Blockchain-based Firmware Update Framework for Internet-of-Things Environment

Alexander Yohan¹, Nai-Wei Lo², Suttawee Achawapong³
Department of Information Management
National Taiwan University of Science and Technology
Taipei, Taiwan
nwlo@cs.ntust.edu.tw²
{d10309802¹, m104098173³}@mail.ntust.edu.tw

Abstract—Internet-of-Things is becoming an important technology for improving the people’s quality of life. With this being the case, a lot of IoT devices are manufactured and the applications of IoT are increasing drastically in the past five years. Improper device management and firmware distribution from the device manufacturer could harm the IoT environment. In this paper, a firmware update framework for IoT devices based on blockchain technology is proposed. The proposed framework aims to securely verify the firmware deployed by the device manufacturer and to securely distribute the firmware to the end-device. A PUSH-based firmware update method is adopted to deliver the new version of firmware from the legitimate vendor. In addition, smart contract and consensus mechanism from blockchain technology are utilized to preserve the integrity of the distributed firmware.

Keywords—Internet-of-Things; firmware update; blockchain; smart contract

I. INTRODUCTION

The applications of Internet-of-Things (IoT) devices increase drastically along with the rapid development of embedded system and wireless communication technology in the past five years. One of the popular uses of IoT devices is in smart home, in which various equipments or devices in a house (e.g. light bulb, refrigerator, TV, air conditioner) are connected to a gateway and can be controlled without the need to have physical contact with the device. According to Gartner report, 3.9 billion units out-of 6.4 billion units of IoT devices in the market are dominated by consumer application-based devices [1]. The total number of IoT devices circulating in the market is predicted to increase by 219% and reached 20.4 billion units by 2020.

As IoT technology grows to become a massive technology, there are many emerging vulnerabilities and security challenges in IoT environments [2–4]. Miessler and Smith [3] listed several vulnerabilities of IoT environment, such as manipulation in code execution flow of the device, seizure of device’s console access, interference in the update process of device firmware. Considering that IoT device has the capability to connect with other devices and to connect with Internet, it is possible for malicious attacker to exploit one of existing IoT vulnerabilities to affect billion of devices.

The significant growth of IoT devices and its applications could cause various issues for the IoT device manufacturer to manage the distributed IoT devices. This is especially the case during the firmware update process of IoT device. A centralized network model for IoT environment might not be suitable and it could lead to single-point of failure. As the blockchain technology is built upon decentralization concept, it could help to distribute the workload of network traffic during the firmware update process to several blockchain nodes [2], [5], [6]. In addition, one of the principal characteristics of blockchain technology is data transparency, which means all transaction data within the blockchain network is observable by any parties in the blockchain network.

In this paper, a firmware update framework for IoT device based on blockchain technology is proposed. The proposed scheme utilizes smart contract [7] and consensus protocol from blockchain technology to verify the firmware integrity during the update process. A push-based firmware update scheme is adopted in blockchain-based environment for the proposed framework. A device vendor/manufacturer creates a contract for the newly released firmware version and publishes the contract to all nodes in the blockchain network. When a new firmware update contract is published to the blockchain network, it must go through peer verification process through the consensus protocol. Once the contract is verified, the passive node will send a notification of newly added firmware version to IoT gateway. Then, the IoT gateway could forward the information regarding firmware update to the registered IoT devices.

The contributions of our work are as follows:

• A novel design of firmware update framework based on blockchain technology is proposed. There are five entities involved in the proposed firmware update framework, namely: vendor repository, vendor node, passive node, IoT gateway, and IoT device.
• Two process workflow diagrams are designed to support the functionalities of the proposed firmware update framework. These two processes are: the process to create firmware update contract and the process to distribute of firmware update.
This paper is organized as follows. Existing works on firmware update mechanism for IoT and existing blockchain-based firmware update mechanism are explained in Section II. The proposed blockchain-based firmware update framework is explained in Section III. Finally, the concluding remarks is presented in Section IV.

II. LITERATURE REVIEW

A. Firmware Update Mechanism for Internet-of-Things

As the popularity of IoT devices grow, various cyber-attacks targeting the IoT devices and its applications are discovered. Several attack on IoT environment targets on the device firmware as in [4], [8], in which malicious firmware is injected into target device to sabotage the functionalities of the corresponding target device. Malicious attacker is able to exploit the vulnerabilities and remotely control the target device to launch denial-of-service or even violate the privacy of the target device owner.

There are two processes to perform the firmware update mechanisms for IoT devices: manual and automatic updates. In the manual update process, the device owner must initiate the firmware update process manually. In general, this update process is adopted in the traditional firmware update mechanism and preferred by device owner with limited network bandwidth or limited network connectivity. However, the manual firmware update mechanism is not efficient since the device owner must do all the manual operations and it is more time consuming. In addition, there is a high chance that human error could happen during the firmware update process. Compared to the manual update process, the automatic update process looks more enticing to be adopted nowadays. As the manufacturer of IoT device could initiate the firmware update process without the active participation from the device owner.

The current automatic firmware update process uses client-server architecture, in which the vendor’s repository is the server side and the IoT device becomes the client side. In general, there are two ways to deliver the firmware from the server to the client: PUSH and PULL methods[9]. The differences between these two methods lie in the initiator of the firmware update process. In the PUSH method, the device vendor initiates the firmware update process by distributing the firmware binary to the IoT device management (gateway). In contrast, the IoT device initiates the firmware update process by sending download firmware binary request to the server of device vendor in the PULL method.

B. Blockchain-based Firmware Update Mechanism

Lee and Lee in [10] proposed a blockchain-based firmware verification and firmware update schemes for embedded devices in IoT environment. In the scheme of Lee and Lee, the blockchain technology is utilized in their proposed firmware update framework to verify the firmware version, verify the authenticity of the firmware, and distribute the firmware binary to the connected nodes in the blockchain network. Each embedded device is designed as one node in the blockchain network. As each embedded device represents each node in the blockchain network, this means that each embedded device needs to store a copy of blockchain ledger in its local storage. As the embedded devices are resource constraints device, the scheme proposed by Lee and Lee might be difficult to be implemented in the real world IoT environment. In addition, there are various kinds of on-the-shelf embedded devices that require different firmware. In this case, a request node might
take longer time to wait for a response. Therefore, the firmware update framework proposed by Lee and Lee does not suitable for heterogeneous IoT ecosystem.

Boudguiga et al. in [11] proposed the application of blockchain technology to update the firmware of IoT devices from different vendors. In the firmware update framework of Boudguiga et al., each IoT device must periodically poll any random node in the blockchain network in order to check the firmware version. When a device vendor publishes a new version of firmware update to the blockchain network, the newly created firmware update needs to be verified first by nodes in the blockchain network through consensus protocol. When one of IoT devices from the associated device vendor wants to perform the firmware update process, the device must create a transaction of firmware update request. In this scheme, the IoT devices would not be able to download the firmware binary from its corresponding vendor unless the nodes in the blockchain network have verified the associated firmware. In addition, all nodes in the blockchain network in the proposed framework of Boudguiga et al. must store all the firmware binaries that have ever published in the blockchain network.

III. PROPOSED FRAMEWORK DESIGN

In this paper, a blockchain-based firmware update framework is proposed. In the proposed firmware update framework, PUSH-based firmware update method is selected to distribute the new version of firmware binary from the repository of device manufacturer to the IoT device. In the proposed framework, the device vendor distributes a new version of firmware by pushing the information related with the corresponding firmware to the blockchain network. Fig. 1 shows the proposed architecture of blockchain-based firmware update framework.

There are five entities in the proposed firmware update framework listed as follows:

- **Vendor repository**: a firmware repository owned by device vendor to store the firmware binaries and provides firmware information.
- **Vendor node**: a node in blockchain network owned by device manufacturer. Vendor node creates and distributes the firmware update contract to the other nodes in the blockchain network. In addition, vendor node acts as miner and actively verifies all transaction in the blockchain network.
- **Passive node**: a node owned by broker or service provider that connecting IoT gateways to the blockchain network. Passive nodes receive and could execute the firmware update contract from vendor node. Each passive node is connected with zero to many IoT gateways.
- **IoT gateway**: a gateway for IoT device such as a Wi-Fi router in smart home environment. IoT gateway stores information of the registered IoT devices, such as device manufacturer, device model, and the installed firmware version. Each gateway is identified by a public address (or wallet address) in a passive node (wallet container).

![Fig. 2. The process flow for creating a new firmware update contract.](image-url)
• IoT device: sensors or embedded devices.

A. Assumptions

Assumptions for the proposed protocol are listed as follows:

1. Each device vendor has at least one vendor node in the blockchain network and one vendor repository to store the firmware binaries and the corresponding information.
2. Vendor repository is connected with vendor node through a secure channel.
3. Passive node does not participate in the mining process and only needs to synchronize the data stored in the node’s local ledger with the data from public ledger data.
4. Each IoT device is connected to IoT gateway through a secure channel.

B. Proposed Framework

The proposed firmware update framework is designed based on Ethereum blockchain platform. The proposed framework consists of two processes: the process to create firmware update contract and the process to distribute the firmware binary file. The firmware verification process utilizes the verification mechanism of blockchain network (i.e. Proof-of-Work) in order to verify the firmware update contract and to verify the integrity of firmware binary file.

The firmware update contract creation process is shown in Fig. 2 and explained as follows:

1. Device vendor develops a new firmware for a specific device and stores the firmware binary and the information associated with the new firmware version into the vendor repository. Once the new firmware update information has been stored in the vendor repository, the vendor issues a firmware update contract creation to the vendor node.
2. The vendor node creates a new firmware update contract and records the new firmware information inside the newly created contract. Afterward, the vendor node deploys the newly created firmware update contract to the blockchain network for the verification process.
3. All the other vendor nodes (the miner nodes) in the blockchain network verify and validate the newly created firmware update contract. After the verification of new firmware update contract has finished, the miner nodes update the validation status of the newly created contract and notify all the other nodes regarding the verification result.
4. The miner nodes collect all firmware update contracts that have been verified and store it into the blockchain’s ledger.

After a firmware update contract is stored in the blockchain’s ledger, the distribution of firmware binary based on the corresponding contract can be executed. The system flow for the distribution process of firmware binary is shown in Fig. 3 and explained as follows:

1. After a new firmware update contract is verified and recorded in the blockchain, the passive node could send a notification about the newly released firmware
update to all IoT gateways managed by the corresponding passive node.

2. The IoT gateway checks the information regarding the newly released firmware update with the information of all IoT devices managed by the corresponding gateway. If the gateway finds any IoT device that matched with the requirement of the firmware update from the received contract, then the gateway will send a request to the associated passive node for detailed information to download the firmware’s binary file.

3. The passive node receives the firmware update request from the gateway. Next, the passive node checks the requirements on the firmware update contract that matched with the received firmware update request. If the requirements are satisfied, the passive node sends the URI of the requested firmware binary to the requesting IoT gateway.

4. After the IoT gateway receives the URI of the requested firmware binary, the gateway sends a request to the vendor repository to download the requested firmware binary.

5. The vendor repository receives the request sent by the corresponding IoT gateway. Afterwards, the vendor repository sends the requested binary file to the requesting IoT gateway.

6. After the IoT gateway has finished downloading the binary file of a firmware, the gateway forwards the firmware binary file to the associated IoT device.

IV. CONCLUSION

As the applications of IoT devices grow significantly, the device manufacturer faced various problems related with the management of the distributed IoT devices. One of the problems faced by the device vendor is the distribution of new version of firmware for the manufactured devices. In the past, a centralized network architecture model is used for distributing the firmware of IoT device. However, the centralized network architecture might not suitable anymore considering the rapid growth of IoT devices application.

In this paper, a blockchain-based firmware update framework for IoT device is proposed. The proposed framework utilizes blockchain technology in order to securely verify the firmware version and to verify the integrity of the distributed firmware binary during the update process. A push-based firmware update scheme is adopted in the proposed framework.

In addition, the proposed firmware update framework consists of two main processes. The first main process is the creation of firmware update contract. In the first process, each vendor is required to create a firmware update contract for each firmware released, and the contract must be deployed to the blockchain network for verification process. Next, the Peer nodes in the blockchain network verify the newly deployed firmware update contract through consensus protocol. The second main process is the distribution of firmware binary to end devices. In this process, secure verification mechanisms is applied to securely distribute the firmware binary from the repository of device manufacturer to the requesting IoT device.

ACKNOWLEDGMENT

The authors gratefully acknowledge the support from TWISC and Ministry of Science and Technology, Taiwan, under the Grant Numbers MOST 105-2221-E-011-080-MY3, MOST 106-3114-E-011-003, and MOST 106-2218-E-011-003.

REFERENCES