sciendo INTERNATIONAL JOURNAL ON SMART SENSING AND INTELLIGENT SYSTEMS

Article | DOI: 10.2478/ijssis-2023-0004 Issue 1 | Vol. 16 (2023)

Biometric authentication sensor with an encryption module for prevention of h/w hacking in digital custody services

Soojun Lee[1,*], Hyeopgoo Yeo[2,*], Mingoo Kang[3,*]

[1]Graduate School of Business, Sejong University, Seoul, South Korea

[2]Division of Software Convergence, Hanshin University, Osan-Si, Gyeonggi-Do, South Korea

[3]Department of IT Contents, Hanshin University, Gyeonggi South Korea

*E-mail: soojunlee@sejong.ac.kr; hgyeo@hs.ac.kr; kangmg@hs.ac.kr

This paper was edited by Subhas Chandra Mukhopadhyay.

Received for publication: November 1, 2022.

Abstract

In this paper, a digital personal safe system was proposed with Fast ID Online (FIDO) transaction authentication and multiple decentralized ID (DID) personal authentications based on a home gateway. This individual custody model of personal multiple authentications will be linked to the transaction authentication of digital assets stored in the storage space of the home gateway by the DID of smart devices and the FIDO server for a public platform that excludes digital asset (cryptocurrency [e.g., Bitcoin] or NFT asset) management based on individual private keys and user interaction (user interface and user experience [UI/UX]) at home. To strengthen the security of the proposed digital custody model, it was proposed to apply a local device to which a biometric sensor equipped with an encryption module that can fundamentally block the hacking of biometric information is applied. It is implemented with Verilog for an embedded fingerprint sensor block and decryption program implemented with C.

Keywords

Digital custody model, home gateway, FIDO, DID, biometric security, embedded encryption LEA.

I. Introduction

Recently, blockchain-based decentralized ID (DID), which has built-in digital identity authentication and mobile identity, has been used as a security means in various fields. In addition to identification verification such as resident registration cards, passports, and driver's licenses, digital IDs can be used for personal identification using distributed IDs based on biometrics [1].

A digital custody model was used in digital asset custody services (DACS). This digital asset management solution was combined for the highest levels of certified home security for safeguarding multiple asset classes with a home gateway [1]. In particular, the terminal and transaction authentication of digital custom services are required with smart devices for personal assets at home.

Recently, custody service has meant protection and management work in financial transactions.

Consignment work refers to the entrustment of digital asset (cryptocurrency [e.g., Bitcoin] or NFT asset) management to another person. A set-top box is a node of a blockchain and can be used as a biometric receiving device for personal identification. Because set-top boxes are fixed and do not move like mobile devices, they are very suitable as devices for storing personal digital assets.

This paper proposes a Fast ID Online (FIDO) transaction and multiple DID personal authentication of individual safes with a home gateway to separate and store the digital assets of multiple people. This is a

Open Access. Published by Sciendo. CC BY-NC-ND
© 2023 Lee et al. This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivs 4.0 License https://creativecommons.org/licenses/by-nc-nd/4.0/

digital custody model that can safely hold digital assets by sharing a DID distributed ledger with members and setting a distributed ID by a set-top box, a digital safe device, with blockchain processing of digital assets.

Additionally, the proposed digital custody model provides enhanced security through encryption of biometric devices in preparation for possible hardware hacking.

II. Related work

a. Digital custody services

The basic compliance of the custody service system by the U.S. Securities and Exchange Commission (SEC) is as follows. The SEC custody rule requires an adviser that has custody of client assets to maintain those assets with a "qualified custodian" such as a bank, broker-dealer, or futures commission merchant, and to have a reasonable basis for believing that the custodian sends quarterly account statements directly to the clients [2, 3].

Within the context of traditional capital markets, custodians provide clients with an array of financial services including settlement, exchange, clearing, and transaction execution. However, one of their most important roles is the safekeeping of investors' assets. Custodians are responsible for holding and maintaining securely investors' assets in both electronic and physical form.

Recently, as the digital asset market continues to grow, there is an ever-increasing volume of digital assets flowing through the financial system. Individuals and institutions therefore begin to accumulate digital assets that exhibit significant value, and safeguarding of these virtual assets begins to take on greater priority. Digital asset custody also provides services such as exchanging, clearing, settlement, and safekeeping of virtual assets in the same context as financial assets. The importance of a digital assets custody service is beginning to increase because the nature of digital assets characterizes them with a greater vulnerability compared with traditional assets. Digital assets can have security vulnerabilities in services or payments that trade, digital wallets that are implemented, and computer devices, and they are actually exposed to hacking risk [7].

b. Structure of FIDO authentication

Figure 1 shows in detail biometric authentication process by FIDO including fingerprint registration process and fingerprint login process. The FIDO Universal Authentication Framework (UAF) is a standard for users to allow authentication methods such as biometrics or PINs without a password in mobile apps such as Android and iOS, which are currently

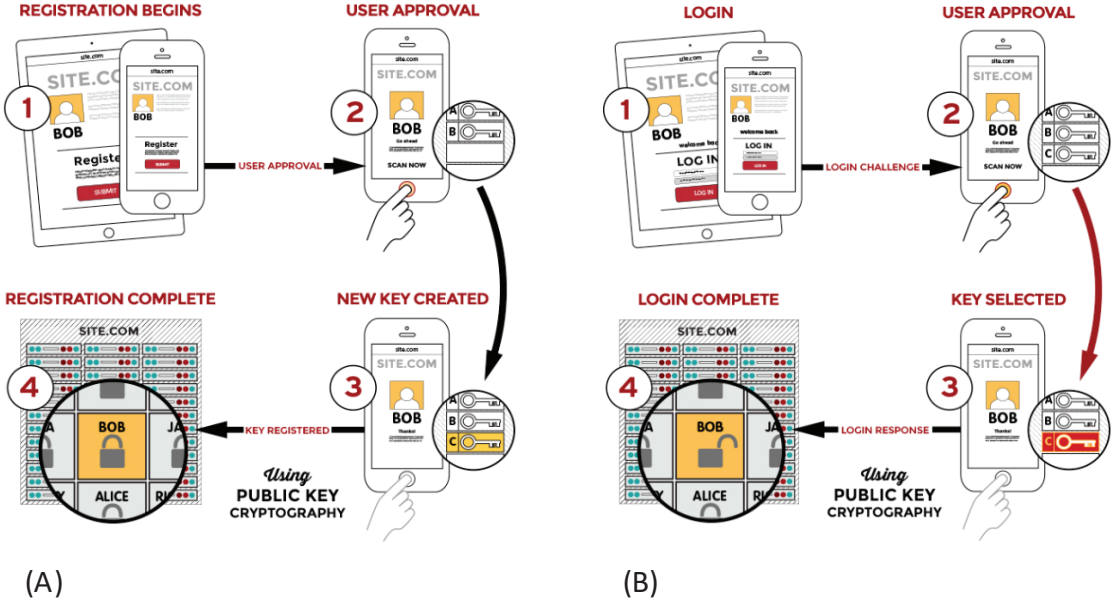


Figure 1: Biometric authentication process by FIDO: (A) Fingerprint registration process. (B) Fingerprint login process [4]. FIDO, Fast ID Online.

limited to mobile apps. FIDO U2F is a standard that allows additional authentication using hardware that includes an authentication key after authenticating once with an ID and password to enhance security. It is primarily intended for use by specific users or internal employees who require a high level of security [4].

FIDO2 is an improved standard that integrates these two standards and can be used anywhere, including the web, as well as the existing mobile environment. It consists of two standards: web authentication for web browsers and client to authenticator protocol (CTAP) for authenticators. Currently, various web browsers support the web authentication API [5, 6]. The user can authenticate more conveniently and safely because the client authentication service can be performed in various environments more easily by using the API provided by the web browser. Also, because the CTAP2 standard supports backward compatibility, the existing authentication method using hardware that includes an authentication key can be used as it is in the case of U2F [4].

In particular, FIDO transactions and multiple DID authentication can be used for a digital personal safe that stores digital assets separately, as described in Section 3.

III. Digital asset and custody model

a. Digital asset

A digital wallet of digital assets is a tool for storing, managing, and using digital currency. Digital wallets can be divided into software wallets and hardware wallets according to their form. Additionally, they can be divided into hot and cold wallets according to whether the storage of the private key and the execution of the signature is offline or online as well as based on the question of whether an active Internet connection needs to be used [7]. A cold wallet is a type of digital wallet that can store a private key (private key) that can prove ownership of cryptocurrency. Cold wallets are known for their relatively high security and are convenient because they can store various digital assets in one place [8]. According to the method by storing and executing the private key, it can be divided into a wallet based on a blockchain and a centralized wallet. Mostly centralized wallets are used [10].

Cold wallets can be also referred to as hardware wallets because they are not connected to the Internet and usually take the form of hardware such as a USB or card [1]. It is recommended that digital assets should be stored in cold wallets for security. The cold wallet transaction procedure is briefly as follows. After creating a transaction history offline, signing a private key, and entering a generated transaction online, the cold wallet transaction is completed. Therefore, a hardware wallet has a low risk of being exposed to hacking and phishing crimes. There is no need to worry if your hard wallet is lost or stolen, as each hardware wallet has a 24-word recovery phrase. Without a hardware wallet, it is possible to prove ownership of digital assets with only a recovery code. Of course, the recovery code must be kept safe and must not be exposed to others. If the private key of a digital asset stored in a hot wallet connected to the Internet is hacked, a hacking incident may occur. A cold wallet is less likely to be hacked, but the transaction speed is slow. In general, digital wallets come in many forms, and the security risks they are exposed to also vary [8].

The key file private key/mnemonic phrase of the encrypted digital wallet is stored in a terminal device such as a PC or mobile device, and the security risk becomes very high if the terminal device is not secure. Security problems in the terminal operating environment mainly include software viruses, and vulnerabilities in the operating system and hardware. Therefore, a secure digital wallet should be designed to prevent the possibility of theft of the private key/mnemonic due to the operating environment and also have the ability to resist man-in-the-middle attacks. Due to the security risk of the file storage method, the private key/mnemonic phrase file storage directory access right, storage format, and encryption algorithm must be carefully designed. It is necessary to prevent falsifying in the application installation package, and the development process security design during application operation must also be strengthened due to the security risk of the application itself [8].

In terms of convenience, it is used in the order of virtual asset exchange, hot wallet, and cold wallet. But in terms of security, it is used in the opposite order. Many financial institutions provide custody service for customers' digital assets (Bitcoin, NFT, etc.).

b. Proposal of digital custody services

Digital assets are extremely different from traditional assets, particularly physical assets, in terms of appropriate security measures. While a traditional asset such as cash or stocks may be held by a qualified custodian in a safe or lockbox, a digital custodian safeguards digital assets by ensuring that investors' private keys are maintained securely. Digital custody

services for storing digital assets can use virtual asset exchanges and blockchain wallets.

This paper proposes a digital custody method and its service method by combining the advantages of a digital asset storage method using a digital wallet and an authentication method using DID, and a method to further strengthen authentication security [1]. Digital assets (e.g., cryptocurrency, NFT assets) will be stored and displayed with a home gateway (like a set-top box) for personal digital custody at home [1, 21]. Access to the digital assets in digital custody from the home gateway is possible with FIDO authentication, and access from the outside through the Internet is set to enable FIDO authentication only from devices registered in advance.

Figure 2 shows the conceptual proposed custody model using a set-top box as a home gateway. The set-top box can be used as a storage device for digital assets, as well as a server for FIDO transactions. It includes the authentication module for FIDO transaction authentication. The DIDs are identified by authentication such as digital signatures or biometric information in the FIDO authentication server in the process of connecting the user terminal to biometric authentication and transaction processing, which will be discussed in more detail in the next section.

Additionally, it is equipped with a blockchain-based DID server function so that it can be used as a home gateway for personal authentication. The storage of the home gateway is installed in an individual space, and personal digital assets can be stored according to FIDO biometric authentication in a local space. Individual private keys are managed with DID personal authentication. Therefore, access to digital assets stored digitally at the home gateway (custody) is possible through FIDO authentication, and external access via the Internet is set to enable FIDO authentication only from devices registered in advance. This makes it difficult to access from the outside and provides a storage method that has the function of a cold wallet and, unlike mobile devices, does not involve the risk of becoming lost.

In addition to IPTV service, the home gateway can provide services by adding functions such as digital asset storage, FIDO authentication, DID authentication, and metaverse connection. Therefore, the home gateway that stores digital assets can allow another digital backup in case of failure or loss.

IV. Implementation of custody model

a. Implementation of digital custody

Figure 3 shows in detail the proposed custody model based on a home gateway set-top box as a storage device for digital assets. Web authentication provides

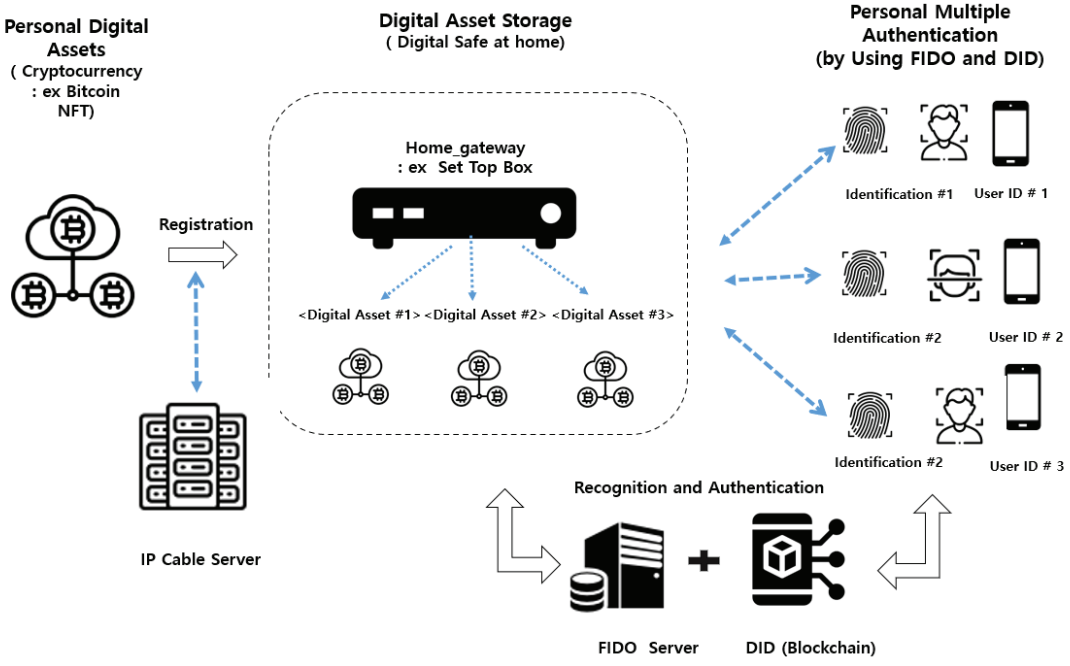
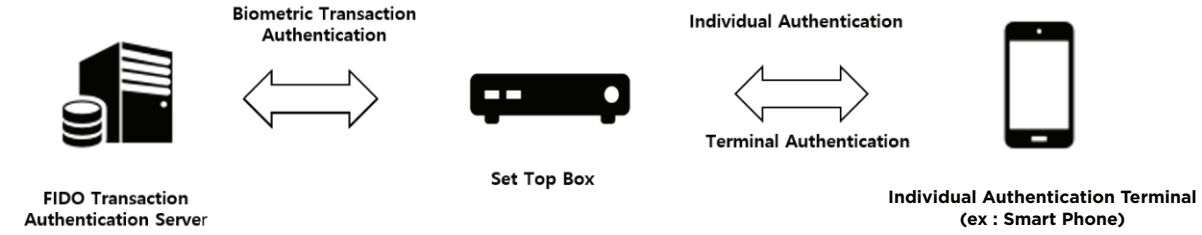
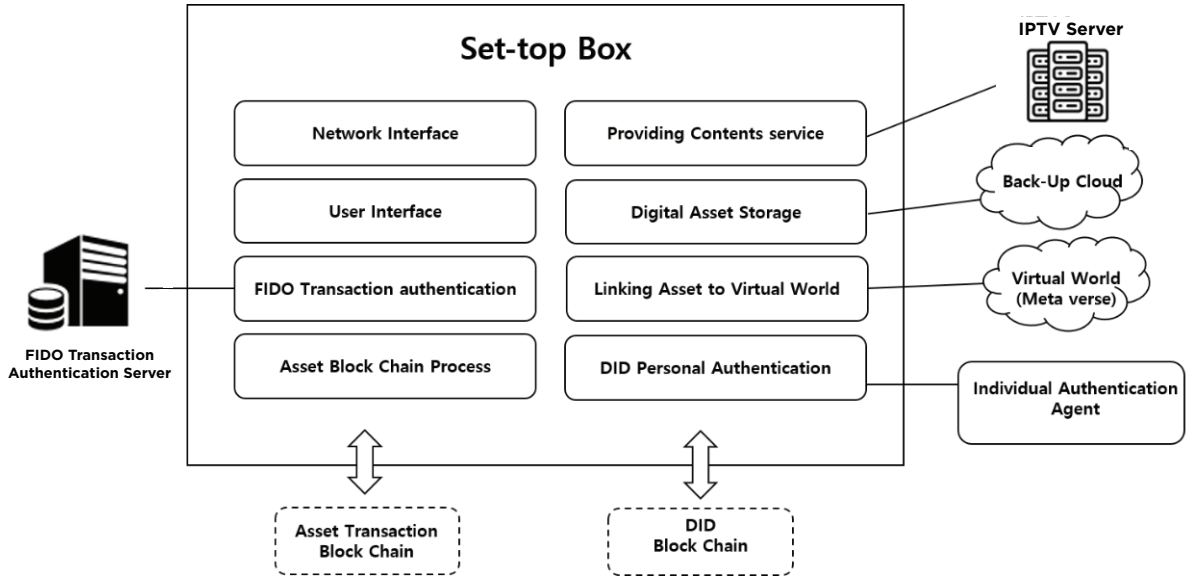


Figure 2: The conceptual proposed custody model of digital assets using a set-top box (home gateway). FIDO, Fast ID Online; DID, decentralized ID.



(A)



(B)

Figure 3: Design of digital asset custody service model based on home gateway: (A) simplified diagram and (B) detailed features of set-top box as a home gateway. FIDO, Fast ID Online, DID, decentralized ID.

an authentication function by downloading standardized API definitions to a web browser and related web platform infrastructure as a method for Internet users to securely authenticate on multiple websites and devices. It is possible to implement it in the form of computer-readable code on a computer-readable non-volatile recording medium. There are various types of non-volatile recording storage devices, such as a hard disk, Solid State Drive (SSDs), Compact Disc Read Only Memory (CDROMs), Network Attached Storage (NAS), magnetic tapes, web disks, cloud disks, etc. These storage devices may be implemented in a form in which codes are distributed and executed in number of storage devices connected through a network. It also may be implemented in the form of a computer program stored in a medium to execute a specific authentication procedure [1].

Figure 4 shows the DID authentication process for the proposed custody model. In the case of digital asset backup, general access is not allowed and access is only possible after obtaining permission from all DID members. In this case, the existing digital assets are discarded and the digital asset registration procedure for FIDO authentication must be performed again. The DID-based custody platform can be serviced by linking the service provider with the home gate installed in the home, and it can be realized by linking with the blockchain of limited individuals who share the service through the home gateway.

DID-based biometric authentication is applied for security authentication of custody platform users who use home gateways. Additionally, the FIDO transaction authentication server is connected to the FIDO transaction module of the home gateway to perform

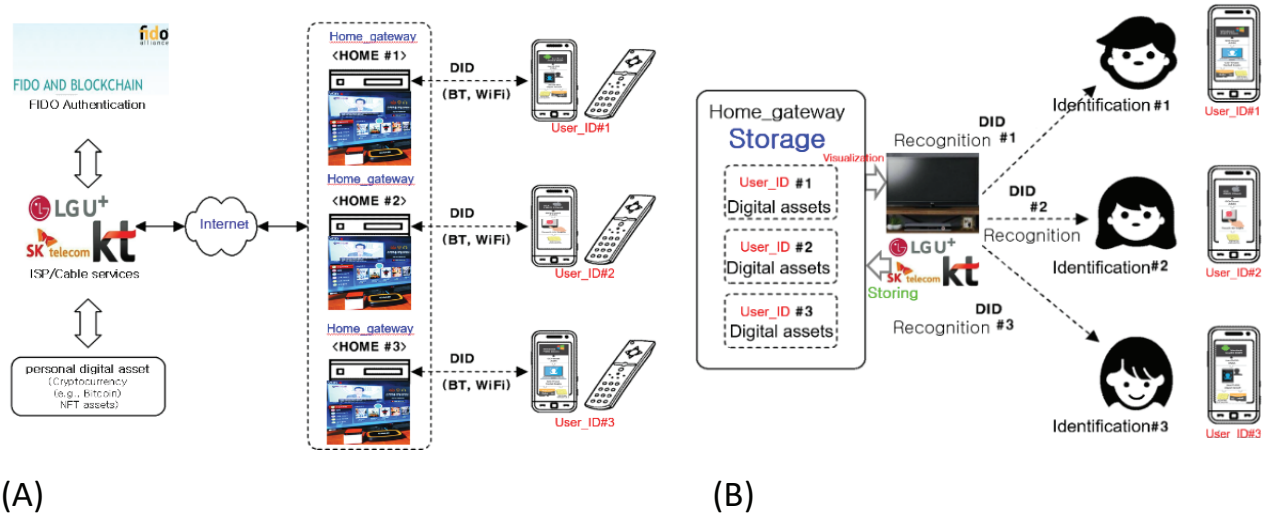


Figure 4: The DID-based custody model: (A) custody model using home gateway, and (B) the storage of the home gateway by the DID for custody service. DID, decentralized ID.

authentication tasks. In this case, personal authentication by the biometric information of an individual DID device input from the home gateway receiving device is used.

The biometric authentication server is a component that performs biometric authentication through user ID and bio-template matching by cooperative operation with the FIDO authentication server and user terminal in the real world, and provides the biometric authentication result to the transaction authentication server. After receiving the user ID and biometric data (e.g., fingerprint data) from the user terminal, biometric authentication is performed by cooperative operation with the FIDO authentication server. At this time, a hybrid server that provides multiple biometric authentication can be configured. In other words, it is possible to provide biometric authentication of any one of various types of biometric information (e.g., fingerprint, face, iris, etc.), and through this, various authentication methods can be provided to multiple users.

The multiple authentication methods are applicable to a specific user; for example, both face recognition and iris recognition are possible. At this time, it is preferably configured to apply the most recent one among these authentication methods for the biometric authentication server. Additionally, it is possible to build a multi-domain authentication system by performing terminal and user identification using multi-biometric authentication. And users can build integrated hardware for personal authentication that can simultaneously receive biometric authentication in a general-purpose operating system (e.g., Windows Hello authentication) and FIDO2 authentication.

The biometric authentication server performs biometric authentication through matching user ID and biometric templates (e.g., fingerprint data) by cooperative operation with the FIDO authentication server and the user terminal, and returns the biometric authentication result back to the authentication server. Biometric authentication (multiple biometric authentication) can be provided by any type of biometric information (e.g., fingerprint, face, iris, etc.), and through this, various types of authentication methods can be provided for each user. It allows individual private keys with DID personal authentication and has the advantage of being able to store personal digital assets.

Figure 5 shows the identification information and verification process for each individual based on the distributed ID conceptually, which can include an individual key with DID personal authentication, and FIDO biometric authentication for multiple custody digital assets of several family members. Each user terminal sets a DID that can be used as a unified user account for itself through the DID blockchain [1]. An OpenID relying party (RP), which means trust between groups, is a group of devices that support OpenID. For example, FIDO is also in a mutual RP relationship with the server used by the user [9]. The application server is called an RP server, and the application service client is called an RP client. When the request message sent by the FIDO authentication server is delivered to the RP server, it reaches the FIDO client through the RP client through the network.

Figure 6 shows a set-top box API configuration diagram that authenticates biometric-based DID FIDO

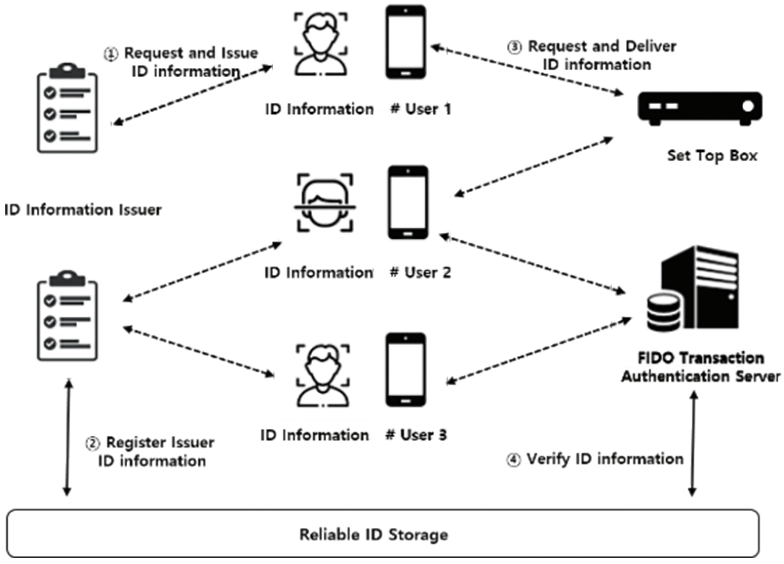


Figure 5: Authentication process for personal digital asset custody model based on multiple DID. DID, decentralized ID.

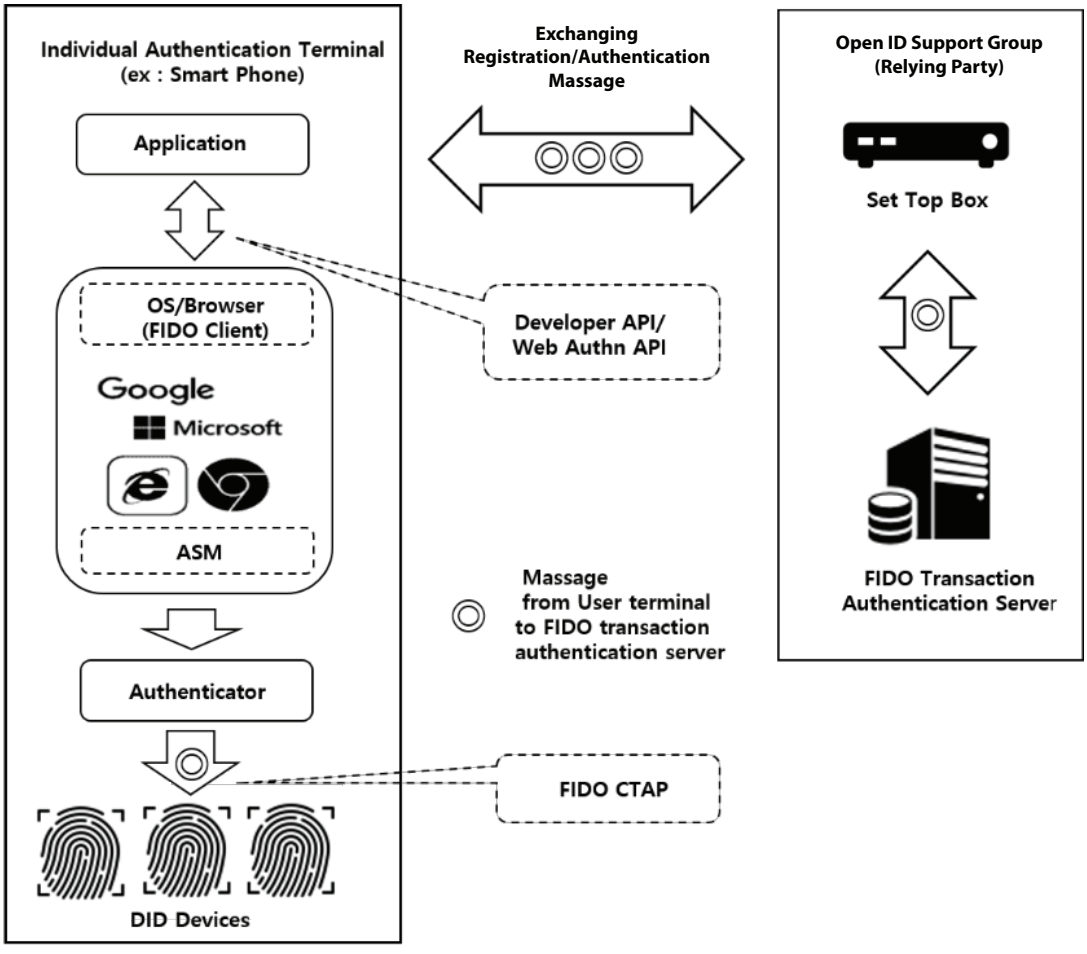


Figure 6: Information processing of the proposed custody model configuration. CTAP, client to authenticator protocol; FIDO, Fast ID Online.

transactions with the construction of a server for the FIDO platform of the proposed custody model and an information processing process to access digital custody. FIDO transaction authentication is linked for user personal authentication and digital asset transaction between the transaction authentication server and the user terminal. The components of FIDO include a FIDO server, FIDO client, authenticator-specific module (ASM), and authenticator. The FIDO authentication server performs the role of a FIDO server and also performs the role of a user terminal FIDO client. The ASM sends the FIDO client's request to the authenticator, and the generated response value is sent back to the FIDO client.

In order to further strengthen the security of the biometric authentication method, the biometric data that can be transmitted from the communication port could be encrypted because of the interception of biometric data when transmitting the fingerprint image data through a communication port, which is generally used when a fingerprint sensor transmits a fingerprint image to a processor to perform matching processing. Therefore, it is required that a biometric sensor can fundamentally prevent the hacking of biometric information [11, 20].

b. Enhancement of biometric security

Figure 7 shows a credit card transaction process based on biometric information security. This is similar to the personal security authentication process of the digital custody service. This shows the process in which biometric information can be hacked by hardware hacking when the biometric information recognition module and authentication information are transmitted. The biometric sensor with a built-in encryption module can further enhance security because biometric information is not hacked due to information encryption even if hardware hacking occurs.

A biometric sensor with a built-in encryption module can solve this problem, because encrypting the obtained private biometric data makes it fundamentally impossible to hack biometric information, even if there were to be an attempt to hack biometric data through the communication port of local (mobile) devices.

Figure 8 shows that if the fingerprint sensor contains the encryption block and transmits the encrypted fingerprint image through communication port, even if a communication port interception hack occurs, the biometric authentication information is encrypted. In this case, actual biometric information hacking does not occur because the fingerprint image cannot be restored without the authentication key [12, 19]. Through this, authentication information hacking can be fundamentally blocked. Therefore, it is possible to perform double security processing when applying biometric authentication, which further enhances security by applying image encryption

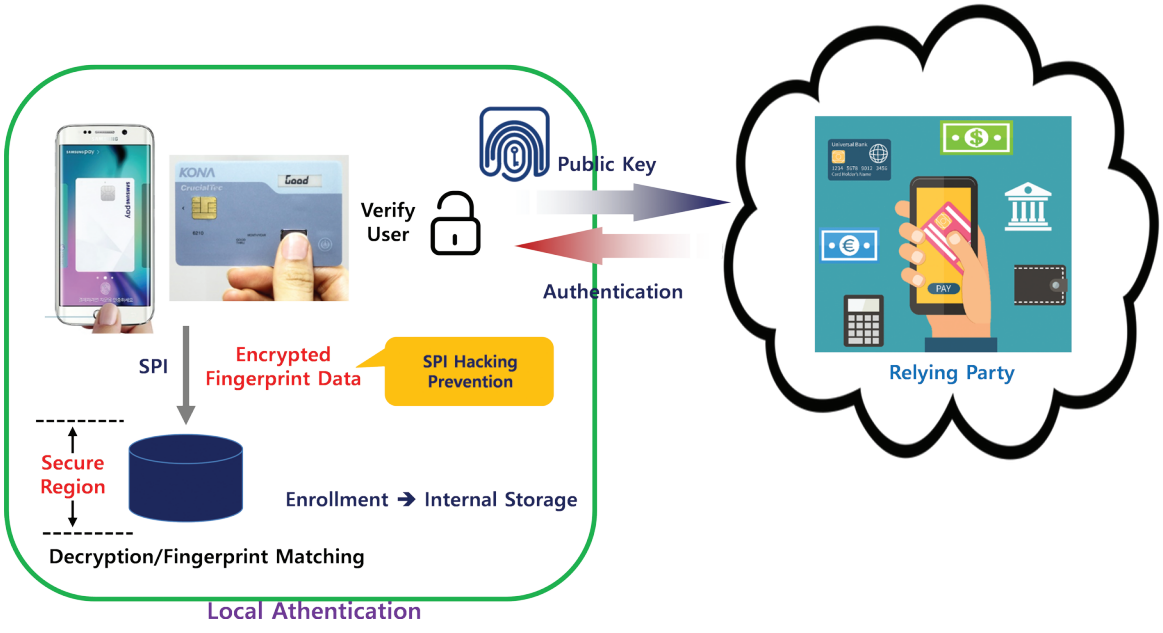


Figure 7: An example of hardware hacking prevention of biometric information in the biometric authentication process.

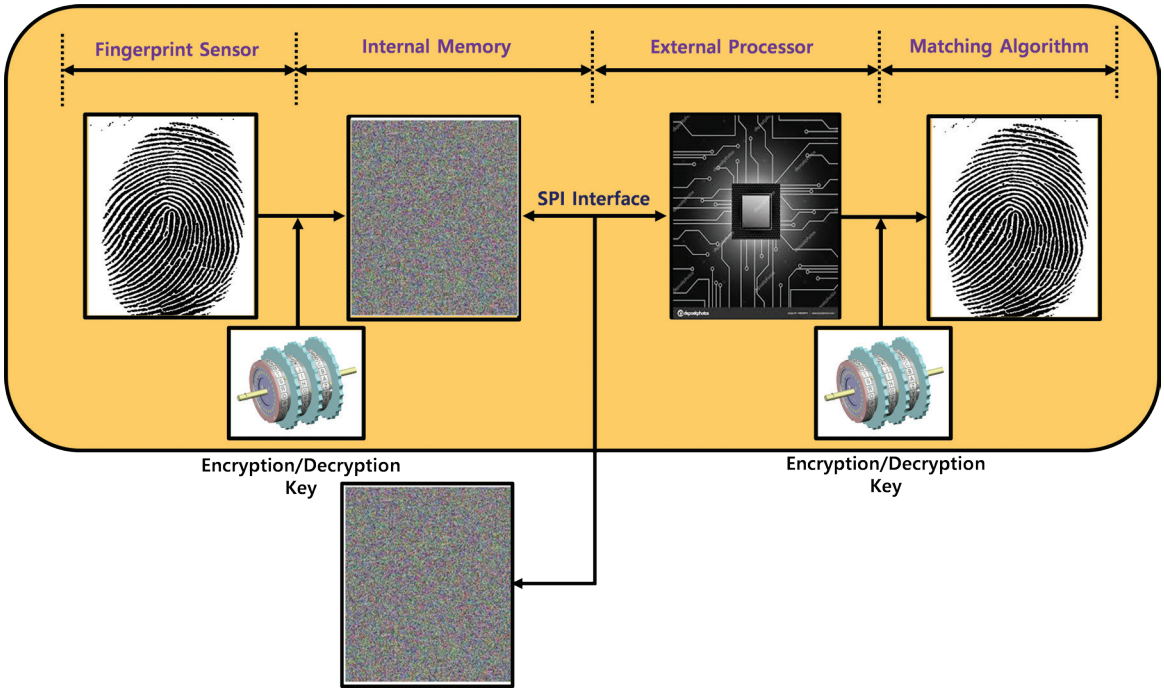


Figure 8: The proposed biometric sensor embedded with an encryption module to prevent hardware hacking and a system schematic to restore it.

technology to the fingerprint sensor IC. It has the advantage of being able to store personal digital assets, and security can be further strengthened.

However, including an encryption module inside the fingerprint sensor chip can be a big burden on power consumption as well as possibly necessitate an increase in chip size. Therefore, in the case of such an embedded module, an algorithm that provides an effective and strong encryption function with low power consumption, together with reducing the burden associated with an increased chip size, is required. A fingerprint sensor with embedded encryption module that applies a lightweight encryption algorithm (LEA) can provide simple and strong encryption suitable for mobile or IoT applications [13].

Figure 9 shows the process of performing one round operation for decryption in a LEA block cipher. XOR-based round architecture provides an architecture suitable for mobile while providing efficient and strong encryption. The decryption process is the reverse of the encryption process. For example, if during encryption an XOR operation is followed by a modulo addition operation and a right rotation is performed last, during decryption, a left rotation operation is performed and then a modulo subtraction operation followed by an XOR operation is performed. Also, at the end of each round, since a 32-bit left rotation was performed at the time of encryption, a 32-bit right rotation must be performed at the time of decryption.

The process of performing one round operation for encryption in the LEA block cipher is as follows. Xi[0] to Xi[3] each means a message of 32 bits. Since a 128-bit message is used, four divided-into-32 bits are used. And the six round keys used in the i-th round are all 32 bits from RKi[0] to RKi[5]. It can be seen that the operation used in each round uses only XOR, add, and rotate operations with 32-bit modules, which provides effective encryption with low power consumption.

Figure 10 shows the architecture of the LEA block cipher algorithm for IP design. The cipher algorithm for an embedded module generates encrypted or decrypted 128-bit data results by applying a 128-bit master key. [16] The message buffer may consist of four registers of 32 bits, which are used to eliminate performance degradation due to the data size mismatch between 128-bit messages and 32-bit external data interfaces required for round operation.

The LEA cipher algorithm is implemented with a 128-bit cipher text using 128 master keys for a 128-bit message, and 24 round operations are performed. The LEA encryption algorithm can be divided into a key scheduling part and a round operation block that performs data randomization [22]. The implemented LEA with Verilog can be an embedded fingerprint

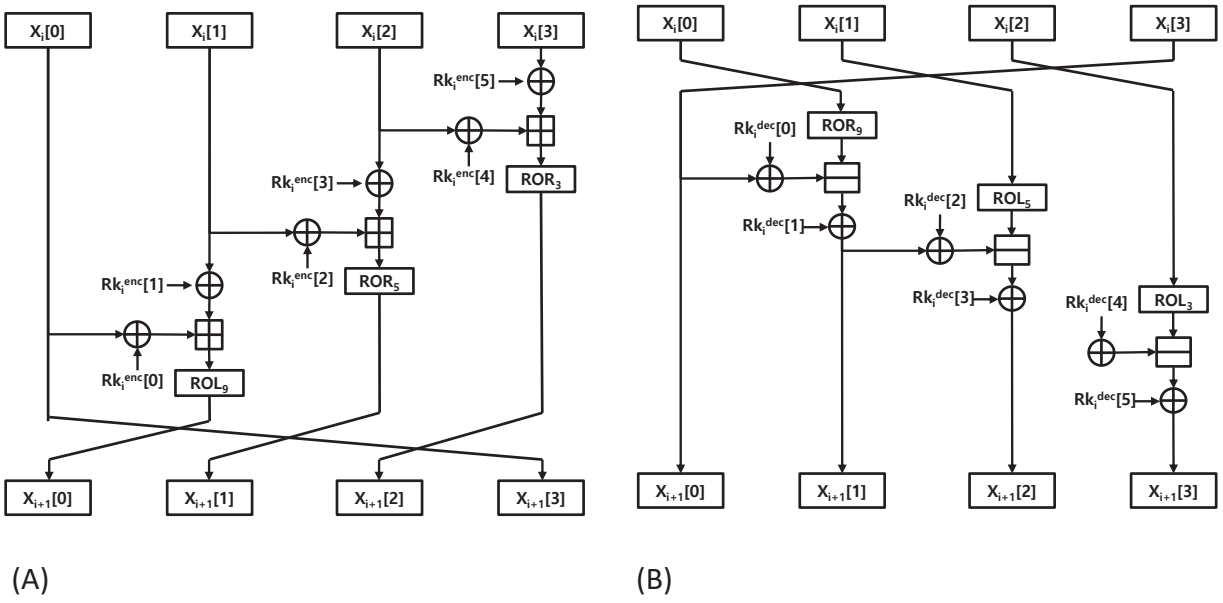


Figure 9: LEA round function: (A) for encryption, and (B) for decryption. LEA, lightweight encryption algorithm.

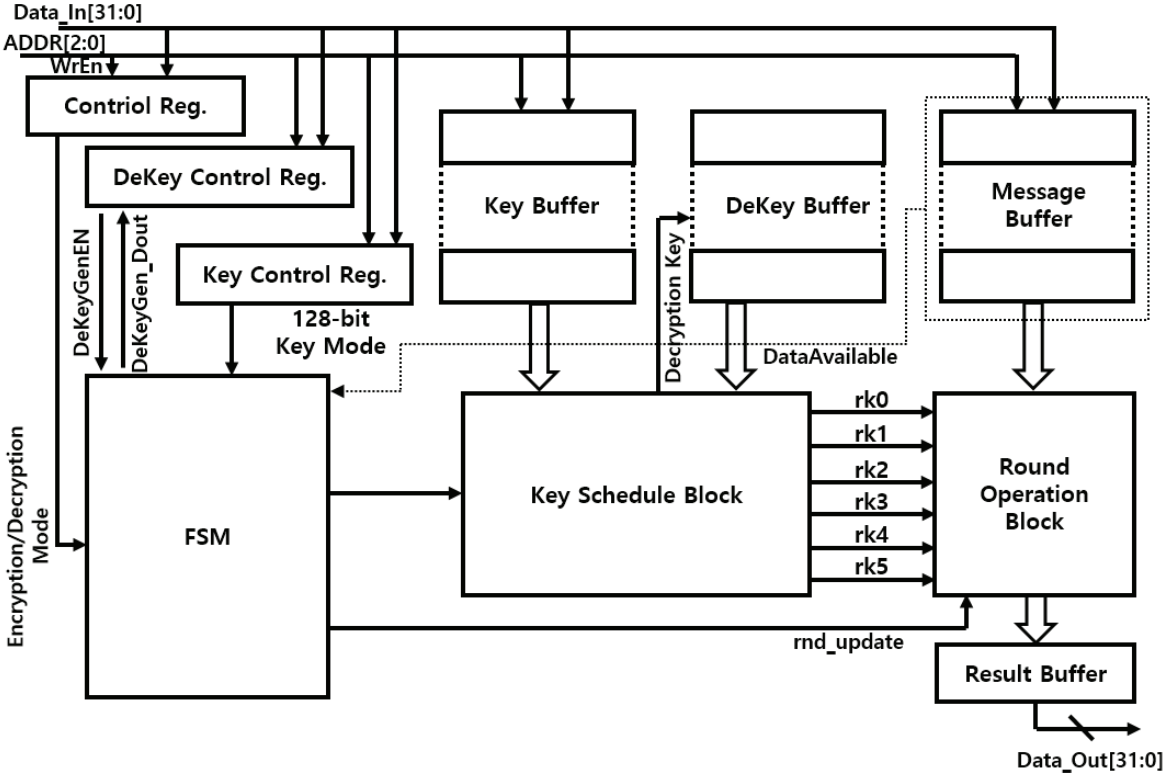


Figure 10: Architecture of the LEA block cipher algorithm for IP design. LEA, lightweight encryption algorithm.

```
always @(posedge clk or negedge reset)
 if (~reset) begin
   rk0 <= 32'h0; rk1 <= 32'h0; rk2 <= 32'h0;
        rk3 <= 32'h0; rk4 <= 32'h0; rk5 <= 32'h0;  end
 else if (RndKeyGenEn==1'b1) begin
        if (EncryptMode) begin
           if (K128Mode) begin
                       rk0 <= TempK0; rk1 <= TempK1; rk2 <= TempK2;
                 rk3 <= TempK1; rk4 <= TempK3; rk5 <= TempK1;
                end else begin //(192-, 256-bit key)
                 rk0 <= TempK0; rk1 <= TempK1; rk2 <= TempK2;
                 rk3 <= TempK3; rk4 <= TempK4; rk5 <= TempK5; end
        end
        else begin //DecryptMode
          if (K128Mode) begin
                       rk0 <= KReg0; rk1 <= KReg1; rk2 <= KReg2;
                 rk3 <= KReg1; rk4 <= KReg3; rk5 <= KReg1;
              end  else begin
                 rk0 <= KReg0; rk1 <= KReg1; rk2 <= KReg2;
                 rk3 <= KReg3; rk4 <= KReg4; rk5 <= KReg5; end
        end
 end
```

Figure 11: Round-key generation Verilog code for KeySchedule module.

sensor to enhance security [14]. The encryption block designed in the fingerprint sensor chip only performs encryption [15]. The PC decryption program was written in C code and implemented to perform the same function as the decryption function of the encryption/decryption block designed as a chip to perform the LEA decryption program.

The 128-bit data to be executed next to the message block currently being processed is stored as a burst in the message buffer in advance during encryption/decryption for the current message block, and then immediately after the encryption/decryption of the currently executing message block is completed. As a result, it achieves the maximum throughput of IP by simultaneously providing a message block in the message buffer. As soon as four complete input data are received, encryption or decryption is performed according to the setting value of the LEA encryption/decryption module [17].

The encryption and decryption codes can be set in the message window and are set arbitrarily for testing. It is assumed that the fingerprint image is stored in memory. The set encryption code is loaded, and the fingerprint image output from the memory with the loaded encryption code passes through the LEA encryption block and is encrypted.

Figure 11 shows a part of the round-key generation block of the KeySchedule block, which is the main functional block that performs LEA encryption [18]. The whole code is too long to show within the present article, but it was well-designed for compatibility with the purpose of synthesizable code.

Decryption can be performed with a C program to check whether the decryption process was successful. This program can be ported to a PC, mobile, IoT device, etc., to perform decryption. Figure 12 shows part of the decryption code among the LEA decryption codes, and this is the main code for LEA decryption.

The original image is 8-bit data, but during the encryption process, the four image data are combined and encrypted into 32-bit data, and so the 32-bit data is processed at once in the decryption process. The input streams data of 32-bit are again divided into four 8-bit data inside the code, and the original data is restored through a round function operation.

c. Authentication simulations

Figure 13 shows the fingerprint image and encrypted fingerprint image output with LEA encryption. Figure 13B is the encrypted fingerprint image

```
void LEA_Dec(uint32_t* roundkey, uint32_t* data)
{
	uint32_t* block =  data;
	uint32_t* rk =  roundkey;
	uint8_t i, j;

	uint32_t b0 = block[0];
	uint32_t b1 = block[1];
	uint32_t b2 = block[2];
	uint32_t b3 = block[3];

	rk += 92;

 for (uint16_t j = 0 ; j < num_of_data/4 ; j++) {
	b0 = block[j*4+0];
	b1 = block[j*4+1];
	b2 = block[j*4+2];
	b3 = block[j*4+3];

	for (i = 0; i < 6; ++i) {
		b0 = (rot32r9(b0) - (b3 ^ rk[3])) ^ rk[0];
		b1 = (rot3215(b1) - (b0 ^ rk[2])) ^ rk[0];
		b2 = (rot3213(b2) - (b1 ^ rk[1])) ^ rk[0];
		rk -= 4;

		b3 = (rot32r9(b3) - (b2 ^ rk[3])) ^ rk[0];
		b0 = (rot3215(b0) - (b3 ^ rk[2])) ^ rk[0];
		b1 = (rot3213(b1) - (b0 ^ rk[1])) ^ rk[0];
		rk -= 4;

		b2 = (rot32r9(b2) - (b1 ^ rk[3])) ^ rk[0];
		b3 = (rot3215(b3) - (b2 ^ rk[2])) ^ rk[0];
		b0 = (rot3213(b0) - (b3 ^ rk[1])) ^ rk[0];
		rk -= 4;

		b1 = (rot32r9(b1) - (b0 ^ rk[3])) ^ rk[0];
		b2 = (rot3215(b2) - (b1 ^ rk[2])) ^ rk[0];
		b3 = (rot3213(b3) - (b2 ^ rk[1])) ^ rk[0];
		rk -= 4;
	}

	// Results
	block[j*4+0] = b0;
	block[j*4+1] = b1;
	block[j*4+2] = b2;
	block[j*4+3] = b3;

	rk += 96;
  }
}
```

Figure 12: LEA decryption C code for fingerprint image restoration. LEA, lightweight encryption algorithm.

transmitted from the sensor chip in the encrypted output mode. The average image value is 128, and random image output appears, which shows that the LEA encryption process is working as designed and shows the result of decrypting the image delivered to the decryption program with the same encryption code.

As shown in Figure 13, it was confirmed that the encrypted fingerprint image was restored to the original fingerprint image through the decryption process and the implemented LEA encryption block with Verilog works effectively and as designed. In the future, the LEA module implemented in Verilog code will be embedded in the biometric sensor chip. The finger-

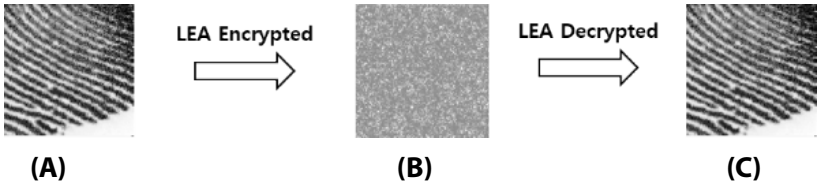


Figure 13: Fingerprint sensor image with embedded LEA module: (A) original fingerprint image, (B) LEA encrypted image, and (C) LEA decrypted image. LEA, lightweight encryption algorithm.

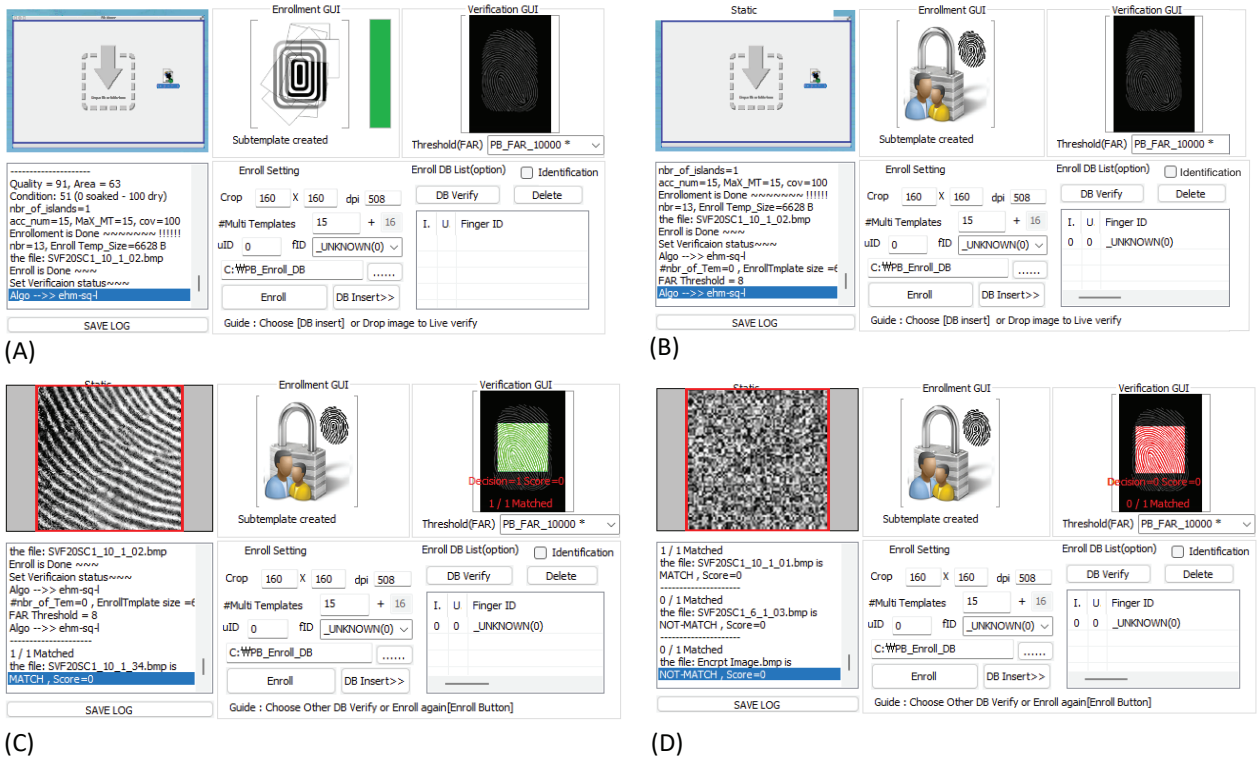


Figure 14: Fingerprint information enrollment process: (A) 16 DB enrollment, (B) DB verify and lock, (C) authentication process, and (D) authentication failure with encrypted fingerprint image.

print sensor chip and the associated hardware platform will be implemented in the next research.

Assuming that hardware hacking occurred during local authentication, the authentication process was performed using an encrypted fingerprint image to which the LEA algorithm was applied and a general fingerprint image.

Hardware hacking methodologies, such as an ATM duplicator, mainly use unauthorized hardware access as the modus operandi through which to carry out hacks. The fingerprint image obtained in advance was registered as an authentication DB, and the authentication process was attempted under the assumption that hardware hacking had occurred. The Precise Biometrics (PB) authentication algorithm, which is very reliable in mobile and online authentication, was used [23].

Figures 14A,B shows the process of registering the user's fingerprint DB and verifying and locking the registered DB, respectively. Figures 14C,D shows the results of authenticating the final output image after registering a general fingerprint user and applying LEA encryption to the fingerprint chip, and the result of authenticating the reconstructed fingerprint through the decryption process.

If authentication is attempted with the user's fingerprint, authentication is completed normally. In the case of hardware hacking, even if the fingerprint image is hacked, authentication cannot be successful with the encrypted image, as shown in Figure 13D.

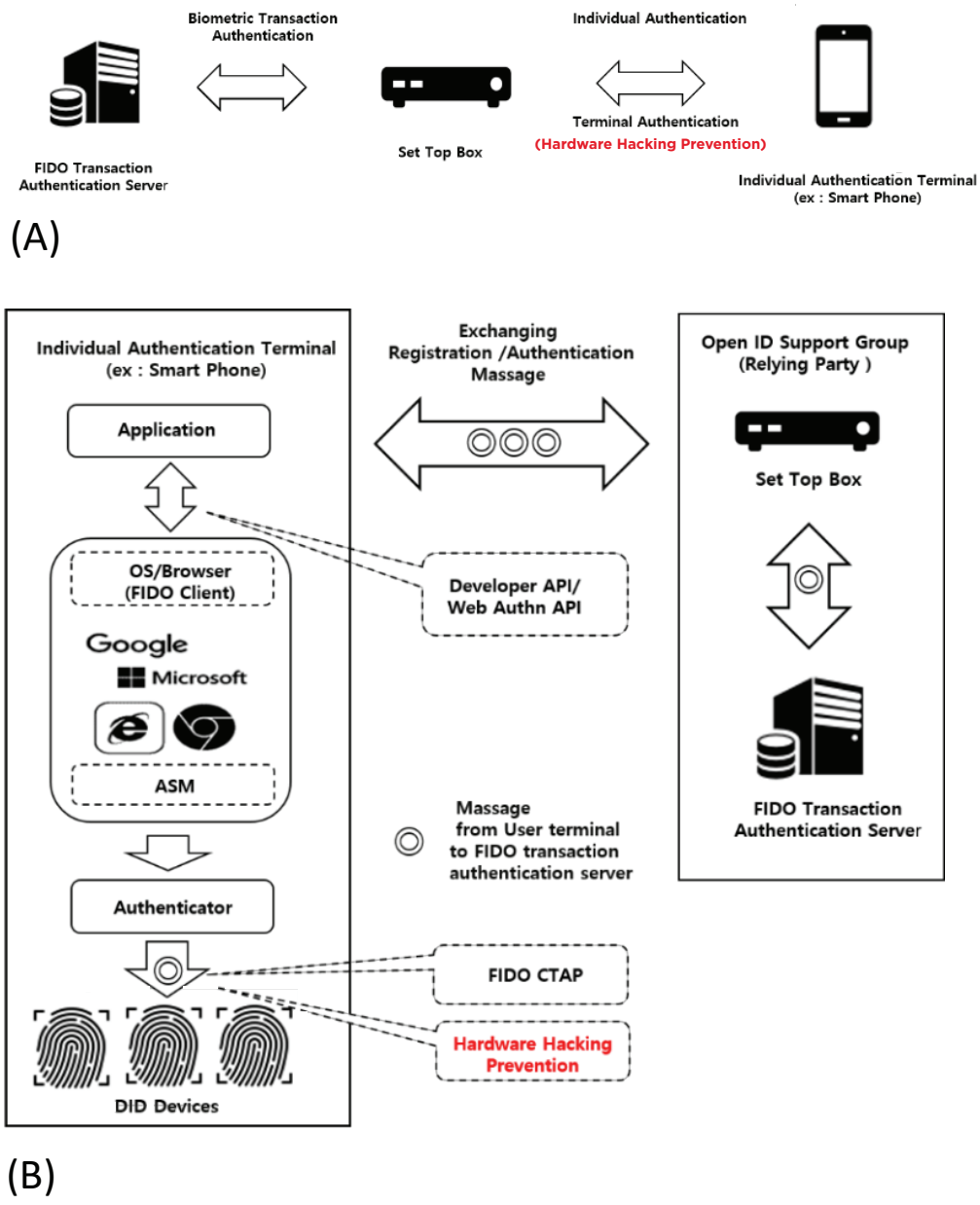


Figure 15: The proposed digital custody model with a biometric authentication device with an embedded encryption module, (A) using a set-top box as a home gateway and (B) authentication and information transfer processing.

Authentication is possible only when decryption takes place via the unique key assigned to the fingerprint chip.

d. Digital custody model for enhanced biometric security

Figures 15A,B shows a simplified custody model and information processing using a home gateway and biometric encryption embedded module, respectively. Of course, as shown in Figures 2 and 5 above, they are modified forms with a biometric encryption module applied. This architecture provides further enhanced security.

IV. Conclusions and discussion

Digital assets will continue to increase with the passage of time and the attendant widespread adoption

of technology, and thus the need for a device that would ensure safe storage and security for digital assets in the future is raised. This paper proposed a digital custody service model using a home gateway, which has almost no risk of digital assets being lost. Digital assets are safely stored in the home gateway, and access to these assets is possible only through a private key and biometric authentication. An individual key is managed with DID personal authentication with blockchain technology, and FIDO biometric authentication for multiple custody digital assets of several members that can be stored and managed separately.

To strengthen security, it was proposed to apply a local device to which a biometric sensor equipped with an encryption module that can fundamentally block the hacking of biometric information is applied. It is implemented with Verilog for embedded fingerprint sensor block and a decryption program implemented with C.

The proposed digital custody model can be applied to any type of asset that will be released in the future and provides enhanced security. Of course, keeping in mind the possibility for a failure of the set-top box, or the need for its upgrading or servicing, a strategy to safely protect digital assets through back-up and to enable migration is required, and this is intended for exploration in further research.

Acknowledgments

This work was supported by a Korea Environmental Industry & Technology Institute (KEITI) grant, funded (No. G232022012511) by the Korea government (Ministry of Environment).

References

[1] Mingoo Kang, et al., “individual digital safe system for set-top box by use of FIDO transaction certification and multiple DID personal identification”, Korea patent 10-2021-0126039, 2021.09.24

[2] https://www.sec.gov/

[3] https://www.sec.gov/info/smallbus/secg/custody_rule-secg.htm

[4] https://fidoalliance.org/

[5] E. Klieme, J. Wilke, N. van Dornick and C. Meinel, “FIDOnuous: A FIDO2/WebAuthn Extension to Support Continuous Web Authentication,” 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp. 1857-1867, 2020

[6] Lyastani, S. G., Schilling, M., Neumayr, M., Backes, M., & Bugiel, S. “ Is FIDO2 the Kingslayer of User Authentication? A Comparative Usability Study of FIDO2 Password-less Authentication,” inIEEE Symposium on Security and Privacy,pp. 268-285, May 2020

[7] Peter Smith, Nipun Srivastava,” A Market Overview of Custody for Digital Assets “ Deloitte Digital Custodian Whitepaper, June 2020

[8] Mingoo Kang, Seungpil Hong. Sangchul Shin and Sangyep Nam, Digital Asset and Security, Sanghakdang, 2022

[9] Rivera-Dourado, Martiño, et al. ‘An Analysis of the Current Implementations Based on the WebAuthn and FIDO Authentication Standards.” Engineering Proceedings7.1(56). 2021

[10] Biryukov, A., & Tikhomirov, S. “Security and privacy of mobile wallet users in Bitcoin, Dash, Monero, and Zcash.”Pervasive and Mobile Computing,59, 101030. 2019

[11] Yeo, Hyeopgoo. “Touch fingerprint sensor based on sensor cell isolation technique with pseudo direct signaling.” International Journal on Smart Sensing and Intelligent Systems, vol.12, no.1, pp.1-9. 2019

[12] E. Rahmawati et al., “Digital signature on file using biometric fingerprint with fingerprint sensor on smartphone.” 2017 International Electronics Symposium on Engineering Technology and Applications (IES-ETA), pp. 234-238. 2017

[13] Lee, D., Kim, D. C., Kwon, D., & Kim, H. “ Efficient hardware implementation of the lightweight block encryption algorithm LEA.”Sensors,vol 14(1),pp 975-994. 2014

[14] J. Sun, Q. Zhong, L. Kou, W. Wang, Q. Da and Y. Lin, “A lightweight multi-factor mobile user authentication scheme.” IEEE INFOCOM 2018 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), pp. 831-836. 2018

[15] Katuk, Norliza, and Ikenna Rene Chiadighikaobi. “An Enhanced Block Pre-Processing of PRESENT Algorithm for Fingerprint Template Encryption in the Internet of Things Environment.” International Journal of Communication Networks and Information Security,13.3 pp. 474-481. 2021

[16] Hong, D., Lee, J. K., Kim, D. C., Kwon, D., Ryu, K. H., & Lee, D. G. (2013, August). “LEA: A 128-bit block cipher for fast encryption on common processors.” Ininternational workshop on information security applications(pp. 3-27). Springer, Cham. 2013

[17] Sonh, S. “ Design of Encryption/Decryption IP for Lightweight Encryption LEA.”Journal of Internet Computing and Services,18(5), vol 8. 2017

[18] Hong, D., Lee, J. K., Kim, D. C., Kwon, D., Ryu, K. H., & Lee, D. G. "LEA: A 128-bit block cipher for fast encryption on common processors." In international workshop on information security applications(pp. 3-27). Springer, Cham. August 2013.

[19] D. Cho, "A Simple Fingerprint Fuzzy Vault for FIDO." KSII Transactions on Internet and Information Systems, vol. 10, no. 11, pp. 5674-5128, 2016.

[20] Y. Chen, Y. Ge, W. Wang and F. Yang, "A Biometric-based User Authentication and Key Agreement Scheme for Heterogeneous Wireless Sensor Networks." KSII Transactions on Internet and Information Systems, vol. 12, no. 4, pp. 1779-1798, 2018

[21] Gyeong-Jin Ra and Im-Yeong Lee. 2018. "A Study on KSI-based Authentication Management and Communication for Secure Smart Home Environments."KSII Transactions on Internet and Information Systems, 12, 2,pp 892-905.2018

[22] Y. Zhang and X. Jia, "Fast image encryption algorithm based on substitution and diffusion." KSII Transactions on Internet and Information Systems, vol. 12, no. 9, pp. 4487-4511, 2018

[23] https://precisebiometrics.com