The Journal of Supercomputing
https://doi.org/10.1007/s11227-018-2496-1

Blockchain-based mobile fingerprint verification and automatic log-in platform for future computing

Jun-Ho Huh[1] · **Kyungryong Seo**[2]

Abstract
Door locks and user authentication are the major issues in the current banking industry. There are a number of user future computing techniques, and security is especially essential to these methods. Existing digital door locks have the problem of opening easily with a stolen PIN number or by electrical shock. Thus, this study proposed and implemented an integrated automatic log-in platform based on mobile fingerprint recognition by applying the blockchain theory. As a result of this research, a convenient, integrated automatic log-in platform with powerful security has been constructed using a smartphone-based fingerprint recognition function. There are three major functions of the platform. First, it is possible to authenticate the user in PC, mobile device, and IoT environments through fingerprint recognition. Second, the platform includes SDK to develop application software for user authentication and IoT services. Last is its strengthened security using the blockchain theory to prepare against tampering/forging/leaking of a user's fingerprint information by hackers.

Keywords Blockchain · IoT · ICT · Door lock · Automatic log-in platform · Platform · Architecture · Computer Architecture

1 Introduction

Future computing reflects a super-connected society. It is believed that technology that can apply an explosive increase in big data to a service most safely and efficiently is required in our super-connected society. It may be a blockchain. Big data sharing is very

✉ Kyungryong Seo
krseo@pknu.ac.kr

Jun-Ho Huh
72networks@cup.ac.kr; 72networks@pukyong.ac.kr

[1] Department of Software, Catholic University of Pusan, Busan, Republic of Korea

[2] Department of Computer Engineering, Pukyong National University at Daeyeon, Busan, Republic of Korea

Published online: 26 July 2018

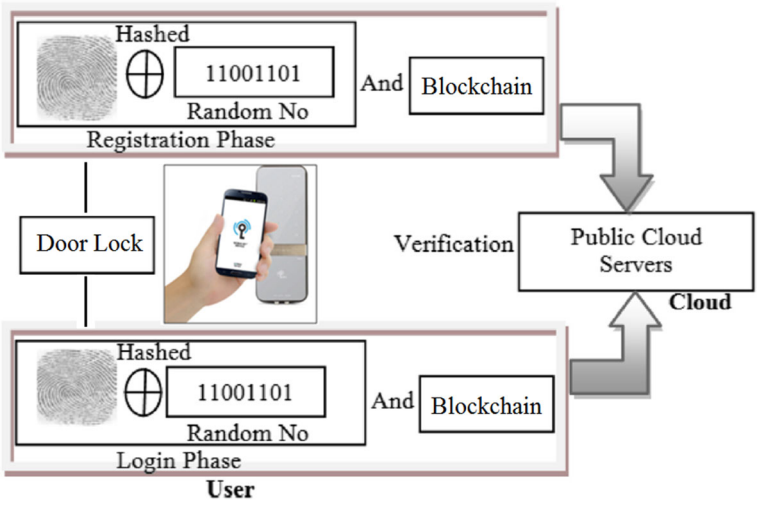

Fig. 1 Proposed framework of mobile fingerprint recognition and automatic log-in platform

limited domestically and internationally due to hacking and security threats. However, as big data-based digital conversion becomes a survival strategy, it is expected that blockchain technology will attract attention in the future.

Thus, the authors attempted to construct a platform with which fingerprint recognition-based authentication can be performed with the user's PC, mobile, and other IoT devices based on the information sent from the mobile devices mounted with a fingerprint recognition function. Figure 1 shows the proposed framework of mobile fingerprint recognition and automatic log-in platform.

Meanwhile, each hash value was created with a private key and subsequently included in the fingerprint information stored in the blockchain network to prevent extortion/forging/tampering/leaking of fingerprint information by hackers.

This paper focuses on designing and implementing a "Mobile Fingerprint Recognition and Automatic Login Platform Framework" to address the problem of security vulnerabilities in future computing technology for the multimedia equipment to be used in the forthcoming age. For the recognition of fingerprints, this system was constructed by tightening its security with blockchain technology, and the system was confirmed to be working flexibly.

This study tried to deal with a private blockchain rather than a conventional bitcoin (virtual money)-based public blockchain. Blockchain is a distributed system that can safely store and verify transactions and other usage data without centralized control. The data produced in these distributed networks will be massive, and machine learning and cognitive computing technologies will become more important.

2 Related research

Currently, the majority of researchers involved in the development of security solutions consider blockchain as a viable, robust, and sustainable cybersecurity solution because of its unique data distribution environment [1]. Instead of keeping information in a third-party storage or a centralized data center, the same information is individually stored in interlinked computers so that if there are any security breaches, the entire networked computer systems will protect the information by rejecting any updates or changes made abnormally [2]. Also, for wire transfer, the blockchain system requires a number of keys or signatures (aka multisig) to complete the transaction. Such an enhanced scheme provides a new level of security and privacy. Although not perfect, the security of the blockchain technology is still considered to be the highest security measure available. Its redundant and distributed data storage form prevents hackings more effectively than the existing security technologies. For example, for the bitcoin transactions, the identical ledgers are stored in multiple computer systems interlinked in a network as backups so that a hacker has to deal with all of them to break into one's account and steal the coins [3].

It is estimated that over 50% of the storage systems should be penetrated to successfully take over an account and clean out the data in it. Another well-established security scheme can be found in OpenBazaar which is a bitcoin-based multi-signature-protected decentralized marketplace started in 2016 [4]. As the user information is not kept in its database, hackers cannot get an access to a bitcoin wallet without the proper keys. It is possible for the hackers to obtain the keys illegally, but still they will need multiple signatures (multisig) to seize and move the funds in the targeted account [5]. Currently, many security systems around the world are adopting a concept called "security through obscurity, which literally means that the security mechanism and implementation of a system are being kept in the dark.

Yet, like all other security approaches, this also has its weakness; the secrets never last. There is always a possibility that a person or a group will finally figure out the security mechanism. A suitable example of such a case can be found in the financial sector where the Society for Worldwide Interbank Financial Telecommunications (SWIFT) code is widely used. After observing unexpected system failures involving the SWIFT code-based transaction system, some of the researchers of security engineering have started to argue that such a system is outdated and its security is questionable. The examples of failure include the unauthorized transactions of 18 million US dollars kept in the Bangladesh Central Bank (2016) through the SWIFT network of the New York Federal Reserve Bank [6] and the similar attempts targeting some of the banks in Southeast Asia [7]. Although these crimes could have been prevented by using the blockchain technology, the recent successful cases of hackings have made the researchers to question the robustness of the blockchain-based systems.

Despite the weakness in the bitcoin transaction systems, it seems that the blockchain can still be the best alternative as most of the hacking attempts have been successful in the other systems that have stored the private keys. Some time ago, Coward stressed that a transaction of bitcoins was successful without any security breaches, but this was in 2016 [8] and the hacking attempts targeting bitcoins have become more sophisticated in recent years. As for privacy protection, most of the private information leaks in

the past paper-oriented systems occurred due to malicious attempts to capture the primary data. By contrast, the privacy violations in the twenty-first-century cyberage were caused by the illegal use of information acquired legally [9].

Nowadays, the firms around the globe keep massive information and there always is a possibility that someone with malicious intent would abuse them for his/her own benefit, but it is also possible to use them innovatively. It seems appropriate to quote a text by [10] who stressed by saying, "most innovative secondary uses haven't been imagined when the data is first collected" [10].

It has been neglected the fact that people actually concerned about their privacy. That is, until the early phase of cyberage, they had no choice but to submit most of their private information to governments, financial institutions, or other authorities to claim their rights or to conduct their respective businesses. Those who had received such information were quite free from any restrictions of accessing, sharing, keeping, using, and selling them. However, after witnessing the ever increasing number of crimes involving private information, they have become more aware of the importance of privacy protection. Also, since the number of the online-based services carried out by the cloud services providers (CSPs) is also increasing rapidly, the issues focusing on privacy and security have become one of the most widely discussed subjects [11]. The uniqueness of blockchain is that the personal data can only be viewed under the authorization of the very person and the data will not be stored in a system that supports transactions. The encrypted data of an account holder are almost impossible to be compromised [12] such that the level of security or the data protection is incomparably high. Thus, the blockchain-based applications can establish themselves as a sort of "killer application" because of their high level of security in transmission and storage of digitized and encrypted documents. This type of applications are already validated and available in financial, shipping, and insurance industries playing a major role in verifying or validating the identity of individual subjects or assets [13, 14].

Meanwhile, a blockchain-based distributed vehicular network architecture for the smart cities was proposed in one of the authors' past studies [15], but in this study, an architectural concept involved in the construction of a secure and reliable distributed transport management system is described together with a proposal of the DistBlock-Net model which is a sort of distributed mesh network architecture for IoT systems based on an SDN and the blockchain technology [16]. A flow rule update approach is used to perform updates securely and check the validity of the flow rule tables applied in the mesh network. Further, the authors' extended work includes a design of a blockchain-based distributed cloud architecture for a scalable IoT network using SDN fog nodes [17]. Bahga et al. [18] proposed a decentralized platform for industrial IoT (IIoT) based on the blockchain technique for removal of a trusted intermediary and construction of a peer-to-peer network, whereas Christidis et al. [19] examined some of the blockchain applications in addition to smart contracts in IoT system. Xia et al. [20] proposed a blockchain-based trustless medical data sharing scheme among the cloud service providers. This scheme is based on a concept of sharing medical data in the cloud and allowing auditing, data provenancing as well as controlling of shared medical data. Meanwhile, a secure energy trading system applicable to IIoT was proposed by Li et al. [21, 22].

In the UN future report, the blockchain was chosen as one of the key technologies of the Fourth Industrial Revolution. Blockchain is a technology that provides security for a public account book; in 2016, the Bank of Korea described it as "the technology that dispersively manages the account book of transaction records loaded on a P2P network" [23–26]. Likewise, US IT research company Gartner has named it one of the promising strategic technologies of the future, and it expects the total value of blockchain-based businesses to reach 10 billion US dollars in 2022 [24]. Although blockchain was initially developed as a technology for storing bitcoins, there were many problems for them to be recognized as normal currency due to the price volatility and anonymity involved in digital currencies [25–28].

For this reason, blockchain technology began to receive attention, and various research projects are being conducted since it is possible to implement a free, secure P2P service based on the agreement between users when blockchain is used as a platform.

The blockchain theory used for the digital currency "bitcoin" is an innovative concept that will be able to ease users' inconvenience and improve security service. The theory makes it almost impossible to forge or tamper with user information and hack the block data. Even if the data have been acquired, they are heavily encrypted. For this reason, the technology based on this theory will be an excellent solution for information leaks [29–33].

Currently, most of the popular browsers on the market are from overseas (e.g., IEs, Chrome, Firefox, Opera, Safari, etc.). Chromium is an open-source browser with good potential for the Korean browser market. This browser offers fast processing capability and supports various operating systems including Android, Windows, Linux, and Mac [34–37].

Recently, the fingerprint authentication API for Android 6.0 Marshmallow has been released, and iOS adopted "Touch ID." In addition, Chinese smartphone manufacturers such as Meizu and Huawei have introduced new products mounted with fingerprint recognition modules, and the number of such smartphones is expected to increase rapidly [38–40].

In 2009, Satoshi Nakamoto published a paper [25], which proposes a solution to prevent the double payment problem using a P2P distributed network-based timestamp server. The solution method in this study started from a timestamp server. The timestamp server collects the block hash of the time-recorded items and widely publishes the hash like a newspaper or Usenet post [41–44]. This timestamp history proves that the data were explicitly present at that time to be included in the hash. Each timestamp history includes timestamps from past transactions and forms a reinforcing chain.

The operation of the network is as follows: Firstly, the new key details are known to all nodes. Secondly, each node collects a new key history into a block. Thirdly, each node performs a process of finding a job proof for the block. Fourthly, when a node successfully performs a proof of operation, it sends the block to all nodes. Fifthly, nodes only approve the block if all transactions are not previously used but valid. Finally, the nodes show intention of approval of that block through the process of generating the next block by using the approved block as a previous hash. Nodes always regard the longest chain as correct and work to continue to expand the chain. If two nodes are to announce the next block of different versions simultaneously, some

Fig. 2 Fingerprint recognition log-in client target system using a smartphone mounted with fingerprint recognition module

nodes will receive one of them first. In this case, each node performs work on the block it received first, but stores it in case other branches of the chain become longer. If a proof of work is generated that is longer on either side of the chain, the length of the chain branch is no longer equal and each node switches its work to a longer chain. It does not need the new transaction history notification to be delivered to all nodes, but if it is delivered to more nodes, it will be included in the block more quickly. Block notifications are also not vulnerable if they are missing. If a node does not receive a block, it will receive the next block and will recognize it as missing and request it again.

Thus, the target system shown in Fig. 2 has been developed to provide better convenience to users. The system allows the user to perform authentication without going through a separate log-in process on a Web page (or application's log-in screen) displayed by the desktop/laptop, smartphone, or IoT device of the current user. In other words, when the user's fingerprint is recognized by the smartphone mounted with a fingerprint recognition module, the authentication packet will be delivered to the user's device.

Figure 3 shows the application principle of the blockchain theory. If the user's personal information such as fingerprint information is leaked due to an attack against the server, there will be a huge problem. In order to prevent such a security problem, the user's private key is used to create a hash value for the fingerprint information, and the value will then be documented in the blockchain, which will be almost impossible to hack. In this case, the fingerprint information and the private key cannot be ascertained by the hash value; even if the information has been leaked, the hacker will not be authenticated if the private key does not match. Moreover, since the hash value documented in the blockchain network will be verified by plenty of computer resources, outside forging/tampering attacks seeking to steal the information are almost impossible.

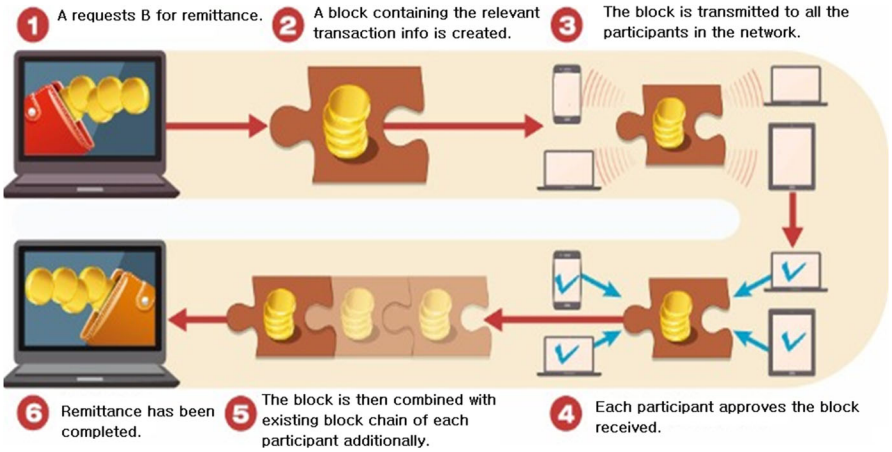

Fig. 3 Application principle of the blockchain theory

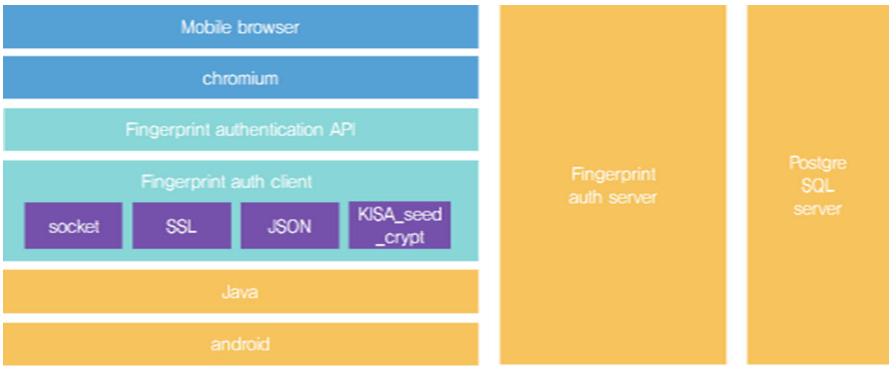

Fig. 4 Mobile user authentication client architecture

3 Design of prevention of forging/tampering attacks and fingerprint information using blockchain theory

3.1 Design of contents

The developed contents are divided into three parts. First is the development of a user authentication client using the mobile fingerprint recognition function. This part has been implemented such that the fingerprint information extracted with a fingerprint authentication API will be encrypted, stored, and decrypted through the Android Keystore System (Fig. 4). Additionally, using the fingerprint information, a mobile Web browser has been developed using Chromium, an open-source Android platform-based Web browser, to perform user authentication for the Web service.

Second is the development of SDK to support fingerprint-based user authentication in both application program and IoT system. This SDK has been implemented to be able to perform fingerprint-based user authentication in both application program

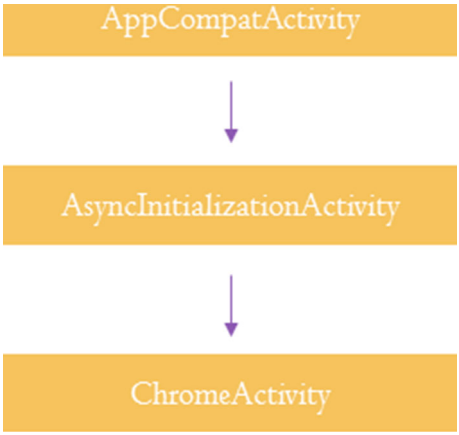

Fig. 5 Activity inheritance structure

and IoT system by opening a communication session in the authentication server to proceed with the user authentication process.

Third is the development of an authentication server using the blockchain theory. Here, the user's fingerprint information and the private key-based hash value are documented in the server by applying the public blockchain theory. A method of uncovering an act of forging/tampering and counteracting it has been designed for implementation as well. The mobile user authentication client has been developed as an independent Chromium-based (open-source) browser. Chromium is built with Android SDK 23 and the GN build system. Fingerprint permission should be registered in the Android_Manifest.xml file to perform fingerprint authentication; for this, an upgrade to Android SDK 24 is necessary, and the program (i.e., BUILD.gn file) should be modified to use the upgraded version. Here, the Java files added or modified to use the GN build system should be registered in the java_source.gni file as well. Additionally, to use an additional library or an external module, the external module should be included in the third-party file so that this module can be built by creating the BUILD.gn file. The inheritance structure of Chromium's main_activity is shown in Fig. 5.

3.2 Design of mobile user fingerprint authentication service architecture

The mobile user fingerprint authentication service always operates in the background to perform mobile fingerprint authentication (Fig. 6). If fingerprint recognition has been performed when other activities are not being executed, the activity that instructs the user to input the password will be executed, followed by another activity that displays the list of PC and IoT devices once the password has been entered. The fingerprint authentication API is supported by the Android Marshmallow version or higher, and fingerprint authentication can be authenticated with this API.

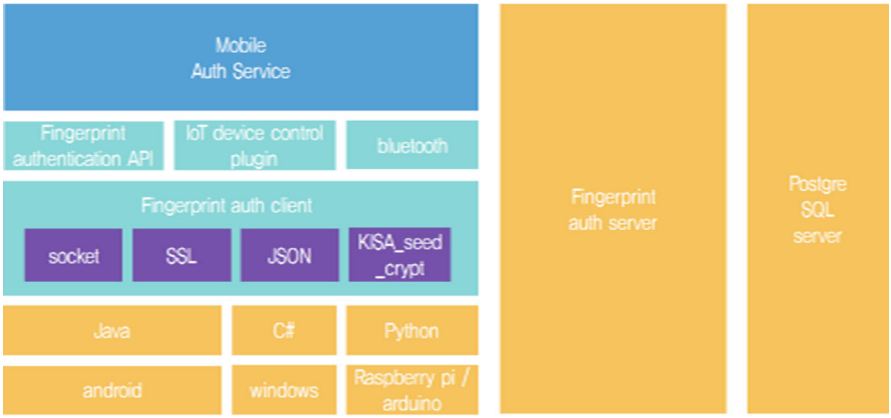

Fig. 6 Architecture of mobile user fingerprint authentication service

3.3 Design of PC and IoT device architecture

In the mobile user fingerprint authentication service, after pressing the PC device to be authenticated, its information will be encrypted and transmitted to the fingerprint auth server along with fingerprint and password information. The fingerprint auth server then proceeds with authentication and opens a communication session with the PC user authentication client through the PC's unique number documented in the block to perform additional authentication. For the IoT device, a similar process is carried out. Once authentication is successfully completed, the service selects the IoT device control plug-in to communicate with the current IoT device and initiate control. This IoT device control plug-in is a self-developed module, and different plug-in modules can be developed for individual IoT devices and registered for the service. In other words, a third-party developer can develop their own plug-in for registration, and it will be able to work with the service. The unique number of an IoT device can be obtained from the IoT device control plug-in, and the number is documented in the blockchain. The selected IoT device and the IoT device control plug-in perform Bluetooth communications between themselves, with the communication protocol to be used to be decided by the former.

3.4 Design of PC user authentication client architecture

The PC user authentication client performs authentication on the Web through the mobile user fingerprint authentication service (Fig. 7). The SSL communications will be carried out between the fingerprint auth client and fingerprint auth server when the latter opens the communication session. Here, the data are exchanged by using JSON-type synchronized communications. The process scenario of the PC user authentication client was composed in order of PC registration, Web site registration, and user authentication.

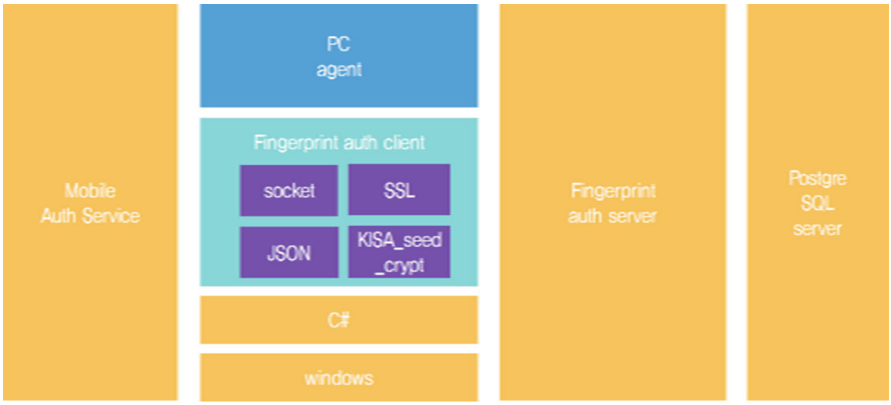

Fig. 7 Architecture of PC user authentication client

3.5 Design of user registration and IoT device control client architecture

A Web site that has completed its registration is allowed to perform user authentication. Once authentication of a user's fingerprint and password is successful at the fingerprint auth server, the relevant block will be located in the blockchain by using the private key, and its contents will be checked. Then, after analyzing the domain, it will find the URL of the user authentication page and open a communication session with the fingerprint auth client module using the unique number of the PC. The fingerprint auth server encrypts the URL and the account information and sends them to the PC user authentication client as JSON data (serialized object). The client then decrypts the data received and delivers the account information to the Web site user authentication page to request authentication. When successful, it will be redirected to the original screen through the client.

The IoT device control client has been developed using Raspberry Pi and Arduino (Fig. 8). Through Bluetooth communications, the process will be carried out in order of mobile user authentication service → fingerprint auth server → mobile user authentication service → IoT device control client. This process is different from the authentication process of the PC user authentication client, which performs authentication service in order of mobile user authentication service → fingerprint auth server → PC user authentication client. For the service, an IoT device control plug-in should be developed to communicate with the client. Such a plug-in should contain a Bluetooth communication protocol and the unique number of the device to communicate with the control client, at the same time following the guidelines of interface and other specifications to connect with the mobile user authentication service.

The unique information of the IoT device control client will be documented in a block when performing Bluetooth pairing initially, and an adequate IoT device control plug-in will then be searched for by using this information after performing user authentication before commencing communications between the IoT device control plug-in and the control client.

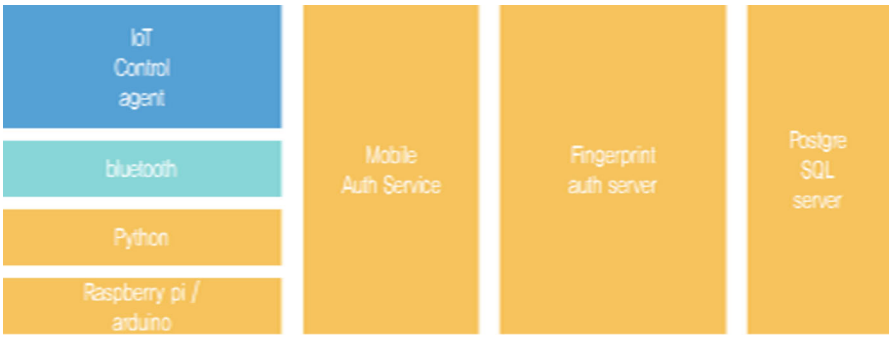

Fig. 8 Architecture of IoT device control client

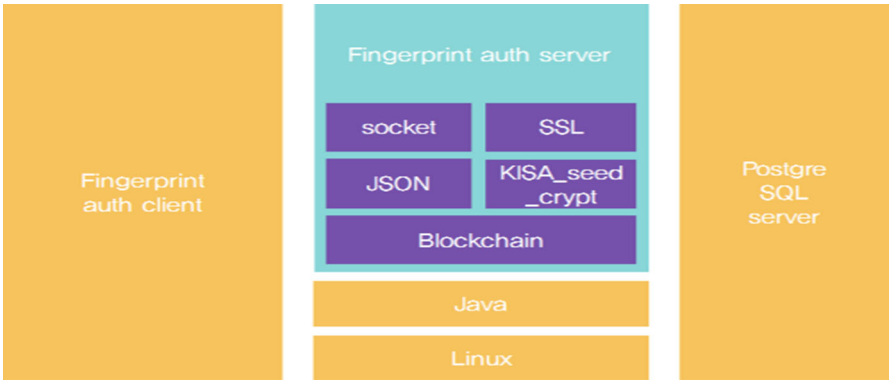

Fig. 9 Architecture of user authentication blockchain server

3.6 Design of user authentication blockchain server and user registration

This server carries out socket communications with the mobile user authentication service, mobile user authentication client, and fingerprint auth client module of the PC user authentication client. The data will be exchanged by assuming a JSON form. The server also performs encryption and SSL communications through the KISA_seed_crypt module.

In order to register a user, a new block should be added in the blockchain. Data such as fingerprint information and private key as well as the hash values of the information related to user authentication are documented in the new block, and proof of work will be performed initially. Proof of work refers to a process carried out by the miner who needs to prove the hash algorithm to create a new block. Once the process is successful, the contents are to be relayed to the entire nodes in the blockchain where the validity of proof of work will be examined. Afterward, the new block is connected to the last block in the blockchain, and the hash values of the previous block will be documented in the new block. Figure 9 shows the architecture of the user authentication blockchain server.

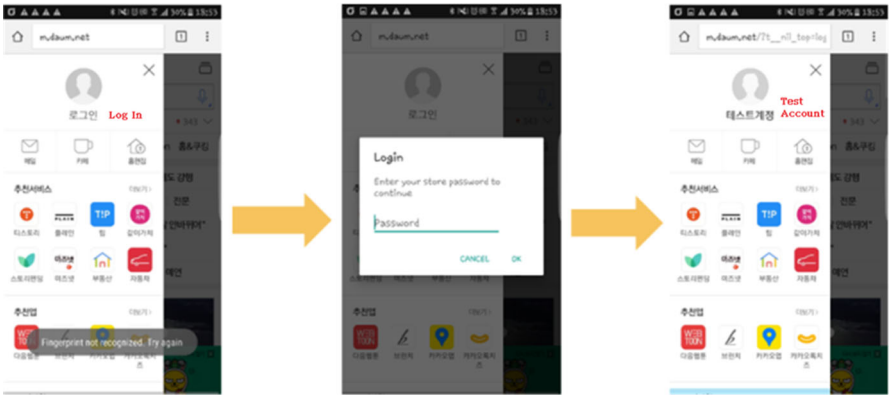

Fig. 10 Screen of mobile user authentication scenario showing the recommendation service, recommending app, and test account

4 Implementation of prevention of forging/tampering attacks and fingerprint information using the blockchain theory

4.1 Implementation of contents

To perform user fingerprint authentication on the Chromium browser, add initialization AddFingerprintActivity that inherits AsyncInitializationActivity and let ChromeActivity inherit it. InitializationAddFingerprintActivity brings up a password input fragment once the fingerprint has been recognized through the mobile fingerprint sensor. After the user inputs his/her password, the password itself, fingerprint information, device information, and domain information are encrypted and transmitted (i.e., SSL communication) to the blockchain server for authentication. The browser then proceeds with authentication and redirects to the page where the user was. Figure 10 shows the screen of the mobile user authentication scenario showing the recommendation service, recommending App, and test account.

4.2 Implementation of service subscription

When executing the mobile user fingerprint authentication service, the user simply needs to subscribe to the service once initially (Fig. 11). Subscription will be completed after entering the user's e-mail address, mobile phone number, and password, all of which will then be compared with the existing data. If the subscription is a new one, the information will be stored in the database.

4.3 Implementation of PC registration

PC registration is performed only once in the beginning to interwork with the mobile user authentication service. When the PC device registration button is pressed, the e-mail address and authentication number registered at the time of service subscription

Fig. 11 Service subscription scenario

will be displayed. The name of the PC in use is then entered together with this pre-registered information, and such information will be transmitted to the fingerprint auth server along with the user's fingerprint information. A relevant block will be looked up in the blockchain, and the data will be documented on that block (Fig. 12).

4.4 Implementation of site registration

To set the user registration method as the fingerprint recognition method, the account information of the relevant service should be documented in the block.

After entering the account information and pressing the registration button at the PC user authentication client, the information will be transmitted to the fingerprint auth server along with the domain information, and they will then be documented in a relevant block where the domain information registered in the database of PostgreSQL server will also be stored together with the device information. In the PC user authentication client, the list of database-registered sites is shown to the user (Fig. 13).

4.5 Implementation of user authentication

Once the data have been received from the mobile user authentication service for user authentication, it will find the relevant block and bring up its contents by using the fingerprint information and private key documented in the block. The contents include the following data: PC device information, ID, password, and domain information for

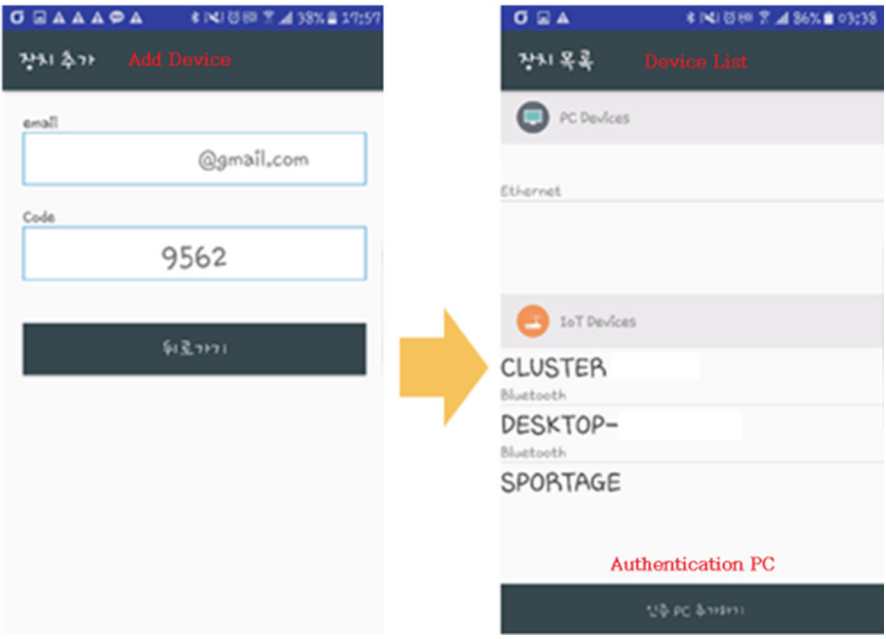

Fig. 12 PC registration scenario

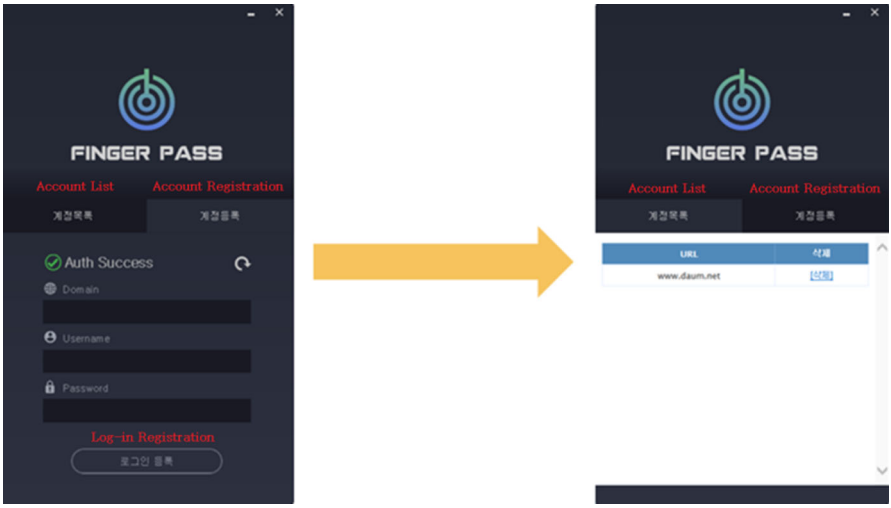

Fig. 13 Site registration scenario

PC user authentication; and IoT device information, unique number of communication, and fingerprint information for user authentication to control IoT devices. After bringing up the contents from the block, the server sends the data for user authentication to the PC user authentication client to authenticate PC users or to the mobile user authentication service to authenticate IoT device users (Fig. 14).

Fig. 14 User authentication screen

5 Conclusion and future work

The existing digital door locks had the problem of opening easily with a stolen PIN number or an electric shock. Thus, in this study, a blockchain-applied integrated log-in platform based on the fingerprint verification technology is proposed and implemented for mobile devices such as smartphones or tablets. As a result of this research, a convenient integrated automatic log-in platform which exhibits a strong security function has been constructed. The contribution of this study is that the proposed blockchain-based platform allows users to utilize the platform in a manner of UI/UX.

This research focused on allowing the users to perform their authentications more conveniently. At the same time, the research concentrated on the authentication methods that will allow safer and better protection of sensitive personal information and biometric data.

Recently, in the ROK, the number of incidents concerning the leakage of personal information has been rapidly increasing in various personal service areas including the banking industry where security is of utmost importance. Despite such a situation, many companies and banks are still reluctant to devise a countermeasure due to additional costs; they simply continue to introduce new services without providing fundamental solutions. Therefore, the authors expect the proposed system to be useful and convenient to the users. The authors also hope that the proposed system will be helpful in devising other automatic log-in platforms that can be used for household safes and other applications. In the authors' future work, the improvement of security levels of the proposed system will be considered by disclosing the source codes online and off-line as an open source through the authors' work. The author expects that this research on the blockchain and its applications will be a platform technology for future computing.

Acknowledgements The first draft of this paper was presented at The International Conference on Big data, IoT, and Cloud Computing (BIC 2017) [45], August 22–24, 2017, Republic of Korea. This work was supported by the National Research Foundation of Korea (NRF) Grant funded by the Korea government (MSIT) (No. 2017R1C1B5077157).

References

1. Schutzer D (2016) CTO corner: what is a Blockchain and why is it important? FSRoundtable. Retrieved from http://fsroundtable.org/cto-corner-what-is-a-blockchainand-why-is-it-important/. Accessed 1 June 2018
2. Kestenbaum R (2017) Why bitcoin is important for your business. Forbes. Retrieved from https://www.forbes.com/sites/richardkestenbaum/2017/03/14/why-bitcoinis-important-for-your-business/3/#2da6d4c72b3b. Accessed 1 June 2018
3. Due.com. (2017) How blockchain improves security and transaction times. Nasdaq. Retrieved from http://www.nasdaq.com/article/how-blockchain-improves-securityand-transaction-times-cm771339. Accessed 1 June 2018
4. Higgins S (2016) Hours after launch, OpenBazaar sees first drug listings. CoinDesk. Retrieved from http://www.coindesk.com/drugs-contraband-openbazaar/. Accessed 1 June 2018
5. Young J (2016) Hackers eye e-commerce platforms, bitcoin-based OpenBazaar to capitalize. The Cointelegraph. Retrieved from https://cointelegraph.com/news/hackerseye-e-commerce-platforms-bitcoin-based-openbazaar-to-capitalize. Accessed 1 June 2018
6. Tech (2017) Kaspersky releases more evidence that North Korea was linked to Bangladesh SWIFT hack. Retrieved from http://tech.firstpost.com/news-analysis/kasperskyreleases-more-evidence-that-north-korea-was-linked-to-bangladesh-swift-hack-370229.html. Accessed 1 June 2018
7. Baker M (2017) Why SWIFT's days are numbered, and what's next. MSPmentor. Retrieved from http://mspmentor.net/technologies/why-swift-s-days-are-numberedand-what-s-next. Accessed 1 June 2018
8. Coward J (2016) Meet the visionary who brought blockchain to the industrial IoT. IOT World News. Retrieved from http://www.iotworldnews.com/author.asp?section_id=495&doc_id=728962. Accessed 1 June 2018
9. Etzioni A (2015) A cyber age privacy doctrine: more coherent, less subjective, and operational. Brooklyn Law Rev 80(4):1263–1265
10. Mayer-Sch€onberger V, Cukier K (2013) Big data: a revolution that will transform how we live, work and think. Houghton Mifflin Harcourt, Boston
11. Kshetri N (2014) Big data's impact on privacy, security and consumer welfare. Telecommun Policy 38:1134–1145
12. Seth S (2017) Banks need to be centralized—could blockchain be the answer? Finance Magnates. http://www.financemagnates.com/cryptocurrency/bloggers/banksneed-centralized-blockchain-answer/. Accessed 1 June 2018
13. Mainelli M (2017) Blockchain will help us prove our identities in a digital world. Harvard Business Review. Retrieved from https://hbr.org/2017/03/blockchain-willhelp-us-prove-our-identities-in-a-digital-world. Accessed 1 June 2018
14. Kshetri N (2017) Blockchain's roles in strengthening cybersecurity and protecting privacy. Telecommun Policy 41:1027–1038
15. Sharma PK, Moon SY, Park JH (2017) Block-VN: a distributed blockchain based vehicular network architecture in smart city. J Inf Process Syst 13(1):184–195
16. Sharma PK et al (2017) DistBlockNet: a distributed blockchains-based secure SDN architecture for IoT networks. IEEE Commun Mag IEEE 55(9):78–85
17. Sharma PK, Chen MY, Park JH (2018) A software defined fog node based distributed blockchain cloud architecture for IoT. IEEE Access 6:115–124
18. Bahga A, Madisetti VK (2016) Blockchain platform for industrial internet of things. J Softw Eng Appl 9(10):533–546
19. Christidis K, Devetsikiotis M (2016) Blockchains and smart contracts for the internet of things. IEEE Access 4:2292–2303
20. Xia Q et al (2017) MeDShare: trust-less medical data sharing among cloud service providers via Blockchain. IEEE Access 5:14757–14767
21. Li Z et al (2017) Consortium blockchain for secure energy trading in industrial internet of things. IEEE Trans Industr Inform 278–307
22. Sharma PK, Park JH (2018) Blockchain based hybrid network architecture for the smart city. Future Gener Comput Syst 1–6
23. Bank of Korea (2016) Development strategy of digital innovation and payment service. In: Bank of Korea Payment and Settlement System Conference, pp 1–4 **(in Korean)**

24. Gartner (2016) Retrieved from http://www.gartner.com/events/na/orlando-symposium/
25. Nakamoto S (2008) Bitcoin: a peer-to-peer electronic cash system, pp 1–9
26. Antonopoulos AM (2014) Mastering bitcoin: unlocking digital cryptocurrencies. O'Reilly Media Inc., Sebastopol, pp 1–73
27. Beverly Y, Garcia-Molina H (2003) PPay: micropayments for peer-to-peer systems. In: Proceedings of the 10th ACM Conference on Computer and Communications Security. ACM, pp 300–310
28. Yoo HW (2016) Implementation and performance improvement plan of blockchain-based electronic ballot system. Graduate School of Information and Communication, Ajou University, Suwon, pp 1–34 **(in Korean)**
29. Kim SH, Yang JY, Kim YJ (2015) A study on the selfish mining of blockchain. In: 2015 Autumn Conference. The Korean Institute of Communications and Information Sciences, pp 1–4 **(in Korean)**
30. Cheon IG (2015) Android programming, easy explanations with pictures. Rev (3). Life and Power Press **(in Korean)**
31. Peters GW, Panayi E, Chapelle A (2015) Trends in crypto-currencies and Blockchain technologies: a monetary theory and regulation perspective. J Financ Perspect 3(3):1–43
32. Gervais A, Karame GO, Wüst K, Glykantzis V, Ritzdorf H, Capkun S (2016) On the security and performance of proof of work blockchains. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. ACM, pp 3–16
33. Underwood S (2016) Blockchain beyond bitcoin. Commun ACM 59(11):15–17
34. Zyskind G, Nathan O (2015) Decentralizing privacy: using blockchain to protect personal data. In: Security and Privacy Workshops (SPW). IEEE, pp 180–184
35. Kiayias A, Koutsoupias E, Kyropoulou M, Tselekounis Y (2016) Blockchain mining games. In: Proceedings of the 2016 ACM Conference on Economics and Computation. ACM, pp 365–382
36. Huh J-H, Seo K (2016) Design and test bed experiments of server operation system using virtualization technology. Hum Centric Comput Inf Sci 6(1):1–21
37. Huh J-H, Otgonchimeg S, Seo K (2016) Advanced metering infrastructure design and test bed experiment using intelligent agents: focusing on the PLC network base technology for smart grid system. J Supercomput 72(5):1862–1877
38. Huh J-H (2017) PLC-based design of monitoring system for ICT-integrated vertical fish farm. Hum Centric Comput Inf Sci 7(20):1–19
39. Moon S-Y, Park J-H (2016) Efficient hardware-based code convertor of a quantum computer. J Converg 7:1–9
40. Nagaraju S, Parthiban L (2015) Trusted framework for online banking in public cloud using multi-factor authentication and privacy protection gateway. J Cloud Comput Adv Syst Appl 4(1):1–23
41. Massias H, Avila XS, Quisquater J-J (1999) Design of a secure timestamping service with minimal trust requirements. In: 20th Symposium on Information Theory in the Benelux, pp 1–8
42. Haber S, Stornetta WS (1991) How to time-stamp a digital document. In: Conference on the Theory and Application of Cryptography. Springer, pp 437–455
43. Bayer D, Haber S, Stornetta WS (1993) Improving the efficiency and reliability of digital time-stamping. Seq II: Methods Commun Secur Comput Sci 329–334
44. Haber S, Stornetta WS (1997) Secure names for bit-strings. In: Proceedings of the 4th ACM Conference on Computer and Communications Security. ACM, pp 28–35
45. Huh J-H, Seo K (2017) Design and implementation of mobile fingerprint recognition and automatic log-in platform framework. BIC 2017:1