BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

Keamanan informasi menjadi suatu aspek kritis dalam pengelolaan data pada era digital ini, terutama ketika ada sistem yang melibatkan basis data untuk menyimpan informasi rahasia dan bernilai tinggi [1]. Selain rahasia dan bernilai tinggi, informasi juga merupakan sebuah kekuatan dan kekuasaan yang sangat menentukan nasib dari pemilik informasi tersebut [2]. Dalam penggunaan sehari-hari, banyak perusahaan bahkan departemen pemerintah menyimpan data rahasia dalam sistem penyimpanan data terdistribusi. Namun, data tersebut memiliki risiko rusak bahkan dicuri oleh peretas [3]. Salah satu contohnya ada pada sistem pengadaan berbasis *web*.

Sistem pengadaan melibatkan seluruh proses perolehan barang maupun jasa dari sumber eksternal [4]. Dalam perolehan barang maupun jasa, terdapat proses permintaan atau *requisition* terlebih dahulu dan akan diteruskan ke *supplier* sampai pada akhirnya barang maupun jasa sudah didistribusikan oleh *supplier* [5]. Sistem pengadaan menyimpan seluruh data yang dibutuhkan di *database* agar proses perolehan barang maupun jasa dapat berjalan dengan lancar [6]. Salah satu contohnya adalah data *supplier*. Data *supplier* tidak boleh jatuh ke orang yang tidak bertanggung jawab karena setiap perusahaan akan memilih *supplier* yang terbaik untuk memastikan keunggulan produk atau jasanya [7]. Sebuah perusahaan dapat berkembang dengan selalu berupaya untuk memproduksi barang maupun jasa yang unik, menarik, berbeda, dan memiliki nilai tambah bagi konsumennya. Maka dari itu, setiap perusahaan memiliki salah satu aset yang mempunyai nilai ekonomi yang tinggi, yaitu rahasia dagang. Rahasia ini harus terjaga dengan baik agar produk atau jasa yang dimiliki suatu perusahaan tidak mudah ditiru atau dicuri informasinya [8, 9]. Data *supplier* juga termasuk sebagai rahasia dagang, karena jatuhnya data tersebut ke tangan yang salah dapat berujung ke penyalahgunaan data seperti peniruan barang atau jasa yang dapat merugikan pihak perusahaan yang memiliki informasi tersebut [10].

Kelemahan pada sistem yang berada di jaringan komputer seringkali diabaikan, sehingga jika terdapat ancaman atau serangan pada sistem tersebut, dampaknya akan parah dan merugikan [11]. Untuk meminimalisir bahaya dan

kerugian dari penyalahgunaan layanan pada seluruh aplikasi berbasis jaringan saat ini, penilaian kerentanan atau biasa lebih dikenal sebagai *vulnerability assessment* harus dilakukan [11–13]. *Vulnerability assessment* dapat dilakukan dengan menggunakan *Open Web Application Security Project* (OWASP) *Top Ten* untuk menganalisis keamanan sistem dengan mengidentifikasi kerentanan pada aplikasi *web* [14]. OWASP *Top Ten* memiliki komunitas yang cukup besar, yaitu lebih dari 46000 partisipan, lebih dari 65 organisasi perusahaan, dan juga banyak pendukung akademis [15]. OWASP *Top Ten* sendiri berisikan 10 risiko keamanan teratas untuk aplikasi *web* yang laporannya diberikan oleh OWASP setiap 3 tahun [14].

Untuk mengurangi risiko keamanan tersebut, metode enkripsi dapat menjadi salah satu cara yang efektif untuk melindungi data dari ancaman keamanan seperti akses yang tidak sah, pencurian data, dan serangan siber lainnya [16]. Di dalam dunia enkripsi, metode Rijndael, yang telah diadopsi sebagai *Advanced Encryption Standard* (AES), telah terbukti efisien serta andal dalam melindungi data [17, 18]. Selain itu, AES juga merupakan algoritma enkripsi simetris yang lebih umum dikenal saat ini dan sering digunakan oleh banyak orang [19]. AES dengan panjang kunci sebesar 128 bit dapat melakukan enkripsi aplikasi sebesar 2 *megabyte* hanya dalam waktu 0.153 detik, dekripsi dalam waktu 0.305 detik, dengan memori yang digunakan hanya sebesar 14.7 *kilobyte* [20]. Penggunaan AES dengan panjang kunci sebesar 256 bit dapat meningkatkan keamanan juga karena untuk mendapatkan kunci asli AES-256, diperlukan algoritma serangan yang lebih rumit, perhitungan yang lebih banyak, jumlah data yang harus dikumpulkan untuk menyerang sistem enkripsi lebih banyak, sehingga memakan waktu serang yang lebih lama [21].

Advanced Encryption Standard (AES) dapat digabungkan dengan *Galois/Counter Mode* (GCM) sebagai solusi pengamanan data dengan menggabungkan operasi perhitungan keamanan *Galois/Counter* dengan enkripsi block Rijndael atau biasa disebut AES-GCM [22, 23]. Kombinasi ini dilakukan karena GCM merupakan salah satu mode yang paling aman untuk menggunakan *Advanced Encryption Standard* (AES) [22] dan juga merupakan mode operasi enkripsi autentikasi yang menggabungkan dua fungsi terpisah, yaitu untuk enkripsi (AES-CTR) dan satu lagi untuk autentikasi (GMAC) [24]. Keunggulan lain dari GCM berada pada penerimaan *Initialization Vectors* (IV) yang panjangnya dapat dipilih secara bebas dan disesuaikan dengan kebutuhan keamanan pada sebuah aplikasi [24]. GCM tidak hanya menyediakan keamanan [23–25], tetapi saat dilakukan perbandingan performa implementasi di perangkat lunak antara

Galois/Counter Mode (GCM), *Electronic Codebook* (ECB), *Cipher Block Chaining* (CBC), *Cipher Feedback* (CFB), *Output Feedback* (OFB) yang terinisiasi dengan *cipher* AES, GCM memiliki performa terbaik dalam melakukan enkripsi dengan waktu rata-rata 32,13 detik [24]. AES-GCM dapat melakukan enkripsi *input* sebesar 4 MB hanya dalam waktu 0,4 detik dan *input* sebesar 1,61 GB hanya dalam waktu 160,45 detik [24]. Keunggulan performa AES-GCM diperoleh karena algoritma ini dapat memanfaatkan pemrosesan paralel secara maksimal untuk meningkatkan kecepatan dan efisiensi enkripsi [24].

Berdasarkan latar belakang di atas, diperlukan suatu keamanan data pada sistem pengadaan berbasis *web* yang diimplementasikan dengan *Galois/Counter Mode* (GCM) menggunakan metode Rijndael.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah di atas, rumusan masalah dari penelitian ini adalah sebagai berikut.

1. Bagaimana cara mengimplementasikan *Galois/Counter Mode* (GCM) untuk keamanan data pada sistem pengadaan berbasis *web* dengan metode Rijndael?
2. Bagaimana tingkat risiko keseluruhan pada implementasi *Galois/Counter Mode* (GCM) untuk keamanan data pada sistem pengadaan berbasis *web* dengan metode Rijndael?
3. Berapa durasi enkripsi dan dekripsi AES-GCM pada sistem pengadaan berbasis *web*?

1.3 Batasan Permasalahan

Penelitian ini perlu dibatasi ruang lingkupnya agar fokus dan mudah dianalisis. Oleh karena itu, penelitian ini memiliki beberapa batasan masalah, yaitu:

1. AES-GCM diterapkan pada sistem pengadaan berbasis *web* pada *environment* VPS Ubuntu dengan *Web Server* NGINX.
2. AES yang digunakan pada penilian ini adalah AES-256.
3. Penelitian berfokus pada perlindungan data *supplier* dan hanya mencakup kategori OWASP *Cryptographic Failures*.

4. Fitur yang dimiliki oleh sistem pengadaan berbasis *web* ini adalah *login* dan CRUD data *supplier*.

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah yang sudah ditentukan, tujuan dari penelitian ini adalah sebagai berikut.

1. Mengimplementasikan *Galois/Counter Mode* (GCM) untuk keamanan data pada sistem pengadaan berbasis *web* dengan metode Rijndael.
2. Mengukur tingkat risiko keseluruhan pada implementasi *Galois/Counter Mode* (GCM) untuk keamanan data pada sistem pengadaan berbasis *web* dengan metode Rijndael.
3. Mengukur durasi enkripsi dan dekripsi AES-GCM pada sistem pengadaan berbasis *web*.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini adalah untuk membantu perusahaan agar dapat menjaga keamanan data pada sistem dengan mengimplementasikan metode enkripsi untuk mencegah terjadinya kebocoran data.

1.6 Sistematika Penulisan

Berisikan uraian singkat mengenai struktur isi penulisan laporan penelitian, dimulai dari Pendahuluan hingga Simpulan dan Saran.

Sistematika penulisan laporan adalah sebagai berikut:

- Bab 1 PENDAHULUAN
  Bab 1 membahas alasan dilakukannya penelitian ini, yaitu untuk mengamankan data *supplier* agar tidak bocor. Selain itu, Bab 1 juga menjelaskan rumusan masalah, batasan masalah, tujuan penelitian, dan manfaat yang diharapkan dari penelitian ini.

- Bab 2 LANDASAN TEORI
  Bab 2 berisikan teori-teori yang menjadi landasan dalam penelitian ini, yaitu penjelasan mengenai Algoritma Rijndael (AES), *Galois/Counter Mode*

(GCM), AES-GCM, *Vulnerability Assessment*, OWASP *Top Ten*, *Testing for Weak Encryption*, dan *OWASP Risk Rating*.

- Bab 3 METODOLOGI PENELITIAN
  Bab 3 membahas metodologi penelitian yang digunakan dalam penelitian ini, seperti tahapan-tahapan yang dilakukan selama penelitian ini dan menampilkan gambaran *flowchart* dari sistem yang sudah mengimplementasikan AES-GCM untuk melindungi data *supplier*.

- Bab 4 HASIL DAN DISKUSI
  Bab 4 membahas tentang hasil dari penelitian yang dilakukan, seperti hasil implementasi yang isinya merupakan potongan kode dari pengimplementasian enkripsi terautentikasi dan dekripsi terautentikasi AES-GCM pada halaman *supplier master data* dan tampilan halaman *supplier master data*, *testing for weak encryption*, dan hasil pengujian.

- Bab 5 KESIMPULAN DAN SARAN
  Bab 5 berisikan kesimpulan yang didapat dari pembahasan bab-bab sebelumnya dan saran yang diberikan untuk penelitian serupa selanjutnya.