

BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi di Indonesia telah mengalami banyak kemajuan. Salah satu kebutuhan yang sangat besar akan teknologi informasi yaitu kebutuhan akan sistem informasi. Pada awal perkembangannya, arus informasi yang semakin marak untuk menggunakan media digital, bagi pihak-pihak perusahaan institusi dan terutama menjaga keamanan data atau organisasi tersebut agar terhindar dari gangguan pihak lain yang mempunyai pesan ataupun hal yang ingin disampaikan secara rahasia dan penting [1]. Digitalisasi menjadi suatu hal yang tidak dapat dihindari sehingga tiap-tiap pihak khususnya organisasi harus andal merespon perubahan agar dapat terus bersaing [2].

Politeknik Negeri Sriwijaya sebagai lembaga pendidikan memiliki aturan administrasi dalam menjalankan fungsinya sebagai sebuah institusi. Dalam pengelolaan administrasi di Politeknik Negeri Sriwijaya, beberapa prosedur distribusi dokumen masih dilakukan secara konvensional dengan melalui tahapan yang cukup panjang. Salah satu permasalahan yang sering ditemui yaitu apabila pimpinan atau pihak terkait yang dibutuhkan sedang tidak berada ditempat, maka proses administrasi akan ikut terhambat.

Dewasa ini, distribusi dokumen surat-menyurat sudah mulai digantikan dengan surat digital seiring dengan semakin berkembangnya teknologi. Surat digital ialah surat yang ditulis atau didistribusikan menggunakan media digital berdasarkan fitur yang tersedia dalam media tersebut [3]. Selain dianggap lebih efisien, penggunaan surat digital dapat menghemat waktu dan sumber daya karena sifatnya yang tidak terbatas pada ruang dan waktu.

Disisi lain, suatu komunikasi dengan pihak lain terkadang memerlukan proses pertukaran informasi, sehingga dibutuhkan suatu mekanisme untuk menjamin keabsahan informasi tersebut [4]. Untuk menerapkan sistem digital dalam proses administrasi maka diperlukan sebuah sistem validasi yang dapat membuktikan

keaslian informasi yang diperoleh dari media digital benar oleh pihak yang bersangkutan. Hal ini dapat diatasi menggunakan metode autentikasi.

Ada beberapa metode untuk melakukan autentikasi. Salah satunya adalah menggunakan *password* dan *username*. Namun penggunaan kedua hal tersebut tidak dapat memastikan bahwa hak akses pengguna tidak dapat diretas oleh pengguna lain. Kerahasiaan merupakan bagian penting untuk menjaga isi informasi dari siapapun kecuali yang memiliki otoritas atau kunci rahasia untuk membuka informasi tersebut [5].

Salah satu metode yang digunakan untuk menambah lapisan keamanan tersebut adalah dengan menambahkan metode *One Time Password* (OTP), yaitu sebuah metode autentikasi yang menggunakan satu kunci *password* bersifat sementara dan akan hangus setelah beberapa saat [6]. *Password* ini merupakan sebuah kode acak yang selalu berubah dan hanya bisa dipakai satu kali [7].

Pada penelitian ini, akan digunakan metode *One Time Password* sebagai sistem validasi bahwa persetujuan yang diberikan pada surat digital benar oleh pihak yang bersangkutan. Kode acak didapat dengan menggunakan algoritma SHA-512 sebagai pembangkit kode OTP. Algoritma SHA-512 termasuk jenis fungsi *hash* yang merupakan pengembangan dari algoritma SHA-1 [8]. Algoritma ini merupakan algoritma dengan panjang nilai *hash* yang dihasilkan sepanjang 512 bit sebagai fungsi *hash* [6].

Sistem ini menggunakan teknologi android untuk memudahkan akses ke sistem administrasi dengan fitur yang mengutamakan informasi dan kecepatan akses agar lebih mudah dikunjungi sehingga proses persetujuan surat dapat dilakukan dari mana saja dengan memanfaatkan *QR code* sebagai bukti digital. *QR code* (*Quick Response Code*) ialah salah satu jenis kode matriks yang dikembangkan sebagai kode yang dapat menerjemahkan konten dengan kecepatan tinggi [9]. Metode *QR code* dapat menyimpan data di dalamnya yang dapat mengakses informasi data tersebut dengan respons cepat [10] melalui perangkat seluler yang terhubung ke *database* [11]. Pemilihan *mobile* android untuk salah satu pengembangan aplikasi selain lebih mudah dalam pengoperasiannya dan juga sifat *mobile* yang fleksibel jadi salah satu alasannya.

Berdasarkan analisis tersebut, maka penulis tertarik dan ingin menuangkannya dalam bentuk tugas akhir yang berjudul “**Perancangan Aplikasi Autentikasi Surat Digital dengan Metode *One Time Password* SHA-512 di Kantor Pusat Administrasi Politeknik Negeri Sriwijaya**”.

1.2 Perumusan Masalah

Berdasarkan latar belakang yang telah dipaparkan sebelumnya maka didapatkan perumusan masalah sebagai berikut:

1. Bagaimana tahapan perancangan aplikasi untuk meningkatkan proses administrasi surat-menyurat di Kantor Pusat Administrasi Politeknik Negeri Sriwijaya?
2. Bagaimana tahapan perancangan algoritma SHA-512 untuk membangkitkan kode *One Time Password* sebagai sistem validasi persetujuan surat digital?
3. Bagaimana hasil pengujian implementasi tiap menu pada aplikasi surat digital di Kantor Pusat Administrasi Politeknik Negeri Sriwijaya?
4. Bagaimana hasil pengujian tingkat keamanan algoritma SHA-512 pada kode *One Time Password* sebagai sistem validasi untuk persetujuan surat digital?

1.3 Pembatasan Masalah

Agar permasalahan yang dibahas pada tugas akhir ini tidak keluar dari topik pembahasan maka batasan yang akan dibahas adalah mengenai hal-hal sebagai berikut:

1. Data administrasi yang digunakan pada aplikasi ini yaitu berupa surat masuk, surat keluar dan disposisi surat.
2. Aplikasi yang akan dibangun berjalan pada *platform* android dan web.
3. Kode *One Time Password* sebagai sistem validasi surat dikirim melalui *email* pengguna.

1.4 Tujuan

Adapun tujuan dari pembuatan tugas akhir ini adalah sebagai berikut :

1. Membangun aplikasi surat digital untuk meningkatkan sistem administrasi surat-menyurat di Politeknik Negeri Sriwijaya.
2. Membangun sistem validasi persetujuan pada surat digital menggunakan metode *One Time Password* algoritma SHA-512.
3. Dapat menganalisis kinerja aplikasi surat digital yang diimplementasikan di Politeknik Negeri Sriwijaya.
4. Dapat menganalisis kinerja algoritma SHA-512 pada kode *One Time Password* sebagai sistem validasi untuk persetujuan surat digital.

1.5 Manfaat

Adapun manfaat yang diharapkan pada penulisan tugas akhir ini, antara lain:

1. Membantu proses administrasi surat-menyurat di Kantor Pusat Administrasi Politeknik Negeri Sriwijaya agar berjalan lebih efektif.
2. Membantu proses administrasi untuk persetujuan surat digital pada aplikasi agar lebih terjamin keamanannya menggunakan *One Time Password* SHA-512.
3. Membuktikan kinerja aplikasi surat digital untuk mendukung proses surat-menyurat di Politeknik Negeri Sriwijaya.
4. Membuktikan kinerja algoritma SHA-512 pada kode *One Time Password* sebagai sistem validasi untuk persetujuan surat digital.

1.6 Metode Penulisan

Untuk mempermudah penulisan dalam penyusunan tugas akhir maka metode yang digunakan adalah sebagai berikut:

1.6.1 Metode Studi Pustaka

Metode pengumpulan data mengenai pembuatan aplikasi dengan Metode Pengembangan Perangkat Lunak *Prototype dan One Time Password* sebagai sistem autentikasi menggunakan algoritma SHA-512 yang bersumber dari buku, internet, artikel, dan lain-lain.

1.6.2 Metode Eksperimen

Metode ini dilaksanakan dengan cara merancang aplikasi yang akan dibuat.

1.6.3 Metode Observasi

Metode pengamatan terhadap permasalahan dan data yang ada sebagai acuan pengambilan informasi. Dalam hal ini, observasi dilakukan di Kantor Pusat Administrasi Politeknik Negeri Sriwijaya Palembang.

1.6.4 Metode Wawancara

Metode yang dilakukan dengan cara wawancara atau konsultasi dengan dosen pembimbing, pihak *staff* UPT TIK, *staff* Bagian Administrasi Umum dan Keuangan Politeknik Negeri Sriwijaya dan pihak lain yang berhubungan dengan proyek penulis.

1.7 Sistematika Penulisan

Untuk mempermudah dalam penyusunan laporan tugas akhir yang lebih jelas dan sistematis maka penulis membaginya dalam sistematika penulisan yang terdiri dari beberapa bab pembahasan dengan urutan sebagai berikut:

BAB I PENDAHULUAN

Bab ini mengutarakan latar belakang dan alasan pemilihan judul, tujuan penulisan, pembatasan masalah, metodologi dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini menguraikan tentang landasan teori yang mendukung dan mendasari cara kerja dari aplikasi yang akan digunakan.

BAB III METODOLOGI PENELITIAN

Bab ini menjelaskan tentang proses pembuatan aplikasi seperti perancangan dan tahap-tahap perancangan, blok-blok diagram, langkah kerja aplikasi dan prinsip kerja dari aplikasi.

BAB IV HASIL DAN PEMBAHASAN

Bab ini berisikan tentang pembahasan dan analisa aplikasi.

BAB V KESIMPULAN DAN SARAN

Pada bab ini berisikan tentang kesimpulan dan saran dari pokok permasalahan yang telah dievaluasi pada bab-bab sebelumnya.