Scientific Proposal

Introduction:

With the sharp increase in the number of intelligent devices, the Internet of Things (IoT) has gained more and more attention and rapid development in recent years. It effectively integrates the physical world with the Internet over existing network infrastructure to facilitate sharing data among intelligent devices. However, its complex and large-scale network structure brings new security risks and challenges to IoT systems. To ensure the security of data, traditional access control technologies are not suitable to be directly used for implementing access control in IoT systems because of their complicated access management and the lack of credibility due to centralization. we propose a novel attribute-based access control scheme for IoT systems, which simplifies greatly the access management.

Attribute-based access control (ABAC) is one of the most suitable decentralized models for large-scale, flexible, and dynamic IoT scenarios. When used in IoT environments, ABAC can provide fine-grained and flexible control over each device's access requests. We use Blockchain technology to record the distribution of attributes to avoid single point failure and data tampering. The access control process has also been optimized to meet the need for high efficiency and lightweight calculation for IoT devices.

Main Work

Access control mechanisms for ABAC must be able to verify subject attributes, verify access control policies (rules), verify object attributes, and verify environmental conditions for a subject to be able to execute a policy on the object (e.g., allow or deny access). Almost always, the subject is assumed to be human. The subject could also be a non-person entity (NPE), such as a self-contained service or application. For scalability, the policy can be altered based on the current situation by adding or removing attributes.

Attributes are considered the heart of ABAC. The attributes can be defined as a set of four elements: $A \in \{S, O, P, E\}$, where:

(i) A is the attribute that has a key-value pair structure, A = {name: value}.
(ii) S is the subject's attribute. It identifies the identity and characteristics of the entity that launches the access request, such as a person's ID, name, position, and age.
(iii) O defines the object's attribute, which is the attribute of the accessed resource, such as service IP address, network protocol, and resource type.
(iv) P defines the permission attribute. It represents the permissioned operation the subject can perform on the object, such as reading, writing, and executing.
(v) E is the environment's attribute, which means the environment information at the time the access request is generated, such as the location and time.

A device resource model in this paper is defined as {Device}⟶{resource}⟶{url}. The access policy defines the subject's (user's) access rights to the object (resource). Instead of requesting resources directly from the device, the users get the resource data via a URL from the Blockchain system after checking permission. The process is according to the following steps:

(1) The resource is published on the Internet by the device that generates the URL for that resource

(2) The URL of that resource is stored on the blockchain

(3) The users request authorization from the blockchain system based on attributes

(4) The blockchain distributes URLs to authorized users

(5) Using the URL, the users pull or download resource data from the Internet

Conclusion:

This proposed model is a blockchain-based access control model that employs the blockchain as the trusted center of the access control model and implements the access control policy through the use of smart contracts. The data stored on the blockchain is trustworthy and credible because of its tamper-proof and no single point of failure features. The proposed model is fully decentralized (no third-party required), user-transparent, fault-tolerant, scalable, and compatible with a wide range of IoT access control models. The proposed model utilizes smart contracts to achieve a flexible, scalable, and fine-grained access control process based on the ABAC method.