BAB I

PENDAHULUAN

1.1 Latar Belakang

Sistem keamanan dalam komunikasi nirkabel merupakan salah satu hal penting yang harus diperhatikan. Kanal komunikasi nirkabel dianggap sebagai kanal yang rentan terhadap berbagai macam serangan. Pada sistem komunikasi nirkabel, informasi dirambatkan menggunakan gelombang radio melalui udara terbuka. Proses pengiriman tersebut memungkinkan terjadinya pelacakan dan pengumpulan data secara tersembunyi oleh penyadap [1]. Salah satu contoh terdapat 22 juta ancaman terhadap *Internet of Things (IoT) smartcity* yang lebih tepatnya adalah penyerangan CCTV di kota Libanon pada tahun 2017 [2]. Para penyadap atau peretas melakukan *cyberattack* dengan cara menanamkan sebuah *malware* dan mendeteksi lokasi melalui perangkat yang telah tersadap [3]. Menurut laporan Kaspersky Lab bahwa terdapat 120.000 lebih *malware* yang menyerang IoT selama tahun 2018, statistik menunjukkan bahwa propagasi *malware* IoT yang paling populer masih berusaha secara paksa membobol kata sandi atau yang dikenal dengan *brute force*, *brute force* ini telah terdeteksi sebanyak 93% [4]. Contoh kejahatan *cyberattack* tersebut dapat terjadi pada saat pengiriman maupun penerimaan pada jaringan komunikasi elektronik seperti telemetri atau IoT [5].

Diperlukan sebuah metode untuk melindungi informasi yang dikirim melalui komunikasi radio dari serangan atau penyadapan yang menyebabkan perubahan, kerusakan, dan kebocoran informasi. Kriptografi adalah ilmu dan seni untuk menjaga kewanitaan pesan. Kriptografi dapat digunakan sebagai metode untuk melindungi informasi. Pada penelitian sebelumnya dilakukan analisis tentang keamanan dari sistem komunikasi nirkabel seperti interkoneksi *Internet of Thing (IoT)* dan pengiriman surat elektronik dengan beberapa metode kriptografi untuk mengamankan data-data yang dikirimkan melalui komunikasi nirkabel. Parameter yang diteliti, yaitu keberhasilan enkripsi data dan kecepatan proses enkripsi serta kecepatan pengiriman. Maka penelitian ini dilakukan perancangan dan pembuatan perangkat keamanan data pada komunikasi radio dengan metode penelitian mengirimkan data *plaintext* sebesar 2 *bytes* sampai 16 *bytes* dari perangkat

pemancar ke penerima. Parameter yang diteliti adalah hasil enkripsi, kecepatan enkripsi, kecepatan pengiriman, hasil dekripsi, kecepatan dekripsi, dan presentase data hilang saat pengiriman. Perangkat ini menggunakan metode kriptografi *Corrected Block Tiny Encryption Algorithm (XXTEA)* yang ditanamkan pada mikrokontroler Arduino Nano. Perangkat ini juga dilengkapi dengan aplikasi berbasis Windows yang berfungsi sebagai antarmuka pengguna untuk melakukan konfigurasi perangkat, yaitu konfigurasi waktu, *baudrate*, kunci, dan alamat radio.

1.2 Tujuan Penelitian

Tujuan utama yang ingin dicapai dalam tugas akhir ini, yaitu:

1. Membuat perangkat yang dapat meningkatkan keamanan atau merahasiakan data yang dikirim menggunakan modul radio NRF24.
2. Membuat aplikasi untuk konfigurasi perangkat tersebut.

1.3 Ruang Lingkup Penelitian

Tugas akhir ini melingkupi spesifikasi berikut:

1. Perangkat yang dibuat harus mampu mengkonversi data dari bentuk *plaintext* menjadi bentuk *ciphertext* dan sebaliknya menggunakan metode kriptografi *Corrected Block Tiny Encryption Algorithm (XXTEA)*.
2. Perangkat yang dibuat harus mampu mengirimkan data dalam bentuk *ciphertext* dari pemancar menuju penerima menggunakan modul radio NRF24I01 PA LNA.
3. Perangkat yang dibuat harus mampu berintegrasi dengan perangkat lain melalui komunikasi serial *Universal Synchronous Asynchronous Receiver Transmitter (USART)*.
4. Perangkat yang dibuat dapat dikonfigurasi melalui aplikasi antarmuka oleh pengguna melalui laptop/PC, yaitu konfigurasi waktu, *baudrate*, kunci, dan alamat radio.

1.4 Metodologi

Metodologi yang digunakan untuk menyelesaikan tugas akhir ini adalah:

1. Studi literatur

Tahap awal dalam pengerjaan tugas akhir ini adalah melakukan studi terhadap beberapa literatur yang berkaitan dengan keamanan jaringan komunikasi.

2. Eksplorasi

Eksplorasi dilakukan terhadap spesifikasi perangkat yang akan dibuat dan terkait penggunaan komponen *hardware* dan *software* apa saja yang dapat membantu dalam pembuatan perangkat.

3. Perancangan

Setelah mengeksplorasi, langkah selanjutnya adalah merancang perangkat untuk mendapatkan hasil sesuai dengan tujuan yang ingin dicapai.

4. Implementasi dan analisis

Langkah selanjutnya adalah melakukan pengimplementasian terhadap rancangan perangkat lalu melakukan analisis dari hasil yang diperoleh.

5. Pelaporan tugas akhir

Langkah terakhir dari penyusunan tugas akhir ini adalah penyusunan laporan tugas akhir.

1.5 Sistematika Penulisan

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

1. BAB I. PENDAHULUAN

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

2. BAB II. DASAR TEORI

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

3. BAB III. ANALISIS DAN PERANCANGAN

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

4. BAB IV. IMPLEMENTASI DAN PENGUJIAN

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

5. BAB V. PENUTUP

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