BAB I
PENDAHULUAN

1.1. Latar Belakang

Penerapan *security system* dalam *smart home* dapat berupa deteksi wajah (*face detection*), deteksi sidik jari (finger print), *Close Circuit Tele Vision* (CCTV), *smart door lock* dan masih banyak lagi yang lainnya yang dapat dilakukan secara otomatis menggunakan perangkat digital. *Security system* terkait akses *smart home* melibatkan proses *authentification* dan *identification* ekspresi wajah pengguna [1].

Sistem keamanan (*security system)* dalam penyimpanan *database* (basis data) atau informasi adalah hal yang sangat penting dan tidak bisa diabaikan begitu saja. Semakin tinggi tingkatan teknologi komputer, maka akan semakin tinggi pula tingkat ancaman yang akan mengancam keamanan data didalam komputer. Kerahasiaan suatu file yang tersimpan pada komputer harus diberikan pengamanan dan sudah menjadi persyaratan mutlak yang sangat diperlukan untuk melindungi file tersebut terhadap berbagai ancaman seperti dapat dengan mudah seseorang melihat, merusak, mencuri ataupun menyalahgunakan data atau informasi penting melalui jaringan komputer. Kriptografi menjadi tujuan agar data atau informasi tidak dapat dibaca oleh orang yang tidak berhak. Dalam kriptografi ada istilah yang disebut dengan enkripsi (*encryption*) yaitu proses penyamaran data dari *plaintex*t (data asli) menjadi *chiperterx*t (data tersandi) dan dekripsi (*decryption*) yaitu proses pemgembalian chipertext menjadi *plaintext* kembali [2].

Kriptografi dapat dikatakan sebagai ilmu atau seni untuk menjaga keamanan pesan. Ketika suatu pesan dikirim dari suatu tempat ke tempat lain isi pesan tersebut mungkin dapat disadap oleh pihak lain yang tidak berhak untuk mengetahui isi pesan tersebut. Untuk menjaga pesan, maka pesan tersebut dapat diubah menjadi suatu kode yang tidak dapat dimengerti oleh pihak lain. Enkripsi adalah sebuah proses penyandian yang melakukan perubahan sebuah kode atau pesan dari yang bias dimengerti, disebut plainteks, menjadi sebuah kode yang tidak bisa dimengerti, disebut dengan *cipherteks* [3].

Homomorphic merupakan suatu sifat algoritma enkripsi yang membuat *ciphertext*-nya dapat dilakukan komputasi meskipun belum didekripsi terlebih

dahulu. Komputasi yang didukung biasanya penambahan, pengurangan, atau bahkan perkalian dengan konstanta tertentu, yang akan menghasilkan keluaran yang sesuai dengan teks asli. Oleh karena itu, *homomorphic property* pada suatu algoritma enkripsi dapat dimanfaatkan. Terdapat dua jenis enkripsi homomorfik yaitu *partially homomorphic encryption* (PHE) dan *fully homomorphic encryption* (FHE). PHE merupakan jenis enkripsi homomorfik yang memungkinkan dilakukannya satu jenis operasi tertentu pada *ciphertext*. Sementara itu FHE merupakan jenis enkripsi homomorfik yang memungkinkan kedua jenis operasi penjumlahan dan perkalian dilakukan pada *ciphertext* [4].

Lalu selanjutnya penelitian yang dilakukan di tahun 2016 dengan judul "Implementasi Kriptografi Klasik Pada Komunikasi Berbasis Teks" yang dimana pada penelitian ini akan diimplementasikan kriptografi klasik sebagai metode untuk melakukan proses enkripsi dan dekripsi data teks yang dikirimkan melalui aplikasi chat. Dari proses pengujian diperoleh bahwa proses enkripsi dan dekripsi dapat menjaga kerahasiaan data [5]. Selanjutnya, penelitian pada tahun 2018 dengan judul "Enkripsi Data Menggunakan *Advanced Encryption Standart* 256" yang menjelaskan hasil akhir penelitian dimana, kriptografi mendukung aspek keamanan informasi, yaitu perlindungan kerahasiaan. Oleh karena itu kebutuhan untuk menjaga kerahasiaan data dan informasi adalah aplikasi *cryptographic*. Prosesnya berupa enkripsi dan dekripsi yang digunakan oleh pengguna untuk mengamankan data tanpa mengubah isi data. Aplikasi ini memiliki kunci 32 karakter tetapi dalam penggunaannya dibuat menjadi 2 kunci, yaitu kunci publik dan privat di mana kunci publik adalah kunci yang diisi oleh pengguna sesuai dengan keinginan, sedangkan kunci privat adalah kunci default yang dimasukkan oleh aplikasi secara acak untuk memenuhi panjang 32 karakter. Algoritma AES yang digunakan adalah algoritma AES256 di mana algoritma ini menggunakan prinsip dengan jumlah putaran berdasarkan kunci [6]. Penelitian sebelumnya terkait kemanan dan kerahasiaan data pernah dilakukan oleh Zulfikar, et al pada penelitian yang berjudul "Kriptografi untuk Keamanan Pengiriman Email Menggunakan *Blowfish* dan *Rivest Shamir Adleman* (RSA)" pada tahun 2019 yang dimana gambaran hasil penelitian bahwa Kriptografi RSA yang populer dengan penggunaan kunci publiknya digunakan untuk mengamankan salah satu komponen dari *Blowfish* yaitu kunci simetris.

Penelitian ini bertujuan membuat sistem yang dapat mengamankan pesan email dan kunci simetris sebelum dilakukan proses pengiriman dengan mengkombinasikan kriptografi Blowfish dan RSA diharapkan dapat meningkatkan keamanan secara lebih. Tahap uji serangan *brute force* yang dilakukan sebanyak tiga kali menghasilkan plaintext yang tidak utuh dan tahap uji ukuran data setelah dienkripsi membengkak sebesar 0,09KB dari hal tersebut maka kombinasi teknik kriptografi yang digunakan aman dan efisien [7].

Maka berdasarkan uraian yang telah dipaparkan diatas, penulis akan menggunakan judul "Pembuatan *Database* Terenkripsi *Homomorphic* Untuk Melindungi Privasi Pengguna Pada *Smart Home*" dalam proses penelitian ini.

1.2. Rumusan Masalah

Berdasarkan pada uraian latar belakang didapatkan beberapa rumusan masalah sebagai berikut:

1. Bagaimana implementasi enkripsi *database* pada teknik *homomorphic encryption* untuk melindungi privasi pengguna?
2. Bagaimana hasil analisis saat dilakukannya pengukuran waktu enkripsi dan dekripsi secara *real time* pada deteksi kondisi emosi wajah pengguna?
3. Bagaimana proses implementasi agar saat melakukan pengujian dan pengukuran tetap pada stabil kecepatan akses jaringan internetnya dan tidak terjadi masalah?

1.3. Tujuan dan Manfaat

Berdasarkan pada rumusan masalah, maka berikut adalah tujuan dan manfaat yang ingin dicapai dari penelitian ini, yaitu:

1. Mempelajari teknik *homomorphic encryption* untuk melakukan enkripsi *database* privasi pengguna.
2. Mempelajari pembuatan *database* terhadap data yang terenkripsi *homomorphic* untuk melindungi privasi pengguna.

Manfaat dari penelitian ini diharapkan dapat membuat perangkat lunak yang mengimplementasikan teknik order *homomorphic encryption* beserta teknik pembuatan *database* yang akan digunakan untuk melindungi privasi pengguna

dan diharapkan menjadi referensi untuk pengembangan sistem informasi selanjutnya.

1.4. Batasan Masalah

Seperti yang telah dipaparkan pada Sub bab 1.1, berikut adalah batasan-batasan masalah dari penelitian ini:

1. Penelitian dibatasi dengan menggunakan metode enkripsi Homomorphic.
2. Pada aplikasi ini proses enkripsi/dekripsi dan pengiriman data dapat dilakukan pada multifile. Jumlah file dibatasi sebanyak 10 file dengan maksimum ukuran file 1 GB pada sekali proses enkripsi atau dekripsi untuk kunci yang sama, untuk menghindari proses enkripsi yang terlalu lama.
3. Aplikasi hanya mengenkripsi file tunggal (bukan folder) karena enkripsi folder akan menyebabkan satu serangan terhadapnya akan berakibat pada semua file yang ada di folder tersebut.
4. Pada sistem yang dibangun difokuskan pada proses pengamanan data dengan pencegahan pembacaan file oleh pihak-pihak yang tidak berhak.
5. Hasil akhir file enkripsi akan menghasilkan file terenkripsi dan waktu terenkripsi akan disimpan serta dikelola di *database*.
6. Aplikasi dibuat menggunakan bahasa pemrograman Phyton dan menggunakan *database* MySQL, serta dijalankan dengan menggunakan *Web Server Local*.
7. Aplikasi dibuat untuk diimplementasikan pada *Smart Home*.

1.5. Metode Penelitian

Metode penelitian yang akan digunakan dalam skripsi ini adalah metode eksperimental. Dalam penelitian ini, akan digunakan dan diuji coba teori-teori yang mungkin dapat menyelesaikan masalah dari skripsi ini. Berikut adalah langkah-langkah metode penelitian yang dilakukan.

1. Studi Literatur

   Pada tahap ini, penulis mengumpulkan serta membaca dari berbagai sumber seperti buku, artikel, jurnal dan beberapa referensi informasi yang bersumber dari internet untuk memudahkan penulis dalam pemahaman

dalam masalah yang dibahas.

2. Desain Sistem

   Penulis membuat desain sistem dan menganalisis metode yang digunakan dalam menyelesaikan masalah.

3. Implementasi Sistem

   Tahap pembuatan sistem setelah desain sistem dan perancangan sebelumnya telah selesai dibuat.

4. Tahap Pengujian dan Analisis

   Pada tahap ini, pengujian sistem dilakukan untuk mengamati data-data yang diinginkan. Pengujian dilakukan dengan cara mengukur waktu proses enkripsi dan dekripsi data.

5. Bimbingan Dosen

   Penulis melakukan diskusi dan konsultasi terkait penelitian dengan dosen pembimbing mengenai hasil pengujian dan analisis sistem.

6. Pembuatan laporan

   Penyusunan laporan akhir dan membuat kesimpulan dari hasil yang didapatkan selama melakukan penelitian dari awal hingga akhir.