BAB I
PENDAHULUAN

1.1. Latar Belakang

Dewasa ini, penggunaan teknologi informasi telah merambah berbagai bidang, antara lain kesehatan, pendidikan, pemerintahan, politik, dan lainnya. Berbagai informasi baik yang bersifat umum ataupun bersifat rahasia dipertukarkan melalui komunikasi dalam jaringan menjadikan aspek keamanan mutlak untuk diperhatikan. Data milik personal maupun pemerintah tidak luput dari ancaman pihak yang tidak bertanggung jawab. Kriptografi dan penyembunyian informasi merupakan salah satu upaya yang dapat dilakukan untuk meningkatkan keamanan pada sistem berbasis teknologi informasi dan komunikasi (TIK).

Data pada pemerintahan adalah salah satu data yang memiliki potensi untuk dicuri serta disalahgunakan oleh pihak yang tidak bertanggung jawab. Seperti dilansir dari The Washington Post sebanyak 21.5 juta orang dirugikan pada kejadian pertasan terhadap investigasi latar belakang oleh pemerintah yang diumumkan pada 9 Juli 2015 (Rein & Peterson, 2015). Menurut United States Office of Personnel Management (OPM) data yang berhasil diretas dan dicuri antara lain angka *social security,* riwayat tempat tinggal, riwayat pendidikan, riwayat pekerjaan, informasi yang berkaitan dengan keluarga, pekerjaan atau bisnis, kesehatan, kriminial, riwayat finansial, dan informasi lainnya. Sebagian data yang berpindah tangan tersebut juga berisikan data sidik jari. Data sidik jari hasil retasan tersebut memiliki keterbatasan untuk disalahgunakan, namun di sisi lain OPM juga mengakui bahwa hal tersebut dapat berubah seiring dengan berkembangnya teknologi (The Guardian, 2015).

Masalah kemanan utama pada *e-government* adalah kerahasiaan, integritas informasi, autentikasi terhadap informasi atau perlindungan hak cipta, nir-penyangkalan, kontrol terhadap penyalinan dan lainnya. Sistem berbasis TIK harus terjamin keamanannya guna melindungi kerahasiaan informasi milik warga

serta mitra bisnis. Keamanan, keaslian, dan verifikasi harus selaras diaplikasikan dengan privasi, dan pemerintah harus menjamin atas pengamanan terhadap aspek kerahasiaan serta privasi dari informasi tersebut. *Digital watermarking* pada dasarnya merupakan sebuah alat untuk menjaga hak cipta atau otentikasi terhadap data *digital* namun berdasarkan sifatnya maka *digital watermarking* dapat meningkatkan keamanan dari sistem e-*government* (Dilip, Vinay, & Sahu, 2007).

Fetra Syahbana, *Country Manager* F5 Networks Indonesia pada perbincangannya dengan selular.id, menjelaskan bagaimana pentingnya perlindungan data di sektor layanan publik, misalnya asuransi BPJS kesehatan. Ungkapnya, jika berhasil diretas, maka berbagai data penting milik masyarakat dapat saja diubah oleh para peretas. Data penting tersebut termasuk di dalamnya riwayat penyakit dan rekam medis (SELULAR.ID, 2015).

Sistem *monitoring* kontrak kerjasama PUSLITBANG Teknologi Mineral dan Batubara (*tek*MIRA) merupakan sistem yang ditujukan untuk melakukan kegiatan pemantauan terhadap kontrak kerjasama serta memiliki fitur untuk mengarsipkan dokumen sebagai lampiran dari suatu kontrak kerjasama. Lampiran yang dapat diunggah oleh staf sub bidang afiliasi berupa naskah kontrak kerjasama beserta dokumen lainnya yang sudah dibubuhi tanda tangan dan cap kedua belah pihak dan berisikan pasal-pasal ketentuan kerjasama dalam format PDF. Data kontrak kerjasama beserta lampiran perlu untuk diamankan mengingat tingginya nilai informasi yang dimiliki (Dilip, Vinay, & Sahu, 2007)

J. Sireesha (2005) pada *Secure Virtual Election Booth with Two Central Facilities*, memaparkan desain protokol *secure election* dengan *two central facilities*, yaitu *Central Legitimization Agency* (CLA) dan *Central Tabulating Facilities* (CTF). Penelitian tersebut memanfaatkan kunci simetri dan fungsi *hash* untuk menjaga privasi dan menghindari kecurangan dalam kegiatan pemungutan suara. Terlebih, Sireesha menyebutkan bahwa protokol tersebut dapat diadaptasi untuk diimplementasikan lebih lanjut. Penelitian serupa telah dilakukan oleh Rojali Budi Permadi (2014) menunjukan hasil yang baik dalam pemanfaatan

protokol *two central facilities* pada sistem *e-voting*. Terlebih Permadi menyebutkan keberadaan algoritma AES dan RSA membantu pengamanan terhadap proses pengiriman data serta terpenuhinya aspek kerahasiaan. Muhammad Ilyas Sikki dkk. (2014) pada penelitiannya yaitu Pengembangan Sistem *E-Voting* dengan Protokol *Two Central Facilities* menggunakan *Fingerprint* sebagai Otentikasi *Voter* mengungkapkan keberhasilan dari protokol *Two Central Facilities* dalam mengotentikasi *voter*.

Abdel-Karim Al Tamimi (2014) pada penelitiannya melakukan perbandingan performa dari algoritma enkripsi ternama, antara lain *Data Encryption Standard* (DES), 3DES, Blowfish dan *Advanced Encryption Standard* (AES). Pada simulasinya dengan menggunakan bahasa pemrograman C# Al Tamimi menyimpulkan bahwa dari sisi performa AES memang berada pada posisi akhir ketimbang 3 algoritma lainnya. Namun AES direkomendasikan pada aplikasi yang membutuhkan tingkat keamanan tinggi dan melibatkan blok data besar.

Penelitian yang dilakukan oleh I-Shi Lee dan Wen-Hsiang Tsai (2010) memaparkan bagaimana memanipulasi *whitespace* atau karakter *null space* antar teks pada berkas PDF untuk menyimpan suatu data. Penelitian ini turut memanfaatkan *Huffman coding* guna membantu memperkecil jumlah data yang hendak disisipkan pada berkas PDF tersebut. Disebutkan bahwa dengan memanipulasi kode spasi “A0” dan “20” antar kata pada berkas PDF menunjukan hasil yang baik sehingga dapat digunakan untuk membantu dalam proteksi hak cipta, serta otentikasi berkas PDF.

Berdasarkan berbagai penelitian yang telah diungkapkan sebelumnya, pada penelitian ini sistem monitoring kontrak kerjasama akan dimodifikasi dengan menyertakan protokol *two central facilities* beserta algoritma AES dan *whitespace manipulation.* Protokol tersebut akan berperan dalam menjaga agar sistem hanya dapat melayani user yang telah terdaftar atau memiliki hak akses. Algoritma *whitespace manipulation* akan digunakan untuk melakukan klaim atas berkas PDF

sehingga berperan untuk menjaga integritas data, sedangkan algorima AES akan diterapkan pada proses enkripsi dan dekripsi saat proses pengiriman data. Penelitian ini diharapkan dapat memberikan gambaran baru seputar penggunaan protokol *two central facilities* di luar *e-voting*. Penelitian ini menjadikan sistem monitoring kontrak kerjasama PUSLITBANG tekMIRA sebagai studi kasus. Sistem hasil modifikasi memanfaatkan Oracle VM VirtualBox sebagai sarana untuk mensimulasikan keberadaan CLA dan CTF.

1.2. Rumusan Masalah

Rumusan masalah dalam penelitian ini adalah:

1. Bagaimana pengaruh penggunaan protokol *two central facilities* pada Sistem Monitoring Kontrak Kerjasama PUSLITBANG *tek*MIRA?
2. Bagaimana pengaruh algrotima AES dan *whitespace manipulation* pada Sistem Monitoring Kontrak Kerjasama PUSLITBANG *tek*MIRA berdasarkan aspek kerahasaiaan (*confidentality*), integritas data (*data integrity*), otentikasi (*authentification*), dan nir-penyangkalan (*non-repudiation*)?

1.3. Tujuan

Sejalan dengan permasalahan yang telah dirumuskan, maka tujuan yang ingin dicapai pada penelitian ini adalah:

1. Membuktikan pengaruh penggunaan protokol *two central facilities* pada Sistem Monitoring Kontrak Kerjasama PUSLITBANG *tek*MIRA serta melakukan evaluasi terhadap kinerjanya.
2. Membuktikan pengaruh penggunaan algoritma AES dan *whitespace manipulation* pada Sistem Monitoring Kontrak Kerjasama berdasarkan aspek kerahasaiaan (*confidentality*), integritas data (*data integrity*), otentikasi (*authentification*), dan nir-penyangkalan (*non-repudiation*).

1.4. Batasan Masalah

Batasan masalah yang diteliti antara lain:

1. Format *file* yang digunakan adalah PDF.
2. Ukuran *file* maksimum untuk keperluan penelitian adalah 500 KB. Batasan ukuran *file* tersebut disesuaikan dengan spesifikasi komputer yang digunakan.
3. Simulasi dari sistem yang dikembangkan akan dijalankan pada sebuah komputer dengan dua buah *virtual machine* dengan memanfaatkan Oracle VM VirtualBox.

1.5. Sistematika Penulisan

Dalam penyusunan skripsi ini, sistematika penulisan dibagi menjadi beberapa bab sebagai berikut:

BAB I PENDAHULUAN

Bab ini menguraikan tentang latar belakang masalah, rumusan masalah, maksud dan tujuan, batasan masalah, metode penelitian, dan sestematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini memaparakan beberapa teori yang mendukung dalam pembuatan perangkat lunak, seperti kritpografi, algoritma AES, penyembunyian informasi, *digital watermarking*, protokol, protokol *two central facilites*, CLA, dan CTF.

BAB III METODOLOGI PENELITIAN

Bab ini merupakan penjabaran dari implementasi algoritma AES dan *whitespace manipulation* pada Sistem Monitoring Kontrak Kerjasama PUSLITBANG *tek*MIRA yang menggunakan protokol *two central facilities*. Mencakup analisis, dan desain model sistem.

BAB IV HASIL PENELITIAN DAN PEMBAHASAN

Pada bab ini akan dibahas secara mendalam mengenai hal-hal yang dilakukan selama penelitian berlangsung, mulai dari proses modifkasi protokol *two central facilities*, pembangunan perangkat lunak, hingga proses pengujian protokol *two central facilities* serta algoritma AES dan *whitespace manipulation* yang akan digunakan untuk menjawab apa yang sudah dirumuskan dalam rumusan masalah.

BAB V KESIMPULAN DAN SARAN

Pada bab ini berisi tentang kesimpulan dari BAB IV dan saran yang diajukan agar dapat menja di bahan pertimbangan untuk rekomendasi penelitian selanjutnya.