BAB I PENDAHULUAN

1.1 Latar Belakang

Dengan perkembangan pandemi Covid 19 di seluruh dunia, aktivitas masyarakat diluar harus dikurangi demi menekan angka penyebaran Covid 19. Otomatis, aplikasi seperti Microsoft Office menjadi populer untuk menulis dokumen berkaitan dengan pekerjaan, sekolah dan sebagainya. Isi dari dokumen tersebut bisa berupa data rahasia atau data pribadi individual, dan hal ini dapat mengundang pihak tidak berkepentingan untuk mendapatkan data yang terkandung didalamnya. Sebagai contoh, berita kebocoran data 91 juta warga Indonesia pengguna Tokopedia yang terjadi pada 2 Mei 2020, dimana data yang didapatkan dijual pada forum bernama RaidForums (Hafis, 2020). Data yang bocor salah satunya adalah kata sandi, dimana data kata sandi yang datanya ada yang di *hash* menggunakan SHA2-384 dan MD5. SHA2-384 tergolong dalam jenis *hash* yang susah untuk di pecahkan, sedangkan kata sandi yang menggunakan MD5 sudah dipastikan dapat dipecahkan tergantung dengan sumber daya yang dimiliki oleh penyerang . Kasus ini menunjukkan bahwa sangat penting bagi pengguna dan perusahaan untuk selalu mengamankan datanya, salah satunya dengan menggunakan teknik kriptografi yang kuat dan tidak mudah untuk dipecahkan bila data dicuri.

Pada umumnya, kriptografi merupakan metode yang digunakan untuk mengamankan data sehingga kerahasiaannya dapat terjaga. Berdasarkan jenis kuncinya, kriptografi terbagi menjadi dua, yaitu kriptografi kunci simetris dan kriptografi kunci publik. Penelitian pada kali ini akan menggunakan dua algoritma kriptografi, yaitu algoritma AES dan Bcrypt. Bcrypt merupakan algoritma *hasing* yang dibuat dari Blowfish, yang penciptanya merupakan peneliti keamanan, yaitu Niels Provos dan David Mazières. Algoritma ini menggunakan salt acak yang dapat mempersulit pembuatan dan penggunaan tabel pencarian(Sinaga, 2017).

Beberapa penelitian telah dilakukan terkait dengan algoritma Bcrypt dan AES. Menurut penelitian yang dilakukan oleh Batubara(2020), kinerja algoritma Bcrypt cukup baik untuk bertahan dari serangan *brute force*pada karakter abjad dan campuran. Pada penelitian yang dilakukan oleh Yafie(2020), dari 20 fungsi hash yang menjadi bahan uji, Bcrypt memiliki nilai hash per detik paling kecil, yaitu 265 hash per detik yang menandakan bahwa Bcrypt memiliki keamanan yang paling baik dari penyerangan *brute force*.AES dipilih sebagai algoritma enkripsi file dokumen pada penelitian ini berdasarkan penelitian dari Handoyo dan Subakti pada tahun 2020 berhasil membuat aplikasi berbasis website yang bertujuan untuk mengamankan data dokumen menggunakan AES serta dari penelitian yang dilakukan oleh Meko(2018) yang membuktikan bahwa AES memiliki kecepatan enkripsi sebesar 1.508 kb/s dan kecepatan dekripsi mencapai 1.433 kb/s, lebih cepat dibandingkan DES, IDEA dan Blowfish.

Penelitian yang dilakukan oleh Kumar dan Chaudhary(2016) menggunakan algoritma yang sama dengan skripsi penulis yang berjudul *Password Security Using Bcrypt with AES Encryption Algorithm*. Pada penelitian ini, data penting akan disimpan didalam *list* termasuk *username* dan *password*, yang selanjutnya akan diamankan dengan kata sandi. Kata sandi lalu di *hashing* menggunakan Bcrypt dan di enkripsi menggunakan AES. Data berbentuk *list* lalu disimpan dalam format windws registry. Pengguna bisa membuka data pada *list* dengan memasukkan *password* yang sudah diamankan pada proses sebelumnya lalu *password* dilakukan proses dekripsi.

Berdasarkan penelitian terdahulu yang telah disebutkan, maka penulis memutuskan untuk menulis penelitian ini dengan judul Implementasi Algoritma AES dan Bcrypt Untuk Pengamanan File Dokumen.

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas, rumusan masalahnya yaitu:

1. Bagaimana cara mengenkripsi *file* dokumen menggunakan AES agar terlindung dari upaya penyerangan serta dekripsinya?
2. Bagaimana cara mengamankan *secret key* dengan Bcrypt sehingga kunci yang dihasilkan tidak mudah untuk dipecahkan?

1.3 Batasan Masalah

Untuk memperjelas pembahasan penelitian ini, batasan masalah kali iniadalah:

a. Sistem dibangun menggunakan *framework* Laravel.
b. Kriptografi yang digunakan yaitu Bcrypt dan AES 256.
c. Aplikasi pengamanan ini digunakan untuk enkripsi dan dekripsi berjenis *file* .docx dan .pdf.
d. Aplikasi akan dijalankan dengan OS berbasis Windows 10.
e. Ronde *hashing* Bcrypt yang akan diujikan yaitu 10 sampai 20.

1.4 Tujuan dan Manfaat Penelitian

Tujuan penelitian ini yaitu menerapkan algoritma Bcrypt dan AES untuk menghasilkan sistem keamanan yang maksimal yang dapat mencegah penyalahgunaan data oleh pihak yang tidak berkepentingan. Manfaat dari penelitian ini yaitu sebagai bahan refrensi untuk penelitian terkait dengan penggunaan algoritma Bcrypt dan AES pada *file* dokumen.

1.5 Sistematika Penulisan

Penulisan laporan ini mengikuti sistematika penulisan sebagai berikut:

1. Bab I Pendahuluan

   Bab ini merupakan bab yang berisi penjelasan dari latar belakang, rumusan masalah,batasan masalah, tujuan dan manfaat penelitian, serta sistematika penulisan.

2. Bab II Landasan Teori

   Teori-teori yang diperlukan untuk mendukung penyusunan penulisan laporan dari penelitian ini.

3. Bab III Metodologi Penelitian

   Menjelaskan metode yang digunakan, terdiri dari kerangka pikir, tahap penelitian,perangkat yang digunakan dan jadwal penelitian.

4. Bab IV Hasil dan Pembahasan

   Bab ini berisi tentang analisis dan hasil perancangan aplikasi serta implementasinya.

5. Bab V Kesimpulan dan Saran

   Bab terakhir ini berisi kesimpulan dan saran dari penelitian.