先端科学技術研究科　修士論文要旨

所属研究室 (主指導教員)	大規模システム管理 (笠原　正治　(教授))		
学籍番号	1911176	提出日	令和 3年 1月 4日
学生氏名	中西　瑠海		
論文題目	IOTA-Based Access Control Framework for the Internet of Things IOTAに基づいたIoTアクセス制御方式の設計と実装		

要旨

With the rapid dissemination of the Internet of Things (IoT), the number of resources deployed in IoT systems such as devices and data is growing explosively. Since IoT systems often handle private information, it is essential to enforce appropriate access control to prevent unauthorized access. However, conventional access control schemes in which access rights are stored in a centralized server are prone to load concentration and a single point of failure. Although distributed access control schemes leveraging the blockchain technology have been proposed to deal with such problems, they inherit the drawbacks of the blockchain technology, such as high transaction fee and low throughput. To address these limitations, an access control scheme, called the Decentralized Capability-based Access Control framework using IOTA (DCACI), has been proposed based on the next-generation distributed ledger technology IOTA. The idea of the DCACI scheme is to store the access rights of subjects, in the format of tokens, into the IOTA Tangle. However, this scheme suffers from three main drawbacks: 1) providing no concrete implementation of authorization; 2) requiring pre-established secure links between subjects and object owners; and 3) supporting only one-to-one access control. To solve these problems, we propose a novel access control scheme by combining the IOTA technology and the Ciphertext-Policy Attribute-Based Encryption (CP-ABE) technology. The proposed scheme enables access right authorization to a large number of subjects in a small number of operations in large-scale IoT networks, alleviating the burden of object owners. Moreover, the scheme also provides channel security between subjects and object owners by encrypting data using CP-ABE. We show the feasibility of our scheme by implementing a proof-of-concept prototype with IoT devices. We also measure the performance of our scheme in terms of execution time and compare it with DCACI. Experimental results show that, although each operation of our scheme takes longer time than that of DCACI, the total execution time of authorizing a large number of subjects is significantly reduced.