BAB 1
PENDAHULUAN

1.1 Latar Belakang

IoT adalah suatu kondisi dimana perangkat-perangkat fisik yang sebelumnya tidak terkoneksi dengan internet menjadi terkoneksi dengan internet dengan disematkan elektronik, perangkat lunak, sensor, akuator dan konektivitas jaringan sehingga perangkat keras yang tersambung dapat mengumpulkan data dan melakukan pertukaran data antar perangkat [11]. Dengan hadirnya perkembangan IoT maka sudah dipastikan akan mengundang kejahatan *cyber* di jaringan IoT.

Serangan pada perangkat lunak pada sistem IoT bisa menghambat bahkan dapat menghentikan kinerja sistem, Sehingga proses kerja sistem IoT menjadi terganggu karena perubahan data atau pencurian data dari server. Maka dari itu untuk menghindari ancaman kejahatan *cyber* diperlukan sistem keamanan jaringan IoT. Dengan mengembangkan sistem keamanan otentikasi data pada jaringan IoT dengan metode ECDSA diharapkan dapat memproteksi serangan pada jaringan IoT. Tes keamanan jaringan menggunakan metode *false data injection* dan analisis *cost* dari setiap 1 kali pengiriman data dari perangkat IoT menuju server.

Pada penelitian ini terinspirasi dari penelitian sebelumnya yaitu Sistem Keamanan Jaringan IoT Menggunakan Algoritma *Traffic Authentication* [3]. Penulis akan menerapkan metode keamanan yang berbeda namun diterapkan pada sistem yang sama. Akan tetapi, sama-sama melakukan proses otentikasi data yang dikirimkan dari perangkat user yang terhubung jaringan menuju server untuk memastikan bahwa data tersebut berasal dari sensor dan *user* yang dikenal oleh sistem IoT.

1.2 Tujuan dan Manfaat

Tujuan dari penelitian Tugas Akhir ini adalah :

1. Merancang sistem pertahanan jaringan pada sistem IoT menggunakan metoda ECDSA.
2. Meningkatkan sistem keamanan jaringan IoT menggunakan metoda ECDSA.

Manfaat dari penelitian Tugas Akhir ini adalah :

1. Mengimplementasikan sistem keamanan jaringan dengan menggunakan algoritma ECDSA pada jaringan IoT.
2. Mengetahui performansi sistem otentikasi dengan menggunakan ECDSA.

1.3 Rumusan Masalah

Rumusan masalah dalam penelitian Tugas Akhir ini adalah :

1. Bagaimana mengimplementasikan metode sistem keamanan ECDSA pada jaringan IoT.
2. Bagaimana hasil pengujian sistem keamanan di perangkat.
3. Bagaimana hasil Performansi sistem terhadap algoritma keamanan ECDSA.

1.4 Batasan Masalah

Beberapa hal yang menjadi batasan pada tugas akhir ini adalah :

1. Sistem enkripsi *Elliptic Curve Digital Signature Algorithm* sebagai *digital signature*.
2. SHA-256 sebagai *hash* pada sistem ECDSA.
3. Penyerangan menggunakan metode *false data injection.*
4. *Server* IoT berbasis *web server* (apache).

1.5 Metode Penelitian

Dalam penyelesaian penelitian tugas akhir ini dilakukan beberapa metode yang digunakan, yaitu:

1. Studi Literatur

   Mempelajari dan memahami konsep dan teori tentang IoT, mempelajari dan memahami konsep dan teori tentang teknik keamanan, mengetahui konsep dan cara kerja dari ECDSA, mempelajari dan memahami materi lain yang berkaitan dengan keamanan jaringan yang akan diterapkan.

2. Flow Chart

   Membuat alur secara sistematis langkah-langkah proses peertahanan dalam sistem yang diterapkan.

3. Perancangan sistem

   Melakukan perancangan sistem keamanan mengikuti flow chart yang sudah dibuat sebelumnya, kemudian melakukan analisa kembali apakah rancangan sudah tepat atau belum.

4. Implementasi sistem

   Melakukan implementasi terhadap konsep yang sudah dibuat sebelumnya ke dalam *server* dan perangkat IoT, kemudian melakukan pengecekan sistem berhasil diterapkan tanpa ada *bug* atau *error*.

5. Pengujian dan Analisis

   Melakukan pengujian terhadap perangkat IoT dengan melakukan serangan terhadap sistem keamanan dan pertahanan. Setelah melakukan pengujuan terahadap sistem kemudian dilakukan analisis berdasarkan hasil yang telah di dapat.

6. Kesimpulan

   Melakukan penarikan kesimpulan terhadap setiap tahap yang telah dilakukan dan analisis serangan terhadap sistem yang telah dirancang.

1.6 Sistematika Penulisan

Sistematika pada penulisan Tugas Akhir ini terdiri dari beberapa BAB, yaitu:

BAB I PENDAHULUAN

Pada BAB ini membahas tentang latar belakang mengapa diadakannya penelitian, perumusan masalah, tujuan, manfaat, batasan masalah, metodologi penelitian dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Pada BAB ini membahas teori pendukung penyususan tugas akhir. Teori pendukung meliputi konsep dan teori dasar antara lain seperti Internet of Things (IoT), *false data injection* dan Algoritma Elliptic Curve Digital Signature Algorithm (ECDSA).

BAB III PERANCANGAN SISTEM

Pada BAB ini diuraikan mengenai diagram alir sistem, bagaimana penerapan metode Algoritma ECDSA saat berada di perangkat melakukan proses sign dan server melakukan proses pertukaran kunci.

BAB IV PENGUJIAN DAN ANALISIS SISTEM

Pada BAB ini menjelaskan hasil dan analisis dari rancangan sistem beserta keluaran yang didapat berdasarkan nilai dari parameter yang telah ditetapkan

BAB V KESIMPULAN DAN SARAN

Pada BAB ini membahas kesimpulan menurut hasil dan analisis yang telah didapat, selain itu juga berisikan saran untuk memberikan gambaran pada penelitian selanjutnya