Authentication and authorization of Internet of Things devices in a federated environment using distributed ledger technology

mgr inż. Michał Jarosz

Abstract

The implementation of the authentication and authorization process for Internet of Things devices is particularly difficult in federated environments where there is a lack or there is limited trust between organizations. One of the basic prerequisites for federation is the information integration of organizations, which allows the exchange of information and the use of resources that belong to the individual entities that are part of the federation. A crucial challenge when implementing and using a federation environment is to ensure the security of information exchange between different entities. On the other hand, the authentication and authorization operations themselves in such an environment must be implemented according to commonly defined rules. These rules cannot be changed without the knowledge and approval of any federation participant. If authentication and authorization processes involve the Internet of Things environment, in which the number of devices is huge, these processes must be implemented in an efficient, scalable and operator-free manner. The problems of authentication and authorization of IoT devices operating in federated environments are sparsely addressed in the literature. And the solutions themselves presented in the research papers found cannot be considered fully satisfying.

The thesis proposes a solution based on the use of a distributed ledger, which makes it possible to establish common rules for the exchange of information between the organizations forming the ledger. Through the use of chain codes, it is possible to automate the authentication and authorization process while respecting the established rules. The proposed solution is also characterized by the use of symmetric cryptography, which is unique compared to proposals found in the literature for authenticating devices in federated environments. The paper presents the results of an evaluation of the security, performance, and scalability of the proposed solution. The security evaluation includes qualitative as well as formal analysis using appropriate tools. The performance study includes various configurations of the developed solution. This thesis also presents a Petri net model to simulate the performance testing of the distributed ledger for different configurations.

The results obtained confirm the effectiveness of the proposed solution.