BAB I
PENDAHULUAN

1.1 Latar Belakang

Meningkatnya industri nirkabel pada jaman sekarang membuat keamanan pada hal itu semakin dibutuhkan dan harus ditingkatkan. Aplikasi di sektor ekonomi seperti layanan kesehatan, layanan keuangan, dan pemerintah bergantung pada keamanan mendasar yang sudah tersedia di lingkungan komputasi nirkabel. Baik untuk transaksi Web yang aman (terautentikasi, pribadi) dan untuk pengiriman pesan yang aman (ditandatangani, dienkripsi) diperlukan infrastruktur kunci publik yang lengkap dan efisien. Untuk tingkat keamanan yang paling dikenal saat ini, sistem berbasis kurva eliptik dapat diimplementasikan dengan parameter yang mengarah pada keuntungan kinerja yang signifikan. Peningkatan kinerja semacam itu sangat penting dalam arena nirkabel dimana daya komputasi, memori, dan usia baterai perangkat lebih terbatas [1].

Mobile Wireless Sensor Network (MWSN) adalah hasil dari meningkatnya industri nirkabel saat ini dan juga peningkatan dari *Wireless Sensor Network* (WSN) adapun yang menjadi pembeda adalah node yang bergerak. MWSN jauh lebih fleksibel daripada jaringan sensor statis karena dapat digunakan dalam skenario apa pun dan mengatasi perubahan topologi yang cepat. Keuntungan dari MWSN adalah efisiensi energi yang lebih baik, peningkatan cakupan, peningkatan target pelacakan, dan kapasitas saluran yang superior. Biasanya, node sensor terdiri dari transceiver radio dan mikrokontroler yang ditenagai oleh baterai, serta beberapa jenis sensor untuk mendeteksi cahaya, panas, kelembaban, suhu dan lain-lain [2].

Semakin berkembangnya teknologi, keamanan daripada itu juga harus dikembangkan. Penelitian ini berfokus pada performansi keamanan autentikasi di MWSN dengan menggunakan metode algoritma *Elliptic Curve Cryptography* (ECC) dengan *Secure Hash Algorithm* SHA-256. SHA-256 termasuk dalam algoritma satu arah yang cukup kuat dan aman. SHA-256 juga dapat digunakan untuk berbagai kebutuhan yang berkaitan dengan autentifikasi. Untuk mengatasi permasalahan ini, penelitian ini menerapkan algoritma ECC dan SHA-256 yang memungkinan autentikasi secara cepat dan terpercaya antar mobile sensor nodes dan mengamankan komunikasi didalam jaringan dari serangan-serangan yang mungkin terjadi.

1.2 Rumusan Masalah

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

1. Bagaimana cara menerapkan ECC dan SHA-256 pada MWSN?
2. Bagaimana tingkat QoS sebelum dan setelah diterapkan ECC dan SHA pada MWSN?
3. Bagaimana tingkat konsumsi energi sebelum dan setelah diterapkan ECC dan SHA-256 pada MWSN?

1.3 Tujuan dan Manfaat

Adapun tujuan dari Tugas Akhir ini adalah:

1. Menguji kelayakan metode algoritma ECC dan SHA-256 pada MWSN.
2. Melakukan performansi QoS pada metode ECC dan SHA-256 di MWSN.
3. Melakukan performansi tingkat konsumsi energi pad MWSN.

Sedangkan manfaat dari Tugas Akhir ini adalah:

1. Meningkatkan kualitas performansi dari penggabungan metode pada MWSN.
2. Penggunaan metode ECC dan SHA-256 pada MWSN dapat menambah tingkat keamanan informasi yang lebih baik.

1.4 Batasan Masalah

Tugas Akhir ini membatasi permasalahan pada poin-poin berikut ini:

1. Tidak membahasa implementasi dan realisasi sistem.
2. Hanya menggunakan 1 *Access Point*.
3. *Data rate* sebesar 2,4 Mbps.
4. Menggunakan *Bandwidth* sebesar 1 MHz.
5. Sumber energi sebesar 1500 *Joule*.

1.5 Metode Penelitian

1. Studi Literatur
   Studi Literatur dilakukan untuk mempelajari hal-hal yang dibutuhkan untuk perancangan sistem. Sumbernya dari berbagai macam yaitu; Buku, situs jurnal online, situs buku online, maupun jurnal cetak serta teori-teori pendukung dari situs pengembangan resmi yang berkaitan dengan autentikasi, MWSN, ECC dan SHA-256 yang dijadikan bahan dalam pembuatan dasar teori dalam pembuatan tugas akhir ini.

2. Penentuan Parameter
   Setelah Studi Literatur, langkah selanjutnya adalah menentukan parameter yang akan digunakan pada perancangan sistem.

3. Perancangan Sistem
   Perancangan sistem difokuskan pada proses kemanan data yang dikirim dengan menggunakan ECC dan SHA-256. Berupa enkripsi, dekripsi dan *digital signature*.

4. Simulasi
   Pada tahap ini dilakukan simulasi pada *software* untuk pembuatan MWSN serta penggabungan metode algoritma ECC dan SHA-256 pada simulator.

5. Pengujian dan Analisa
   Pada tahap ini dilakukan analisa dari simulasi pada software untuk pengujian enkripsi, dekripsi dan *digital signature* yang telah dibuat.

6. Penarikan Kesimpulan
   Pada tahap ini akan dilakukan penarikan kesimpulan berdasarkan hasil dari simulasi sistem, pengujian dan analisa yang telah dilakukan.

1.6 Sistematika Penulisan

Sistematika penulisan laporan Tugas Akhir adalah sebagai berikut:

- Bab 1 PENDAHULUAN
  Bab ini berisi latar belakang, permasalahan, tujuan, metode penelitian, dan sistematika penulisan.

- Bab 2 DASAR TEORI
  Bab ini berisi penjelasan teori, dan perlengkapan yang digunakan untuk mendukung penelitian.

- Bab 3 PERANCANGAN SISTEM
  Bab ini berisi alur kerja dan alur perancangan sistem.

- Bab 4 HASIL DAN ANALISIS
  Bab ini berisi langkah simulasi dan pengujian yang dilakukan, hasil pengujian, dan analisis dari hasil pengujian yang didapat.

- Bab 5 KESIMPULAN DAN SARAN
  Bab ini berisi kesimpulan dan saran Tugas Akhir ini.