BAB I
PENDAHULUAN

1. 1 Latar Belakang

Saat ini penyadapan sering terjadi dalam pertukaran informasi antar pengguna jaringan komunikasi, seperti pada saat *transfer file* menggunakan teknologi *socket programming*. *Socket programming* memungkinkan kedua perangkat untuk saling berkomunikasi melalui jaringan. Namun pada prosesnya, *data* yang ditransmisikan dapat dengan mudah disadap oleh pihak yang tidak bertanggungjawab. Dalam komunikasi berbasis *socket*, kerentanan terhadap serangan aktivitas pencurian *data* seperti *sniffing*, *phishing*, dan *brute force*, sangatlah tinggi, karena *data* yang dikirimkan melalui jaringan terbuka [1]. Ketika informasi yang diperoleh melalui metode ini digunakan untuk tindakan kejahatan, konsekuensinya bisa sangat besar, contohnya seperti pencurian identitas hingga kerugian finansial [2]. Oleh sebab itu dibutuhkan metode untuk melindungi pertukaran informasi salah satunya dengan kriptografi.

Dalam kriptografi, terdapat algoritma enkripsi, salah satunya adalah *Advanced Encryption Standard* (AES). Algoritma AES digunakan untuk mengenkripsi dan mendekripsi informasi. Enkripsi mencegah *data* sensitif pengguna aplikasi tidak akan bisa dibaca oleh pihak yang tidak bertanggung jawab, serta menjaga kerahasiaan dan integritas *data*. Kelebihan algoritma AES adalah efektivitas biaya dan kemudahannya implementasi dalam memori kecil, menjadikannya pilihan ideal untuk berbagai aplikasi keamanan *data* [3]. AES memiliki tiga varian berdasarkan panjang kunci yang digunakan yaitu AES 128, AES 192, AES 256. Dari tiga varian panjang kunci ini, AES 256 memiliki tingkat keamanan tertinggi dan panjang kunci lebih besar [4].

Penelitian oleh Meko [5] melakukan pengukuran terhadap efektivitas algoritma enkripsi dengan memb*and*ingkan beberapa kriptografi seperti DES, AES, IDEA, dan *Blowfish* dalam melakukan enkripsi dengan melihat perbedaan waktu proses dan ukuran *file*. Beberapa jenis *file* digunakan dalam penelitian ini dengan tujuan untuk menunjang pengukuran kinerja algoritma secara komprehensif dan memastikan hasil penelitian tidak terbatas pada satu jenis atau ukuran *file*. Kemudian, Penelitian Anshori pada tahun 2019 [6] membuktikan *TCP/IP* layak

sebagai sarana pengiriman *file* teks antar *client – server*. Dalam penelitian ini, sistem dikembangkan menggunakan pemrograman *java* serta *socket programming* untuk *client* dan *server* dapat saling berkomunikasi. Meskipun demikian, penelitian tersebut kurang dalam memperhatikan keamanan *data*, dimana *file* teks hanya dikirimkan tanpa enkripsi. Selain itu jika *port* pada *socket* terbuka, dapat membuka celah pencurian *data* oleh pihak yang tidak bertanggungjawab apabila tidak dilindungi dengan mekanisme yang tepat.

Untuk mengatasi permasalahan tersebut, maka dilakukan penelitian penerapan autentikasi enkripsi algoritma AES 256 pada *socket programming*. Kemudian dilakukan pengujian hasil *data* berdasarkan batas autentikasi serta ukuran enkripsi, waktu pengiriman dan kecepatan enkripsi dari masing masing *file* yang dikirimkan sehingga dapat diketahui bahwa sistem bekerja dengan baik dalam enkripsi *file* serta memastikan hanya pengguna sah yang dapat mengakses pengiriman *file*. Proses autentikasi menggunakan verifikasi *password* dan kode *One Time Password* (OTP) yang dikirim melalui *e-mail* untuk mengkonfirmasi identitas pengguna. Setelah proses autentikasi berhasil, *file* yang akan dikirimkan akan dienkripsi menggunakan AES-256. Enkripsi ini melindungi *data* dengan cara mengubah informasi menjadi *ciphertext* yang tidak dapat dibaca tanpa kunci yang sesuai. Transfer *file* dilakukan melalui *socket programming,* untuk *client* dan *server* dapat saling berkomunikasi. Teknik ini memungkinkan *data* yang telah dienkripsi untuk dikirim secara aman dari satu perangkat ke perangkat lain, menjamin bahwa *data* tetap utuh dan aman selama proses *transfer*. Penelitian ini berjudul ”Skema Autentikasi *Password* AES 256 menggunakan *Socket Programming*”.

1. 2 Perumusan Masalah

Rumusan masalah dari penelitian ini adalah :

1. Bagaiman cara mengimplementasikan autentikasi *password* berupa kode OTP dalam proses pengiriman *file* menggunakan enkripsi AES 256 melalui *socket programming*?
2. Bagaimana ketahanan *file* yang terenkripsi algoritma AES menggunakan *socket programming* terhadap serangan *brute force*?

1. 3 Tujuan Penelitian

Tujuan dari penelitian ini adaah :

1. Mengembangkan dan merancang sistem autentikasi yang memastikan hanya pengguna yang terverifikasi yang dapat mengakses, mentransfer *file* dengan cara mengevaluasi batas efektif pengiriman OTP untuk menjaga kepercayaan pengguna.
2. Mengukur ketahanan enkripsi dilihat dari hasil ukuran, waktu enkripsi, kecepatan pengiriman, waktu kirim, dan uji *brute force* terhadap hasil *file* yang sudah terenkripsi.

1. 4 Batasan dan Asumsi Penelitian

Untuk pembahasan dalam penelitian ini tetap dalam topik, maka batasan masalah dari penelitian ini adalah :

1. Penelitian ini menggunakan jaringan lokal yang sama.
2. Penelitian ini menggunakan 8 jenis tipe *file* yaitu : *file* teks (.txt), dokumen (.docx), arsip (.rar), PDF (.pdf), gambar (.png, .jpg), serta *file* video (.mp4) dan *audio* (.mp3).
3. Penelitian ini menggunakan skema autentikasi *kode One Time Password* (OTP) yang dikirimkan melalui *e-mail* pengguna.
4. Penelitian ini menggunakan *Visual Studio Code* Untuk menulis, mengedit, dan menjalankan *script python*, untuk pengiriman OTP melalui *e-mail* dan pengiriman *file* terenkripsi.
5. Penelitian ini hanya melakukan pengujian batas tiga kali terhadap penginputan kode OTP pengguna, uji ketahanan *file* berdasarkan perb*and*ingan ukuran, waktu dan kecepatan yang diperlukan untuk melakukan enkripsi serta uji *brute force* menggunakan aplikasi *cryptools*.
6. Penelitian ini menggunakan algoritma *Advanced Encryption Standard* (AES) 256 untuk enkripsi *file*.

1. 5 Manfaat Penelitian

Melalui penerapan pada penelitian skema autentikasi *password* OTP dan enkripsi AES 256 sebagai enkripsi *file* ini diharapkan meningkatkan kemanan hanya pengguna sah yang dapat akses dan membantu mencegah serangan ancaman pencurian *data* seperti *brute force* pada transfer *file*. Hasil dari penelitian ini dapat

diterapkan pada berbagai sistem yang memerlukan pengamanan *data* informasi serta diharapkan dapat memberikan edukasi dalam melindungi *data* sensitif sehinggan dapat mengurangi kebocoran *data* informasi yang merugikan pengguna**.**

1. 6 Sistematika Penulisan

Penelitian ini terbagi menjadi beberapa bab. Bab pertama merupakan pendahuluan yang berisi latar belakang masalah, perumusan masalah, tujuan penelitian, batasan dan asumsi penelitian, manfaat penelitian. Bab kedua mengulas kajian pustaka yang mencakup teori-teori yang mendasari penelitian ini, termasuk konsep-konsep terkait kriptografi, autentikasi, enkripsi AES 256, dan teknologi *socket programming*. Bab ketiga menjelaskan metodologi penelitian, yang meliputi perangkat yang digunakan, alur penelitian, topologi jaringan, metodologi yang digunakan dalam penelitian, seperti pengujian ketahanan enkripsi dan pengukuran batas pengiriman OTP. Bab keempat berisi pengumpulan *data* dan pengolahan *data* untuk bahan analisis. Bab lima hasil dan pembahasan, yang menyajikan hasil pengujian sistem, analisis ketahanan enkripsi terhadap serangan *brute force*, dan pengaruh ukuran *file* terhadap waktu enkripsi. Bab terakhir adalah kesimpulan dan saran, yang merangkum hasil penelitian, kesimpulan yang diperoleh, serta rekomendasi untuk penelitian atau pengembangan sistem lebih lanjut.