Poster: A Chaincode with Attribute-Based Encryption for Protecting Data in Ledgers

Mio Saiki, Hideharu Kojima, Naoto Yanai, Tatsuhiro Tsuchiya
Graduate School of Information Science and Technology, Osaka University

***Abstract*—Hyperledger Fabric is a platform of smart contracts. It has been increasingly used to deploy many kinds of services. In this paper, we propose two access control mechanisms for Hyperledger Fabric smart contracts or chaincodes. The first mechanism supports private data by storing data encrypted with *attribute-based encryption (ABE)* in a ledger. Because of the feature of ABE, only users with specific attributes can access the data. Furthermore, by combining ABE with *searchable encryption*, the encrypted data can be arbitrarily searched without decryption.**

I. Introduction

In past few years, many applications, such as financial services and food tracking, have been developed by using a smart contract platform named *Hyperledger Fabric* [2]. A famous successful example in academic community is Open Science Chain [1], which provides the reproducibility and transparency of academic data. These applications use a database, called a blockchain or a ledger, to store data and contracts that operate the ledger.

In many scenarios, it is necessary to permit only some specific participants to see the data in the ledger. For example, consider medical studies where many hospitals share patient treatment data. Such private data should not be stored in plaintext to protect privacy of the patients. Even when the data are encrypted, however, the possibility of the private information of the stored data being leaked can be increased if the ledger is publicly accessible or the data is stolen by undesirable users, i.e., attackers. To reduce such a privacy risk, we proposed mechanisms for encrypting the data stored in a ledger in the previous work [6]. These encryption and decryption mechanisms are embedded in a chaincode together with secret keys. However, chaincodes are public in general and anyone can access them easily. Consequently, the previous mechanisms are vulnerable in that secret keys can be revealed by analyzing the chaincode.

In this paper, we propose mechanisms to store encrypted data in a database of Hyperledger Fabric using *attribute-based encryption (ABE)* [4]. ABE allows only users with specific attributes to encrypt/decrypt data. Even if a chaincode is analyzed, unregistered users cannot access the stored data because the chaincode contains only attributes. With the mechanisms, the smart contract platform can be used more flexibly, since it has more control over access to the ledger. Moreover, we propose to combine ABE and *searchable encryption* [5] to search data without decryption. We also discuss how the proposed mechanisms can be implemented.

Network and Distributed Systems Security (NDSS) Symposium 2020
23-26 February 2020, San Diego, CA, USA
ISBN 1-891562-61-4
https://dx.doi.org/10.14722/ndss.2020.23xxx
www.ndss-symposium.org

II. Hyperledger Fabric

Hyperledger Fabric is a smart contract platform for a permissioned blockchain. In addition to Fabric, Hyperledger has five frameworks, namely, Burrow, Fabric, Indy, Iroha, and Sawtooth, as well as five tools, namely, Caliper, Cello, Composer, Explorer, and Quilt. Contracts are called *chaincodes* and can be implemented in a variety of languages. To execute a chaincode in the Fabric, user registration is necessary beforehand. In other words, only registered users can execute the chaincode. The Fabric consists of the following servers: a CA server which manages the execution authority of a chaincode such as user registration, a peer which executes a chaincode and manages a ledger, an orderer which decides the execution order of chaincodes, and a database server which is an entity of the ledger. A peer executes the chaincode and updates the database when the peers agrees on the execution of the chaincode. Hyperledger is used in a variety of applications, including supermarkets, financial companies, supply chains, and health information management (https://www.hyperledger.org/).

Requirements: The target requirements in this work are: *confidentiality*, *access control*, and *searchablity*. To achieve confidentiality, we encrypt private data such as medical data on Hyperledger Fabric. Access control is achieved by allowing only the registered users in a chaincode to encrypt data and store it in a ledger and by permitting only the registered users with designated attributes to decrypt the stored data. Finally, searching encrypted data, i.e., achieving the searchability, is a soft requirement.

III. Related Work

In our previous work [6], we proposed and implemented a method in which a chaincode itself has a key and performs encryption and decryption. However, because a chaincode is publicly accessible in general, anyone can read and analyze content of the chaincode.

Benhamouda et al. [3] explored the addition of private-data support to Hyperledger Fabric using secure multiparty computation (MPC). They integrated secure-MPC protocols within the blockchain architecture. Unlike their work, our mechanisms are able to directly provide access control by means of ABE.

IV. Proposed Mechanisms

In this section, we propose two mechanisms that enable users to store encrypted data into a database of Hyperledger Fabric. The two mechanisms are different in encryption techniques.

(a) Embedding ABE into a chaincode: This mechanism uses ABE. This is different from our previous study in that in the new mechanism a key includes attributes for encryption/decryption. A user needs his/her attributes for encryption. For decryption, on the other hand, the user needs a secret key that is related to the attributes. To utilize ABE, management of a master key is necessary [5]. We believe that a CA server can be useful for this purpose. For instance, when users are registered to a chaincode, the users can receive their attributes together with the corresponding secret keys from the CA.

(b) Embedding ABE and Searchable Encryption into a chaincode: In the proposed mechanism described above, we have one problem: that is, a user cannot search the stored data with keywords. Generally speaking, the use of keywords is important for searching the stored data. To achieve this, we introduce searchable encryption in a chaincode. This method allows users to directly search the stored and encrypted data in the database of Hyperledger Fabric without decryption. Several attribute-based searchable encryption [7], [8] have been proposed. These schemes can be incorporated in our proposed mechanism.

V. Discussion

We proposed two mechanisms on chaincodes in the previous section. Here we discuss how the mechanisms achieve the requirements described in Section II.

Achievement of Requirements: In both mechanisms, a user can store encrypted data with ABE into a database. Also, both mechanisms require attributes for encryption/decryption. Thus, there is only a low probability that attacker finds a way to decrypt stored data. Hence, the confidentiality is achieved by the use of encryption. In addition, ABE allows the user to utilize its own attributes in order to impose access control. In other words, only users with specific attributes can decrypt the encrypted data. Consequently, both mechanisms achieve access control by means of ABE. However, the mechanism **(a)** disallows users to search the stored data directly. In contrast, only the mechanism **(b)** achieves the searchability. Thus, we consider that mechanism **(b)** is the most effective from the viewpoint of the requirements.

Performance Evaluation: In our previous work [6], three processes are needed to search for data, namely, withdraw, decryption, and comparison with given keywords. In contrast, in the proposed mechanism **(b)**, a user can search for the stored data directly from a database of Hyperledger Fabric by means of searchable encryption. Hence, we expect that our proposed mechanism shows better performance. We plan to evaluate the performance more rigorously in future work.

Implementation Approach: We plan to implement the proposed mechanism **(a)** using an ABE library called openABE (https://github.com/zeutro/openabe). To implement mechanism **(b)**, it is also necessary to implement searchable encryption in a chaincode. We believe that the mcl library (https://github.com/herumi/mcl) can be used for this purpose [7], [8].

VI. Conclusion and Future works

In this paper, we proposed two protection mechanisms for a database of Hyperledger Fabric from unregistered users. By introducing attribute-based encryption (ABE) and searchable encryption, protection of the stored data can be achieved. Because ABE enables the registered users to utilize attributes for encryption and decryption, it is hard for unregistered users or adversaries to retrieve information from the stored data, even if the chaincode is completely analyzed. We are now in the process of designing and implementing the proposed mechanisms. Fortunately, we found the mcl library to implement the attribute-based searchable encryption [7], [8]. Our goal in the future is to implement the proposed mechanisms in pure JavaScript for Hyperledger Fabric.

Acknowledgment: This work is supported by JSPS KAKENHI Grant Numbers 18K18049, Secom Science and Technology Foundation, and Innovation Platform for Society 5.0 at MEXT.

References

[1] "Open Science Chain," https://www.opensciencechain.org.

[2] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. D. Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, S. Muralidharan, C. Murthy, B. Nguyen, M. Sethi, G. Singh, K. Smith, A. Sorniotti, C. Stathakopoulou, M. Vukolic, S. W. Cocco, and J. Yellick, "Hyperledger fabric: a distributed operating system for permissioned blockchains," in *Proc. of EuroSys 2018*, 2018, pp. 30:1–30:15.

[3] F. Benhamouda, S. Halevi, and T. T. Halevi, "Supporting private data on hyperledger fabric with secure multiparty computation," *IBM Journal of Research and Development*, 2019.

[4] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proc. of IEEE S&P 2007)*. IEEE, 2007, pp. 321–334.

[5] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in *Proc. of IEEE S&P 2000*, 2000, pp. 44–55.

[6] H. Kojima and N. Yanai, "A chain code mechanism with data encryption onhyperledger fabric," in *Proc. ESORICS 2019, Poster*, 2019.

[7] H. Yin, Y. Xiong, J. Zhang, L. Ou, S. Liao, and Z. Qin, "A key-policy searchable attribute-based encryption scheme for efficient keyword search and fine-grained access control over encrypted data," *Electronics*, vol. 8, no. 3, 2019.

[8] H. Yin, J. Zhang, Y. Xiong, L. Ou, F. Li, S. Liao, and K. Li, "Cp-abse: A ciphertext-policy attribute-based searchable encryption scheme," *IEEE Access*, vol. 7, pp. 5682–5694, 2019.