Proceedings of the International Conference on Industrial Engineering and Operations Management
Toronto, Canada, October 23-25, 2019

Decentralized Access Control Technique for Industrial Internet of Things

Kelechi Eze and Cajetan Akujuobi
The Center of Excellence for Communication Systems Technology Research (CECSTR)
The SECURE Cybersecurity Center of Excellence
Electrical Engineering Department
Prairie View A&M University, Prairie View, TX 77446

Abstract

This research study investigates access control problem in complex Internet of Things networks. The primary objective is to implement an efficient, flexible and scalable access control method that is suitable for protecting Internet of Things (IoT) devices from unauthorized or malicious access. The research finding draws conclusion based on an evaluation method that takes IoT requirements into consideration to recommend the most appropriate access control method. Access control method investigated are Capability-based Access Control, Role-based Access Control, Policy-based access control and Attribute-based access control. Internet of things are characterized by power constrained devices, lightweight communication protocol, dynamic behavior, heterogeneity, enormous scale, intelligence and low latency connectivity and hence demand a different security approach than the traditional computing devices. Access control for the IoTs therefore requires a decentralized, secure and light-weight service and management architecture to solve the issue present in the client-server architecture and meet the growing scale of IoTs. The limitations of the client-server model are single point of failure, scalability issues, management and performance bottlenecks A secure service and management model based on features of and an enhanced blockchain technology is adopted in this research study. Each case of the access control approach is modeled using access control matrix. An access control matrix represents a two-dimensional matrix structure where subjects (users) are related to objects (resources) with their corresponding access rights. A prototype of each of the access control method is implemented on ethereum blockchain platform using devices of varying memory and computational power such as raspberry, sensors and laptops to represent an actual IoT scenario. The prototype uses smart contracts which is a code, token or business logic that run on the blockchain to automatically enforce access control when according to predefined agreements. Evaluation of results is based on requirements of Internet of Things such as security and privacy, decentralization, manageability, resource efficiency and scalability.