BAB 5
SIMPULAN DAN SARAN

5.1 Simpulan

Berdasarkan hasil dari penelitian yang telah dilakukan, berikut adalah kesimpulan yang dapat diberikan.

1. Galois/Counter Mode telah berhasil diimplementasikan pada sistem pengadaan berbasis *web* dengan metode Rijndael. Penggunaan AES-GCM terletak pada proses menyimpan, membaca, dan memperbaharui data *supplier*. Pada proses menyimpan data *supplier* baru, nama dari *supplier* tersebut akan dienkripsi dengan menggunakan AES-GCM untuk memastikan kerahasiaan nama dari *supplier* tersebut. Pada proses membaca data *supplier*, sistem akan melakukan verifikasi pengguna dengan mengirimkan kode OTP ke *email* yang sudah didaftarkan pada akun pengguna tersebut. Jika pengguna sudah melakukan verifikasi, sistem akan melakukan dekripsi pada nama *supplier* tersebut. Pada proses memperbaharui data *supplier*, sistem juga akan melakukan enkripsi dari nama *supplier* tersebut. Meskipun nama dari *supplier* tidak diubah, *ciphertext* dari nama *supplier* tersebut juga akan berubah dikarenakan setiap fungsi enkripsi dipanggil, *key* dan *nonce* yang digunakan untuk melakukan enkripsi pada *plaintext* berbeda-beda/unik.

2. *Vulnerability assessment* telah dilakukan pada sistem pengadaan ini dengan tiga *automated tools* yang berbeda, yaitu dengan PentestTools, HostedScan, dan Acunetix. Hasil dari pengetesan dengan menggunakan *automated tools* PentestTools menunjukkan bahwa sistem pengadaan ini berada di *risk level medium* dengan 18 kerentanan yang diantaranya merupakan dua *medium*, lima *low*, 11 *informational*. Seluruh kerentanan yang ditemukan hanya mencakup dua klasifikasi, yaitu *Security Misconfiguration* dan *Using Components with Known Vulnerabilites*. Hasil dari pengetesan dengan menggunakan *automated tools* HostedScan menunjukkan bahwa sistem pengadaan ini berada di *risk level medium* dengan enam kerentanan yang diantaranya merupakan empat *medium* dan dua *low*. Hasil dari pengetesan dengan menggunakan *automated tools* Acunetix menunjukkan bahwa sistem pengadaan ini memiliki 12 kerentanan yang diantaranya merupakan dua *medium*, enam *low*, dan empat *informational*. Walaupun hasil *vulnerability*

assessment dengan tiga *automated tools* tersebut menunjukkan bahwa sistem pengadaan ini memiliki beberapa kerentanan dan berada di *threat level medium*, seluruh kerentanan tersebut tidak ada yang berhubungan dengan batasan masalah pada penelitian ini, yaitu *cryptography failures*.

3. Telah dilakukan *benchmark* pada fungsi enkripsi terautentikasi dan dekripsi terautentikasi AES-GCM untuk mengukur durasi dalam melakukan enkripsi dan dekripsi. Rentang durasi fungsi enkripsi terautentikasi dan dekripsi terautentikasi pada *plaintext* dengan panjang 12-72 *byte* di *environment production* yang menggunakan CPU Intel Core Processor (Broadwell, IBRS) adalah 3631-4323 *nanosecond* dan 1028-1243 *nanosecond*.

5.2 Saran

Berdasarkan penelitian yang telah dilakukan, terdapat beberapa saran yang dapat membantu penelitian berikutnya untuk meningkatkan kualitas penelitiannya.

1. Melakukan analisis performa AES-GCM pada perangkat dengan spesifikasi yang rendah atau jaringan *bandwith* yang terbatas untuk memberikan gambaran implementasi yang lebih nyata. Dikarenakan meskipun dampak performa pengimplementasian AES-GCM di suatu perangkat tidak begitu berpengaruh pada performa sistem, belum tentu dampak performa sistem pada perangkat lain sama, terutama pada perangkat dengan spesifikasi yang lebih rendah.
2. Melakukan enkripsi pada seluruh *email* yang disimpan pada *database* karena sebagian besar *spam* berasal dari *email* yang ditemukan dari internet dengan menggunakan program *spam-bot*.