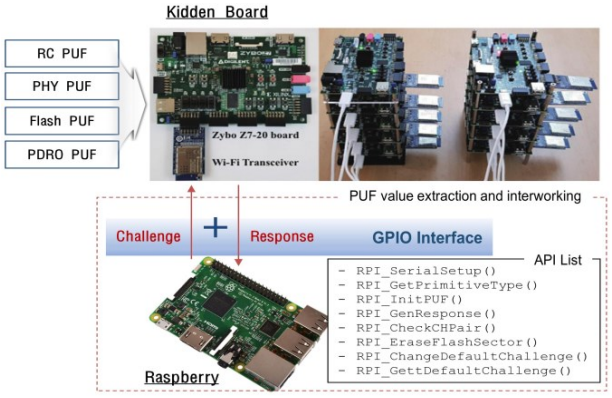

Fig. 6. IoT device prototype

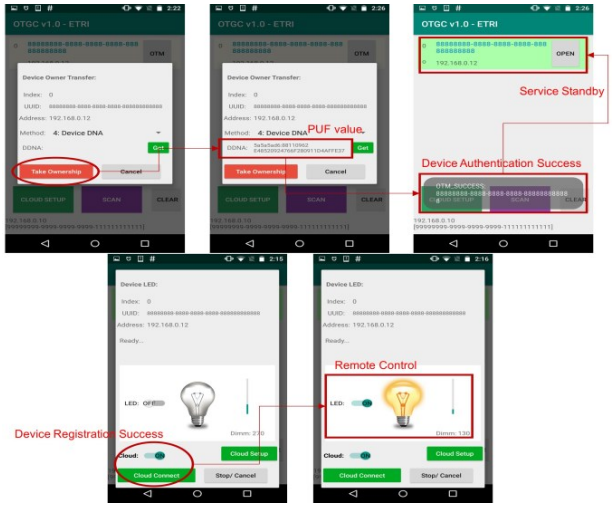

Fig. 7. IoT device authentication service

V. Conclustions

In this paper, we propose a PUF-based architecture that can be applied to the IoTivity open platform of OCF. Because PUF technology is applied while complying with OCF's IoTivity standard, it is expected to be usable in various application service fields by greatly improving the compatibility and security of IoT devices.

Acknowledgment

This work was supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government(MSIT) (No.2022-0-01019, Development of eSIM security platform technology for edge devices to expand the eSIM ecosystem)

References

[1] Byoungkoo Kim, Seoungyong Yoon, Yousung Kang, "PUF-based IoT Device Authentication Scheme on IoT Open Platform," in Proc. of ICTC2021, pp.1873-1875, Oct. 20-22, 2021.

[2] John Ross Wallrabenstein, "Practical and Secure IoT Device Authentication using Physical Unclonable Functions," in Proc. of IEEE 4th Conference on FiCloud, pp.99-106, August 22-24, 2016.

[3] Jaehong Jo, Jaehyun Cho, Rami Jung and Hanna Cha, "IoTivity-Lite: Comprehensive IoT Solution In A Constrained Memory Device," in Proc. of ICTC2018, pp.1367-1369, Oct. 17-19, 2018.