BAB I
PENDAHULUAN

1.1 Latar Belakang

Di abad 21 ini, teknologi informasi semakin berkembang untuk mempermudah pekerjaan manusia setiap hari. Di masa depan, karena kebutuhan manusia yang terus berkembang, komputer akan mendominasi pekerjaan manusia, contohnya remote control perangkat elektronik melalui internet. Orang ingin semua yang terhubung ke internet untuk memenuhi semua kebutuhan mereka. Dengan berkembangnya teknologi dan perangkat internet, semua perangkat elektronik dapat dikendalikan melalui internet. Era dimana semua barang elektronik di sekitar kita terhubung dengan internet dan antar perangkat elektronik tersebut dapat saling berkomunikasi. Dari hal tersebut maka munculnya salah satu konsep yaitu IoT (Internet of Things). IoT adalah suatu pengembangan internet yang terdiri dari perangkat-perangkat keras elektronik yang mampu berkomunikasi secara real time dengan terkoneksi ke internet. Komunikasi pada IoT dapat berupa pertukaran informasi dari data antar perangkat dan proses penyimpanan data di dalam database. Dengan pesatnya perkembangan IoT, saat ini IoT banyak membantu pekerjaan dalam berbagai bidang seperti pabrik mobil, pertanian, kesehatan, manajemen gedung, dan smart home.

Dalam penelitian ini penulis melakukan perekaman data dari sensor detak jantung MAX30105. Sensor MAX30105 adalah sensor pulse terintegrasi yang digunakan untuk non-invasif SpO2 dan detak jatung BPM (*Beats Per Minute*). MAX30105 terdiri dari dua light-emitting diode (LED), LED merah dan LED inframerah, dan fotodetektor dengan pemerosesan sinyal analog dengan noise rendah. Namun pada penelitian ini penulis hanya menggunakan data BPM yang akan dikirim melalui device IoT ESP8266 untuk mentransfer data dari sensor ke platform IoT yang dapat diakses pengguna. ESP8266 terdapat modul *Wi-Fi* dengan integrasi protocol TCP/IP dan 9 SOC mandiri sehingga menjadi salah satu alasan

penulis menggunakan *device* tersebut dapat dengan mudah menyediakan *Wi-Fi* dan terhubung ke internet [1].

Pada proses transfer data pada perangkat IoT, terdapat beberapa protokol komunikasi salah satunya adalah HTTP (*HyperText Transfer Protocol*). HTTP adalah protokol yang berada di layaer aplikasi biasanya digunakan untuk transmisi dokumen Hypertext. HTTP sendiri ialah teks non-linier yang berisikan tautan ke teks lainnya. Pada penilitian ini, HTTP bertindak sebagai penghubung untuk melakukan *post* data pada *web server*. Alasan penulis memilih protokol HTTP karena disini penulis ingin menerapkan konsep keamanan antara *client-server* dengan melakukan pengamanan dari sisi data.

Sistem keamanan yang diterapkan pada penelitian ini bertujuan untuk meningkatkan aspek *confidentiality* dan *non repudiation* demi menajaga informasi dari data detak jantung sangat rentan untuk diakses dan disalahgunakan oleh pihak yang tidak bertanggung jawab. Untuk mencapai tujuan tersebut, pada penelitian ini penulis menerapkan proses pengamanan data menggunakan algoritma pertukaran kunci ECDSA (*Elliptic Curve Digital Signature Algorithm*). ECDSA adalah skema tanda tangan digital (*digital signature*) yang aman secara kriptografis, berdasarkan kriptografi ECC (Elliptic Curve Cryptography) [2]. Data yang sudah di-*sign* dan dienkripsi akan di-*post* menggunakan HTTP pada *web server* Apache setelah itu mekanisme dekripsi data akan dilakukan pada *web server* dan data tersebut nanti akan diverifikasi menggunakan algoritma keamanan dan jika berrhasil, maka data tersebut akan disimpan pada *database* MySQL.

1.2 Rumusan Masalah

Berdasarkan latar belakang tersebut, maka rumusan masalah dari Tugas Akhir ini adalah sebagai berikut:

1. Bagaimana cara menerapkan metode ECDSA pada sensor detak jantung pada device ESP8266?
2. Berapa nilai pengujian QoS sebelum dan setelah diterapkan ECDSA pada device ESP8266?
3. Berapa nilai pengujian *memory usage* sebelum dan setelah diterapkan ECDSA pada device ESP8266?
4. Bagaimana hasil dari serangan *data sniffing* yang dilakukan?

1.3 Tujuan

Adapun tujuan dari penelitian ini adalah:

1. Dapat menerapkan sistem *signature*, enkripsi, dan dekripsi pada pengiriman data melalui HTTP ke *database*.
2. Meningkatkan aspek keamanan dari sisi *confidentiality* dan *non repudiation*.
3. Mengetahui nilai QoS dan konsumsi memori yang didapat dalam menerapkan sistem keamanan.
4. Mengetahui bentuk data yang terkirim melalui HTTP ke database.

1.4 Batasan Masalah

ECDSA merupakan algoritma keamanan yang menawarkan varian dari algoritma DSA (Digital Signature Algorithm) yang menggunakan kriptografi kurva elips. Untuk memperkecil cakupan dari tugas akhir ini diperlukan Batasan-

batasan. Adapun Batasan yang diambil untuk tugas akhir ini adalah sebagai berikut:

1. Perangkat IoT yang digunakan menggunakan Sensor MAX30100 dan ESP8266.
2. Data yang digunakan dalam perekaman dari sensor adalah data denyut jantung.
3. Ukuran *key* pada algoritma keamanan 256 bit.
4. Database yang digunakan adalah MySQL
5. Proses signature dan enkripsi dilakukan pada ESP8266.
6. Proses dekripsi dan verifikasi signature dilakukan pada web server.
7. Penyerangan dilakukan berupa data sniffing melalui Wireshark.
8. Server IoT berbasis web server Apache.

1.5 Rencana Kegiatan

1.5.1. Studi Literatur

Mempelajari teori dan konsep mengenai IoT, mencari jenis device yang bisa untuk melakukan penelitian, mengkaji paper, jurnal, dan buku referensi yang dapat membatu dalam proses penelitian.

1.5.2. Perancangan Sistem

Membuat langkah-langkah proses enkripsi-dekripsi dan signature, dan melakukan proses perancangan, kemudian melakukan analisa kembali apakah langkah-langkah tersebut sudah benar dan dapat diimplementasi.

1.5.3. Implementasi

Melakukan implementasi terhadap konsep yang sudah dibuat ke dalam perangkat IoT dan server, kemudian melakukan pengecekan apakah terdapat *bug* atau *error* yang terjadi.

1.5.4. Analisi dan Pengujian

Melakukan analisis terhadap cost dan QoS pada sistem, kemudian melakukan simulasi serangan dengan aplikasi wireshark untuk melakukan data sniffing.

1.5.5. Kesimpulan

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

1.6 Jadwal Kegiatan

Jadwal kegiatan penulis dalam mengerjakan penelitian ini adalah sebagai berikut:

Tabel 1.1 Tabel jadwal kegiatan

	Bulan ke-					
Kegitatan	1	2	3	4	5	6
Identifikasi Masalah						
Perancangan Sistem						
Implementasi						
Evaluasi						