Authentication on a Decentralized Blockchain Mechanism for IoT-Based Outdoor Temperature Monitoring Systems

1st Yehezkiel Kacik Micha Simbuang
School of Computing
Telkom University
Bandung, Indonesia
yehezkielsimbuang@student.telkomuniversity.ac.id

2nd Farah Afianti
School of Computing
Telkom University
Bandung, Indonesia
farahafi@telkomuniversity.ac.id

***Abstract*—IoT (Internet of Things) is a system that transmits data from sensors to smart devices using a network to create a more efficient performance. IoT devices generate data, some of which may be important. For example, in the case of an outdoor temperature monitoring system where if the IoT device data is successfully modified by an attacker, this will affect the IoT system's decisions and cause unwanted conditions or situations. The first step in securing IoT data is to implement authentication and access control mechanisms in the IoT system. However, traditional IoT systems have limitations in handling and implementing authentication mechanisms. In this study, the authors proposed a decentralized IoT system and apply an authentication mechanism using a blockchain to overcome problems in outdoor temperature monitoring systems. The obtained results show that the blockchain can be used to add authentication and access control mechanisms to outdoor temperature monitoring systems.**

***Key words*—Authentication, Blockchain, IoT**

I. Introduction

IoT (Internet of Things) is a system that transmits data from sensors to smart devices using a network to create a more efficient performance. IoT has limitations in terms of data storage, power, and computing [1]. Currently, IoT plays an important role in the field of human life such as smart homes, healthcare, and others. However, with the involvement of a large number of devices, IoT applications face many challenges, including data integrity, security, and durability [2].

IoT devices generate data, some of which may be important. For example, in the case of an outdoor temperature monitoring system, if the data of an IoT device is successfully modified by an attacker who breaks into the IoT network, this will of course affect the IoT system's decision and will cause conditions or situations that are not wanted by agencies that are engaged in this field.

The first step in handling cases like the one above is to implement authentication and access control mechanisms to restrict access to the IoT network. However, traditional IoT systems have limitations in handling and implementing authentication mechanisms. The IoT system is also expected to work in a distributed manner with a minimum delay so that the devices in the system can communicate properly [1].

Blockchain can be used to overcome problems in monitoring outdoor temperatures that still use traditional IoT systems. The decentralized nature of the blockchain and its cryptographic capabilities make it a safe place to store sensitive data [3]. Smart contracts contained in blockchain also offer access control mechanisms on IoT systems and devices. Communication latency between IoT systems and devices can be overcome by using a fog computing architecture that places some communication, control, storage, and management at the edge of the network rather than setting up a dedicated channel for more centralized remote infrastructure [1].

II. Related Work

This section discusses the work related to blockchain and authentication mechanisms for IoT systems carried out in recent years.

Khalid, U et al [1] proposed A decentralized lightweight Blockchain-based authentication mechanism for IoT systems. The problem identified by the researchers in this article is that the Proof-of-Work consensus protocol used in this study is cumbersome to apply to IoT devices with limited power and resources.

Zhaofeng, M et al [4] proposed the Blockchain-based Decentralized Authentication Modeling Scheme in Edge and IoT Environment In their study, the researchers used BlockAuth as a modeling scheme. The problem identified by the researchers in this article is that the BlockAuth implementation has a high time complexity of On^2.

Tian, Z et al [5] proposed the Feasibility of Identity Authentication for IoT Based on Blockchain. In their study, the researchers improved the key-sharing scheme with a decentralized Blockchain as a Key Distribution Center.

Sibarani, I et al [6] proposed Blockchain Implementation based on BigchainDB and Tendermint on IoT Data Storage Systems. In their study, the researcher developed a storage system capable of storing various IoT data, namely structured and unstructured data in a decentralized manner.

Ourad, A et al [7] proposed Using Blockchain for IOT Access Control and Authentication Management. In their