1. PENDAHULUAN

1.1. Latar Belakang

Salah satu tantangan penelitian di bidang IoT adalah masalah keamanan. Jumlah perangkat yang dapat dihubungkan satu sama lain melalui Internet dapat menciptakan potensi besar untuk serangan. Objek pada IoT bisa dimanipulasi untuk proses pengumpulan, penyimpanan, dan analisis data. Data tersebut dibutuhkan oleh aplikasi kesehatan, pendidikan, transportasi, dan industri untuk pemanfaatan kehidupan manusia. Peningkatan penggunaan data dalam IoT berpotensi menyebabkan beberapa aktivitas serangan dari malicious node, mengingat bahwa aktivitas objek IoT mungkin terbuka untuk siapa saja [1].

Untuk mendeteksi serangan yang dapat terjadi di dalam lingkungan IoT, harus diawali dengan mengenali kemungkinan resiko yang dapat terjadi. Dengan menyediakan objek yang memiliki keamanan yang memadai dapat mengurangi resiko. Mengamankan objek adalah hal penting yang bisa pertama kali dilakukan untuk menjaga proses komunikasi data antar objek [1]. *Trustworthiness Management* adalah salah satu aspek keamanan untuk mengamankan objek IoT. Ini bertujuan untuk meningkatkan kerja sama antara entitas dalam sistem terdistribusi dengan memprediksi perilaku objek di masa depan berdasarkan perilaku sebelumnya [2].

Terdapat berbagai bentuk ancaman dan serangan terhadap objek pada IoT yang dapat menyebabkan penyalahgunaan data pada objek IoT tersebut. Salah satu bentuk serangan pada objek IoT adalah *on-off attack*. Pada jenis serangan ini, objek berprilaku secara acak. Sewaktu-waktu berprilaku sebagai objek yang tidak berbahaya dengan memberikan *real trust value* pada *trustworthiness management*, namun terkadang berprilaku sebagai objek yang berbahaya dengan memberikan *false trust value* pada *trusthiness management* [1].

Berdasarkan hal tersebut dibutuhkan sebuah cara untuk mengamankan objek IoT yaitu menggunakan aspek nilai kepercayaan dari metode *Trustworthiness*

Management. Adapun pendekatan yang akan dilakukan yaitu dengan cara implementasi berdasarkan aspek nilai kepercayaan dari *Trustworthiness Management*.

1.2. Perumusan Masalah

Adapun rumusan masalah yang dibuat berdasarkan latar belakang diatas, yaitu bagaimana mengamankan objek IoT terhadap serangan *on-off attacks* (*Bad-mouting attacks*, *Good-mouting attacks*, *Ballot-stuffing attacks*) dengan menggunakan *Trustworthiness Management*.

1.3. Tujuan

Adapun perumusan masalah yang telah dibuat berdasarkan latar belakang diatas yaitu mendeteksi objek yang melakukan serangan *On-off Attack* (*Good-mouthing attacks, Bad-mouthing attacks)* dengan menggunakan manajemen *Trustworthiness* juga menghitung tingkat keberhasilan dan waktu yang dibutuhkan server untuk pendeteksian objek.

1.4. Batasan Masalah

Adapun tujuan yang dibuat berdasarkan perumusan masalah diatas, diantaranya yaitu.

1. Keterbatasan kemampuan objek untuk melakukan komputasi algoritma yang kompleks. Penulis disini menggunakan ESP8266 sebagai mikrokontroler yang berperan sebagai *objek* yang terhubung pada server. Penggunakan ESP8266 untuk mengetahui kemampuan alat melakukan implementasi pada penelitian ini.
2. Keterbatasan kemampuan objek untuk melakukan blok pada suatu jaringan sebagai langkah pencegahan terhadap serangan *on-off attack* hingga pada akhirnya tindakan yang dilakukan berupa peringatan yang ditampilkan pada antarmuka web sederhana.
3. Pembuatan jaringan sederhana menggunakan Raspberry pi 3 b+ sebagai server.
4. Penggunaan authentikasi yang sudah disediakan oleh MQTT Broker.

1.5. Sistematika Penulisan

Sistematika penulisan dalam penulisan Tugas Akhir ini adalah sudah dijelaskan pada bagian pertama mengenai latar belakang dari penelitian, perumusan masalah dari penelitian, tujuan dari penelitian, batasan masalah dari penelitian, dan sistematika penulisan. Pada bagian dua dijelaskan penelitian sebelumnya dan landasan teori yang dapat mendukung penelitian. Pada bagian tiga dijelaskan gambaran umum sistem dan skenario pengujian yang telah dibuat. Pada bagian empat dijelaskan hasil pengujian yang telah dilakukan. Pada bagian lima dijelaskan kesimpulan dan saran dari hasil penelitian yang telah dilakukan.