Journal of Engineering and Applied Sciences 13 (3): 771-775, 2018
ISSN: 1816-949X

Sharing the Attribute Information based on Blockchain

[1]Tae-Kyung Kim and [2]Jang-Mook Kang
[1]Department of Internet Security Engineering as a Service, MyongJi College, Seoul, Korea
[2]Department of Big Data Industry Security, Namseoul University, Cheonan, Korea

Abstract: A blockchain is a digitized, decentralized, public ledger of all cryptocurrency transactions. These days, many companies in several sectors are adopting blockchain technology. Because it is considered as a functional technology for improving existing technologies. In this study, we have presented a sharing the attribute information based on blockchain which can support the enhanced authentication service in a secure and transparent way.

Key words: Blockchain, authentication, attribute, identity management, decentralized, public ledger

INTRODUCTION

As more and more devices are connected, the interactions between the devices are increasing even more. The security of these interactions is essential and authentication is an important factor of security on the internet. Authentication means a mechanism that verifies the identities of interacting entities. Also, the need for more secure and transparent authentication service is increasing. In this study, we suggest the authentication model which shares the attribute information based on blockchain which can support the authentication service in a secure and transparent way.

A blockchain is a digitized, decentralized, public ledger of all cryptocurrency transactions. Constantly growing as blocks (the most recent transactions) are recorded and added to it in chronological order, it allows market participants to keep track of digital currency transactions without central record keeping. Each node (a computer connected to the network) gets a copy of the blockchain which is downloaded automatically. Blockchain technology has attracted tremendous interest from wide range of stakeholders including finance, healthcare, utilities, real estate and government agencies. Blockchain networks utilize a shared, distributed and fault tolerant ledger platform that every participant in the network can share but no entity can control (Tosh *et al*., 2017).

Many companies in several sectors are adopting blockchain technology. The blockchain idea can now be applied to any need for a trustworthy record. For example, as a system of record the blockchain can be used. Cryptographic keys in the hands of individuals allow for new ownership rights and a basis to form interesting digital relationships. Because it is not based on accounts and permissions associated with accounts because it is a push transaction and because ownership of private keys is ownership of the digital asset, this places a new and secure way to manage identity in the digital world that avoids exposing users to sharing too much vulnerable personal information. Blockchain technology enables entities independent of each other to rely on the same shared, secure and auditable source of information in a way that fits well with a system of wide spread digital identity.

Preliminaries

Blockchain: A blockchain is a decentralized, distributed and public digital ledger that is used to record transactions across many computers so that the record cannot be altered retroactively without the alteration of all subsequent blocks and the collusion of the network. The blockchain has following common elements (Lee, 2017).

Replicated ledger: A distributed ledger is a consensus of replicated, shared and synchronized digital data geographically spread across multiple sites, countries or institutions. There is no central administrator or centralized data storage. The blocks are distributed and replicated among the blockchain nodes.

Cryptography: Integrity of all transactions shared among the blockchain nodes is supported with digital signatures and specialized data structures (e.g., hash-based data structure called Merkle tree (Merkle, 1987). Authenticity of transactions is supported with digital signatures. Privacy of transactions is also, supported with anonymous addresses for transaction.

Consensus: Transactions that are exchanged among the blockchain nodes over the internet need to be validated

Corresponding Author: Tae-Kyung Kim, Department of Internet Security Engineering as a Service, MyongJi College, Seoul, Korea

before adding to the existing blocks. A consensus among the blockchain nodes is required for the validation. For a public blockchain, a representative consensus algorithm is Proof-of-study (PoW) (Nakamoto, 2008) which is used by Bitcoin. Practical Byzantine Fault Tolerance (PBFT) (Castro and Liskov, 2002; Clement *et al*., 2009) is a representative consensus algorithm used by Hyper Ledger Fabric (Cachin, 2016) for a private blockchain.

Peer-to-peer networking: All transactions are shared without a centralized control actor over the internet. In other words, the blockchain nodes are connected through a peer-to-peer network over the internet, not through the client-server model, due to no trust entity involvement.

Blockchain technology also has some weakness. Every node runs the blockchain to maintain consensus across the blockchain. This gives extreme levels of fault tolerance, ensures zero downtime and makes data stored on the blockchain forever unchangeable and censorship-resistant. But all this is wasteful as each node repeats a task to reach consensus burning electricity and time on the way. This makes computation far slower and more expensive than on a traditional single computer. The blockchain ensures a strong degree of security for its chain but the risk of managing private keys exists. The private keys are used to prove ownership of a certain asset or data in the blockchain but those keys could be lost or stolen by attackers. Another issue is block size.

Each transaction or block added to the chain increases the size of the database. As every node must maintain the chain to run, the computing requirements increase with each use. Network performance is also considered. The transactions per sec is one of major performance factors that most of the blockchain implementations is trying to improve. As transactions need to be broadcasted to blockchain nodes connected through a peer-to-peer network, the network could be easily congested (Lee, 2017).

Attribute aggregation model: Many of the internet services require that the user must prove their identities before accessing the services. With the propagation of various internet services, personal authentication has been requested in various ways. Recently, entity authentication using the aggregated attributes has been studied. Attribute aggregations is the mechanism of collecting attributes of an entity retrieved from multiple identity service providers (Table 1).

There are 7 types of attribute aggregation models. These models are classified into 7 types Sadek (Ferdous and Poet, 2013; Klingenstein, 2007; Chadwick and Inman, 2009; Kim, 2017).

Identity management service should be provided from the service provider. As the number of internet services increases, attribute aggregation-based authentication is suggested as one of the solutions to improve the security

Table 1: Types of attribute aggregation models

Models	Description
Application database model	Simplest form of attribute aggregation model Service provider might store user attributes such as a local identifier, group membership, etc. Local attributes can be retrieved later using this mapping to determine if the user is authorized to access a service
SP (Service Provider)-mediated model	SP allows the user to aggregate attributes from multiple IDPs (Identity Providers) in a single session User is forwarded to different IDPs one after another where the user is authenticated separately and returns to the SP with the IDP-supplied attributes The user is forwarded to different IDPs one after another where the user is authenticated separately and returns to the SP with the IDP-supplied attributes
Linking service model	Combination of the linking and identity relay model Consists of a special type of SP called the Linking Service which is used by the user using a LS-supplied identifier Identifier is used to link different IDPs
Identity federation/linking model	IDPs allow the user to create a pair-wise link between two IDPs To create the link, the user has to visit and authenticate to the first IDP The first IDP will ask the user if she wants to federate this IDP with another IDP If chosen, the user will be asked to federate the second IDP with the first one
Identity proxying model	SP allows a user to aggregate attributes from multiple IDPs using a highly trusted IDP The user is forwarded to the trusted IDP at first and then the trusted IDP forwards the user to other multiple IDPs After the user is authenticated separately at each IDP, the user returns back to the trusted IDP with an assertion including attributes
Identity relay model	Generalized case of the proxying model Identity relay model use intermediary IDP (or relay IDP) instead of a trusted IDP User attribute information is forwarded to the relay IDP at first and then the relay IDP forwards the user to other multiple IDPs
Client-mediated model	The functionality of the relay IDP has been replaced by an intelligent user agent or application that has the capability to aggregate attributes from different IDPs SP informs the client about the IDPs that it trusts Client forwards the user to each of these IDPs After respective authentication at each IDP, the client receives assertions from all IDPs and present the combined set of assertions to the SP

of authentication. However, in the attribute aggregation models, the security of a third party is important. Therefore, we would like to enhance the security of third party using the blockchain technology.

MATERIALS AND METHODS

Proposed blockchain based sharing the attribute

Overview: Sharing the attribute information based on blockchain is designed for providing enhanced authentication service. The involved four entities are as follows (Fig. 1).

Blockchain based third party: It is the third party that connect the different ID providers and provide transparency to each ID provider's attribute information.

- ID provider: it is the ID provider to its service provider
- Service provider: it normally has a service offering users
- User: it is a user registered or not to the service provider

The user wants to use a service offered by service provider. The blockchain based third party maintains the private blockchain. The service provider has access to the third party blockchain but only a read permission, not a write permission. The third party writes a ID provider's ID, ID provider's public key, etc. The service provider reads the user's ID and password from its own ID provider when the user requests to access its service with the ID. The ID provider access the third party to check the same ID which is in other ID provider. If the same, ID exist in the other ID providers, the own ID provider begins the mutual authentication procedure for the accessing the attribute information of the user. If the ID provider needs other information of the user, it would be possible to request the extra information from the other ID provider.

Procedures

User registration: The user registers his ID and password to the service provider and the ID should be uniquely generated.

Virtual ID creation: The ID provider which in the service provider, create virtual ID. The rule for generating virtual ID can use the cryptographic hash function.

Third party blockchain registration: The ID provider creates a pair of private key and public key. The ID provider's public key and user's virtual ID are securely transferred from the ID provider to the third party. Also, a secure channel between the ID provider and the third party is assumed. The third party creates a digital signature over ID provider's public key and virtual ID using its own private key. The third party then registers ID provider's public key and virtual ID with the created digital signature in the third party blockchain. This registration is performed as a blockchain transaction that is broadcasted to third party blockchain nodes. The registration is then stored at the third party blockchain.

Mutual authentication: When the user wants to access a service offered by service provider, the user only log in the service provider, then the ID provider in the service provider checks the user's virtual ID if it exists on the

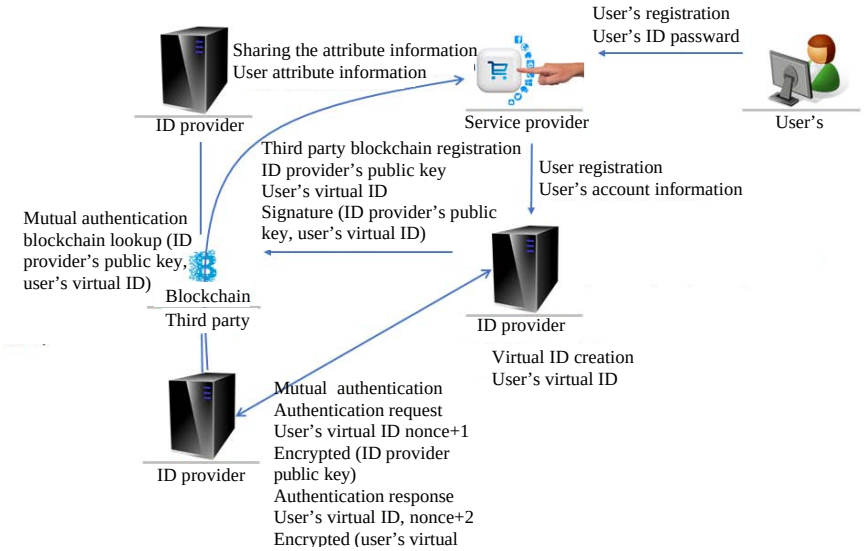

Fig. 1: Procedures for blockchain based sharing the attribute

records of the third party blockchain. If existed, using the information in third party blockchain, the ID provider performs mutual authentication with other ID providers.

Sharing the attribute information of user: The ID provider may request the other ID providers some attribute information required for enhance user authentication service to the user (Fig. 1).

RESULTS AND DISCUSSION

Blockchain technology: As the third party blockchain is a private blockchain. For the consensus algorithm there are four main methods of finding consensus in a blockchain: the Practical Byzantine Fault Tolerance algorithm (PBFT), the Proof-of-study algorithm (PoW), the Proof-of-Stake algorithm (PoS) and the Delegated Proof-of-Stake algorithm (DPoS). Among these algorithms, the PBFT method of establishing consensus requires less effort than other methods. Therefore, the PBFT algorithm would be used. Compared with the PoW algorithm, the PBFT algorithm is providing embedded design optimizations such as reducing the size and number of messages exchanged between nodes. The third party blockchain is connected to several ID providers. Therefore, several ID providers should consist of trusted agencies.

Sharing user attribute: Once the user attribute information is provided to the service provider, the provided user attribute information is used to enhance the user authentication. The attribute information can be person information, public DB, environment information, etc.

Enhanced user authentication: Service provider can authenticate the user with its own attribute information and other service provider's same user attribute information. Sharing the same user's various attribute information, ID theft could be prevented. Sharing the user's attribute information could provide a solution for enabling or preventing access to age-related services and web content. Also, it can prevent cyber-bullying by or to a person.

CONCLUSION

Many of the internet services require that the user must prove their identities before accessing the services. With the propagation of various internet services, personal authentication has been requested in various ways. We consider blockchain technology as authentication service using a sharing the attribute information. Blockchain technology enables entities independent of each other to rely on the same shared, secure and auditable source of information in a way that fits well with a system of widespread digital identity.

This study has presented a sharing the attribute information based on blockchain which can support the authentication service in a secure and transparent way. Each procedure of the proposal has been described in detail. As discussed, enhanced authentication could provide preventing ID theft and enabling or preventing access to age-related services and web content.

REFERENCES

Cachin, C., 2016. Architecture of the hyperledger blockchain fabric. Proceedings of the Workshop on Distributed Cryptocurrencies and Consensus Ledgers, July 25-29, 2016, PODC, Chicago, Illinois, USA., pp: 1-4.

Castro, M. and B. Liskov, 2002. Practical byzantine fault tolerance and proactive recovery. ACM Trans. Comput. Syst., 20: 398-461.

Chadwick, D.W. and G. Inman, 2009. Attribute aggregation in federated identity management. Comput., 42: 33-40.

Clement, A., E.L. Wong, L. Alvisi, M. Dahlin and M. Marchetti, 2009. Making byzantine fault tolerant systems tolerate byzantine faults. Proceedings of the 6th USENIX Symposium on Networked Systems Design and Implementation, April 22-24, 2009, USENIX, Boston, Massachusetts, pp: 153-168.

Ferdous, M.S. and R. Poet, 2013. Analysing attribute aggregation models in federated identity management. Proceedings of the 6th International Conference on Security of Information and Networks, November 26-28, 2013, ACM, Aksaray, Turkey, ISBN:978-1-4503-2498-4, pp: 181-188.

Kim, T.K., 2017. A study on the utilization of internet service through sharing the certified attribute information. Intl. Inf. Inst. Tokyo, 20: 1106-1099.

Klingenstein, N., 2007. Attribute aggregation and federated identity. Proceedings of the International Symposium on Applications and the Internet Workshops, January 15-19, 2007, IEEE, Hiroshima, Japan, pp: 26-26.

Lee, J.H., 2017. BIDaaS: Blockchain based ID as a service. IEEE. Access, 6: 2274-2278.

Merkle, R.C., 1987. A digital signature based on a conventional encryption function. Conf. Theor. Appl. Cryptographic Tech., 1: 369-378.

Nakamoto, S., 2008. Bitcoin: A peer-to-peer electronic cash system. J. Netw. Comput., 1: 1-30.

Tosh, D.K., S. Shetty, X. Liang, C.A. Kamhoua and K.A. Kwiat *et al*., 2017. Security implications of blockchain cloud with analysis of block withholding attack. Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, May 14-17, 2017, IEEE Press, Madrid, Spain, ISBN:978-1-5090-6610-0, pp: 458-467.