BAB III

ANALISIS SISTEM YANG BERJALAN

A. Gambaran Umum Objek Penelitian

Objek penelitian yang digunakan oleh penulis dalam penelitian ini adalah para individu yang tidak memiliki sistem secara independen layaknya perusahaan untuk mengamankan kata sandi dan dokumen serta data-data penting yang bersifat rentan terhadap seranga. Masalah keamanan merupakan salah satu aspek penting dari sebuah sistem informasi, sayang sekali masih banyak pihak yang kurang peka dan perhatian dalam masalah keamanan ini.

Saat ini dunia tengah berada dalam era informasi, pada era informasi keberadaan suatu informasi mempunyai arti dan peranan yang sangat penting bagi semua aspek kehidupan, serta merupakan salah satu kebutuhan hidup bagi semua orang baik individual maupun organisasi, sehingga dapat dikatakan bahwa dalam masyarakat informasi, informasi telah berfungsi sebagaimana layaknya aliran darah sumber kehidupan bagi tubuh manusia. Salah satu temuan yang memberikan pengaruh paling besar dalam masyarakat informasi adalah ditemukannya internet. Hadirnya internet sebagai bentuk teknologi baru menyebabkan manusia tidak mampu terlepas dari arus komunikasi dan informasi. Internet telah menyebabkan terjadinya satu lompatan besar dalam kehidupan. Sama halnya dengan teknologi lainnya, internet tidak bebas nilai. Teknologi akan menjadi efektif jika kita memberi perhatian pada kegunaan dari teknologi yang disesuaikan dengan nilai-nilai sosial maupun pribadi serta adanya peraturan pemerintah yang melindungi masyarakat dari dampak negatif yang ditimbulkannya.

Berdasarkan berbagai kejadian pada beberapa tahun ke belakang, Indonesia merupakan negara yang lemah *cyber-securitynya*. Hal ini dapat diketahui dari maraknya berbagai kejadian, salah satunya adalah peretasan terhadap data kartu debit nasabah sebuah bank karena hacker berusaha menyusup ke sistem pengamanan kartu nasabah bank yang terjadi pertengahan Mei 2014 menjadikan catatan betapa buruknya *cyber-security* di Indonesia.

B. Analisis Sistem yang Berjalan/ Analisis Kesenjangan

Indonesia sebenarnya saat ini tengah dalam keadaan mendesak *cyber-security* atau keamanan dunia maya karena melihat kenyataan bahwa tingkat kejahatan di dunia maya atau *cyber crime* di Indonesia sudah mencapai tahap memprihatinkan. Namun berbeda dengan penangganan kejahatan lainnya, *cyber-security* membutuhkan pemikiran yang komprehensif untuk menangganinya.

C. Metodologi Penelitian

Pada penelitian ini penulis menggunakan teknik pengumpulan data dan analisis data kualitatif. Data yang dibutuhkan berupa sejumlah data-data rahasia yang bersifat nyata seperti username/ email dari kata sandi sejumlah akun yang sering digunakan pada umumnya.

1. Teknik Pengumpulan Data

Untuk mendukung keperluan penelitian ini, penulis memerlukan sejumlah data pendukung. Teknik pengumpulan data yang digunakan dalam penelitian ini adalah teknik kualitatif.

a. Data yang dibutuhkan oleh penulis

1. Data primer

Data primer adalah data yang diperoleh langsung dari lapangan seperti dengan melalui metode observasi.

2. Data sekunder

Data sekunder adalah dokumen-dokumen atau literatur-literatur dari buku, internet, jurnal, dan lain sebagainya. Pengumpulan data sekunder dilakukan dengan mengambil seluruh/ sebagian dari sekumpulan data yang telah dicatat atau dilaporkan.

b. Teknik pengumpulan data yang digunakan

1. Studi Pustaka

Studi pustaka adalah jenis pengumpulan data yang meneliti berbagai macam dokumen yang berguna yang berhubungan dengan penelitian, studi pustaka yang dilakukan dalam penelitian ini adalah studi pustaka sekunder. Dimana studi pustaka sekunder adalah dokumen yang ditulis berdasarkan oleh laporan/ cerita orang lain seperti biografi dan jurnal serta buku-buku berisikan teori-teori yang menjadi landasan penelitian ini.

2. Dokumentasi

Pada penelitian ini, penulis membutuhkan data berupa sampel-sampel data yang nyata yang digunakan oleh penulis yang nantinya akan disimpan di dalam database dengan metode kriptografi algoritma AES dan digunakan untuk proses *testing* dan autentikasi pada sistem.

2. Teknik Analisis Data

A. Metode Algoritma AES

Penulis akan menganalisis efektivitas sistem dan penggunaannya terhadap data yang ada, sehingga proses login dapat dibuat menjadi lebih efisien dan aman.

3. Teknik Pengukuran Data

Teknik pengukuran data yang digunakan oleh penulis adalah berdasarkan parameter dari enkripsi AES atau yang lebih dikenal dengan Rijndael. Metode enkripsi ini menyimpan informasi menggunakan algoritma penyandian blok. Blok menyusun masukan teks biasa dan keluaran ciphertext (teks tersandikan), yang diukur dalam bit. Secara keseluruhan, AES terdiri dari tiga penyandian blok yaitu AES-128, AES-192 dan AES-256. Masing-masing penyandian AES mengenkripsi dan dekripsi data dalam blok 128 bit menggunakan kunci kriptografi untuk 128, 192 dan 256-bit, dengan 256-bit merupakan yang paling aman. Untuk kunci 128-bit, ada 10 putaran proses enkripsi, 12 putaran untuk kunci 192-bit dan 14 putaran untuk kunci 256-bit. Berikut ini adalah operasi Rijndael (AES)

1. Ekspansi kunci utama.
2. Pencampuran subkey.
3. Ulang dari i=1 sampai i=10 Transformasi : ByteSub (subtitusi per byte) ShiftRow (Pergeseren byte perbaris) MixColumn (Operasi perkalian GF(2) per kolom).
4. Pencampuran subkey (dengan XOR).
5. Transformasi : ByteSub dan ShiftRow.
6. Pencampuran subkey.

Teknik pengukuran data yang digunakan penulis dalam sistem ini adalah 256-bit. Penulis menggunakan kriptografi aes dengan panjang kunci 256-bit

karena semakin panjang kunci enkripsi, semakin sulit untuk membukanya, selain itu AES256 sudah dianggap sangat aman dan secara teoritis tahan terhadap serangan paksa komputer quantum.