BAB I
PENDAHULUAN

1.1 Latar Belakang

Pada era modern ini, sudah banyak sekali bidang yang menerapkan digitalisasi untuk menyelesaikan permasalahan yang dihadapi, sebagai contoh adalah pengarsipan dokumen surat, Pengarsipan adalah suatu proses yang dimulai dari penciptaan, penerimaan, pengumpulan, pengaturan, pengendalian, pemeliharaan dan perawatan serta penyiapan arsip berdasar pada ketentuan yang berlaku [1].

Direktorat Pengembangan Teknologi Informasi (Dit. PTI) adalah salah satu Unit Kerja pada Universitas Bhayangkara Jakarta Raya (Ubhara Jaya) yang mana adalah sebuah Perguruan Tinggi Swasta yang berada dibawah naungan Yayasan Brata Bhakti. Sebagai salah satu Unit Kerja pada instansi pendidikan, Dit. PTI tentu mempunyai banyak sekali dokumen seperti Nota Dinas (ND) masuk mapun keluar, Surat Tugas (ST) dan Surat Keputusan (Skep) yang masuk setiap hari, minggu ataupun bulan bahkan tahun. Beban kerja pengarsipan yang dilakukan Dit. PTI dilihat dari masuk dan keluarnya dokumen surat, untuk surat yang masuk berkisar 5 sampai 6 surat perharinya, ini sudah termasuk Surat Tugas (ST), Surat Keputusan (Skep) dan Nota Dinas (ND). Dan untuk surat yang keluar jumlahnya relatif berbeda perharinya, dikarenakan kebutuhan dari ND yang masuk. Dengan masuk dan keluarnya dokumen surat yang terjadi setiap hari, dan jika menumpuk tentunya akan sulit sekali untuk mencari dokumen tertentu jika dibutuhkan kembali.

Untuk menyelesaikan masalah tersebut, Dit. PTI mempunyai sebuah aplikasi berbasis web dengan nama Arsip Surat untuk mengarsipkan dokumen surat serta dapat mempermudah dalam pencarian dokumen surat. Sebelum dilakukannya penelitian ini, penulis pernah beberapa kali memberikan kontribusi pada aplikasi arsip surat yang sedang berjalan ini, diantaranya:

1. Migrasi penyimpanan *file* arsip dari *server* FTP (*File Transfer Protocol*) ke *Google Drive* dikarenakan *server* lokal untuk penyimpanan penuh dan tidak bisa diakses.
2. Perbaikan *query* yang menyebabkan duplikasi dari *list* data yang tampil pada aplikasi.
3. Perbaikan dalam menampilkan *list* data yang melambat dikarenakan data membawa *base*64 *file* arsip yang julmah *string*nya sangat panjang.
4. Menambahkan *dropdown* untuk *filter* data arsip yang ditampilkan berdasarkan tahun.
5. Perbaikan *export* data dari .csv menjadi .xlsx, sekaligus perbaikan dalam memilih data apa saja yang akan ditampilkan ketika di-*export*.

Meskipun begitu aplikasi arsip surat ini masih hanya terbatas pada pengarsipan dokumen surat saja dan belum ada pengamanan lebih lanjut untuk mengamankan dokumen surat yang akan diarsipkan serta pengamanan pada saat mengakses dokumen surat yang sudah diarsipkan kedalam aplikasi dan dikhawatirkan terjadi kebocoran data.

Arsip berfungsi sebagai salah satu rekam jejak atas dokumen yang diterima oleh instansi maupun yang dikirim oleh instansi. Umumnya arsip memliki fungsi sebagai penunjang aktivitas adminstrasi, sarana pengambil keputusan, bukti pertanggungjawaban, sumber informasi, dan sarana komunikasi.

Untuk mencegah kebocoran data serta mengamankan dokumen surat lebih baik lagi, diperlukan suatu metode untuk menjaga kemanan dokumen surat yang sudah diarsipkan kedalam aplikasi, yaitu dengan menggunakan metode kriptografi. Pada metode kriptografi ada proses yang disebut dengan enkripsi yaitu penyamaran data yang pada awalnya adalah *plaintext* menjadi *chipertext*, dan ada proses yang disebut dengan dekripsi yaitu kebalikan dari enkripsi untuk mengubah *chipertext* kembali menjadi *plaintext*.

Plaintext adalah teks asli informasi yang masih bisa dibaca secara umum, dapat diartikan juga sebagai masukan dalam suratu proses enkripsi atau juga sebagai hasil keluaran dari proses dekripsi. *Ciphertext* adalah *plaintext* yang sudah

disembunyikan dan sudah tidak bisa lagi dibaca secara umum, biasanya *ciphertext* dihasilkan dari proses enkripsi.

Enkripsi adalah proses dimana informasi atau data yang hendak dikirim diubah menjadi bentuk yang hampir tidak dikenali sebagai informasi awalnya dengan menggunakan algoritma tertentu. Dekripsi adalah kebalikan dari enkripsi yaitu mengubah kembali bentuk tersamar tersebut menjadi informasi awal. Sebuah pesan atau data yang masih asli dan belum mengalami penyandian dikenal dengan istilah *plaintext* [2].

Untuk implementasi metode kriptografi pada pengembangan sistem ini akan menggunakan algoritma AES-256. *Advanced Encryption Standard* (AES) merupakan algoritma *symmetric key cryptographic* yang dapat digunkan untuk mengamakan data. Algoritma AES (*Advanced Encryption Standard*) adalah blok*chipertext* simetrik yang dapat mengenkripsi (*encipher*) dan dekripsi (*decipher*) informasi. Algoritma AES (*Advanced Encryption Standard*) mengunakan kunci kriptografi 128, 192, dan 256 bits untuk mengenkrip dan dekrip data pada blok 128 bits. Pemilihan ukuran blok data dan kunci akan menentukan jumlah proses yang harus dilalui untuk proses enkripsi dan dekripsi [2]. Alasan penulis memilih algoritma AES pada penelitian ini salah satunya adalah algoritma AES ini sudah ditetapkan sebagai standar pengamanan data oleh NIST (*National Institute of Standards and Technology*) dan digunakan oleh NSA (*National Security Agency*) yang keduanya merupakan badan atau organisasi besar di Amerika Serikat. Alasan lainnya adalah dari panjangnya jumlah kunci algoritma AES (128-bit, 192-bit, 256-bit) membuat algoritma ini sangat kuat terhadap serangan *brute force*.

Pada penelitian skripsi ini, penulis lebih menitikberatkan pada keamanan dokumen surat sebelum menggunakan dan sesudah menggunakan metode enkripsi algoritma AES (*Advanced Encryption Standard*). Karena jika dilihat dari sisi hak akses dokumen surat, sebelumnya sudah ada pada aplikasi arsip surat yang aksesnya dibedakan tiap unit kerja, meskipun pengguna yang aktif hanya Dit, PTI saja. Setiap unit kerja hanya bisa melakukan read write pada dokumen suratnya masing-masing. Untuk proses enkripsi terjadi di belakang aplikasi dan user tidak akan merasakan perbedaan saat mengakses dokumen sebelum atau setelah

diterapkannya metode enrkipsi algoritma AES-256 (*Advanced Encryption Standard*) ini. Dengan diimplementasikannya algoritma AES-256 (*Advanced Encryption Standard*) pada pengembangan sistem ini, diharapkan pengarsipan dokumen surat pada aplikasi arsip surat berbasis web akan menjadi lebih baik dan aman.

1.2 Identifikasi Masalah

Dari latar belakang diatas, penulis dapat mengidentifikasi masalah dari penelitian skripsi ini, yaitu belum diterapkannya metode untuk mengamankan dokumen surat yang akan diarsipkan menggunakan aplikasi dan pengamanan pada saat mengakses dokumen surat yang sudah diarsipkan kedalam aplikasi.

1.3 Rumusan Masalah

Berdasarkan uraian diatas, dapat dirumuskan masalah utama yang penulis temukan dalam penelitian skripsi ini yaitu: "Bagaimana cara mengimplementasikan algoritma AES-256 (*Advanced Encryption Standard*) pada sistem yang sudah berjalan, yaitu aplikasi arsip surat berbasis web untuk mengamankan dokumen surat yang diarsipkan menggunakan aplikasi dan pengamanan pada saat mengakses dokumen surat yang sudah diarsipkan menggunakan aplikasi di Direktorat Pengembangan Teknologi Informasi Universitas Bhayangkara Jakarta Raya".

1.4 Batasan Masalah

Pembahasan yang dilakukan dalam penelitian skripsi ini memiliki beberapa batasan masalah, diantaranya:

1. Pengembangan sistem hanya dilakukan pada satu aplikasi, yaitu aplikasi arsip surat berbasis web.
2. Lingkup penelitian hanya dilakukan pada Unit Kerja Direktorat Pengembangan Teknologi Informasi Universitas Bhayangkara Jakarta Raya.
3. Pengembangan sistem ini dilakukan untuk memperkuat keamanan dokumen digital pada aplikasi arsip surat berbasis web.

1.5 Tujuan dan Manfaat Penelitian

Tujuan dan manfaat dari penelitian skripsi ini dengan membawa tema implementasi atau pengembangan sistem adalah sebagai berikut:

1. Bagi Penulis
    a. Untuk memenuhi salah satu syarat kelulusan strata statu yang telah ditentukan oleh universitas.
    b. Dapat menerapkan ilmu yang telah didapatkan penulis selama perkuliahan.
2. Bagi Instansi

    Dapat menghasilkan sistem aplikasi yang telah diterapkan metode pengamanan data untuk mengamankan dokumen arsip surat yang akan diarsipkan menggunakan aplikasi serta pengamanan pada saat mengakses dokumen surat yang sudah diarsipkan kedalam aplikasi.
3. Bagi Akademis

    Hasil dari penelitian skripsi ini dapat dijadikan bahan bacaan dan referensi bagi pembaca umum yang akan melakukan penelitian dengan tema atau judul serupa.

1.6 Sistematika Penulisan

Adapun sistematika dalam penulisan laporan penelitian skripsi ini adalah sebagai berikut:

Bab I Pendahuluan

Bab ini menjelaskan uraian singkat mengenai latar belakang, identifikasi masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, tempat dan waktu penelitian, metode penelitian, dan sistematika penulisan.

Bab II Landasan Teori

Bab ini memuat tinjauan pustaka yang berhubungan dengan topik penelitian, meliputi hal-hal yang berhubungan dengan peracangan sistem

informasi, arsip atau pengarsipan, surat, dan berbagai teori penunjang yang berhubungan dengan materi yang terkait dengan tugas akhir.

Bab III Metodologi Penelitian

Bab ini menjelaskan tentang obyek penelitian, kerangka penelitian, analisis sistem berjalan, permasalahan, analisis ususlan sistem, analisis kebutuhan sistem.

Bab IV Perancangan Sistem dan Implementasi

Bab ini menjelaskan tentang hasil yang dicapai dari penelitian skripsi yang dilakukan serta pembahasan lebih lanjut mengenai hasil yang telah dicapai.

Bab V Penutup

Bab ini merupakan bab terakhir yang berisi kesimpulan, dan saran yang diusulkan untuk pengembangan lebih lanjut agar tercapai hasil yang lebih baik.