BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Saat ini keresahan tentang kondisi kesehatan terus berkembang terutama untuk untuk penduduk lanjut usia. Dengan begitu teknologi untuk memantau kondisi kesehatan dengan biaya rendah, dan terpercaya menjadi solusi yang dibutuhkan [4]. Salah satu teknologi yang digunakan adalah *Machine to Machine* (M2M) *communications* yang dimanfaatkan pada *Internet of Things* (IoT) untuk pemantauan kesehatan dengan biaya rendah.

Sistem pemantauan kesehatan dengan menggunakan sensor yang biasa disebut *Wireless Body Area Network* (WBAN) merupakan perangkat yang biasanya di ditanam langsung pada tubuh pengguna atau pada perangkat yang dapat dikenakan seperti rompi, perangkat ini dapat terus memantau keadaan fisik manusia dan mengirimkan data tersebut ke sebuah *server* melalui kanal jaringan. Data tersebut kemudian dapat di analisa sehingga kondisi kesehatan pengguna yang mengkhawatirkan dapat ditangani [4].

Data merupakan aset yang memiliki nilai terutama pada saat ini dimana penggunaan teknologi *cloud computing*, *big data*, dan *internet of things* telah banyak digunakan. Data RME (Rekam Medis Elektronik) terutama informasi kesehatan yang dilindungi memilik resiko yang lebih besar jika terjadi pembobolan data, dikarenakan perubahan data seperti penambahan dosis obat dapat mengakibatkan kematian bagi pengguna. Beberapa tahun belakangan data untuk kasus pembobolan data medis diseluruh dunia terus meningkat yang mengakibatkan adanya beberapa regulasi baru untuk kasus tersebut [3]. Beberapa serangan seperti serangan *Distributed Denial of Service* (DDoS) yang dicontohkan oleh *Mirai Botnet* menunjukan bahwa semua jenis perangkat yang terhubung dapat di exploitasi untuk kejahatan [2].

Pada WBAN beberapa metode untuk menjaga dan melakukan autentikasi data telah dipertimbangkan dengan penggunaan algoritma seperti DES, 3DES, BLOWFISH, RC4, RSA, AES [5] untuk mengekripsi, mendekripsi, dan

memunculkan kunci untuk data baik *private key* atau *public key* pada perangkat yang terhubung. Metode yang digunakan juga dapat di bagi mejadi beberapa bagian berdasarkan klasifikasinya seperti berdasarkan fungsinya atau kunci dari metode tersebut. Kunci yang digunakan dapat dibagi berdasarkan beberapa parameter tertentu seperti parameter biologi atau non biologis [4].

Beberapa penelitian telah dilakukan untuk metode *biological key based freamework* seperti penelitian yang dilakukan J. Chukwunonyerem [1], penelitian tersebut menggunakan data ECG yang diambil dari Physionet *database* dan *microcontroller* CC2420 penelitian tersebut menghasilkan kunci yang unik dan mengurangi konsumsi daya yang digunakan. Penilitian selanjutnya dilakukan oleh Koushik Karmakar [4] yang pada penelitian tersebut menggunakan gambar telapak tangan atau jempol sebagai data yang digunakan untuk membangkitkan kunci biologis. Ada juga penelitian yang dilakukan oleh Karthikeyan M. Venkatesan [15] yang menggunakan data ECG untuk menghasilkan kunci dengan besar 128 *bit*.

Pada penilitian ini kunci yang digunakan untuk melakukan enkripsi dan dekripsi berasal dari informasi biologi dari tubuh manusia yang memiliki keunikan sendiri. Informasi yang digunakan pada penilitian ini berasal dari data *electrocardiogram* (ECG) karena data ECG setiap orang memiliki bentuk identitas yang unik [1].

1.2 Rumusan Masalah

Adapun permasalahan yang dapat dibahas dalam pembuatan penelitian metode enkripsi AES dengan *biological key based framework* ini sebagai berikut:

1. Bagaimana cara mendesain dan mengimplementasikan teknik enkripsi yang mampu menjaga data pada WBAN?
2. Bagaimana cara meminimalisir proses komputasi enkripsi dan *delay* pada alat pemantauan kesehatan?
3. Bagaimana cara menghasilkan kunci untuk enkripsi yang unik dengan proses komputasi yang rendah dan penggunaan daya yang sedikit pada WBAN?
4. Bagaimana cara implementasi metode enkripsi AES dengan *biological key based framework* pada WBAN?

5. Bagaimana menganalisis performansi metode enkripsi AES dengan *biological key based framework* pada WBAN?

1.3 Tujuan dan Manfaat

Tujuan dilaksanakan penelitian Tugas Akhir ini sebagai berikut:

1. Dapat memunculkan kunci yang unik untuk mengekripsi data yang ada dengan menggunakan metode enkripsi dengan kunci dari informasi biologi.
2. Mengetahui performansi dalam menggunakan metode enkripsi dengan kunci dari informasi biologi pengguna dengan beberapa parameter yaitu waktu untuk validasi, waktu membaca data, waktu enkripsi, waktu untuk menyimpan data, waktu untuk menghasilkan kunci, waktu mengambil data, waktu dekripsi. Dari Tujuan yang dikemukakan nantinya akan terdapat jawabannya di kesimpulan.
3. Mengetahui efektifitas penggunaan metode enkripsi dengan kunci dari informasi biologi dalam implementasi WBAN.

1.4 Batasan Masalah.

Pada Tugas Akhir ini terdapat beberapa batasan masalah sebagai berikut:

1. Penelitian Tugas Akhir ini menggunakan metode *biological key based framework* dengan data biologi ECG.
2. Penelitian pemantauan kesehatan berbasis *wireless body sensor networks*.
3. Pengukuran analisis menggunakan parameter waktu untuk enkripsi, waktu dekripsi, waktu enkripsi, *avalanche effect*, korelasi data terenkripsi dengan data asli, *throughput*, dan *delay*.
4. Penelitian ini menggunakan data dari sensor ECG.
5. Penelitian ini tidak membahas perangkat dan sensor secara rinci.
6. Algoritma enkripsi yang digunakan pada penilitain ini adalah AES dengan menggunakan kunci dari informasi biologi.

1.5. Metode Penelitian

Metode Penelitian yang diterapkan dalam penelitian Tugas Akhir ini, diantaranya sebagai berikut:

1. Studi Literatur

   Tahap ini melakukan studi literatur dengan mengumpulkan referensi yang dibutuhkan untuk memperoleh informasi dan data yang berkaitan khususnya mengenai WBAN, sistem keamanan jaringan, metode enkripsi, metode autentikasi.

2. Perancangan metode enkripsi.

   Tahap ini melakukan perancangan alur enkripsi yang akan dilalui oleh data perancangan dilakukan menggunakan *AES-256* dengan menggunakan kunci dari informasi biologi.

3. Analisis dan Evaluasi

   Tahap ini melakukan analisis performansi sistem WBAN dengan parameter waktu yang digunakan selama proses enkripsi hingga dekripsi.

4. Penarikan kesimpulan

   Tahap ini melakukan penarikan kesimpulan berdasarkan hasil simulasi dan analisis performansi metode enkripsi.