BAB I
PENDAHULUAN

1.1 Latar Belakang

Komputer sudah menjadi salah satu bagian dalam manusia untuk memenuhi berbagai kebutuhan hidup. Pada masa teknologi seperti saat ini berbagai peralatan sudah dikomputeriasi terutama pada kegiatan manusia yang berulang-ulang. Komputer juga digunakan sebagai alat penyimpanan serta menjadi alat kontrol yang handal berdasarkan program yang diberikan oleh manusia terhadapnya. Komputer dapat saling berhubungan melalui sistem jaringan, dimana antara komputer satu dengan lainnya menggunakan sebuah protokol sebagai penghubungnya. Sistem jaringan telah berkembang dengan begitu pesat, pada saat ini jaringan komputer tak hanya menggunakan media kabel sebagai penghantar data namun telah menggunakan internet sebagai media perantaranya.

Menggunakan internet seorang pengguna dapat menjelajah kedunia maya dengan leluasa. Penggunaan jaringan internet juga telah digunakan untuk perusahaan, organisasi maupun individu untuk memenuhi kebutuhan sehari-hari seperti untuk pertukaran sebuah informasi atau data. Pertukaran informasi atau data haruslah diimbangi dengan keamanan yang memadahi mengingat kebutuhan manusia atas kerahasiaan suatu informasi agar tidak terjadi tindak kejahatan seperti pencurian yang dapat merugikan perseorangan, organisasi atau perusahaan.

Keamanan jaringan dalam komputer sudah menjadi bagian yang sangatlah penting dalam sistem untuk menjaga validitas dan integritas data. Dengan adanya keamanan yang memadahi dapat menjaga aset perusahaan agar tetap aman sehingga dapat mewujudkan visi dan misi. Bagi perusahaan, instansi maupun

individu yang menggunakan alat bantu teknologi informatika sebagai operasional, faktor keamanan menjadi salah satu yang utama karena menyangkut data dan aset. Salah satu cara untuk menjaga keamanan tersebut adalah dengan menerapkan hak akses dan enkripsi pada login sebuah aplikasi menggunakan SHA-1 (*Secure Hash Algorithm*) pada id (*password*).

Hak akses merupakan sebuah batasan seorang user untuk masuk kedalam sistem. Adanya pembatasan tersebut sebuah informasi atau data akan terhindar dari kesalahan pemberian sebuah informasi dari orang yang tidak berhak. SHA-1 merupakan kriptografi dengan metode pengenkripsian dimana data password akan dienkripsi atau diubah kedalam bentuk hash pada saat awal registrasi/pendaftaran yang tersimpan di database agar tidak mudah diketahui orang lain. *Password* yang telah dienkripsi tersebut nantinya digunakan sebagai validitas *user* dan *password* ketika *login*. Jika *user* dan *password* tidak sama atau invalid akan dilakukan penolakan akses ke sistem.

Dari uraian diatas serta mengingat kebutuhan akan kerahasiaan dari user, penulis mencoba membangun keamanan pada login user. Penulis mengangkat masalah tersebut kedalam penyusunan Skripsi yang berjudul "Sistem Keamanan Login Menggunakan Hak Akses dan Kriptografi".

1.2 Rumusan Masalah

Mengingat luasnya cakupan masalah yang timbul diatas, maka dapat dirumuskan beberapa masalah sebagai berikut:

1. Bagaimana menciptakan sistem autentikasi *id* dan *password* pada *user* yang aman?

2. Bagaimana mencegah pengaksessan data dari pihak yang tidak memiliki wewenang?

1.3 Batasan Masalah

Berdasarkan rumusan masalah diatas maka dapat diberikan batasan masalah sebagai berikut:

1. Autentikasi yang diteliti terfokus pada sisi *user*.
2. Tidak membahas sistem secara keseluruhan hanya terfokus pada sistem login.
3. Ruang lingkup yang dijalankan terfokus pada sisi *user*.
4. Bahasa pemrograman yang digunakan adalah php dan html.
5. Aplikasi ini dibuat menggunakan dreamweaver, MySQL dan XAMPP, browser mozilla.
6. Media yang digunakan adalah laptop, jaringan local dan seperangkat *server local*.
7. Pendemoan hanya dilakukan pada jaringan lokal (*intra*).

1.4 Maksud dan Tujuan Penelitian

Semakin berkembangnya kemajuan teknologi setiap harinya maka akan semakin dibutuhkan keaamanan yang memadahi pula untuk mengamankan aset bagi perusahaan, instansi maupun individu. Dengan diterapkannya enkripsi pada *login user* menggunakan algoritma SHA-1 sebagai autentikasi untuk keamanan akan membantu dalam mengamankan aset dari tindak kejahatan serta dapat mewujudkan visi serta misi organisasi atau perusahaan.

1.5 Manfaat Penelitian

Hasil dari penelitian ini diharapkan dapat memberikan manfaat kepada:

1. Penulis

   Merupakan syarat utama dalam mencapai kelulusan serta dapat menerapkan ilmu pengetahuan yang telah diperoleh penulis selama duduk dibangku perkuliahan.

2. Masyarakat

   Karya ilmiah ini dapat menjadi acuan dalam pengembangan selanjutnya tentang keamanan data dari tindak kejahatan dibidang IT.

1.6 Metode Penelitian

Metode Penelitian digunakan untuk memudahkan pada saat melakukan pencarian sumber-sumber data maupun teori-teori pendukung karya ilmiah. Dengan diterapkannya metode penelitian, karya ilmiah menjadi lebih terarah sesuai tujuan dan menghindari dari plagiatisme.

1.6.1 Metode Pengumpulan Data

1.6.1.1 Metode Observasi

Tahap ini dilakukan pengamatan secara langsung pada objek tentang keamanan *login* yang telah diterapkan, untuk pengembangan selanjutnya.

1.6.1.2 Metode Wawancara

Tahap ini dilakukan wawancara terhadap narasumber yang memiliki data-data operasional perusahaan. Wawancara ini dilakukan untuk mendapatkan informasi yang menjadi dasar untuk melakukan penelitian.

1.6.1.3 Metode Literatur

Tahap ini dilakukan untuk mencari dan mempelajari sumber-sumber informasi dari artikel, jurnal dan internet yang berkaitan dengan keamanan jaringan login menggunakan SHA-1.

1.7 Sistematika Penulisan

Untuk memperoleh gambaran yang mudah dimengerti dan komperehensif mengenai isi dari penulisan skripsi ini, secara global dapat dilihat dari sistematika pembahasan dibawah ini:

BAB I : PENDAHULUAN

Pada BAB I membahas tentang kerangka penulisan dan meliputi latar belakang masalah, batasan masalah, tujuan penelitianm manfaat penelitian, metode penelitian dan sistematika penulisan yang digunakan dalam penyusunan skripsi.

BAB II : LANDASAN TEORI

Pada BAB II berisi mengenai tinjauan pustaka serta teori-teori yang berasal dari studi literatur bersumber dari buku, jurnal dan internet. Pada skripsi ini studi literatur tersebut akan penulis jadikan sebagai bahan panduan dalam membangun keamanan login dengan metode SHA-1.

BAB III : ANALISIS DAN PERANCANGAN

Pada BAB III berisi mengenai bagaimana menganalisa dan merancang keamanan akun klient agar tidak mudah diketahui orang.

BAB IV : IMPLEMENTASI DAN PEMBAHASAN

Pada BAB IV berisi mengenai tata cara pembuatan dan urutan dalam pekerjaan, hasil yang akan diperoleh saat proses berlangsung serta hasil akhirnya.

BAB V : PENUTUP

Pada BAB V berisi mengenai kesimpulan dan saran dari penulis mengenai pengembangan Penerapan SHA-1 Sebagai Keamanan Login dan beberapa informasi daftar pusataka.