PUF-based Authentication Scheme for IoT Devices

Seungyong Yoon, Byoungkoo Kim, Yousung Kang, and Dooho Choi
Cryptographic Engineering Research Section
Electronics and Telecommunications Research Institute
Daejeon, Republic of Korea
{syyoon, bkkim05, youskang, dhchoi}@etri.re.kr

***Abstract*— This paper is about mutual authentication technology between devices with minimal user intervention in a large-scale IoT environment using PUF (Physical Unclonable Function). Most of the existing authentication schmes have been studied focusing only on device-to-server authentication, but the proposed method provides a mutual authentication between devices and devices that utilize the authentication server as a reliable intermediary. We can defend against information leakage, replay attacks, man-in-the-middle attacks, physical attacks, and machine learning based modeling attacks that can occur from various security threats of IoT devices through the proposed method in this paper.**

Keywords—IoT; device; PUF; authentication

I. INTRODUCTION

With the recent development of IoT technology, various devices and services are emerging that provide convenience to human life in many fields, such as smart homes, smart cars, and smart factories. However, cases of hacking damage of IoT devices are frequently reported, and the economic and social losses caused by them are increasing day by day. This is because the IoT environment is easily and widely exposed to security vulnerabilities and security threats. Most IoT devices cannot apply the security technology used in existing PCs or servers due to power and resource limitations, so they applied only lightweight security technology or minimal security functions, or loaded no security functions at all. In addition, a huge number of devices are connected to the Internet for 24 hours, and they are being fed by hackers because they are exposed to an easily accessible physical environment. The IoT device has a very inconvenient user interface, and it is difficult to apply security patches to newly discovered vulnerabilities, so security management is not properly performed. Security incidents such as information leakage due to hacking, DDoS (Distributed Denial of Service) attacks, and damages caused by illegal copying or forgery are constantly occurring.

In this situation, PUF, a hardware-based security technology, is getting attention. PUF is a technology that allows each device to have hardware-specific characteristics, such as a human fingerprint or iris, and a digital fingerprint that enables devices to have different characteristics even if they are made in the same manufacturing process. In other words, no matter how much the device is manufactured in the same way, it cannot be duplicated by its unique characteristics [1].

If PUF technology is applied to various application fields of the IoT environment, security can be greatly improved. Typical examples are genuine product authentication, firmware copy protection, device authentication, unique identifier generation, and real-time security key generation. In particular, if the PUF technology is used in the authentication field, a unique identifier and an authentication key for identifying each device can be generated inside the device without externally injecting it. In addition, since there is no need to have a separate internal nonvolatile memory for storing each identifier and authentication key, cost reduction effect can be expected. These PUF technologies have different output values (Response) for the same input value (Challenge), even if the circuits are produced by the same process. It can be used as a means to authenticate each device. That is, in the manufacturing process, the CRP (Challenge-Response Pair) database for device authentication is stored and built in advance in the authentication server, and compared to the CRP generated through the PUF of the device to be authenticated, authentication for each device is enabled [2].

Most of the existing PUF-based authentication methods have been studied with a focus on device authentication between devices and servers [3][4][5][6][7]. However, in various IoT environments, user needs are expected to be mutually authenticated and secure data communication not only between the device and the server (Device-to-Server), but also between the device and the device (Device-to-Device). Therefore, it is time to research and develop a PUF-based mutual authentication technology between device and device.

II. PROPOSED PUF-BASED AUTHENTICATION SCHEME

This paper provides a PUF-based mutual authentication method between device and device to enhance the security of IoT devices. Only one initial CRP is stored in the database of authentication server, and CRP for future authentication is updated during the execution of the authentication process. This minimizes server storage space, solves management problems caused by device growth, and solves security vulnerabilities that expose the entire CRPs when the server is hacked. In addition, it proposes a countermeasure against a machine learning based modeling attack by encrypting and transmitting response information for a challenge during the authentication process. By using the authentication server as a reliable intermediary, it provides a mutual authentication method between device and device that is newly increasing in demand. Finally, the proposed scheme is characterized by

providing a secure channel function through exchanging a session key for protecting a data communication channel while performing an authentication protocol.

A. System Model

The system model for PUF-based mutual authentication between devices in an IoT environment consists of an authentication server and devices. The authentication server acts as a trusted intermediary, and the devices are the subjects of mutual authentication and communication. Fig. 1 shows this system model. We assume that the authentication server acts as a reliable intermediary without resource constraints, and the IoT device has many resource constraints and basically has all PUF modules in the system model. It is also assumed that the authentication server and the device can communicate with each other via the Internet. As the IoT technology developed, device authentication technology began to emerge, and research on device-to-server authentication (1) has been actively conducted. This paper presents a solution for a device-to-device (2) mutual authentication technique that has not yet sufficiently researched and developed.

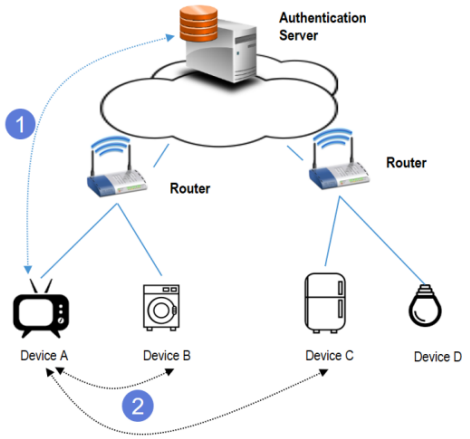

Fig. 1. System Model

B. Authentication Method

First, it is assumed that in the pre-stage of mutual authentication, the authentication server has previously built a CRP database. That is, in the manufacturing process step, the device identifier and CRP are extracted from the IoT device to build a database. At this time, each device registers only one PUF-based unique identifier and initial CRP required for authentication in the database. By storing only the initial one CRP in the authentication server, it is possible to minimize the database storage space for the server's CRP, and solve the management problem due to the increase of devices in a large-scale IoT environment. In addition, by minimizing CRP exposure when the server is hacked, the CRP exposure vulnerability for all devices can be solved.

Fig. 2 and Fig. 3 show the mutual authentication process between devices using PUF. In order to mutually authenticate between device A and device B, each device uses a trusted authentication server as an intermediary. The authentication server manages the device ID and the initial CRP required for authentication as a database. Response information for the challenge used for mutual authentication is transmitted by encryption, so it is possible to prevent machine learning based modeling attacks by fundamentally blocking eavesdropping or interception from a hacker. In addition, by sharing the session key during the execution of the mutual authentication protocol, data can be more securely communicated by encrypting and transmitting data with the shared session key between devices after authentication is completed.

Fig. 2 shows the initial flow of PUF-based mutual authentication between devices. This is performed in each step when one device (A) wants secure communication with the other device (B).

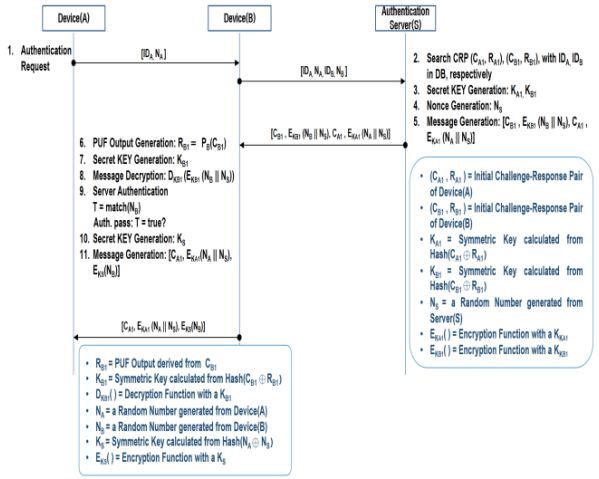

Fig. 2. Initial flow of PUF-based mutual authentication between devices

Fig. 3 shows the late flow of PUF-based mutual authentication between devices. This is done at each stage after the initial process in Fig. 2 is completed.

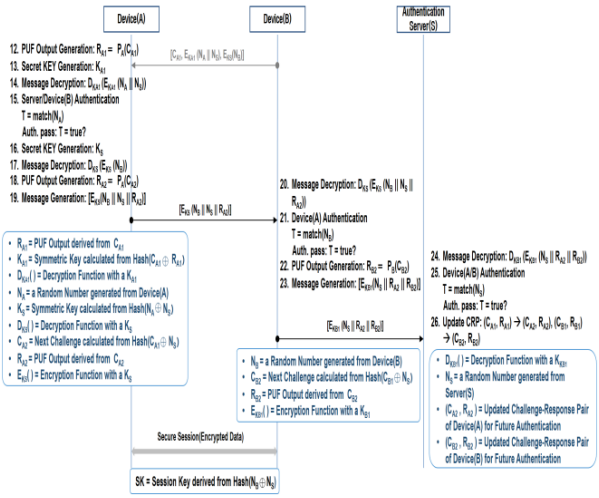

Fig. 3. Late flow of PUF-based mutual authentication between devices

III. Security Analysis

The proposed authentication method can prevent the following attacks that can occur from various security threats of IoT devices.

- Prevention of information leakage: We can prevent the threat of information leakage by using PUF technology in IoT devices. This is because information such as a device identifier and a secret key does not need to be injected externally, and this important information is not stored in a separate storage space such as memory. In addition, when the authentication server is hacked by a hacker, only one CRP per device is stored in the database, so information leakage can be minimized.
- Protection against Replay attacks: An attacker can secretly possess communication information between a device and an authentication server or between a device and a device, and then perform a replay attack on a target to be attacked after a certain time. The proposed method can prevent such a replay attack because it performs mutual authentication every session for communication.
- Protection against Man-in-the-middle attacks: The proposed method uses cryptographic communication using a secret key, so even if an attacker is sniffing in the middle, spoofing cannot be performed without knowing the CRP-based secret key. It is also safe against spoofing attacks, impersonation attacks, message tampering attacks and man-in-the-middle attacks.
- Protection against Physical attacks (Cloning attacks)[8]: It is secured from physical replication attack because authentication is performed by using the PUF module mounted on the IoT device.
- Protection against Side channel attacks[9]: Since PUF is also a kind of hardware composed of circuits, there is a possibility of side channel attack. The security for proposed authentication scheme is guaranteed according to whether the PUF chip has countermeasures against these attacks.
- Protection against Machine learning based modeling attack [10][11]: Because CRP is not directly exposed during the authentication process, and mutual authentication is performed using a CRP-based secret key, learning data cannot be acquired in the middle. As a result, machine learning based modeling attacks can be fundamentally blocked.

IV. Conclusion

This paper provides a mutual authentication scheme between devices with minimal user intervention, so it can be applied to large-scale IoT environments, and it is not necessary to inject information such as a secret key from outside by utilizing PUF technology. Since it is not stored in a separate storage space, it enhances security by blocking the source of exposure threats. In addition, there are no additional costs and risk of replication compared to hardware solutions such as HSM (Hardware Security Module), SE (Secure Element), TPM (Trusted Platform Module), and TrustZone. It provides a symmetric key based device mutual authentication method that can also be applied to the lightweight IoT devices, and effectively blocks man-in-the-middle attacks and replay attacks. In addition, secure communication is ensured by providing a secure channel function by sharing a secure session key for data transmission between devices during authentication protocol execution. When the mutual authentication method between IoT devices using PUF provided in this paper is applied to a large-scale IoT environment with weak security, it prevents security incidents such as information leakage caused by hacking, DDoS attacks, and damages caused by illegal copying or forgery. It is expected to drastically reduce the economic and social losses incurred.

Acknowledgment

This work was supported by Institute of Information & communications Technology Planning & Evalution (IITP) grant funded by the Korea government (MSIT) (No.2018-0-00230, Development on Autonomous Trust Enhancement Technology of IoT Device and Study on Adaptive IoT Security Open Architecture based on Global Standardization [TrusThingz Project]).

References

[1] C. Herder, M. Yu, F. Koushanfar and S. Devadas, “Physical Unclonable Functions and Applications: A Tutorial”, Proc. IEEE, Vol. 102, No. 8, pp. 1126-1141, August 2014.

[2] G. Suh, and S. Devadas, “Physical Unclonable Functions for Device Authentication and Secret Key Generation”, Proc. ACM/IEEE Design Automation Conference, pp. 9-14, June 2007.

[3] Y. Yilmaz, S. Gunn, and B. Halak, “Lightweight PUF-Based Authentication Protocol for IoT Devices, Proc. IEEE 3rd International Verification and Security Workshop, pp. 38-43, July 2018.

[4] M. Yu, M. Hiller, J. Delvaux, R. Sowell, S. Devadas, and I. Verbauwhede, “A Lockdown Technique to Prevent Machine Learning on PUFs for Lightweight Authentication”, IEEE Transactions on Multi-scale Computing Systems, Vol. 2, No.3, pp.146-159, July 2016.

[5] P. Gope and B. Sikdar, “Lightweight and Privacy-Preserving Two-Factor Authentication Scheme for IoT Devices”, IEEE Internet of Things Journal, Vol.6, No.1, pp.580-589, February 2019.

[6] V. Yanambaka, S. Mohanty, E. Kougianos, and D. Puthal, “PMsec: Physical Unclonable Function-Based Robust and Lighweight Authentication in the Internet of Medical Things”, IEEE Transactions on Consumer Electronics, Vol.65, No.3, August 2019.

[7] S. Yoon, B. Kim, Y. Kang, and B. Choi, “Security Enhancement for IoT Device using Physical Unclone Functions”, Proc. IEEE ICTC, pp. 1457-1459, October 2019.

[8] C. Helfmeier, C. Boit, D. Nedospasov and J. P. Seifert, “Cloning Physically Unclonable Functions,” In 2013 IEEE Hardware-Oriented Security and Trust (HOST), pp.1-6, June 2013.

[9] D. Merli, D. Schuster, F. Stumpf and G. Sigl, “Side-Channel Analysis of PUFs and Fuzzy Extractors,” Trust and Trustworthy Computing, LNCS 6740, pp. 33-47, June 2011.

[10] U. Ruhrmair, F. Sehnke, J. Solter, G. Dror, S. Devadas, and J. Schmidhuber, “Modeling Attacks on Physical Unclonable Functions”, Proc. ACM CCS, pp. 237-249, October 2010.

[11] U. Ruhrmair, J. Sölter, F. Sehnke, X. Xu, A. Mahmoud, V. Stoyanova, G. Dror, J. Schmidhuber, W. Burleson, and S. Devadas, “PUF Modeling Attacks on Simulated and Silicon Data,” IEEE Transactions on Information Forensics and Security, vol. 8, no. 11, pp. 1876-1891, November 2013.