

ABSTRAK

PERANCANGAN ALGORITMA *TWO FACTOR AUTHENTICATION* UNTUK KEAMANAN JARINGAN *INTERNET OF THINGS*

Oleh

DIPAMADYA KALINGGA

Internet of Things (IoT) adalah struktur dimana objek atau orang diberikan identitas eksklusif dan kemampuan untuk berbagi data melalui jaringan (internet) tanpa memerlukan interaksi langsung antara manusia dengan manusia atau interaksi manusia ke komputer. Salah satu tantangan yang harus diatasi untuk mendorong meluasnya implementasi IoT adalah faktor keamanan. Salah satu metode untuk mengamankan Jaringan IoT yaitu dengan metode *Two Factor Authentication (2FA)*. Metode *2FA* yaitu suatu metode login yang memerlukan dua faktor autentikasi. *Two Factor Authentication* itu menggabungkan dua metode autentikasi yaitu *Something You Know* (*password* statis atau *password* milik pengguna pribadi) dengan *Something You Have* (token atau kode acak yang berubah-ubah). Pada penelitian ini akan dibangun suatu sistem keamanan jaringan IoT dua autentikasi yaitu berupa *password* dan OTP (*One time password*) yang harus diinput oleh *client* atau perangkat IoT untuk dapat mengirim data sensor suhu dan kelembapan ke dalam *server*. Hasil pengujian sistem menunjukkan sistem yang memenuhi parameter keamanan jaringan data *Confidentiality Integrity Availability* (CIA) dimana untuk parameter *confidentiality*, OTP berfungsi sebagai *key* untuk mengamankan sistem dari *client* yang tidak berhak mengakses *server*, dan juga dilakukan perbandingan proses enkripsi data pada saat proses pengiriman data dengan layanan IoT *thingspeak*. Pada pengujian parameter *integrity*, tidak terdapat perubahan besar data pada saat pengiriman dan saat data sensor diterima di *database* dimana besar data yang dikirim dan diterima konstan yaitu 88 bytes. Pengujian parameter *availability* dilakukan dengan pengambilan data selama 24 jam, dimana selama 24 jam tersebut ESP8266 dapat mengirim data suhu dan kelembapan secara terus menerus dengan interval waktu 5 menit. Data yang diterima dari ESP8266 berjumlah 288 buah data dengan nilai berupa suhu dan kelembapan dan tidak ada satupun data yang *error*. Nilai suhu memiliki nilai rata-rata 25,78 dimana nilai tertinggi adalah 30,7 dan nilai terendah adalah 24,1. Nilai kelembapan memiliki nilai rata-rata 85,14 dimana nilai tertinggi adalah 95 dan nilai terendah adalah 60.

Kata Kunci: *Internet of Things, Security IoT, Two Factor Authentication, One Time Password, Confidentiality Integrity Availability.*

ABSTRACT

DESIGN OF TWO FACTOR AUTHENTICATION ALGORITHM FOR INTERNET OF THINGS SECURITY

By

DIPAMADYA KALINGGA

The Internet of Things (IoT) is a structure where objects or people are given exclusive identities and the ability to share data over a network (internet) without requiring direct human-to-human interaction or human-to-computer interaction. One of the challenges that must be overcome to encourage the widespread implementation of IoT is the security factor. One method for securing the IoT Network is the Two Factor Authentication (2FA) method. The 2FA method is a login method that requires two authentication factors. Two Factor Authentication combines two authentication methods, namely Something You Know (a static password or password belonging to a personal user) with Something You Have (a random token or code that changes). In this research, a two-authentication IoT network security system will be built, namely in the form of a password and OTP (One time password) which must be input by the client or IoT device to be able to send temperature and humidity sensor data to the server. The results of system testing show that the system meets the parameters of data network security Confidentiality Integrity Availability (CIA) where for the confidentiality parameter, OTP functions as a key to secure the system from clients who are not entitled to access the server, and also compares the data encryption process during the data transmission process with thingspeak IoT services. In testing the integrity parameter, there is no change in data size when sending and when sensor data is received in the database where the amount of data sent and received is constant, namely 88 bytes. Availability parameter testing is carried out by collecting data for 24 hours, during which 24 hours the ESP8266 can send temperature and humidity data continuously at 5 minute intervals. The data received from the ESP8266 totals 288 pieces of data with values in the form of temperature and humidity and none of the data has an error. The temperature value has an average value of 25.78 where the highest value is 30.7 and the lowest value is 24.1. The humidity value has an average value of 85.14 where the highest value is 95 and the lowest value is 60.

Key Words: Internet of Things, Security IoT, Two Factor Authentication, One Time Password , Confidentiality Integrity Availability.