ABSTRACT

Internet of Things (IoT) is an emerging paradigm in information technology that integrates development in sensing, computing, and communication to improve existing services in everyday life. In general, IoT refers to physical objects that are connected to the network. These physical objects consist of sensors and actuators that can exchange data to offer improved quality of service in everyday life. When data transfer occurs, the data exchanged is sensitive data so that the data is vulnerable to security launched by the attacker, one of which is the Sybil attack. Sybil attacks allow IoT users to be cheated by other devices because there is no prior checking of device information. In this study, the authors propose a trust management method based on authentication and the value of trust. After testing on two scenarios, the system is able to detect Sybil attacks quickly and accurately. The average time needed to detect a sybil attack is 9,3287 seconds. Then, the average time needed to detect intruder objects in the system is 18.1029 seconds. The accuracy produced in each scenario is 100%, so it can be concluded that the accuracy generated by the system for detecting Sybil attacks is 100%.

Keywords: IoT, Sybil Attack, Trustworthiness Management, Authentication.