

BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

Pada era teknologi sekarang ini, kebutuhan akan kecepatan dan keakuratan informasi mutlak diperlukan oleh siapa saja dan dimana saja. Kebutuhan akan informasi menjadi semakin kompleks, sehingga kemudahan dalam pengaksesan data dan informasi merupakan satu hal yang wajib diperhatikan. Seiring waktu berjalan, manusia dituntut untuk mampu memanfaatkan segala sumber daya teknologi untuk mendapatkan semua informasi tersebut. Dengan implementasi aplikasi teknologi informasi diharapkan akan membawa pengaruh besar dalam rangka perbaikan pola kehidupan manusia menuju masyarakat modern.

Perkembangan teknologi informasi saat ini telah mampu menjembatani pertukaran data dan informasi dua arah secara *online* menggunakan media internet. Saat ini, internet menjadi media yang paling praktis untuk melakukan komunikasi data, karena internet mampu menggabungkan ribuan bahkan jutaan komputer di seluruh dunia menjadi sebuah jaringan global. Di dalam jaringan internet terdapat milyaran data dan informasi yang bersifat kompleks dan detail yang bisa diakses oleh siapa saja dan dari mana saja. Dengan jaringan internet yang makin kompleks maka makin sulit pula sistem otentikasi menjaga keabsahan pengguna yang *login* pada sistem berbasis internet.

Dalam menyusun skripsi ini, penulis mengambil obyek penelitian pada cabang teknologi informasi terkait keamanan data, yaitu penggunaan sertifikat digital sebagai metode otentikasi klien pada *website*. Oleh karena itu, penulis memilih judul “ANALISIS DAN PERANCANGAN SISTEM OTENTIKASI KLIEN PADA WEBSITE MENGGUNAKAN SERTIFIKAT DIGITAL DENGAN SKEMA INFRASTRUKTUR KUNCI PUBLIK”. Skripsi ini berdasarkan studi implementasi aplikasi *website* dengan menerapkan penggunaan sertifikat digital untuk otentikasi klien.

Penggunaan sertifikat digital di Indonesia cenderung masih relatif sedikit. Dibuktikan dengan masih minimnya pengaplikasian sertifikat digital pada *website* di Indonesia dan juga kurangnya kesadaran masyarakat tentang keamanan data personal di dunia maya. Saat ini server *website* cenderung hanya menggunakan *username* dan *password* untuk mengidentifikasi dan menyaring pengguna *website*. Namun cara ini menjadi sangat rapuh dengan makin banyaknya *software* ilegal untuk melakukan pengambilan data di internet secara tersembunyi, termasuk mengambil data *username* dan *password* melalui teknik *spoofing* dan *cracking*.

Setelah itu, sistem otentikasi mengalami perkembangan lagi dengan adanya penambahan *captcha*. *Captcha* juga dianggap masih cukup baik untuk menyaring pengguna yang *login* ke sistem, namun memiliki kelemahan yaitu belum sepenuhnya menunjukkan identitas pengguna. Oleh karena itu, sertifikat digital merupakan solusi atas permasalahan ini. Data personal maupun institusional pemilik sertifikat digital telah terintegrasi didalamnya, sehingga menjamin bahwa pemilik sertifikat digital memang benar-benar pengguna yang *login* ke sistem.

Dalam manajemen sertifikat digital dikenal istilah Infrastruktur Kunci Publik (IKP). IKP adalah sebuah cara untuk otentikasi, pengamanan data dan perangkat anti sangkal. IKP dibangun dari beberapa sistem yang saling berkolaborasi. Dengan sistem yang dibangun ini, diharapkan informasi yang berharga dari pemilik *website* akan terjaga dan tidak bisa diakses dengan mudah oleh pengguna yang tidak berhak.

1.2. Rumusan Masalah

Adapun beberapa rumusan masalah yang bisa dirangkum berdasar latar belakang masalah di atas, antara lain adalah sebagai berikut:

1. Komponen apa saja yang terlibat dalam sistem otentikasi klien pada *website*.
2. Bagaimana cara membangun sistem otentikasi klien pada *website* yang relatif aman.
3. Bagaimana cara membangun aplikasi *website* dengan menerapkan penggunaan sertifikat digital untuk otentikasi klien.

1.3. Batasan Masalah

Dalam menyusun skripsi, penulis akan memberi batasan atas permasalahan yang diambil, agar penulisan isi tidak melebihi kerangka batasan. Adapun batasan masalahnya adalah sebagai berikut:

1. Penerapan atas sistem aplikasi yang dibuat, serta solusi atas permasalahan yang telah tercantum dalam rumusan masalah.

2. Perangkat lunak (*software*) yang digunakan dalam membuat aplikasi diantaranya adalah JDK, JBoss AS, MySQL, EJBCA, Apache, dan *web browser* serta beberapa *software* pendukung.

1.4. Tujuan Penelitian

Adapun tujuan dari penelitian yang penulis ajukan adalah sebagai berikut :

1. Bagi penulis
 - a. Sarana implementasi dari hasil proses pembelajaran selama masa perkuliahan di STMIK AMIKOM Yogyakarta.
 - b. Mendukung karir sebagai Petugas Komunikasi di Departemen Luar Negeri Republik Indonesia.
 - c. Salah satu syarat kelulusan untuk mendapat gelar Sarjana Komputer.
2. Bagi teknologi informasi
 - a. Penggunaan aplikasi teknologi informasi sebagai media informasi melalui sistem otentikasi yang aman.
 - b. Pemecahan atas permasalahan dalam penerapan aplikasi otentikasi klien pada sistem informasi berbasis *website*.

1.5. Manfaat Penelitian

Adapun manfaat dari penelitian yang penulis ajukan adalah sebagai berikut :

1. Bagi pengguna *website*

Memberi jaminan kepada pengguna *website* bahwa tidak ada pengguna lain yang bisa menggunakan hak aksesnya.

2. Bagi teknologi informasi

Sarana implementasi ilmu terapan dari teknologi informasi, serta memberikan kontribusi pada perkembangannya di Indonesia.

1.6. Sistematika Penulisan

Agar penyusunan skripsi dapat terkonsep sesuai urutan dan uraian secara sistematis, maka penulis akan menggunakan sistematika penulisan sebagai berikut:

Bab I. Pendahuluan

Pada bab ini akan diuraikan tentang latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, sistematika penulisan, dan rencana penelitian.

Bab II. Tinjauan Pustaka dan Landasan Teori

Pada bab ini akan dibahas tentang tinjauan pustaka dan landasan teori berupa paparan data dari beberapa bahan pustaka terkait penggunaan sertifikat digital untuk otentikasi klien pada *website* dan aplikasi yang akan dibangun oleh penulis.

Bab III. Analisis dan Perancangan Sistem

Pada bab ini akan diuraikan tentang analisis sistem otentikasi klien pada *website* dengan sertifikat digital menggunakan skema IKP yang saat ini umum digunakan, alat penelitian berupa *software* dan *hardware* yang digunakan, cara penelitian, metode penelitian, dan implementasi dari aplikasi yang dibangun. Diuraikan juga tentang perancangan aplikasi *website* yang digunakan sebagai sarana pengujian sistem otentikasi klien pada *website* dengan sertifikat digital.

Bab IV. Hasil Penelitian dan Pembahasan

Pada bab ini akan dibahas tentang pengujian aplikasi, hasil pengujian dan pembahasan hasil pengujian.

Bab V. Kesimpulan dan Saran

Pada bab ini berisi kesimpulan dari pembahasan atas permasalahan terkait implementasi aplikasi otentikasi klien pada *website* dengan menggunakan sertifikat digital. Penulis juga memberi saran yang diharapkan dapat memperbaiki aplikasi yang telah dibuat.

1.7. Rencana Penelitian

Rencana penelitian ini telah dijadwalkan selama 3 (tiga) bulan, dimulai pada Bulan Oktober 2009 sampai dengan Bulan Desember 2009, dengan jadwal selengkapnya sebagai berikut:

Tabel 1.1. Rencana Penelitian

No.	Uraian Kegiatan	Target Output	Jadwal Pelaksanaan																				
			Oktober				November				Desember												
			Minggu ke				Minggu ke				Minggu ke												
			1	2	3	4	1	2	3	4	1	2	3	4									
1.	Identifikasi a. Info mendasar tentang keamanan informasi, sertifikat digital dan skema PKI b. Mendata sistem yang sudah ada	Identifikasi mendasar untuk sistem aplikasi yang sudah digunakan dan keamanannya																					
2.	Pengumpulan Data a. Studi pustaka b. Questioner	Mendapatkan data selengkap-lengkapya tentang otentikasi klien pada website dengan sertifikat digital menggunakan skema IKP.																					
3.	Perancangan Aplikasi a. Skema alur pembuatan sertifikat digital dan penggunaannya b. Perkiraan penggunaan software c. Keamanan aplikasi	Rancangan sesuai skema IKP																					
4.	Pembuatan Aplikasi a. Realisasi rancangan aplikasi b. Konfigurasi aplikasi	Membangun aplikasi sesuai rancangan yang telah dibuat																					
5.	Uji Coba dan Evaluasi	Implementasi pembuatan sertifikat digital dan penggunaannya untuk otentikasi klien pada website																					
6.	Pendokumentasian Penelitian	Laporan penelitian																					