BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan teknologi informasi dan komunikasi yang terus berkembang apalagi di bidang *IoT (Internet of Things*). Penerapan *IoT* semakin bermunculan di masyarakat, sebagai contohnya dalam sistem monitoring air kolam. Setiap sistem monitoring kebanyakan atau bahkan hampir semua tidak memiliki pengamanan data. Seperti halnya sistem monitoring pada umumnya, alat sistem monitoring air kolam yang dimiliki divisi roket unikom juga tidak memiliki pengamanan untuk data-data sensor yang dimiliki. Data-data dari alat sistem monitoring air kolam biasanya disimpan pada sebuah *database* yang terintegrasi oleh internet, maka setiap alat sistem monitoring menggunakan sebuah layanan *cloud* yaitu *Database as a Service (DBaaS)*. Layanan *DBaaS* pada umumnya bersifat *open source*. Layanan yang bersifat *open source* tentunya sangat membantu karena mudah untuk diatur sesuai dengan kebutuhan kita. Namun dibalik setiap kemudahan yang diberikan tentu mempunyai kelemahan juga, yakni setiap data tersimpan di dalamnya pun dapat dimanipulasi oleh beberapa oknum yang tidak bertanggung jawab.

Pada tahun 2000, serangan *DDOS* terjadi pada beberapa situs web terkenal seperti Amazon mengalami *"downtime"* selama beberapa jam. Ada lagi serangan yang pernah dilancarkan pada tahun 2002 ketika 9 dari 13 root *DNS* server diserang dengan menggunakan *DDoS* yang sangat besar yang disebut dengan *"Ping Flood"*. Beberapa server pada tiap detiknya mendapatkan lebih dari 150.000 request paket ICMP. Tetapi serangan hanya berlangsung selama setengah jam sehingga lalu lintas internet tidak terlalu terpengaruh oleh serangan tersebut. Setidaknya tidak membuat kerusakan yang fatal. *Denial Of Services Attack* yang merupakan serangan yang paling mudah dipasang dan yang paling merusak. Kebocoran data yang terjadi bisa

saja bukan hanya dari data alat sistem monitoring saja melainkan data *IP Address* yang kita tahu itu bisa membahayakan data-data pribadi kita.

Setiap layanan atau platform penyelenggara sistem elektronik dalam hal ini hosting maupun database *Firebase* belum tentu aman dari kebocoran data pribadi, dikarenakan sekarang setiap layanan Penyelenggara Sistem Elektronik (PSE) mengharuskan kita untuk memasukan data pribadi kita.

Untuk mencegah seperti masalah-masalah tersebut diperlukan sebuah algoritma pengamanan data. Enkripsi adalah proses teknis yang mengonversikan informasi menjadi kode rahasia, sehingga mengaburkan data yang terkirim, diterima, atau disimpan. Pada dasarnya, sebuah algoritma digunakan untuk mengacak data, sebelum pihak penerima memulihkan kembali data yang diacak tersebut menggunakan kunci dekripsi. Proses enkripsi dan dekripsi menggunakan satu atau lebih kunci enkripsi[5].Enkripsi dibagi menjadi dua jenis, simetris dan asimetris, tergantung pada kunci yang digunakan. Enkripsi simetris menggunakan kunci yang sama untuk enkripsi dan dekripsi, sedangkan enkripsi asimetris menggunakan kunci yang berbeda. Kunci asimetris dianggap lebih aman daripada kunci simetris, tetapi algoritma yang tersedia masih terbatas dan membutuhkan lebih banyak waktu untuk digunakan. Enkripsi simetris dapat dikatakan aman jika kunci yang digunakan merupakan kombinasi kompleks angka dan huruf. Menggunakan kunci yang lebih panjang pasti meningkatkan keamanan. Salah satu algoritma eksekusi cepat simetris adalah *Advanced Encryption Standard (AES)*[6].

AES menggunakan algoritma Rijndael yang telah memenangkan sayembara terbuka yang dilakukan oleh NIST (National 9 Institute of Standard and Technology). Jenis algoritma kriptografi AES (atau Rijndael) ini bersifat simetris dan cipher blok. Dengan demikian algoritma ini mempergunakan kunci yang sama saat enkripsi dan dekripsi, serta masukkan dan keluaran berupa blok dengan urutan data sebesar 128 bit. Urutan data yang sudah terbentuk dalam satu kelompok 128 bit tersebut disebut sebagai blok data atau plaintext yang nantinya akan dienkripsi menjadi chipertext. Cipher key dari AES terdiri dari key dengan panjang 128 bit, 192 bit, atau

256 bit. Perbedaan panjang kunci akan mempengaruhi jumlah round (putaran) yang akan diimplementasikan pada algoritma AES ini. Ada 10, 12, atau 14 putaran dalam AES yang sesuai dengan ukuran kunci yang digunakan. Dengan ini dapat diambil kesimpulan kekuatan algoritma AES tergantung dari panjangnya kunci. Karena dengan panjangnya kunci semakin banyak kombinasi enkripsinya.

Berdasarkan dari setiap masalah-masalah yang tertera di atas diperlukan sebuah pengamanan sistem monitoring kualitas air di kolam ikan agar dapat menunjang keamanan dari sistem monitoring kualitas air tersebut.

1.2 Identifikasi Masalah

Berdasarkan latar belakang yang telah dijelaskan, maka permasalahan dalam penelitian ini adalah sebagai berikut:

1. Alat sistem monitoring air kolam tidak memiliki algoritma untuk pengamanan data.
2. Data yang disimpan di dalam layanan *Database as a Service (DBaaS)* dalam hal ini *Firebase* tidak terenkripsi.
3. Dibutuhkan sebuah media untuk mengolah data yang masih dalam keadaan terenkripsi dan menampilkan data tersebut.

1.3 Maksud dan Tujuan

Berdasarkan permasalahan, maka maksud dari penelitian ini adalah menerapkan pengamanan pada transmisi data alat sistem monitoring air kolam. Tujuan dari penelitian ini adalah:

1. Sistem yang dibangun menerapkan algoritma pengamanan enkripsi terhadap alat sistem monitoring air kolam.
2. Sistem yang dibangun akan mengatur dalam proses pengiriman data yang terhubung dengan layanan *Database as a Service (DBaaS)* tetap dalam keadaan terenkripsi.
3. *Website* yang dibangun mampu mengolah data yang masih terenkripsi di *Firebase* dan menampilkannya

1.4 Batasan Masalah

Ada beberapa batasan masalah yang dapat dijelaskan sebagai berikut:

1. Enkripsi pada alat sistem monitoring.
2. Dekripsi data pada *website.*
3. Sistem berbasis algoritma AES-CBC 128 bit.

1.5 Metodologi Penelitian

Metode penelitian eksperimen sering digunakan dalam penelitian adalah laboratorium. Namun demikian, bukan berarti pendekatan ini tidak dapat digunakan dalam penelitian sosial, termasuk penelitian pendidikan. Borg & Gall (1983) mencatat bahwa penelitian eksperimental adalah penelitian yang paling dapat diandalkan (paling berharga) dari sudut pandang ilmiah karena dilakukan dengan kontrol yang ketat untuk kondisi variabel non-eksperimental.

1.5.1 Metode Pengumpulan Data

Pada penelitian ini, saya mengumpulkan data dan informasi terkait penelitian dengan menggunakan beberapa metode yaitu:

1. Observasi

   Observasi adalah mengumpulkan data dan informasi dengan cara mengamati dan meninjau langsung lokasi penelitian.

2. Studi Pustaka

   Studi pustaka merupakan metode pengumpulan data dengan mencari informasi yang relevan dengan tujuan penelitian. Informasi tersebut dapat diperoleh dari berbagai referensi seperti buku, jurnal, skripsi/tesis, situs internet, dan sumber-sumber lain.

1.6 Sistematika Penulisan

BAB 1 PENDAHULUAN

Pada bab ini berisi uraian latar belakang masalah, identifikasi masalah, maksud dan tujuan, batasan masalah, metodologi penelitian, tahap pengumpulan data, model pengembangan perangkat lunak dan sistematika penulisan.

BAB 2 LANDASAN TEORI

Pada bab ini akan membahas berbagai konsep konsep dasar dan teori-teori pendukung yang berhubungan dengan pembangunan sistem.

BAB 3 ANALISIS DAN PERANCANGAN

Pada bab ini akan membahas tentang deskripsi sistem, analisis kebutuhan dalam pembangunan sistem serta perancangan sistem.

BAB 4 IMPLEMENTASI DAN PENGUJIAN

Pada bab ini akan membahas tentang deskripsi sistem, analisis kebutuhan dalam pembangunan sistem serta perancangan sistem.

BAB 5 KESIMPULAN DAN SARAN

Pada bab ini berisi kesimpulan yang diperoleh dari hasil pengujian sistem, serta saran untuk pengembangan aplikasi yang telah dirancang.