BAB I
PENDAHULUAN

1.1. Latar Belakang

Telemetri merupakan suatu proses pengukuran parameter obyek (benda, ruang, kondisi alam) dengan jarak tertentu yang hasil dari pengukuran tersebut akan dikirimkan baik melalui media kabel maupun nirkabel [1][2]. Penggunaan sistem komunikasi nirkabel semakin populer sekarang ini, karena aplikasi teknologi nirkabel memberikan informasi dan komunikasi yang cepat dan mudah dibandingkan dengan komunikasi dengan kabel [2]. Pada kemajuan era digital seperti sekarang ini pengguna lebih banyak menggunakan *Internet of Things* (IoT) untuk mengirimkan data atau informasi melalui media komunikasi nirkabel. Secara umum, IoT adalah sistem yang digunakan untuk menghubungkan objek-objek cerdas dengan objek yang lainnya, serta lingkungan dengan komputasi awan melalui jaringan internet [3][4].

Pengiriman data dari sensor yang satu dengan yang lainnya ke komponen penerima biasanya dikenal dengan istilah node, dimana node-node tersebut saling terhubung antara yang satu dengan yang lainnya dalam suatu topologi jaringan atau dikenal dengan istilah *wireless sensor network* (WSN) [5]. WSN merupakan suatu sistem komunikasi yang dapat menghubungkan node-node sensor. Komunikasi yang digunakan dapat bermacam-macam seperti Bluetooth, IR, *Wi-Fi*, dan Radio [6]. Jaringan komunikasi yang digunakan pada arsitektur IoT biasanya menggunakan *Wi-Fi* untuk terhubung ke internet. Dengan adanya sistem komunikasi yang benar, maka informasi analog dari lingkungan dapat dikirimkan dalam bentuk data atau digital melalui sensor. Informasi tersebut diambil secara real-time, kemudian diubah kedalam format yang sesuai untuk ditransmisikan melalui jaringan. Selanjutnya, data akan diolah oleh pengolah cerdas dengan teknologi komputasi cerdas tertentu, untuk mencapai tujuan IoT [7][8].

Data sensor yang terkirim dari sebuah node biasanya mengandung makna atau informasi yang penting bahkan privasi pengguna. Sedangkan, salah satu isu yang menjadi kelemahan pada masalah penggunaan IoT yaitu keamanan dan privasi data [9][10]. Permasalahannya terletak pada kerentanan suatu jaringan pada sistem komunikasi yang dapat disadap. Hal ini bukan menjadi tidak mungkin dan bisa saja berbahaya jika privasi pengguna dapat diketahui oleh orang lain selain user melalui data yang didapat tersebut [11].

Penyadapan data khususnya pada IoT termasuk tindakan kejahatan atau dikenal dengan istilah *Cybercrime*, dimana orang yang berperan dalam tindakan *Cybercrime* ini disebut *sniffer* [12]. Menurut Kominfo, dalam menghadapi perkembangan teknologi yang memasuki era *internet of thing* (IoT), keterhubungan menurut Menteri rudiantara menjadi hal yang sangat penting." Era IoT dan big data memungkinkan semua terhubung dengan *cyberspace* atau jaringan siber" [13]. Selain itu, menurut *avast* "IoT membawa risiko yang signifikan bagi seluruh ekosistem digital, hal ini karena sebagian besar perangkat yang terlibat tidak mempunyai sistem keamanan bawaan yang melindunginya dari serangan peretas. Selanjutnya menurut peneliti keamanan di kapersky "ketika orang menjadi semakin dikelilingi oleh perangkat pintar, kami menyaksikan bagaimana serangan IoT juga kian meningkat" [14].

Adapun solusi yang dapat digunakan untuk mengatasi *sniffing* data tersebut supaya tidak dapat dibaca oleh orang lain. Caranya yaitu dengan menerapkan enkripsi data [15]. Enkripsi merupakan suatu proses yang digunakan untuk mengubah data *plaintext* atau pesan asli menjadi pesan yang tidak dapat terbaca karena sudah disandikan dengan kunci tertentu. Pada tugas akhir ini, peneliti akan merancang alat yang bernama CRYPTOBLE. CRYPTOBLE merupakan alat yang dapat mengenkripsi pesan atau *plaintext* menjadi *ciphertext* melalui jaringan *Wi-Fi*, dengan tujuan supaya pesan tidak dapat terbaca. Selain itu pesan yang telah terubah menjadi *ciphertext* akan diubah kembali menjadi *plaintext*. Algoritma yang akan digunakan untuk proses enkripsi dan dekripsi yaitu AES-128-CBC [16][17][18].

1.2. Tujuan Penelitian

Tujuan utama yang ingin dicapai dalam tugas akhir ini, yaitu merancang prototype dalam bentuk produk keamanan berupa CRYPTOBLE yang akan digunakan untuk mengenkripsi data melalui jaringan komunikasi *Wi-Fi*. Kemudian melakukan pengujian performansi alat seperti menghitung kelayakan lamanya waktu enkripsi dan dekripsi data dan menganalisa dengan pengaruh suatu jarak serta memeriksa apakah terjadi *loss* data atau tidak.

1.3. Ruang Lingkup Penelitian

Tugas akhir ini melingkupi spesifikasi berikut:

a) Implementasi algoritma kriptografi AES yang telah ada pada library Arduino IDE. Algoritma AES kemudian diimplementasikan pada jaringan komunikasi *Wi-Fi*,
b) Alat yang dibuat harus mampu mengenkripsi dan mendekripsi data *plaintext* yang sedang beroperasi pada jaringan komunikasi *Wi-Fi*.
c) *Development* yang digunakan pada penelitian ini yaitu Website.

1.4. Metodologi

Metodologi yang digunakan untuk menyelesaikan tugas akhir ini adalah:

a) Studi literatur

Tahap awal dalam pengerjaan tugas akhir ini adalah melakukan studi literatur yang berkaitan tentang aspek keamanan pada perangkat elektronik seperti sensor devices. Selanjutnya bagaimana cara mengamankan data hasil keluaran berupa nilai sensor yang akan ditransmisikan atau telemetri melalui jaringan komunikasi *Wi-Fi*.

b) Eksplorasi

Eksplorasi dilakukan terhadap cara mengamankan hasil keluaran perangkat elektronik dengan metode enkripsi.

c) Implementasi

Setelah mengeksplorasi, langkah selanjutnya adalah mengimplementasikan algoritma kriptografi pada CRYPTOBLE untuk melakukan proses enkripsi.

d) Analisis

Langkah selanjutnya adalah melakukan analisa performansi pada CRYPTOBLE dalam proses mentransmisikan data pada end device seperti *server* pada komunikasi *Wi-Fi*. Analisis tersebut meliputi seberapa lama waktu yang dibutuhkan, konsumsi daya, kompleksitas ruang, dan tingkat keberhasilan algoritma kriptografi dalam melakukan enkripsi maupun dekripsi.

e) Pelaporan tugas akhir

Langkah terakhir dari penyusunan tugas akhir ini adalah penyusunan laporan tugas akhir dan publikasi jurnal.

1.5. Sistematika Penulisan

Laporan tugas akhir ini akan diuraikan dalam lima bab dengan sistematika penulisan sebagai berikut:

a) **BAB I. PENDAHULUAN**

Bab ini menjelaskan latar belakang pengambilan judul yang diangkat pada tugas akhir ini, tujuan pengerjaan penelitian/tugas akhir, ruang lingkup penelitian/tugas akhir, metodologi yang digunakan, serta sistematika penulisan laporan tugas akhir.

b) **BAB II. DASAR TEORI**

Bab ini memuat pengetahuan dasar dan penjelasan teori yang digunakan dan berhubungan dengan tugas akhir.

c) **BAB III. ANALISIS DAN PERANCANGAN**

Bab ini berisi tentang perancangan alat yang akan dibuat berdasarkan hasil studi literatur, eksplorasi, dan analisis yang telah dilakukan.

d) **BAB IV. IMPLEMENTASI DAN PENGUJIAN**

Bab ini memuat implementasi dari alat yang telah dirancang dan evaluasi pengujian terhadap kinerja alat secara keseluruhan.

e) **BAB V. PENUTUP**

Bab ini berisi kesimpulan dari keseluruhan proses pengerjaan tugas akhir dan saran untuk pengembangan lebih lanjut.