International Journal of Advanced Research in Big Data Management System
Vol. 3, No. 2 (2019), pp.15-20
http://dx.doi.org/10.21742/ijarbms.2019.3.2.03

Implementation of Integrated Authentication Service using Blockchain and One Time QR Code for Access Control in U-city Environment

Jai Yong Kim[1], Yong Hoon Jung[2], Dae Seung Yang[3], Moon-Seog Jun[4]

[1,2]Dept of Computer Science, Univ. of Maryland
[3]BaaSLAB
[4]Dept. of Computing in Soongsil University.
[1]raient007@gmail.com, [2] jung7773@naver.com, [3]yds.baasid@gmail.com,
[4]mjun@ssu.ac.kr

Abstract

This paper proposes an integrated user authentication system that can be used for access control in U-city environment. The proposed integrated authentication system issues an EID capable of acting as an electronic ID to a user based on a smartphone, and verifies and verifies the access to a building or a specific space using the issued EID.

Unlike the user authentication using a smart card, it can be used in on / off-line environment because authentication service is provided in web service environment. Based on the issued EID, one-time authentication information is used in the authentication process in the form of One Time QRcode to provide a secure authentication process from security breaches such as retransmission attacks. In addition, the security and security of the network and computing environment have been improved because the user's authentication information is issued and verified in a blockchain-based decentralized system rather than the existing centralized system.

Keywords: *U-city, ICT, User Authentication, SSO, Block Chain*

1. Introduction

With the rapid development of IT technology, IT convergence technology is actively progressing in many places related to various industries and daily life besides the IT field. In particular, the convergence of ICT technology created a new environment called U-city with the development of ubiquitous and IoT. Advanced IT technology has become very involved in people's daily lives, as well as in defense, medical, and industrial fields. "U-city" encompasses new technologies and environments that extend to the urban realm, covering almost every life radius of a person[1][2].

The role of key, a representative tool used for access control, has changed to the form of ID Card and Smart Card using RFID and NFC technology, one of the ICT technologies. In addition, as biometric technology is developed, fingerprints and iris information uniquely possessed by humans are also used as a tool for access control. However, ID Cards and Smart Cards must have a separate tool for authentication, which leads to increased costs for building and maintaining the system, and misuse due to theft and loss. In addition, the authentication method

Article history:
Received (March 12, 2019), Review Result (April 28, 2019), Accepted (November 10, 2019)

Print ISSN: 2208-1674, eISSN: 2208-1682 IJARBMS

using biometric information has a low recognition rate of fingerprints and irises used for authentication.

This paper proposes a blockchain-based integrated authentication system in the U-city environment without a separate authentication tool. Integrated authentication system enables access control and access control using EID issued without separate authentication tool. EID is used for user authentication. EID can be used only once or within a certain time. The EID issued to the user can be used as an integrated ID that can be used on / off-lines

2. Related Work

2.1. Smart Card (Electronic Identification)

Smart cards used as electronic identification cards are mainly used for identification, authentication, and digital signatures, and replace the existing identification information that is used offline, making it more secure and reliable. It can be identified and can be used consistently in an online environment.

Smart Card is a credit card size that has an integrated circuit chip with the ability to handle a specific task by having a microprocessor, card operating system, security module and memory as shown in Figure 1. It's a plastic card. These cards are attracting attention as a representative technology of the information age because of their excellent security and ease of portability, and the characteristics that can be used in daily life such as transportation, health care, identification, distribution, and public complaints.

2.2. Security Protocol of Electronic Identification

The electronic identification card is based on the International Passenger Organization's Basic Access Control (PAC), Passive Authentication (PA), Active Authentication (AA) and EAC (ExtendedAccessControl) is configured based on the standard.

BAC is an access control mechanism that prevents data stored on an electronic identification chip from being illegally read by an attacker and eavesdropping of information transmitted between the identification card and a reading system. PA is a security mechanism that indicates that the information contained in the chip's LogicalDataStructure (LDS) has not been modified. The electronic card issuer applies the encryption method to store information about the chip in the electronic ID card and encrypts the information in the chip through an electronic signature using a hash. AA is a security mechanism that obtains a legitimate electronic identity card and prevents duplication of a chip with the same information and function. AA technology uses a key pair embedded in the chip (Active Authentication Private / Public Key) to verify that the chip has not been duplicated by question-and-answer authentication of the reader and electronic identity card[4][5]. EAC is an access control mechanism that prevents countries without access rights from accessing biometric information, such as fingerprints and irises, stored on electronic identity chips.

3. Integrated Authentication Service using Blockchain and OTP in Web Service Environment

The proposed technique uses the authentication information of users authenticated by a trusted authority, so that it is possible to continuously authenticate users without additional membership or preparation for authentication later.

The organization that checks the user's authentication information and provides the service to the user is called an Onlie Service Provider (OSP). In addition, WegoIT is a system that provides an authentication protocol by first verifying user's personal information and generating authentication information. OSP basically assumes that it performs preliminary authentication process with WegoIT. Users and OSPs will be issued a WegoIT EID through WegoIT, which will enable them to use a secure integrated authentication system.

3.1. System Components

WegoIT Integrated Certification System, which operates on a blockchain basis, consists of WegoIT Core, which creates a Serial Number for the generation of WegoIT EIDs, and WegoIT App, which registers a public key with a blockchain, and creates a pair of public and secret keys for users and provides UI to users.

3.1.1. System Core

WegoIT Core creates Serial Number for WegoIT EID generation and checks the validity of WegoIT EID by preventing serial numbers from being duplicated. WegoIT Core also registers the public key created in the user's WegoIT App on the blockchain and stores and distributes user information in the blockchain through WegoIt core.

3.1.2. WegoIT App

The WegoIT App installed in the user's device creates a key pair using the BIP39 algorithm (mnemonic code), and requests WegoIT Core to create and verify the WegoIT EID QR code. Among the key pairs created by WegoIT App, the public key is registered in the blockchain through WegoIT Core, and WegoIT App encrypts the challenge value sent by WegoIT Core for the public key registration with the private key and sends it along with the public key.

3.2. WegoIT EID Structure and Generationt

3.2.1. WegoIT EID Structure

WegoIT EID is the minimum information to identify an individual. It consists of name, date of birth, email and mobile phone number.

Table 1. WegoIT EID structure

Serial No	Name	Birthday	Issue date	Extension	Result	DS(Digital Signature)

3.2.2. WegoIT EID Generation

In the WegoIT App, the WegoIT EID is represented by a QR code. When a user requests WegoIT EID generation, the user creates an OTP in WegoIT Core, and creates and sends a QR code in combination with WegoIT EID. WegoIT EID values remain unchanged, and OTPs are created and combined with WegoIT EIDs to prevent image capture, forgery, and delegation.

The created WegoIT EID is registered in the blockchain, and the block information is as follows. The information registered in the blockchain is used to reissue WegoIT EID.

Table 2. WegoIT EID block information

Serial No	WegoIT EID	E-mail	Phone No

3.2.3. QR code Generation

For WegoIT EID verification, OTP must be separated from WegoIT Core. The OTP separation method is as follows. The OTP is inserted at the specific location of the WegoIT EID value, and the inserted location can be confirmed only in the WegoIT Core.

The position where the OTP value is added is the position where the OTP two digits are added to the WegoIT EID and the added value. If it is 63 or more, one digit becomes the position value and the added value.

3.3. WegoIT EID Issue and Authentication

3.3.1. WegoIT EID Issue

First-time users, OSPs, and BSPs can only issue WegoIT EIDs through WegoIT, and OSPs and BSPs cannot OSPs and BSPs can only issue WegoIT EIDs in consultation with WegoIT. Authorized OSPs and BSPs can issue WegoIT EIDs, but verification can only be done through the WegoIT Core.

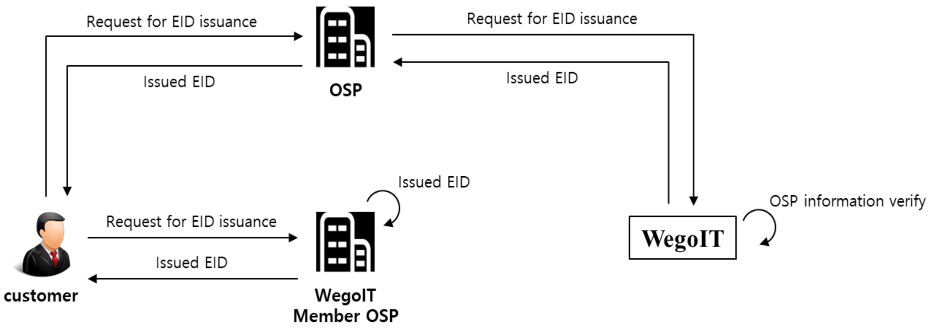

Figure 1. WegoIT EID issuance procedure

WegoIT EID issuance procedure is as follows.

First-time users, OSPs, and BSPs apply for WegoIT EID issuance through WegoIT or WegoIT members (OSP, BPS). The WegoIT or WegoIT member (OSP, BPS) determines whether to create the WegoIT EID after checking the user's information, OSP and BSP information, and determines the creation and rejection of the creation according to the decision.Generating rejection messages or created WegoIT EIDs are passed to users, OSPs, and BSPs. Users can manage WegoIT EID through WegoIT App, and OSP, BSP are available equipment, such as servers or security token.

3.3.2. Using WegoIT EID

WegoIT EID will be an online integrated ID card that can be used on all Web sites without a separate membership. WegoIT EID is used only to prove users when logging in to a web page. Identification purposes using WegoIT EIDs online and offline, for example, resident registration cards, driver's licenses and passports, cannot be used.

Online service provider customers may have members, non-members and WegoIT members. When a member and a WegoIT member log in to OSP or BSP, they can log in by presenting their existing login method or WegoIT E Non-members can use the service only when they register with OSP and BSP separately or apply for issuance of WegoIT EIDs.

To use OSP and BSP services without membership, WegoIT EID is delivered when a login request is made. OSP and BSP request verification of user WegoIT EID to WegoIT Core. If OSP and BSP use WegoIT service, WegoIT EID can be verified. When the user sends the WegoIT EID to OSP and BSP, the user is sent with an electronic signature.

1) Request for service use (WegoIT EID transmission)
2) WegoIT member OSP requests self-verification or WegoITid Core to verify WegoIT EID
3) Communicate the results of verification of WegoIT member OSP or WegoIT Core
4) login complete

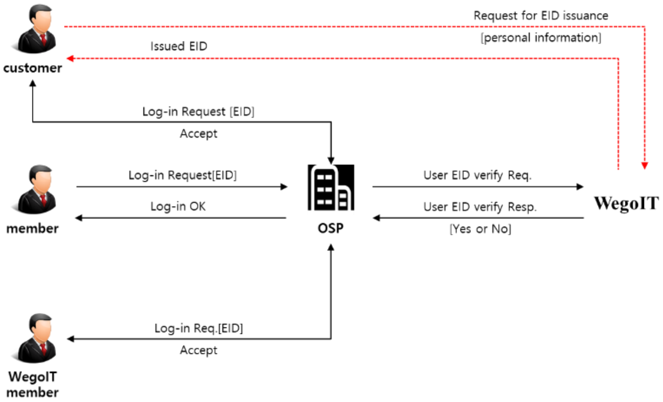

Figure 2. Using WegoIT EID : In case of Member or WegoIT member OSP

4. Conclusion

Blockchain technology works on the basis of decentralized processing and storage that is decentralized from the existing centralized computing environment. Since its inception as a base technology for e-money, utilization in the financial sector and various areas is actively studied and used in many areas. As computing environments change, user authentication technology that identifies users and give them legitimate rights is also changing.

In the web-service environment proposed by this thesis, an integrated authentication system using block chain and OTP provides an environment for safe and convenient user authentication by multiple agencies using a single user information based on the block-chain environment. Since the user's information is stored in a distributed node, not in a centralized system, and authentication systems are provided for various institutions providing diverse services using a single personal information, the risk of hacking and personal information leakage in the existing environment was eliminated. Users can use a variety of online services provided by WegoIT Member OSPs without separate membership procedures, once they receive the WegoIT EID through the proposed system. WegoIT EID authentication information used in the process of obtaining authentication from WegoIT Member OSP has advantages such as Packet Sniffing and Replay Attck because it is one-time information in the form of QR code combined with OTP.

References

[1] Caragliu A and Del Bo C, “Smart cities in Europe,” 「Series Research Memoranda」, Dept. of Economics and Business administration and Econometrics, Amsterdam Univ, (**2009**).

[2] Del Bo C and Florio M, “Infrastructure and growth in the European Union: an empirical analysis at the regional level in a spatial framework,” Departmental Working Papers, No.37, Dept. of Economics, Milan Univ, **(2008)**.

[3] Jun-Cheol Park. “A Secure Single Sign-On Scheme across Multiple Allied Websites using Smartphones”. Journal of Security Engineering, Vol.14, No.3, pp.189-204. (**2017)**.

[4] NIST. "FIPS Publication186-1: Digital Signature Standard (DS-S)" . November (**2008)**

[5] NIST."Interfaces for Personal Identity Verification ". Special Publication800-73-3, **(2010)**

[6] Rob Philpott, Sampath Srinivas, John Kemp, UAF Architectural Overview. Version v1.0-rd-20140209, FIDO Alliance, February **(2014)**.

[7] Sampath Srinivas, Dirk Balfanz, Eric Tiffany, Universal 2nd Factor(U2F) Overview. Versionv 1.0-rd-20140209, FIDOAlliance, February **(2014)**.

[8] Security Technology Research Team, “Comparison of Changes and Characteristics of Identity Information Management Types”, Security Research Department, Financial Security Agency, **(2017)**.03

[9] Kim, Chul-Jin, “An Online Voting System based on Ethereum Block-Chain for Enhancing Reliability”. Journal of the Korea Academia-Industrial, Vol.19, No.4, pp.563-570. **(2018)**. [DOI: 10.5762/KAIS.2018.19.4.563]

[10] Seon-Keun Lee. “A Study on Lightweight Block Cryptographic Algorithm Applicable to IoT Environment”. Journal of the Korea Academia-Industrial, Vol.19, No.3, pp.1-7. **(2018)**. [DOI: 10.5762/KAIS.2018.19.3.1]

[11] Yong-Joon Lee, Taeyeol Jeon, “A Finger print Authentication Model of ERM System using Private Key Escrow Management Server”. Journal of the Korea Academia-Industrial, Vol.20, No.6, pp.1-8. **(2019)**. [DOI: 10.5762/KAIS.2019.20.6.1]

[12] Jae-Wook Heo, Jeong-Ho Kim, Moon-Seog Jun., “Design and Implementation of Blockchain Network Based on Domain Name System”. Journal of the Korea Academia-Industrial, Vol.20, No.5, pp.36-46. **(2019)**. [DOI: 10.5762/KAIS.2019.20.5.36]

[13] Sang Guk Moon, Min Sun Kim, Hyun Joo Kim. “Design of an Integrated University Information Service Model Based on Block Chain”. Journal of the Korea Academia-Industrial, Vol.20, No.2, pp.43-50. **(2019)** [DOI: 10.5762/KAIS.2019.20.2.43]

Authors

Jai Yong Kim
Feb. 2010 : Dept of Computer Science, Univ. of Maryland. (M.S.)
UniHubLAB

Yong Hoon Jung
Feb. 2010 : Dept of Computer Science, Univ. of Maryland. (Ph.D)

Dae Seung Yang
BaaSLAB

Moon-Seog Jun
Feb. 1980 : Dept of Computer Science, Soongsil Univ. (B.S.)
Feb. 1986 : Dept of Computer Science, Univ. of Maryland. (M.S.)
Feb. 1989 : Dept of Computer Science, Univ. of Maryland. (Ph.D)
Mar. 1991 ~ current: Professor with Dept. of Computing in Soongsil University.