

Design and Implementation of a Fingerprint-based Removable Storage Authentication System Using Particle Photon

Joongjin Kook^{1*}

¹Assistnat Professor, School of Information Security Engineering, Sangmyung University, Korea.

*Corresponding Author
ORCID: 0000-0002-0033-388X

Abstract

In this paper, we designed a fingerprint recognition-based portable storage authentication system that can be used in the IoT environments and implemented a prototype to verify its functions. In particular, we used an IoT platform that can support this by focusing on actual productization and mass production, and implemented functions such as registration, recognition, encryption and transmission of fingerprints by combining modules for fingerprint recognition. In addition, an authentication server was configured in order to support IoT-based remote authentication, enabling to store encrypted fingerprint data into the server and issue tokens to authenticated users, which in turn authentication is achieved.

Keywords: Fingerprint, Photon, Fingerprint Authentication, IoT, Embedded System

I. INTRODUCTION

With the development of ICT technology, technology in the security sector has also been rapidly developed. Beyond the physical security, they are evolving into the security using the software and into the personalized security which is simple and free of risk of loss by using users' biometric information. Biometric authentication technology refers to the informatization of the unique physical or behavioral characteristics of each individual. Physical characteristics include gait, intonation, handwriting, and signature [1][2].

In this paper, we studied the structural design of the fingerprint recognition-based portable storage authentication system for strengthening the security of portable storage media, based on fingerprint recognition which is the most widely used in the mobile field among biometrics. Also, we studied implementation methods of its prototypes. In particular, it is expected to contribute to the development of the fingerprint recognition system considering the IoT environments by providing a server/ client structure for not only offline authentication for but also web-based remote authentication.

In this paper, Particle's Photon was used as a platform for the development of fingerprint recognition-based portable storage authentication system, and ADH Technology's GT-511C3 was used as a sensor module for fingerprint recognition. The system consists of the Fingerprint Processing module, which is responsible for the functions of fingerprint registration, input,

encryption, transmission and authentication, and the Authentication Server for remote authentication. The authentication method can be used in various ways by providing both standalone- typed offline authentication and an authentication server-used online authentication functions at the same time.

II. RELATED WORK

Biometric-based authentication technologies have rapidly developed due to the advances in hardware technologies such as SoC, Sensor and MEMS, and the improvements in accuracy/recognition using Deep Learning technology. Fingerprint recognition, in particular, was applied to Apple's iPhone 5S in 2013 first time, and then has been used as a means for user authentication on mobile devices, and has been widely applied to various devices such as digital door locks and vaults. In particular, the fingerprint recognition based biometric was overwhelmingly high at 48%, when looking at the application rate by each biometric technology of 121 global banks in 2014 [3].

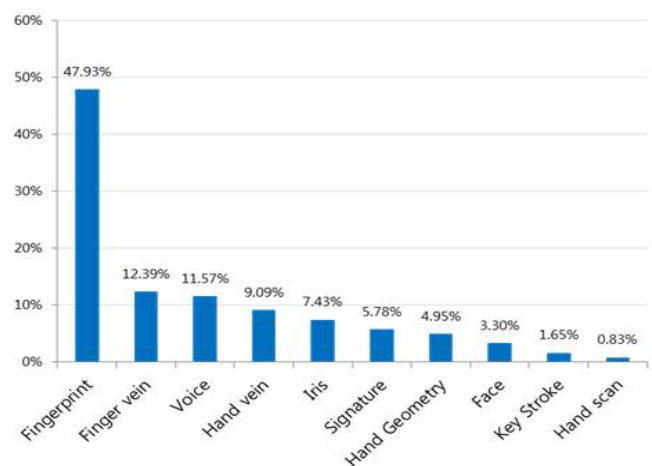


Fig. 1. the application rate by each biometric technology (total 121 Banks)

Fingerprint-based user authentication system has been used in various fields, and the research on the development of a prototype of a medical registration system using Arduino to

reduce patients' waiting time in hospital was also conducted [4]. But the additional module configuration is required for wireless communication because Arduino was used in this research, and MCU's processing capabilities also had a limitation of having a performance as low as about 16MHz because Arduino is mainly used for the purpose of a simple controller.

FingerScanner is a fingerprint scanner system developed using Raspberry Pi, evaluating the usage of CPU and memory required for fingerprint registration and recognition in Raspberry pie, and the accuracy of fingerprint recognition, etc. In addition, it implements the HTTP-based CRUD method to provide Web services [5]. Raspberry Pi is a small computer using the Raspbian operating system to perform general-purpose functions. Therefore, it takes a considerable amount of time for applications for fingerprint recognition and authentication to be executed during reset or power on. This may make application difficult considering various devices which use fingerprint recognition-based authentication, and it is also difficult to supply the Raspberry Pi's BCM283X SoC modules especially when considering productization and mass production.

In this paper, Particle's Photon, which can be used for IoT-oriented devices, was used to overcome these problems. Photon is composed of ARM Cortex M3 processor and WiFi module, which is good for processing the fingerprint data. Also, its application is configured with firmware, so the booting time required for reset or power-on is extremely short, making the execution of the application for fingerprint recognition and recognition possible immediately after startup. Because its board is smaller in size and lower in price than Raspberry pie and it is an open hardware platform provided in a module type, it is also easier to productize and mass-produce. Table 1 shows the comparison of the specifications between Raspberry pie and Photon.

Table 1. The Comparison of Raspberry Pi and Photon

	Raspberry Pi	Photon
Processor	Broadcomm BCM283X ARM Cortex A53 Quad-core @ 1.2GHz	STM STM32F205RGY6 ARM Cortex M3 Single-core @ 120MHz
Memory	1GB	128KB
Storage	Micro SD	Flash 1MB
OS	Raspbian(Linux)	None(Firmware)
Dimension (inch)	3.37 X 2.22	1.44 X 0.27
Cost (US \$)	35(Evaluation Kit)	20(Evaluation Kit) 12(Module)
Comm.	WiFi, BT	WiFi
Production	Impossible	Possible

III. PROPOSED SYSTEM

The fingerprint recognition-based portable storage authentication system proposed in this paper consists of a fingerprint scanner for fingerprint input, a USB storage device for data storage, and a processing module for processing fingerprint inputs and recognition. And an authentication server is additionally composed to support remote authentication. Fig 2 shows the schematic of this system.

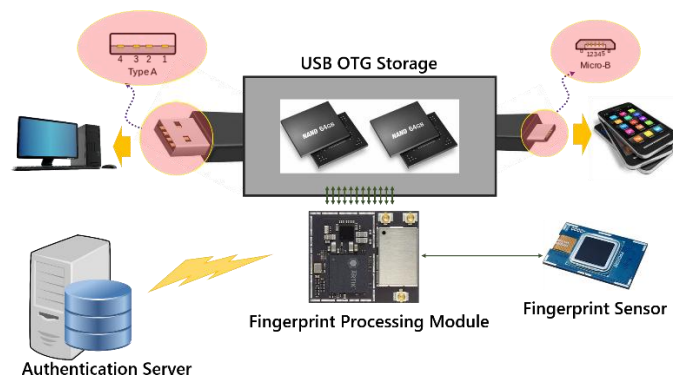



Fig. 2. Fingerprint-based USB mass storage system diagram

III.I Fingerprint Processing Module

The Fingerprint Processing module for processing the registration, recognition, encryption and transmission of fingerprints consists of a fingerprint scanner for fingerprint input and a SoC module for data processing.

ADH Technology's GT-511C3 is used as a fingerprint scanner, and GT-511C3 is capable of high-precision fingerprint recognition using the SmackFinger 3.0 algorithm [6]. The GT-511C3 supports the UART interface for communication with SoC modules and can store up to 200 fingerprint data in internal ROMs.



Item	Value
CPU	ARM Cortex M3 Core
Sensor	optical Sensor
Effective area of the Sensor	14 x 12.5(mm)
Image Size	202 x 258 Pixels
Resolution	450 dpi
The maximum number of fingerprints	200 fingerprints
Matching Mode	1:1, 1:N
The size of template	496 Bytes (template) + 2 Bytes (checksum)
Communication interface	UART, default baud rate = 9600bps after power on USB Ver1.1, Full speed
False Acceptance Rate (FAR)	< 0.001%
False Rejection Rate(FRR)	< 0.1%
Enrollment time	< 3 sec (3 fingerprints)
Identification time	< 1.0 sec (200 fingerprints)
Operating voltage	DC 3.3~6V
Operating current	< 130mA

Fig. 3. GT-511C3 Fingerprint scanner module and specifications

In order to perform the registration, deletion and comparison functions of a fingerprint through a fingerprint scanner, commands must be input from the SoC module via the GT-511C3's UART. In addition, related functions and applications should be implemented in SoC modules in order to perform authentication through the input fingerprint data and to perform processing functions to activate or inactivate the use of USB

storage devices depending on the authentication result. Particle's Photon supports WiFi as SoC module for IoT device development and is used as the SoC module. Photon is a low-cost and light-weight module consisting of STM32 SoC based on ARM Cortex M3.



Fig. 4. Particle Photon, Evaluation kit and SoC module

Photon provides compatibility with Arduino, allowing the development of application using most Arduino libraries, and it consists of single task-based firmware, allowing the quick execution of the application on reset. Fig 4 shows Photon devices in the form of evaluation kits, SoC module with antenna, and SoC module without antenna. Photon is an open hardware platform and can be used for productization and mass production because modules are provided.

Fig 5 shows the schematic of the hardware configuration that combines GT-511C3 and Photon.

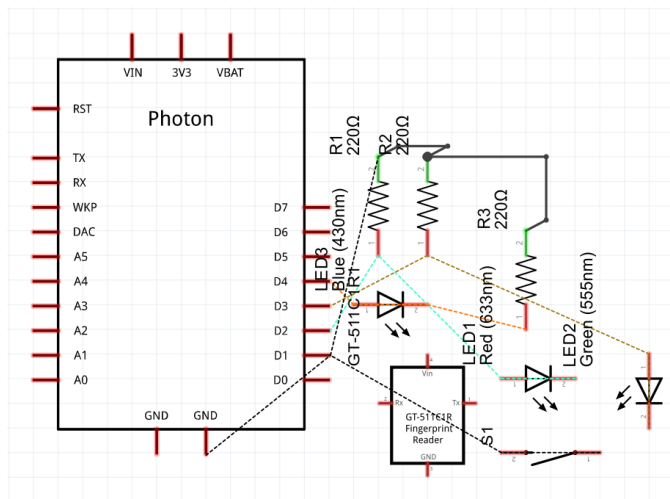


Fig. 5. Fingerprint scanner system schematic

In Fig 4, the command to the fingerprint scanner is input through the input of the S1 key. If the key is kept pressed for 3 seconds, it is activated for the fingerprint recognition mode, allowing the user to receive the fingerprint. If you press and held the key for 5 seconds, it operates in a mode that allows you to receive a new fingerprint. LEDs are configured to indicate success/failure when a new fingerprint is registered or input for user authentication, and LEDs of different colors blink depending on the event type, enabling users to check the status of the authentication procedures.

III.II Mass Storage

The final product should be a single PCB integrated with SoC module, fingerprint scanner, USB mass storage device, and input/output device. However, this paper's purpose is the implementation of the prototype, so the SoC module and the power point of USB storage are relayed and its power is controlled, enabling to activate/inactivate processing of USB storage. Therefore, if the already registered fingerprint matches a newly input fingerprint, the SoC module sends a control command to activate the USB storage device. Fig 5 shows the prototype of a fingerprint recognition-based USB storage device.

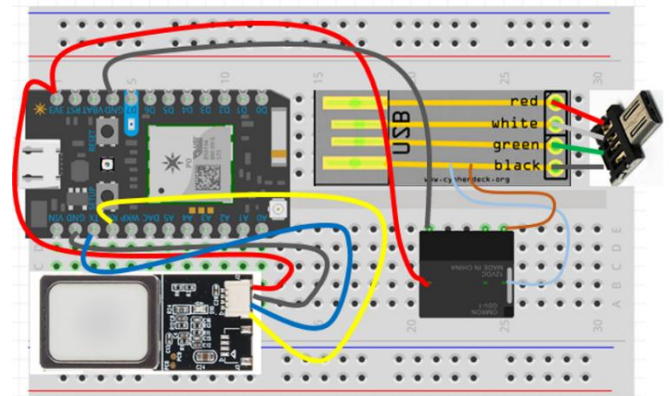


Fig. 6. Prototype of Fingerprint scanner with USB Mass Storage

III.III Authentication Mode

The fingerprint recognition-based USB storage device proposed in this paper is designed to support not only offline but also online authentication. The mode is through the setting of SW uploaded to Photon. In the case of offline, the authentication is performed by comparing with the user's fingerprint previously stored in the GT-511C3 module. In contrast, in the case of online, fingerprints input through the fingerprint scanner are encrypted with AES and transmitted to the server for authentication. Fig 7 and Fig 8 show the conceptual diagram of the two authentication methods.

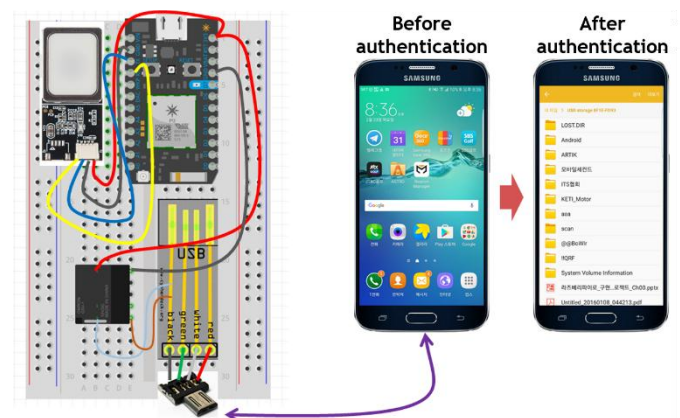


Fig. 7. Offline authentication progress

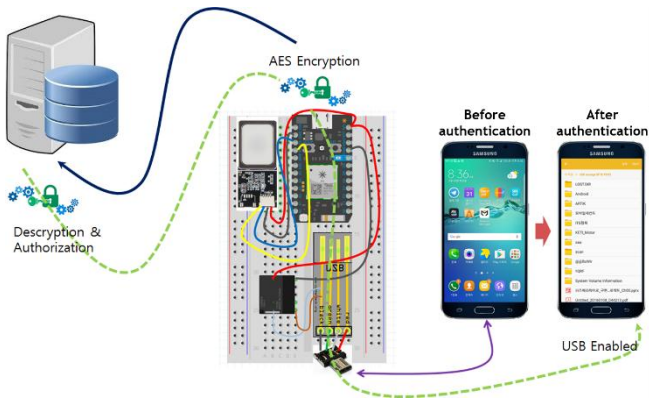


Fig. 8. Online authentication progress

As for offline authentication, as shown in the flowchart in Fig 9, the fingerprint recognition module is activated and waits for input of the command. At this time, the input command is fingerprint recognition or fingerprint registration. It operates in fingerprint recognition mode if input is maintained for 3 seconds using the key of Fig 4, and it operates in fingerprint registration mode and if input is maintained for 5 seconds. In the fingerprint recognition mode, the storage device is activated if the user's input fingerprint is a registered user's fingerprint. If the fingerprint registration mode is requested, a procedure for fingerprint registration of a new user is performed.

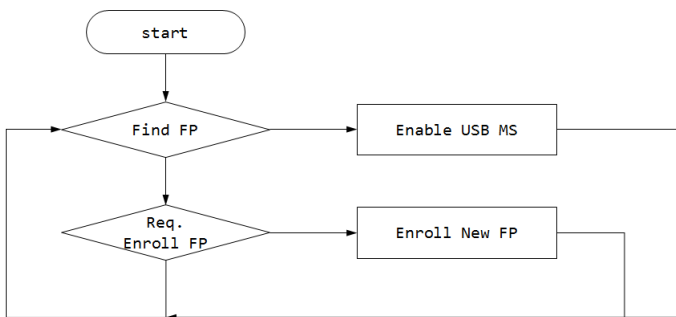


Fig. 9. Prototype of Fingerprint scanner with USB Mass Storage

Fig 10 is a flowchart that shows the online authentication process. Unlike offline authentication, the online authentication process encrypts the input fingerprint to the AES and transmits it to the authentication server. The Authentication server compares it to the registered user and issues a token if there is a match. Even for the request for fingerprint registration, the newly input fingerprint data is encrypted and transmitted to the authentication server, and the server registers the user's data.

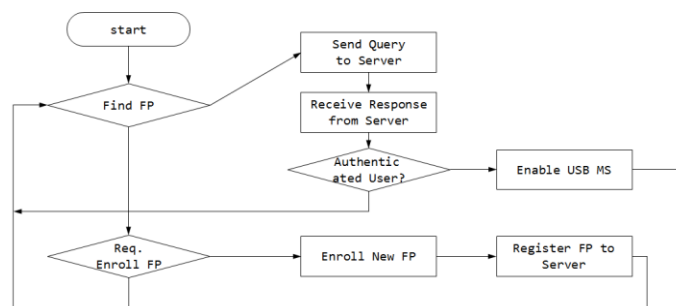


Fig. 10. Prototype of Fingerprint scanner with USB Mass Storage

In order to send encrypted fingerprint data to the authentication server, APIs are configured as shown in Table 2. This API consists of functions for key setup, encryption, and decryption. The APIs for AES-based encryption/decryption are as follows in Table 2.

Table 2. AES Functions

AES Functions
byte set_key (byte key[], int keylen)
void clean ()
void copy_n_bytes (byte * dest, byte * src, byte n)
byte encrypt (byte plain [N_BLOCK], byte cipher [N_BLOCK])
byte cbc_encrypt (byte * plain, byte * cipher, int n_block, byte iv [N_BLOCK])
byte decrypt (byte cipher [N_BLOCK], byte plain [N_BLOCK])
byte cbc_decrypt (byte * cipher, byte * plain, int n_block, byte iv [N_BLOCK])

III.III Authentication Server

When online authentication is performed, the fingerprint data input through the fingerprint scanner is encrypted with AES by the Fingerprint Processing module and transmitted to the authentication server. The authentication server can register it into the server in case of the data of a new user. If the user is already registered, the user authentication is performed by searching through the database and the authentication result is sent back to the Fingerprint Processing module. Fig 11 shows the authentication procedure of the authentication server.



Fig. 11. Prototype of Fingerprint scanner with USB Mass Storage

IV. EVALUATIONS AND RESULTS

The prototype implemented to test fingerprint recognition-based USB storage devices is as shown in Fig 12.

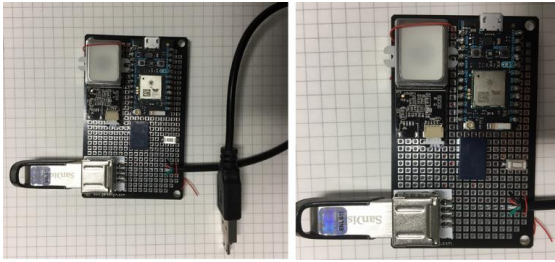


Fig. 12. Prototype of Fingerprint scanner with USB Mass Storage

When the power is on, the SoC module activates the fingerprint scanner and waits for the command to be input through key input. If the key input is kept for 5 seconds, it operates in fingerprint registration mode. At this time, the GT-511C3 module turns on its internal LED to display its status. Input of new fingerprints are performed through the procedures shown in Fig 13.

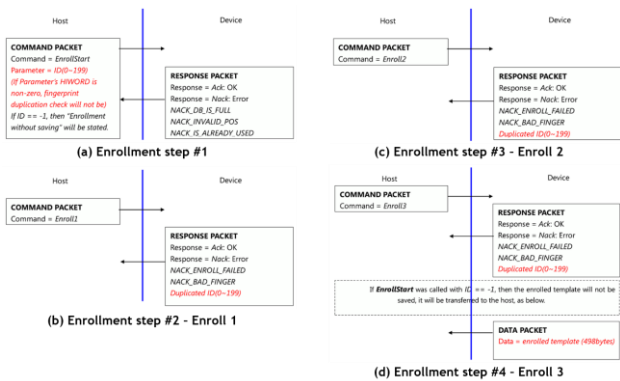


Fig. 13. Fingerprint enrollment process

GT-511C3 receives commands for registration request as shown in Fig 13, gets inputs of the user's fingerprints three times, goes through the verification and registers it.

Once a fingerprint is registered, an authentication mode is available from now on. For the execution of the authentication mode, keep the key input for 3 seconds. When the LED on the fingerprint scanner turns on, touch your finger to input the fingerprint, and GT-511C3 check whether the input fingerprint matches the fingerprint of the registered user and returns the user's ID if there is a matching fingerprint. The procedure for fingerprint recognition is as shown in Fig 14.

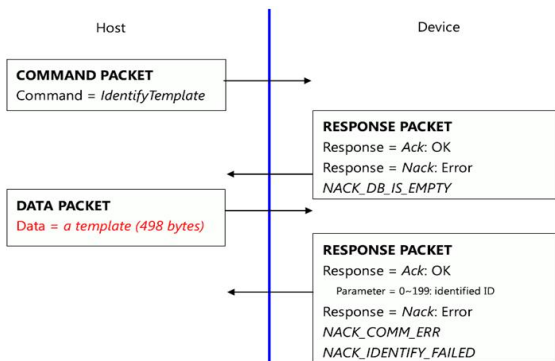


Fig. 14. 1:N fingerprint verification

The authentication server for online authentication is implemented using python and Crypto module is used to decrypt fingerprint data received from the fingerprint processing module.

The registration and recognition of fingerprints are performed normally in both online and offline modes. In the case of online mode, some delay occurs depending on the network conditions. When fingerprint authentication is performed with the system of Fig 12 connected to a smartphone, it can be automatically connected to an app that can check the directory of a USB storage device, as shown in Fig 15, checking the normal recognition.

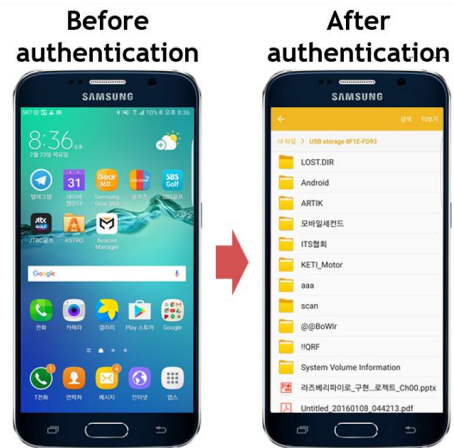


Fig. 15. Automatic Connection of Mass Storage when Fingerprint Recognition

VI. CONCLUSION

In this paper, we studied the design and implementation methods of fingerprint recognition-based portable storage authentication system for IoT and implemented the prototype to verify its functions. In particular, we selected IoT platforms that can support them by focusing on actual productization and mass production, and implemented functions such as registration, recognition, encryption and transmission of fingerprints by combining with a module for fingerprint recognition. For independent operation, a user interface was implemented by configuring keys and LEDs, and key input time was set differently to enable to request for different functions with one key. LEDs were able to display the status of the system (fingerprint registration mode, fingerprint recognition mode, authentication success/failure, etc) In order to support remote authentication, the authentication server was configured to store encrypted fingerprint data on the server and issue tokens to the authorized user.

It is expected that the system in this paper is the reference to the organization of the devices and the software configuration necessary for the development of low-cost fingerprint recognition-based systems, and is used for the development of various products.

REFERENCES

- [1] Younseok, O., 2019, "Growth and Insight of the Biometrics Market," Korea Information Society Development Institute, 31(3), pp. 22-31.
- [2] Hyungyu, L., and Yongkee L., 2018, "Biomatrix Technology Trends Using Physical Characteristics, Commercializations Promotion Agency for R&D Outcomes, 63.
- [3] BIKorea, <http://www.bikorea.net/news/articleView.html?idxno=9326>
- [4] Jonghyun, B., and Donghoon, L., 2018, "A study on Clinic Registration System Using Fingerprint Recognition," Rehabilitation Engineering & Assistive Technology Society of Korea, 12(3), pp. 205-211.
- [5] Jordi Sapes, Francesc Solsona, FingerScanner: Embedding a Fingerprint Scanner in a Raspberry Pi, MDPI Sensors, Vol. 62, No. 2, Feb, 2016, pp.
- [6] Fingerprint algorithms, https://biometrics.mauguet.org/types/fingerprint/fingerprint_algo.htm