IEICE TRANS. INF. & SYST., VOL.E102–D, NO.9 SEPTEMBER 2019

LETTER *Special Section on Log Data Usage Technology and Office Information Systems*

Authentication Scheme Using Pre-Registered Information on Blockchain

Toshiki TSUCHIDA[†a)], ***Student Member***, **Makoto TAKITA**[†], ***Member***, **Yoshiaki SHIRAISHI**[†b)], **Masami MOHRI**[††], ***Senior Members***, **Yasuhiro TAKANO**[†], ***Member***, ***and*** **Masakatu MORII**[†], ***Fellow***

SUMMARY In the context of Cyber-Physical System (CPS), analyzing the real world data accumulated in cyberspace would improve the efficiency and productivity of various social systems. Towards establishing data-driven society, it is desired to share data safely and smoothly among multiple services. In this paper, we propose a scheme that services authenticate users using information registered on a blockchain. We show that the proposed scheme has resistance to tampering and a spoofing attack.

key words: *blockchain, authentication, Internet of Things, pseudo-random function, service cooperation*

1. Introduction

There is a trend to make products evolve with Cyber-Physical System (CPS) that combines real space and cyberspace. In the context of CPS, analyzing the real world data accumulated in cyberspace would improve the efficiency and productivity of various social systems. CPS requires a large amount of real space data for good analysis. Therefore, IoT devices are attracting attention. As the Internet of Things (IoT) industry develops, the number of IoT devices is increasing and the devices are expected to collect more data. By providing IoT services to the whole society, we can obtain big data, but it is difficult to provide the services by an independent organization. Conversely, if different organizations collaborate, a lot of data will be gathered. On the other hand, from the viewpoint of security, there is a risk of data tamper after the data is sent from the IoT devices to the database in the cloud.

The blockchain is one of the Distributed Ledger Technology (DLT) as firstly introduced in [1]. The blockchain is a system that registers information such as transactions in a ledger called a *block*. The transparency of the ledger is maintained by sharing it in all participating nodes. When generating a new block, all participating nodes perform a consensus building (such as Proof of Work (PoW) [2] and PBFT [3]) by verifying the generated block. From the above reasons, it is difficult to rewrite the data registered on the blockchain.

Secure data sharing can be among multiple organizations by registered data from the IoT devices on the same blockchain platform. Besides, in order to trust a data, services want to authenticate a user who provides a data and confirm an owner of the IoT device. In general, when services authenticate a user, the server needs to store the authentication information to verify. If authentication related data is registered on the blockchain, each service need not have the data for verification.

System architectures that include authentication using blockchain have been proposed in [4], [5]. In these systems, the authentication algorithm, the verification algorithm, and the authentication information performed on the blockchain are not provided, so a suitable authentication scheme for the purpose of the system can be applied.

In this paper, we propose an authentication scheme with the following two features; One is that the service need not have authentication information of the user. The other is that the service can authenticate the user at multiple times.

2. Proposed Scheme

2.1 System Model

The system model consists of a user, a service, and a blockchain (Fig. 1). First, the user registers his/her authentication information on the blockchain. The service verifies the user with the registered information on the blockchain and the secret information sent from the user.

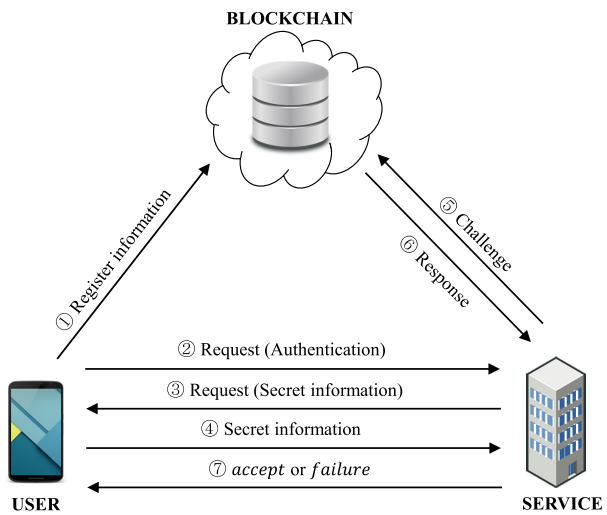

Fig. 1 System model.

Manuscript received November 12, 2018.
Manuscript publicized June 21, 2019.
[†]The authors are with Kobe University, Kobe-shi, 657–8501 Japan.
[††]The author is with Gifu University, Gifu-shi, 501–1193 Japan.
a) E-mail: tsuchida.t@stu.kobe-u.ac.jp
b) E-mail: zenmei@port.kobe-u.ac.jp
DOI: 10.1587/transinf.2018OFL0005

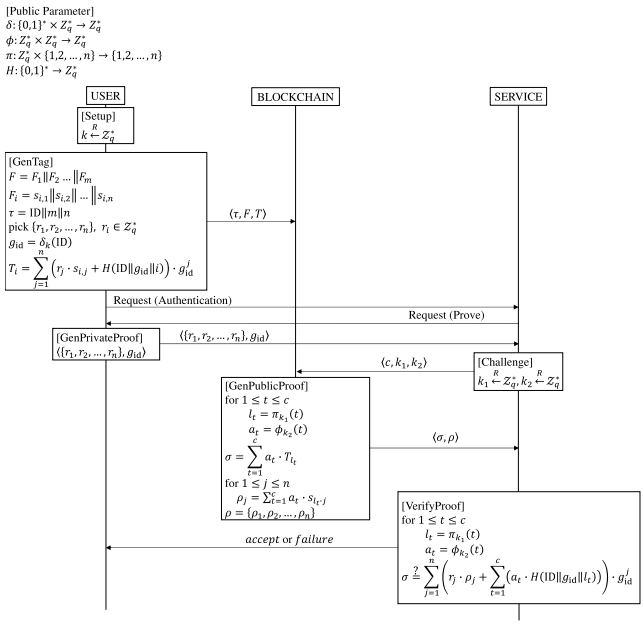

Fig. 2 Flow of our scheme.

We assume the following entities in our scheme.

User: register his/her authentication information on the blockchain and have a secure and private communication link to the service.

Service: verify the user who requests authentication. Verify with the registered information on the blockchain and the secret information sent from the user. The service uses the information only to verify the applicable user.

Blockchain: generate the contract correctly.

Our scheme satisfies the following requirements.

(1) The service need not have the user's authentication information.

(2) The service can authenticate the user at multiple times.

2.2 Algorithms

The following symbols are used in our scheme.

Z_q^*: a multiplicative group of order qth.

$\delta\colon \{0,1\}^* \times Z_q^* \to Z_q^*$: a pseudo-random function.

$\phi\colon Z_q^* \times Z_q^* \to Z_q^*$: a pseudo-random function.

$\pi\colon Z_q^* \times \{1,2,\ldots,n\} \to \{1,2,\ldots,n\}$: a pseudo-random permutation.

$H\colon \{0,1\}^* \to Z_q^*$: a hash function.

ID: identifier.

k: secret key.

$a \overset{R}{\leftarrow} A$: choose a from A at random.

$A\|B$: concatenation of A and B.

Our scheme has six algorithms (Setup, GenTag, Challenge, GenPublicProof, GenPrivateProof, and VerifyProof). The details of them are shown below. The overall flow is as shown in Fig. 2.

Setup: the user generates a secret key $k \overset{R}{\leftarrow} Z_q^*$.

GenTag: the user splits given file F into m blocks and divides each block into n sectors.

$$F = F_1\|F_2\|\cdots\|F_m,$$
$$F_i = s_{i,1}\|s_{i,2}\|\cdots\|s_{i,n}.$$

Next, the user generates τ, picks n random values, and calculates the tag T_i of F_i.

$$\tau = \mathrm{ID}\|m\|n.$$

Choose $\{r_1, r_2, \ldots, r_n\} \in Z_q^*$,

$$g_{\mathrm{id}} = \delta_k(\mathrm{ID}),$$
$$T_i = \sum_{j=1}^{n}(r_j \cdot s_{i,j} + H(\mathrm{ID}\|g_{\mathrm{id}}\|i)) \cdot g_{\mathrm{id}}^j.$$

The user registers $\langle \tau, F, T\rangle$ on the blockchain, where $T = \{T_1, T_2, \ldots, T_m\}$.

Challenge: the service determines the number of blocks and two random values.

Choose c $(1 \le c \le m)$,

$$k_1 \overset{R}{\leftarrow} Z_q^*, \quad k_2 \overset{R}{\leftarrow} Z_q^*.$$

The service sends $\langle c, k_1, k_2\rangle$ to the blockchain.

GenPublicProof: upon receiving the challenge from the service, the blockchain performs the following calculation.

For $1 \le t \le c$,

$$l_t = \pi_{k_1}(t), \quad a_t = \phi_{k_2}(t).$$

$$\sigma = \sum_{t=1}^{c} a_t \cdot T_{l_t},$$

For $1 \le j \le n$,

$$\rho_j = \sum_{t=1}^{c} a_t \cdot s_{l_t,j}.$$

The blockchain sends $\langle \sigma, \rho\rangle$ to the service, where $\rho = \{\rho_1, \rho_2, \ldots, \rho_n\}$.

GenPrivateProof: the user sends his/her secret information $\langle \{r_1, r_2, \ldots, r_n\}, g_{\mathrm{id}}\rangle$ to the service. If an adversary obtains this information, there is a threat of a spoofing attack, so the user should send this information by the encrypted communication.

VerifyProof: upon receiving the response according to the challenge, the service performs the following calculate.

For $1 \le t \le c$,

$$l_t = \pi_{k_1}(t), \quad a_t = \phi_{k_2}(t),$$
$$\sigma' = \sum_{j=1}^{n}\left(r_j \cdot \rho_j + \sum_{t=1}^{c} a_t \cdot H(\mathrm{ID}\|g_{\mathrm{id}}\|l_t)\right) \cdot g_{\mathrm{id}}^j.$$

If $\sigma = \sigma'$ holds, the user passes the verification and the server sends *accept* to the user. Otherwise, the user fails the verification and the server sends *failure* to the

user.

In authentication algorithm, we should not send the same challenge. So, in the challenge algorithm of our scheme, we need to select k_1, k_2, and c without overlapping. Therefore, the service can authenticate the user with the information corresponding to the challenge at $\varphi(q) \times \varphi(q) \times m$ times, where φ is an Euler function.

3. Correctness and Security

3.1 Correctness

The correctness of our scheme is elaborated as follows.

$$\begin{aligned}
\sigma &= \sum_{t=1}^{c} a_t \cdot T_{l_t} \\
&= \sum_{t=1}^{c} a_t \cdot \sum_{j=1}^{n} (r_j \cdot s_{l_t,j} + H(\mathrm{ID}\|g_{\mathrm{id}}\|l_t)) \cdot g_{\mathrm{id}}^j \\
&= \sum_{j=1}^{n} \sum_{t=1}^{c} a_t (r_j \cdot s_{l_t,j} + H(\mathrm{ID}\|g_{\mathrm{id}}\|l_t)) \cdot g_{\mathrm{id}}^j \\
&= \sum_{j=1}^{n} \left(\sum_{t=1}^{c} a_t \cdot r_j \cdot s_{l_t,j} + \sum_{t=1}^{c} a_t \cdot H(\mathrm{ID}\|g_{\mathrm{id}}\|l_t) \right) \cdot g_{\mathrm{id}}^j \\
&= \sum_{j=1}^{n} \left(r_j \cdot \rho_j + \sum_{t=1}^{c} (a_t \cdot H(\mathrm{ID}\|g_{\mathrm{id}}\|l_t)) \right) \cdot g_{\mathrm{id}}^j.
\end{aligned}$$

From the above, if the blockchain correctly generates the signature and the user gives the correct secret information, it passes the verification.

3.2 Security

The registered information on the blockchain is open to all participating nodes and it is difficult to tamper. Therefore, unless the secret information to verify can be reconstructed from the information registered on the blockchain, the user who passes the verification is a legitimate user. We assume the following conditions as an adversary model.

- Not registered, but try to pass the authentication.
- Try to retrieve the secret information to verify from the information registered on the blockchain.

Theorem 1. *If the pseudo-random function is secure, then there exists no adversary to break our scheme with non-negligible probability.*

The information registered on the blockchain is (F, T). An adversary tries to retrieve the secret information for verification $\langle \{r_1, \ldots, r_n\}, g_{\mathrm{id}} \rangle$ from (F, T). T is the tag of F and consists of random value r, s which is a part of F, identifier ID, and g_{id}.

$$T_i = \sum_{j=1}^{n} (r_j \cdot s_{i,j} + H(\mathrm{ID}\|g_{\mathrm{id}}\|i)) \cdot g_{\mathrm{id}}^j$$

Focus on $(r_j \cdot s_{i,j} + H(\mathrm{ID}\|g_{\mathrm{id}}\|i))$. $s_{i,j}$ is masked by the random value r_j. $H(\mathrm{ID}\|g_{\mathrm{id}}\|i)$ is the hash value of ID, g_{id}, and i. Since ID is retrieved from τ and i is index number, the adversary can obtain these values. However, g_{id} is the output of the pseudo-random function whose inputs are secret key k and ID. So, if the pseudo-random function is secure, an adversary cannot obtain g_{id}. Therefore, since we use a cryptographic hash function, an adversary cannot obtain the value $H(\mathrm{ID}\|g_{\mathrm{id}}\|i)$. Accordingly, $(r_j \cdot s_{i,j} + H(\mathrm{ID}\|g_{\mathrm{id}}\|i))$ is like a random value for the adversary. In T_i, g_{id}^j is masked by $(r_j \cdot s_{i,j} + H(\mathrm{ID}\|g_{\mathrm{id}}\|i))$. Hence, an adversary cannot retrieve g_{id}^j from T_i. From above reasons, if the pseudo-random function is secure, the adversary cannot obtain secret information for verification $\langle \{r_1, \ldots, r_n\}, g_{\mathrm{id}} \rangle$ and it is impossible to perform spoofing attack to our scheme. Therefore, the user's authentication information registered on the blockchain is secure, and the service can authenticate the user using it. So, when the service wants to authenticate the user, the service need not have the user's authentication information.

4. Conclusion

In this paper, we proposed the scheme that services authenticate users using authentication information registered on the blockchain. In our scheme, the service verifies by using the registered information on the blockchain and secret information received from the user. The service performs this operation without authentication information of the user as described in Sect. 2.2. Also, the service can authenticate the user at multiple times as described in Sect. 2.2. We informally showed that it is impossible to perform a spoofing attack on our scheme if the pseudo-random function using in our scheme is secure.

Acknowledgments

This study was supported by JSPS KAKENHI Grant Number 16K00184, 18K04133.

References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," http://www.bitcoin.org/bitcoin.pdf, 2008.
[2] C. Dwork and M. Naor, "Pricing via processing or combatting junk mail," CRYPTO '92, Lecture Notes in Computer Science, vol.740, pp.139–147, Springer, Berlin, Heidelberg, 1992.
[3] M. Castro and B. Liskov, "Practical Byzantine fault tolerance," Symposium on Operating Systems Design and Implementation, New Orleans, USA, pp.173–186, Feb. 1999.
[4] Y. Ezawa, M. Takita, Y. Shiraishi, Y. Takano, M. Mohri, and M. Morii, "Design and implementation of authentication and authorization system with blockchain," Computer Security Symposium 2018, Nagano, Japan, pp.842–849, Oct. 2018. (in Japanese)
[5] H. Yang, H. Zheng, J. Zhang, Y. Wu, Y. Lee, and Y. Ji, "Blockchain-based trusted authentication in cloud radio over fiber network for 5G," 16th International Conference on Optical Communications and Networks, Wuzhen, China, pp.1–3, Aug. 2017.