ISSN 1330-3651 (Print), ISSN 1848-6339 (Online)
https://doi.org/10.17559/TV-20230608000709
Original scientific paper

ASM: Augmented Security Module for Commercial IoT Devices

Heeseung SON, Beom Seok KIM*, Jinsung CHO, Ben LEE

Abstract: The rapid expansion of the Internet of Things (IoT) has led to increased concerns regarding the security of IoT systems. Attacks targeting IoT devices, such as code injection and code reuse, have become more sophisticated, compromising device control and functionality. Existing security schemes, designed primarily for the ×86 architecture, are not well-suited for resource-constrained IoT devices. While numerous studies aim to strengthen IoT device security, practical implementation faces challenges due to time-to-market requirements and manufacturing costs. To address these issues, this paper proposes an Augmented Security Module (ASM) that provides essential security services for IoT devices within the same network, requiring minimal device modifications. The ASM includes Hardware Security Modules (HSMs) like Trusted Platform Module (TPM) and Secure Element (SE) to ensure data integrity and execute requested security services. By adding ASM Agents, which perform minimal operations to request security services, IoT devices can easily access the provided security services. The proposed ASM enables flexible adaptation to evolving security requirements at a low cost, meeting practical manufacturing and time-to-market demands. To validate the effectiveness of the proposed ASM, four representative scenarios are presented and analyzed, demonstrating its ability to enhance IoT device security and prevent attacks. The proposed ASM contributes to the widespread adoption of secure IoT systems by ensuring the security of IoT devices within the network.

Keywords: augmented security module; HSM; IoT security; security framework; security service

1 INTRODUCTION

Internet of Things (IoT) is a technology that effectively provides scalability and high productivity through rapid interactions among hyper-connected devices. However, malicious attacks can cause an IoT system to malfunction [1]. For example, in the case of Industrial IoT (IIoT) used in industrial sites, device malfunctioning due to security issues can lead to financial losses and accidents that threaten the safety of workers [2, 3]. Even in the case of Internet of Medical Things (IoMT) for medical support systems, malicious attacks can cause fatalities due to misdiagnoses or directly threaten patients' lives [4, 5].

Typically, most IoT devices use low-power processors and either operate as bare-metal devices or run Real-Time Operating System (RTOS) instead of a heavy, full-functioning OS. Furthermore, some IoT devices perform applications that require real-time capabilities, where specific tasks must be completed before their deadlines expire. Therefore, systems that introduce unpredictability or excessive overhead are unsuitable. These characteristics mean IoT devices do not have sufficient hardware performance to perform security services that require large processing power. In particular, the most significant reason for the malfunctioning of IoT devices is their vulnerability, and enhancing their security is a critical requirement. However, most existing security technologies are unsuitable for executing on IoT devices because they require high-performance processors with dedicated Hardware Security Modules (HSMs) and fully functioning OS [6]. For these reasons, most commercial low-end IoT devices still do not provide minimum security services. Indeed, numerous vulnerabilities in IoT devices have been exploited [7], highlighting the need to develop security systems specifically tailored for IoT devices independent of security techniques employed in IoT networks [8]. Furthermore, prior research analyzing commercial IoT devices and confirming their low security levels is a significant example that supports the necessity to enhance the security of IoT devices [9]. Consequently, research on security systems applicable to IoT devices is imperative for developing IoT systems.

However, applying security systems to all IoT devices is practically difficult for the following reasons. First, integrating security systems requires hardware specifications resulting in an extended development timeline, which is a critical factor in IoT device development where time-to-market is important. Second, it is costly, considering the expense of implementing security systems in IoT devices. Lastly, IoT devices are of various types, and each manufacturer has different types and levels of security systems. This means that substantial resources would be required to evaluate the security of IoT devices developed according to different standards. Therefore, research on security systems for IoT devices that can overcome these practical limitations is indispensable.

To address the aforementioned issues, this paper proposes Augmented Security Module (ASM) that isolates the security requirements from individual IoT devices and implements them on the ASM. The proposed ASM utilizes HSM (Hardware Security Module) to securely store and manage the security-sensitive data of interconnected IoT devices, ensuring integrity, availability, and confidentiality in providing security services. It performs the necessary security services for each device, guaranteeing their secure operation without requiring additional hardware or imposing significant overhead. The proposed ASM can satisfy device-specific security requirements by adding security services in real-time, and IoT devices only require a lightweight client to request security services from the ASM. In addition, since ASM can simultaneously provide security services to multiple IoT devices belonging to the same network, the cost can be reduced compared to implementing a separate security system for each device.

The contributions of the proposed ASM are as follows:

- Separation of security systems from IoT devices: By separating IoT devices from security systems, each device can be operated until its maximum lifespan, and the ASM performs the necessary security services for IoT devices, thereby not increasing the overhead on IoT devices. Furthermore, by separating the development processes of IoT devices and security systems, cost savings can be achieved compared to embedding security systems directly into IoT devices.

- Safe storage of security data for each device: Exposure and abuse of security data are prevented by utilizing HSM built into ASM to create and securely store security data for IoT devices.
- Scalable security service: The security is improved by updating security services to the proposed ASM without changes to IoT devices.

The remainder of this article is organized as follows: Section 2 presents an analysis of IoT security issues and limitations of existing research efforts. Section 3 presents the details of the proposed ASM. Section 4 discusses four security service scenarios that can be performed in the proposed ASM-applied IoT system and analyze its security, economic feasibility, and scalability. Finally, section 5 concludes this article.

2 LITERATURE REVIEW

2.1 IoT System

An IoT system provides various services through the interaction of IoT devices. Therefore, even a single compromised IoT device can cause a malfunction of the entire IoT system. The most serious malfunctions are caused by vulnerabilities in individual IoT devices, which can lead to service disruption of the entire IoT system, leakage of users' information, and financial loss. The vulnerability in IoT devices has been verified in several case studies. Zhao et al. [10] performed an empirical long-term vulnerability analysis on 1362906 IoT devices over a period of 10 months and verified that 28.25% of the devices had at least one N-day vulnerability. Actual vulnerabilities in IoT devices have been verified through our preliminary research that analyzed the security of commercial IoT devices, and examples of attacks, such as Mirai and Hajime botnet or IoT ransomware targeting critical social infrastructure, have been reported [8].

Unlike existing sensor network systems designed for static services such as data collection and monitoring, IoT systems are characterized by high variability [11], which is due to the frequent addition/replacement/removal of devices and the resulting change in the number and type of user requests. As a result, this leads to frequent variations in the amount of data transmission in an IoT system.

Considering these characteristics and potential problems, an IoT system should guarantee robustness and compatibility to provide sustainable services. However, most off-the-shelf commercial IoT systems are not designed with robustness and variability in mind. In addition, the importance of time-to-market requirements and high development/maintenance costs exacerbate these issues [12]. As such, most of the existing commercial IoT systems do not satisfy the fundamental security requirements [7, 8].

2.2 Analysis of Existing Security Service for IoT Devices

Most studies to improve the security of IoT systems have been conducted with a focus on the security of individual IoT devices, which should satisfy the following requirements [6]:

- Confidentiality of security-sensitive data: Generally, a Root of Trust (RoT) in a security system can be obtained by ensuring integrity, confidentiality, and availability of cryptographic keys and credentials. Leakage of cryptographic keys and credentials can result in serious security issues such as loss of control and malfunction. Therefore, obtaining RoT of security services performed by individual IoT devices is an important requirement.
- Low overhead: Because most IoT devices operate on batteries, there are hardware constraints, such as low-end processors and limited memory, to ensure low power consumption. In addition, most IoT services have real-time requirements. However, existing security systems that require large processing power are not suitable for applying directly to IoT devices. Therefore, either modifying the existing security system to satisfy the low-power requirement or developing a new low-power security system that considers the characteristics of IoT devices is necessary.
- Variability of security system for IoT devices: The services provided by an IoT system can be frequently modified according to the user's request, and the amount of data transmitted on the network can vary. Moreover, adding, replacing, and removing IoT devices according to changes in IoT services can further increase the variability of the IoT system. This causes security requirements to increase, and thus a security system that can flexibly respond to these requirements is required.
- Low cost: As mentioned earlier, time-to-market is an important factor in IoT [7]. In addition, development and maintenance costs should be minimized.

Existing studies to enhance the security of IoT devices can be categorized into security platforms for IoT devices, security techniques using HSM, and lightweight encryption algorithms.

- Security platform for IoT devices: Trusted Execution Environment (TEE) is a representative system-level security platform that can improve security by providing an isolated execution environment. Examples of implementations and commercialization of TEEs are ARM's TrustZone and Platform Security Architecture (PSA) [13, 14]. TrustZone and PSA can guarantee secure operation by providing isolation of system resources. However, TrustZone and PSA are ARM processor-dependent platforms, and thus they cannot be applied to IoT devices based on third-party hardware. To overcome this limitation, various studies have been conducted [15, 16].
- HSM-based Security service: HSMs such as Trusted Platform Module (TPM) and SE (Secure Element) can be referred to as RoT in providing secure security services. Recently, efforts to design and develop security services essential for IoT devices based on HSM have been made. A method to prevent malicious attacks such as spoofing has been proposed by generating a device-specific signature using a function that cannot be duplicated physically, i.e., Physically Unclonable Function (PUF) [17]. Cabrera Gutierrez et al. [18] claim that the robustness and reliability of HSM are essential for IoT devices. While countermeasures to improve the security based on these HSMs can optimize the design of IoT devices for specific purposes, development time and cost increase since different hardware and software designs are required for each application.
- Lightweight encryption algorithm: A number of studies on lightweight encryption algorithms designed

considering IoT devices have been conducted [19, 20]. However, most of them are less secure than existing encryption algorithms or have a large overhead to execute on IoT devices.

There are also practical studies that show the security of IoT devices in a real environment can be improved. However, existing schemes have the following limitations from the perspective of the entire IoT system:

- Low flexibility of IoT devices: Since most IoT devices are designed, developed, and produced according to their own standards, a practical IoT system that consists of various heterogeneous IoT devices should be considered. Therefore, applying existing security improvement schemes to these devices would require considering the security requirements of individual devices and lead to implementation methods that are different for each device. The heterogeneity of these IoT devices is a significant obstacle to guaranteeing a certain level of security in configuring the entire IoT system making it impossible to conduct a holistic security evaluation. In addition, this can cause compatibility issues between security services.
- High cost: Fast time-to-market is critical for rapidly increasing the size of IoT systems. However, this also inevitably leads to increasing costs to manufacture IoT devices because of various HSMs needed to ensure their security. In addition, since IoT devices are developed based on the hardware performance required during device manufacturing, replacing a device to provide new security services to existing installed devices is challenging.
- Security scalability: As mentioned before, IoT security requirements can change based on the variability in IoT services. However, existing security services for individual IoT devices do not have the flexibility which responds to this variability. In particular, when the performance of IoT devices does not satisfy new security requirements, they should be replaced with more hardware-enhanced devices, which can significantly increase cost.

The problems mentioned above are the most serious obstacles to implementing practical IoT services. Therefore, it is necessary to develop a new type of security system that comprehensively considers the characteristics of the entire IoT system rather than just focusing on improving the security of individual IoT devices.

3 RESEARCH METHODOLOGY

This section presents the proposed ASM that can guarantee security for all heterogeneous IoT devices within a local network. Details of the proposed ASM are discussed in the following subsections.

As shown in Fig. 1, ASM is a module that executes security services to maintain a certain level of security for all IoT devices existing on the same local network and securely stores security sensitive data on behalf of individual IoT devices. In the proposed model, the IoT internal network to which ASM is applied can be secure because the ASM provides secure proxy services between IoT devices and a server. Furthermore, ASM can guarantee secure execution of security services through RoT-based integrity verification techniques such as secure boot.

Fig. 2 shows the architecture of the proposed ASM and an IoT device. ASM has basic hardware components (i.e., Basic Components) and additional HSM such as TPM, SE, one-time programming (OTP) memory, cryptographic accelerator, and True Random Number Generator (TRNG) as the RoT. The hardware components of ASM should have sufficient processing power to perform security services requested by all IoT devices within the local network and satisfy the security requirements of the IoT system. Typical security services for IoT devices include attested boot, attestation, cryptographic function, secure communication over the internet (i.e., Secure proxy), and other security services required by the IoT service.

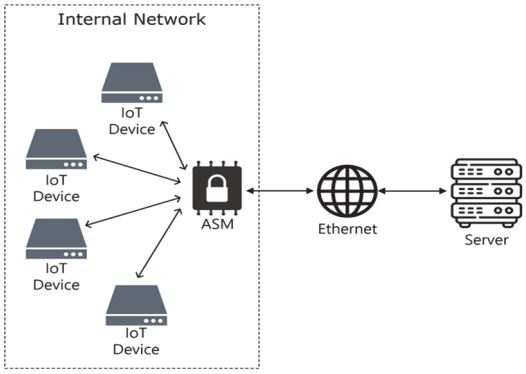

Figure 1 ASM-based IoT system

The ASM Manager manages a set of security services for IoT devices belonging to the same local network, which include Attestation, Secure proxy, Secure Firmware Update, Cryptographic Algorithm, and Authentication. This is achieved by maintaining Device-Service List, which is a list of security services for all the IoT devices. It also provides an interface for individual IoT devices to request security services.

The Security Services define the set operations that ASM can provide to the IoT device, and consist of Server Service and Client Service. The Server Service is performed by the ASM and has the authority to access the HSM, where security-sensitive data such as encryption keys, authentication information, and credentials of individual IoT devices are stored. The Client Service is a module that is dynamically executed by an IoT device when a security service is needed from ASM and collects and transmits the information necessary to perform the security service. In addition, the versions of the Client Service that can operate on the hardware platform of each IoT device are managed by considering the heterogeneity of individual IoT devices.

IoT devices include ASM Agents to interact with ASM, and their roles and operations are as follows.

Security service initialization and request: The ASM Agent performs initialization by communicating with the ASM manager to provide requested security services.

Client service load: The ASM Agent receives Client Service from ASM and loads it into memory.

Information collection and communication with ASM: The Client Service of the IoT device collects information and transmits it to the ASM. It also communicates with the Server Service to exchange the information needed to execute the requested security service.

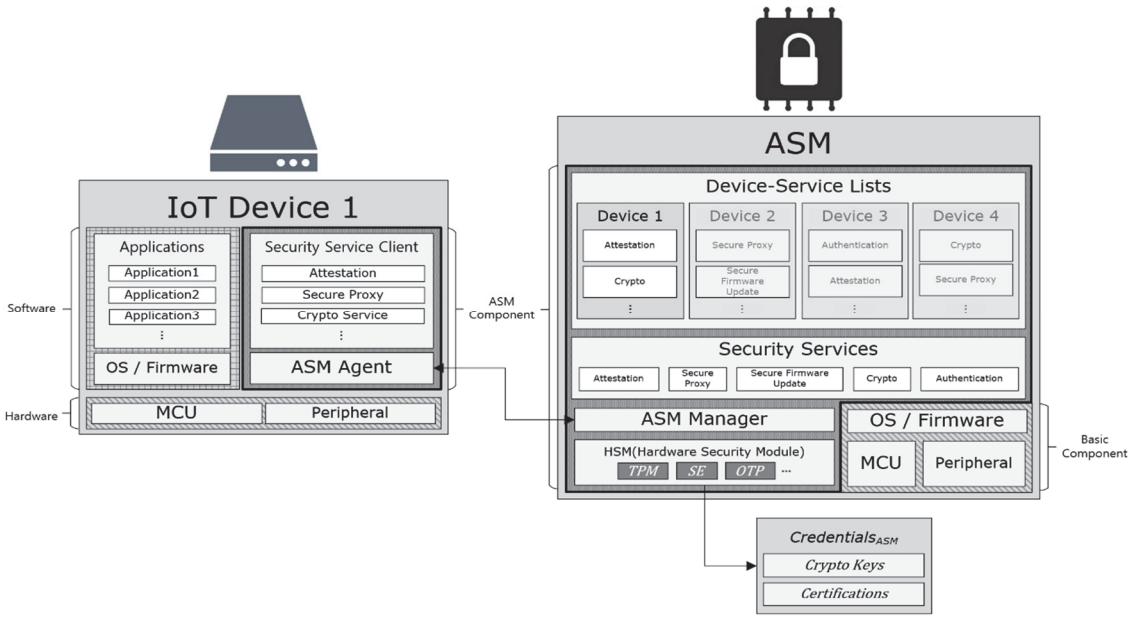

Figure 2 The architecture of the proposed ASM and IoT device

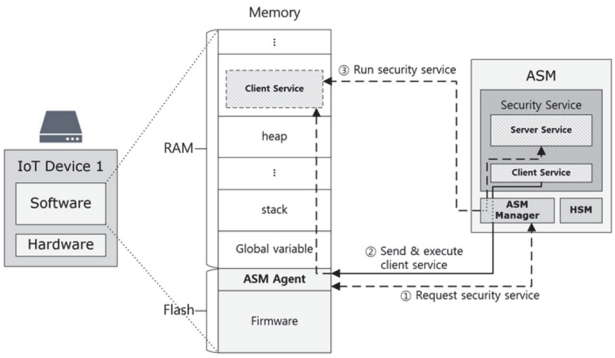

Figure 3 A procedure for requesting security services by IoT devices to ASM

Fig. 3 illustrates the procedure by which an IoT device requests and performs a specific security service from ASM. Security service requests can be initiated in both ASM and IoT devices (1st step of Fig. 3). When a security service is requested, the ASM Manager sends the Client Service image corresponding to the security service requested by the ASM Agent (2nd step of Fig. 3). The ASM Agent of the IoT device loads the received Client Service into its memory and executes it (3rd step of Fig. 3). The Server Service communicates with the Client Service and performs the requested security service by utilizing the security-sensitive data of the IoT device stored in the HSM. When specific information about the IoT device is necessary to perform the requested security service, the Server Service can request it from the Client Service, which collects the information and transmits it to the Server Service. Upon completing the requested security service, the Server Service transmits its execution result to the Client Service. After that, the Client Service notifies the ASM Agent about completing the security service, and the ASM Agent terminates the requested Client Service.

The proposed ASM can securely store security-sensitive data of registered IoT devices through HSM to obtain RoT and guarantee reliable execution of security services. This also reduces the cost of design, implementation, and production of IoT devices because developers only need to add ASM Agents corresponding to the security services needed by IoT devices. IoT devices receive the Client Service from ASM and load it into memory to perform it dynamically. Therefore, the IoT system can be conveniently and inexpensively maintained without the firmware update for the addition/removal/change of security services. When security requirements are enhanced due to the variability of the IoT system, this can be satisfied by adding only the necessary Security Service to ASM. Even if the performance of ASM is insufficient, the security of IoT devices belonging to the same network can be maintained at a certain level only by replacing ASM, not by replacing IoT devices.

4 RESULTS AND DISCUSSION

The proposed ASM is based on our previous research, the ARM Platform Security Architecture (PSA) based secure platform model, which is designed to effectively enhance the security of IoT devices. Our secure platform model includes all the required HSMs for the ASM and provides essential security services such as secure boot, secure firmware update, attestation, cryptographic functions, and key management to reinforce the security of IoT devices within the same network. Furthermore, our secure platform model offers APIs for implementing security functionalities, reducing the development costs associated with creating the ASM. Moreover, our previous research has demonstrated the successful application of the secure platform model to physical IoT devices, validating the feasibility of implementing the proposed ASM based on the secure platform model.

This section presents scenarios for performing attestation and secure firmware update, which are essential security services that can be executed by the proposed ASM. The discussion also includes cryptographic function and secure proxy that can be optimally applied to ensure the basic level of security of IoT devices. In addition, the security evaluation and economic feasibility of the proposed ASM are carried out by analyzing the process of performing the following four scenarios: attestation, secure

firmware update, cryptographic function, and secure proxy.

In all the scenarios, the IoT device performs the initialization routine that the ASM Agent receives from the client service and loads it into memory. Details and security/performance/economic analysis of each scenario after initialization are discussed in the following subsections.

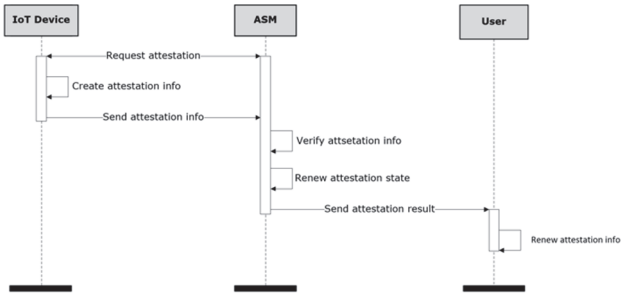

Figure 4 A sequence of the attestation service between ASM and the IoT device

4.1 Scenario I: Attestation

An attestation service verifies the integrity of the current target device by performing verification from a reliable external system through attestation information, which is a combination of unique information of the target device. The first scenario outlines the process of verifying the integrity of each IoT device through the ASM when the requirement for continuous integrity verification of an existing IoT system is added. Fig. 4 illustrates the sequence of communications between ASM and the IoT device to perform attestation, which involve the following:

- The Client Service in the IoT device creates attestation information and transmits it to the Server Service corresponding to the attestation service of ASM.
- The Server Service receives the attestation information and verifies the integrity of the IoT device using the attestation information.
- The IoT device notifies the attestation results to the user.

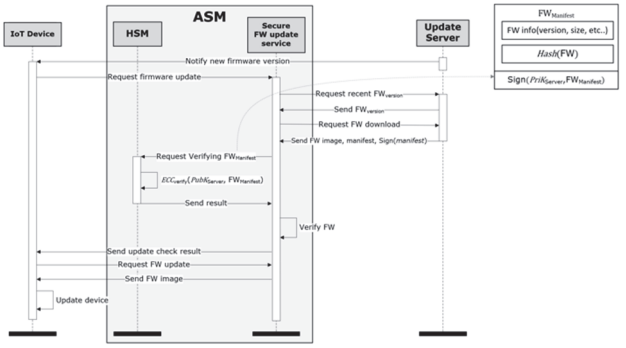

Figure 5 A sequence of the secure firmware update service among ASM, IoT device, and update server

To implement the existing remote attestation service in an IoT environment, a secure connection between the attestation server and the IoT device needs to be established. Therefore, IoT devices require sufficient processing power to run cryptographic algorithms and maintain secure storage to store keys. As mentioned previously, this leads to high manufacturing costs for IoT devices. In contrast, the attestation service is executed in the proposed ASM. In addition, since all the operations to verify the integrity of the IoT device are performed in the ASM, the IoT device only needs to generate and transmit attestation information to ASM.

4.2 Scenario II: Secure Firmware Update

The Secure Firmware Update service verifies the integrity of the firmware image for an IoT device and securely updates it. The services provided by the IoT system are based on IoT devices and require continuous updates. The second scenario illustrates the provision of secure firmware update services through the ASM when the requirement for ensuring the integrity of firmware updates for IoT devices is added. This is performed through information exchange among IoT devices, ASM, and external update servers as shown in Fig. 5, and the detailed operations are as follows:

- The update server notifies the IoT device that the firmware has a new version.
- Upon receiving the notification, the IoT device requests a secure firmware update from the ASM Agent.
- The Secure Firmware Update service requests the latest firmware version information from the update server, and the update server sends this information back to the secure firmware update service.
- After checking the new version of the firmware, the secure firmware update service requests the firmware image from the update server.
- The update server sends a manifest composed of the new firmware image, firmware information (i.e., version and size), and a hash of the firmware image to ASM. In addition, the update server also sends the signature of the manifest generated by the private key of the update server to ASM.
- The Secure Firmware Update service relies on HSM to verify the integrity of the manifest transmitted from the update server. HSM performs asymmetric key algorithms such as ECC to verify the transmitted manifest and sends the verification results to the Secure Firmware Update service.
- If the integrity of the manifest is verified, the Security Firmware Update service hashes the received firmware image and checks its integrity against the hash contained in the manifest.
- If both the firmware image and the integrity of the manifest have been verified, the Secure Firmware Update service sends an update check result to the IoT device, which then requests a firmware update to the Secure Firmware Update service.
- The Secure Firmware Update service sends the firmware image to the IoT device, which is updated with the new version of the firmware.

The Secure Firmware Update service through ASM can prevent attacks such as man-in-the-middle by verifying the integrity of the firmware. In addition, IoT devices can securely perform firmware updates without adding code and hardware, reducing development and maintenance costs or existing security-enhancing methodologies for IoT devices.

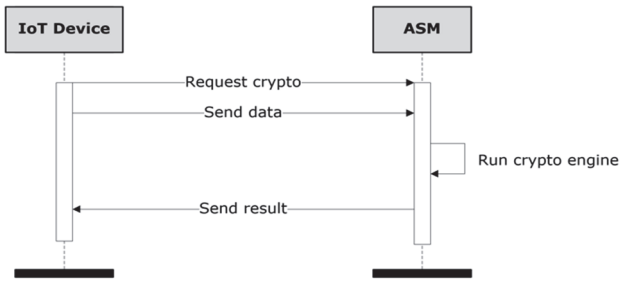

Figure 6 A sequence of the cryptographic function service between ASM and IoT device

4.3 Scenario III: Cryptographic Function

The third scenario addresses the need for direct data operation on IoT devices that guarantees their security, specifically for functions that must be provided when dealing with data that does not contain security sensitive information. In cases where encryption is required for data stored on IoT devices, the process involves requesting the ASM to perform the encryption service. The sequence of cryptographic function is described in Fig. 6, and the detailed operation of the cryptographic function is as follows:

- The Client Service corresponding to the cryptographic function requests encryption and transmits data to be encrypted.
- ASM performs encryption using the cryptographic engine with the key stored in the secure storage and transmits the encryption result to the IoT device.

The cryptographic function used by the proposed ASM can securely and quickly perform the encryption algorithm because of the built-in encryption accelerator and secure storage. Moreover, IoT devices can be developed at a lower cost than existing security-enhancing methodologies for IoT devices because they do not require dedicated software or hardware to store keys and perform cryptographic algorithms.

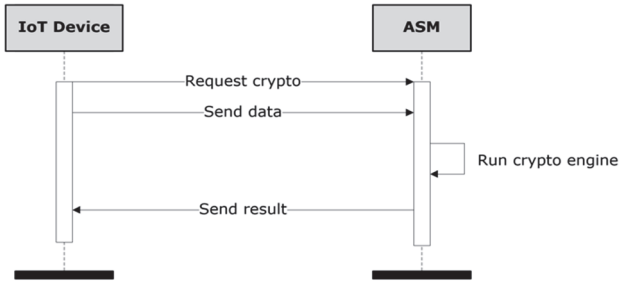

Figure 7 A sequence of the secure proxy service among ASM, IoT device, and external server

4.4 Scenario IV: Secure Proxy

As shown in Fig. 7, Secure Proxy service guarantees an end-to-end secure connection between an IoT device and a server on an external network. The fourth scenario relates to situations where IoT devices require secure data communication with entities outside the local network. It presents a case where the ASM provides a secure proxy service, ensuring safe data transmission between IoT devices and external entities. When an IoT device requires secure communication with a server on an external network, a request is made to the Server Service corresponding to the secure proxy service.

The Server Service notifies the IoT device that the secure proxy service is ready after establishing a secure connection such as OpenSSL with the external server. The certificate, which allows a secure connection to be established with the external server, is safely stored through HSMs in ASM.

When the IoT device transmits data to the external server, raw data is delivered to ASM through the local network.

The Server Service receives raw data from the IoT device, encrypts and signs it using HSM, and transmits it to the external server.

When the external server transmits data to the IoT device, it encrypts and signs the data to be sent and transmits it to ASM.

After receiving the data, the Server Service decrypts the received data and verifies the signature, and if the integrity is verified, the raw data is delivered to the IoT device through the local network.

The ASM establishes a secure connection such as OpenSSL with the external server instead of the IoT device, and therefore, IoT devices need not require cryptographic functions having large processing requirements. In addition, the HSM in ASM also provides secure storage of security-sensitive data, such as keys and certificates, to establish secure connections.

4.5 Summary

The four scenarios presented above prove that an IoT device can satisfy a certain level of security through the security service provided by the proposed ASM. From a practical point-of-view, the secure proxy service of ASM enables secure communication on ASM's internal network and protects against communication attacks from the internet, such as fabrication, modification, and sniffing. In addition, in an IoT system with ASM, all the conditions and requirements necessary to perform security services are implemented in the ASM, and individual IoT devices only need to add the ASM Agent corresponding to the ASM Manager. For this reason, the proposed ASM can be developed and maintained for a low-cost IoT system while providing security for all IoT devices in the local network. Moreover, even when ASM devices need hardware upgrades as security requirements increase, replacing only the ASM can guarantee the security level of the local network. This makes it easier and more economical to improve the security of the entire IoT system.

Meanwhile, the proposed ASM is subject to the constraint that it can only be applied to IoT devices within the same local network. Moreover, to execute client services on host IoT devices, additional memory is required. These limitations should be taken into consideration while implementing the ASM solution, as they may influence the overall deployment and resource requirements for the secure platform model.

5 CONCLUSION

With the proliferation of IoTs, their security concerns are increasing. The problem is that existing security

schemes cannot be applied to IoT systems composed of low-end IoT devices, and various studies have been proposed to improve the security of IoT devices to solve this. However, security techniques for IoT devices are not practical because they increase development time and manufacturing and maintenance costs. In addition, existing security services for IoT devices cannot flexibly respond to the variabilities of an IoT system. To solve these problems, this paper proposed ASM that can provide security services to IoT devices on the local network. The ASM Agent embedded into IoT devices enables the execution of security services provided by the ASM. To verify the security of the proposed ASM, this paper presented and analyzed four security service scenarios that can be implemented in an IoT system with ASM and proved that the proposed ASM can provide a certain level of security while guaranteeing low costs in production and maintenance of the entire IoT system. Therefore, there is no need to integrate dedicated security hardware into each individual IoT device by utilizing ASM. Additionally, when updating security services, only ASM needs to be updated, and the client services can be reloaded, thereby increasing the availability of IoT devices. This approach ensures the convenience and efficiency of security service updates without causing disruptions to the overall functionality of IoT devices. Future research includes the optimized execution methods of ASM agents and security services for IoT devices with limited resources while reducing the overhead on IoT devices.

Acknowledgements

This work was supported in part by the Young Researcher Support Program through the National Research Foundation of Korea (NRF) grant funded by the Ministry of Science, Information & Communication Technology (ICT) and Future Planning (MSIP) under Grant NRF-2018R1C1B6006938; in part by the Basic Science Research Program through NRF grant funded by the Ministry of Education under Grant NRF-2022R1F1A1063724; and in part by the Ministry of Science and ICT (MSIT), South Korea, under the Convergence Security Core Talent Training Business Support Program Supervised by the Institute for Information and Communications Technology Planning and Evaluation (IITP) under Grant IITP-2023-RS-2023-00266615.

6 REFERENCES

[1] Xu, M., Huber, M., Sun, Z., Enagland, P., Peinado, M., Lee, S., Marochko, A., Matton, D., Spiger, R., & Thom, S. (2019). Dominance as a New Trusted Computing Primitive for the Internet of Things. *Proc. of IEEE Symposium on Security and Privacy*. https://doi.org/10.1109/SP.2019.00084

[2] Panchal, A. C., Khadse, V. M., & Mahalle, P. N. (2018). Security Issues in IIoT: A Comprehensive Survey of Attacks on IIoT and Its Countermeasures. *IEEE Global Conference on Wireless Computing and Networking (GCWCN)*. https://doi.org/10.1109/GCWCN.2018.8668630

[3] Jayalaxmi, P., Saha, R., Kumar, G., Kumar, N., & Kim, T. (2021). A taxonomy of security issues in Industrial Internet-of-Things: scoping review for existing solutions, future implications, and challenges. *IEEE Access*, *9*, 25344-25359. https://doi.org/10.1109/ACCESS.2021.3057766

[4] https://fudosecurity.com/blog/2022/02/18/security-vulnerabilities-within-healthcare-miot-devices

[5] https://money.cnn.com/2017/01/09/technology/fda-st-jude-cardiac-hack

[6] Meneghello, F., Calore, M., Zucchetto, D., Polese, M., & Zanella, A. (2019) IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices. *IEEE Internet of Things Journal*, *6*(5), 8182-8201. https://doi.org/10.1109/JIOT.2019.2935189

[7] Alladi, T., Chamola, V., Sikdar, B., & Choo, K. R. (2020). Consumer IoT: Security Vulnerability Case Studies and Solutions. *IEEE Consumer Electronics Magazine*, *9*(2), 17-25. https://doi.org/10.1109/MCE.2019.2953740

[8] Jung, J., Kim, B., Cho, J., & Lee, B. (2022). A Secure Platform Model Based on ARM Platform Security Architecture for IoT Devices. *IEEE Internet of Things Journal*, *9*(7), 5548-5560. https://doi.org/10.1109/JIOT.2021.3109299

[9] Sattar, K. A. & Al-Omary, A. (2020). A survey: security issue in IoT environment and IoT architecture. *Proc on 3rd Smart Cities Symposium (SCS)*.

[10] Zhao, B., Ji, S., Lee, W. H., Lin, C., Weng, H., Wu, J., Zhou, P., Fang, L., & Beyah, R. (2022). A Large-Scale Empirical Study on the Vulnerability of Deployed IoT Devices. *IEEE Transactions on Dependable and Secure Computing*, *19*(3), 1826-1840. https://doi.org/10.1109/TDSC.2020.3037908

[11] Hameed, A. & Alomary, A. (2019). Security Issues in IoT: A Survey. *International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)*. https://doi.org/10.1109/3ICT.2019.8910320

[12] Cozzi, E., Graziano, M., Fratantonio, Y., & Balzarotti, D. (2018). Understanding Linux Malware. *IEEE Symposium on Security and Privacy (SP)* https://doi.org/10.1109/3ICT.2019.8910320

[13] Arm Limited (2009). Arm Security Technology-Building a Secure System using Trust Zone Technology.

[14] Arm Limited (2021). Arm Platorm Security Model 1.1.

[15] Jang, J. & Kang, B. B. (2022). 3rdParTEE: Securing Third-Party IoT Services Using the Trusted Execution Environment. *IEEE Internet of Things Journal*, *9*(17), 15814-15826. https://doi.org/10.1109/JIOT.2022.3152555

[16] Oliveira, D., Gomes, T., & Pinto, S. (2022). uTango: An Open-Source TEE for IoT Devices. *IEEE Access*, *10*, 23913-23930. https://doi.org/10.1109/ACCESS.2022.3152781

[17] Halak, B., Gall, C., Fathir, S., Kit, N., Raymode, R., Gimson, M., Kida, A., & Voncent, H. (2022). Toward Autonomous Physical Security Defenses Using Machine Learning. *IEEE Access*, *10*, 55369-55380. https://doi.org/10.1109/ACCESS.2022.3175615

[18] Cabrera- Gutiérrez, A. J., Castillo, E., Escobar-Molero, A., Álvarez-Bermejo, J. A., Morales, D. P., & Parrilla, L. (2022). Integration of Hardware Security Modules and Permissioned Blockchain in Industrial IoT Networks. *IEEE Access*, *10*, 114331-114345. https://doi.org/10.1109/ACCESS.2022.3217815

[19] Ud Din, I., Bano, A., Awan, K. A., Almogren, A., Altameem, A., & Guizani, M. (2021). LightTrust: Lightweight Trust Management for Edge Devices in Industrial Internet of Things. *IEEE Internet of Things Journal*, *10*(4), 2776-2783. https://doi.org/10.1109/JIOT.2021.3081422

[20] Tao, H., Bhuiyan, M. Z. A., Abdalla, A. N., Hassan, M. M., Zain, J. M., & Hayajneh, T. (2019). Secured Data Collection with Hardware-Based Ciphers for IoT-Based Healthcare. *IEEE Internet of Things Journal*, *6*(1), 410-420. https://doi.org/10.1109/JIOT.2018.2854714

Contact information:

Heeseung SON, PhD student
School of Computing, College of Software, Kyung Hee University,
1732, Deogyeong-daero, Giheung-gu, Yongin-si, Gyeonggi-do 17104,
Republic of Korea
E-mail: toddlf95@khu.ac.kr

Beom Seok KIM, PhD
(Corresponding author)
School of Computing, College of Software, Kyung Hee University,
1732, Deogyeong-daero, Giheung-gu, Yongin-si, Gyeonggi-do 17104,
Republic of Korea
E-mail: passion0822@khu.ac.kr

Jinsung CHO, Professor
School of Computing, College of Software, Kyung Hee University,
1732, Deogyeong-daero, Giheung-gu, Yongin-si, Gyeonggi-do 17104,
Republic of Korea
E-mail: chojs@khu.ac.kr

Ben LEE, Professor
School of Electrical Engineering and Computer Science,
Oregon State University,
Corvallis 97331, OR, USA
E-mail: benl@eecs.orst.edu