BAB I

PENDAHULUAN

1.1 Latar Belakang

Data dan sistem informasi adalah dua hal yang sangat penting saat ini. Berbagai instansi, perusahaan, organisasi, dan lainnya menggunakan teknologi *database* untuk menyimpan dan mengelola perusahaan dan organisasinya. Setelah berkembangnya kemudahan dalam teknologi komunikasi dan informasi hingga kini dirasa penting untuk adanya pengamanan khusus dalam mengamankan informasi dalam komunikasi, karena keamanan suatu sistem merupakan hal yang sangat penting demi menjaga ketersediaan, integritas, dan kerahasiaan data pada suatu institusi atau organisasi. [1]

Sebagaimana diberitakan oleh harian Kompas, Sebulan menjelang pemungutan suara, situs Komisi Pemilihan Umum (KPU) diserang para peretas. Mereka meretas situs KPU menggunakan Internet Protocol (IP) Address dari luar negeri. Ketua KPU Arief Budiman membenarkan adanya peretasan situs KPU (Rakhmat Nur Hakim, Maret 2019). Tirto.id juga memberitakan bahwa sistem keamanan Bank Mandiri mengalami gangguan. Dan Bank Mandiri pun membenarkan soal gangguan pada sistem mereka yang menyebabkan terjadinya pengurangan dan penambahan saldo tabungan nasabah (Alfian Putra Abdi, Juli 2019).

Kedua contoh kasus di atas menyatakan dengan jelas bahwa keamanan data dan keamanan sistem informasi adalah hal yang sangat penting. Salah satu cara

untuk menjaga tiga aspek dalam keamanan sistem informasi yaitu menggunakan ilmu kriptografi. Kriptografi sudah sangat lazim digunakan dalam kehidupan sehari-hari manusia. Contohnya untuk mengirim data, aplikasi-aplikasi tertentu akan mengenkripsi data yang dikirim terlebih dahulu dan ketika sampai ke penerima data didekripsi kembali. Bahkan, untuk login ke email membutuhkan fungsi hash untuk memeriksa kata sandi. Tentunya hal-hal tersebut sangat vital untuk digunakan karena alasan keamanan dan privasi.

Untuk menjaga integritas data dari suatu data, diciptakan suatu mekanisme yang disebut digital signature atau sering juga disebut nilai hash, yaitu kode khusus yang dihasilkan dari fungsi penghasil digital signature. Fungsi hash dalam kriptografi adalah fungsi hash yang berupa sebuah algoritma yang mengambil sejumlah block data dan mengembalikan *bit string* berukuran tetap. String yang dihasilkan tersebut merupakan *hash value*. Perubahan yang dilakukan pada data walaupun sangat kecil, sengaja ataupun tidak, akan menyebabkan perubahan yang sangat banyak pada hasil *hash value*. Bahkan *hash value* dapat menjadi berbeda sama sekali. Data yang di hash sering disebut pesan.

Umumnya dalam kriptografi, ketika mengenkripsi suatu pesan harus dapat didekripsi dengan sempurna. Sedangkan, untuk fungsi hash justru tidak boleh didekripsi. Fungsi hash yang ideal adalah fungsi yang hasil *hasil hash value* tidak dapat didekripsi kembali. Hal ini dimanfaatkan untuk kerahasiaan. Ada berbagai jenis algoritma untuk melakukan hash. Dua diantaranya message digest 5 (MD5) dan SHA 256.[2]

MD5 sudah sangat lazim digunakan sebagai fungsi hash kriptografi. MD5 sering dimanfaatkan untuk memastikan integritas data. Hasil yang didapat dari penggunaan MD5 adalah angka heksadesimal dengan panjang 32 character. MD-5 diciptakan oleh Ron Rivest. MD-5 adalah salah satu algoritma yang digunakan untuk mengetahui bahwa data yang dikirim melalui jaringan tidak mengalami perubahan.

Ada banyak fungsi *Secure Hash Algorithm* (SHA), salah satu diantaranya adalah SHA-256. Pada tahun 2000, NIST (*The National Institute of Standard and Technology*) menciptakan SHA256. Masukan SHA-256 adalah pesan yang memiliki panjang sembarang dengan maksimal panjangnya 264 bit. Keluaran dari SHA-256 adalah hash value yang memiliki panjang tetap sebesar 256 bit. Ada dua tahap penting dalam operasi SHA-256 yaitu *preprocessing* dan hash *computation*. *Preprocessing* terdiri dari tiga langkah yang dimulai dari *padding* pesan, *parsing* pesan, kemudian melakukan proses *set initial hash value*. Setelah *preprocessing* selesai, lakukan proses *hash computation*. Proses ini terdiri dari empat langkah yang dimulai dari proses mempersiapkan *message schedule*, lalu *initialize variable*, kemudian melakukan komputasi sesuai dengan fungsi SHA-256, yang terakhir menjumlahkan variabel yang sudah dikomputasi dengan *initial hash value*. Dari proses inilah *hash value* akan didapatkan. [3]

AES adalah *cipher* blok yang terdiri dari 128 *bit* atau 192 *bit* atau 256 bit. Blok *cipher* adalah *cipher* yang mengenkripsi satu blok data pada satu waktu. Meskipun 128 *bit* kuat dan efisien, 256 *bit* digunakan untuk enkripsi tingkat tinggi.

Ini digunakan oleh sejumlah organisasi di seluruh dunia. AES menggunakan kunci privat tunggal untuk proses enkripsi dan dekripsi.[4]

Ada dua proses dalam ilmu kriptografi yaitu proses enkripsi dan dekripsi. Proses enkripsi dan deskripsi membutuhkan *CPU* untuk melakukan proses komputasi. Semakin besar data yang akan dienskripsi dan deskripsi akan semakin banyak *CPU* yang digunakan dalam kasus ini dapat membuat penurunan kinerja server. Setiap algoritma kriptografi memiliki proses enkripsi yang berbeda dan tinggkat keamanan yang berbeda. Karena penggunaan *CPU* yang banyak akan membuat proses enkripsi memakan waktu yang lama dan juga dapat membuat server menjadi *bottleneck* atau macetnya proses aliran data. Oleh karena itu penelitian ini akan mencari algoritma enkripsi yang lebih efektif dan aman untuk digunakan. Dalam enkripsi data yang sangat banyak dengan menggunakan beberapa skenario untuk mengukur berapa daya *CPU* yang digunakan, *Memory* yang digunakan dan lama waktu proses.

1.2 Rumusan Masalah

Merujuk pada latar belakang yang sudah dijelaskan sebelumnya adalah

1.3 Tujuan Penelitian

Penelitian ini bertujuan untuk:

a. Mencari algortima enkripsi yang efektif dalam proses enkripsi data.
b. Membandingkan kecepatan proses enkripsi *MD5, SHA256,* dan *AES.*
c. Menganalisa parameter yang berpengaruh dalam proses enkripsi.

1.4 Batasan Masalah

Dari rumusan masalah yang diuraikan diatas agar hasil pembahasan tidak melebar dan lebih terperinci. Adapun ruang lingkup permasalahanya sebagai berikut:

a. Aplikasi ini dirancang menggunakan bahasa pemrograman *PHP* dan *NodeJs*.
b. Proses enkripsi dengan memanfaatkan *library* yang ada di *PHP*.
c. Analisis perbandingan kecepatan enkripsi *MD5, SHA256, AES*.
d. Pengujian menggunakan *server virtual* dengan sistem operasi CentOs 7.

1.5 Manfaat Penelitian

a. Sebagai referensi dalam memilih algoritma enkripsi data yang efektif.
b. Menambah pengetahuan tentang perbedaan proses enkripsi.
c. Sebagai syarat untuk menyelesaikan program sarjana informatika di UNIVERSITAS AMIKOM YOGYAKARTA.

1.6 Metode penelitian

a. Studi Literatur

   Bertujuan untuk mengumpulan, memahami, dan mempelajari materi-materi dasar dan literature-literatur yang berkaitan dengan algoritma enkripsi *MD5, SHA256, AES,* dan cara kerja *CPU* dalam melakukan komputasi. Materi-materi yang digunakan dalam penelitian ini bersumber dari berbagai sumber pustaka berupa karya ilmiah, jurnal, paper, dan internet.

b. Analisis dan Perancangan Kebutuhan Sistem

Merancang *System* yang dibutuhkan untuk menggunakan enkripsi *MD5, SHA256, AES,* dan mengumpulkan data yang penggunaan *CPU* dan lama proses enkripsi.

c. Implementasi Sistem

Pada tahap implemetasi ini, akan menggunakan beberapa program untuk melakukan proses enkripsi. Sedangkan untuk mengumpulkan data penggunaan *CPU* dan lama proses menggunakan *htop*.

d. Pengujian Sistem

Hal yang akan diujikan adalah proses pengujian penggunaan *CPU* saat melakukan eksekusi proses enkripsi maupun deskripsi menggunakan aplikasi menghitung *CPU* usage pada webserver apache2 dan menggunakan PHP. Dalam menjalankan program PHP menggunakan *NodeJs* agar bisa menjalankan beberapa perintah secara bersamaan.

e. Analisis Hasil Pengujian

Analisa dari pengujian ini berdasarkan kemampuan sebuah *CPU* dalam mengeksekusi algoritma *CPU, SHA256, AES.*

f. Kesimpulan

Dari hasil analisis, kesimpulan akan dibuat mengenai hasil tes pada parameter yang digunakan dalam penerapan skema brute-force ke sistem otentikasi.

1.7 Sistematika Penulisan

Sistematika penulisan penelitian ini adalah sebagai berikut:

BAB I PENDAHULUAN:

Menjelaskan tentang latar belakang penelitian, rumusan masalah, batasan masalah, tujuan penelitian, metode penelitian dan sistematika penelitian.

BAB II LANDASAN TEORI:

Bab ini mengurai teori-teori yang mendukung judul dan mendasari pembahasan secara detail.

BAB III METODOLOGI PENELITIAN:

Bab yang menjelaskan metode yang digunakan dalam penelitian dan menjelaskan skenario pengujian parameter algoritma enkripsi *CPU, SHA256, AES, Scrypt* terhadap kinerja server.

BAB IV PENGUJIAN DAN ANALISIS:

Bab ini menjelaskan penerapan parameter proses enkripsi, menjelaskan hasil tes yang dilakukan pada sistem, dan menganalisis hasil tes ini.

BAB V KESIMPULAN:

Kesimpulan penelitian dituangkan pada bab ini.