BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi komunikasi digital telah merevolusi cara manusia berinteraksi dan bertukar informasi. Kemajuan infrastruktur jaringan publik memungkinkan komunikasi berlangsung secara cepat dan real time, sehingga aplikasi chatting menjadi salah satu sarana komunikasi yang paling banyak digunakan dalam berbagai aktivitas, baik untuk keperluan pribadi, pendidikan, maupun profesional [1], [2]. Seiring dengan meningkatnya kebutuhan akan sistem komunikasi yang dapat diakses secara fleksibel, aplikasi chatting berbasis web turut berkembang sebagai alternatif yang dapat digunakan melalui peramban tanpa ketergantungan pada platform perangkat tertentu. Di balik kemudahan dan fleksibilitas yang ditawarkan, aplikasi chatting berbasis web menghadapi tantangan serius terkait keamanan komunikasi. Karakteristik komunikasi yang berlangsung melalui jaringan publik menjadikan data yang ditransmisikan rentan terhadap berbagai ancaman keamanan siber. Salah satu ancaman yang paling umum dan berisiko tinggi adalah serangan eavesdropping, yaitu tindakan penyadapan lalu lintas komunikasi oleh pihak yang tidak berwenang dengan cara menangkap paket data yang dikirimkan melalui jaringan. Serangan ini dapat terjadi tanpa disadari oleh pengguna dan berpotensi mengakibatkan kebocoran informasi yang bersifat pribadi maupun sensitif [3].

Untuk melindungi kerahasiaan komunikasi, berbagai aplikasi chatting modern telah menerapkan konsep End-to-End Encryption (E2EE), di mana proses enkripsi dan dekripsi pesan dilakukan langsung pada sisi pengirim dan penerima. Dengan pendekatan ini, pihak perantara seperti server aplikasi hanya berperan sebagai media pengiriman pesan dan tidak memiliki akses terhadap isi komunikasi. Secara konseptual, E2EE mampu meningkatkan tingkat keamanan dan privasi pengguna, terutama dalam lingkungan jaringan publik yang tidak sepenuhnya aman [4]. Meskipun demikian, penerapan E2EE pada aplikasi chatting berbasis web belum sepenuhnya menjamin keamanan komunikasi. Dalam praktiknya, masih terdapat celah keamanan yang muncul akibat lemahnya mekanisme pertukaran kunci, manajemen sesi komunikasi, serta pemilihan algoritma kriptografi yang kurang tepat. Celah-celah tersebut dapat dimanfaatkan oleh penyerang untuk melakukan eavesdropping, sehingga pesan yang seharusnya bersifat rahasia tetap berpotensi diakses oleh pihak ketiga. Kondisi ini menunjukkan bahwa keamanan komunikasi tidak hanya bergantung pada

keberadaan E2EE, tetapi juga pada desain protokol keamanan yang digunakan secara menyeluruh. Dalam konteks kriptografi modern, pendekatan kriptografi hibrid banyak digunakan untuk mengamankan komunikasi end-to-end. Pendekatan ini mengombinasikan algoritma kriptografi simetris yang efisien untuk mengenkripsi isi pesan dengan algoritma kriptografi asimetris yang aman untuk proses pertukaran kunci. Kombinasi tersebut bertujuan untuk memperoleh keseimbangan antara tingkat keamanan yang tinggi dan efisiensi performa sistem, khususnya pada aplikasi chatting berbasis web yang melibatkan pertukaran data secara berkelanjutan [5]. Berdasarkan kajian terhadap penelitian terdahulu, masih terbatas penelitian yang secara spesifik mengevaluasi efektivitas kombinasi algoritma ChaCha20 dan Elliptic Curve Diffie-Hellman Ephemeral (ECDHE) dalam mencegah serangan *eavesdropping* pada skenario komunikasi *chatting* berbasis *web*. Sebagian penelitian membahas algoritma tersebut secara terpisah atau mengombinasikannya dengan algoritma lain, namun belum banyak yang mengkaji penerapannya secara langsung dalam sebuah protokol keamanan komunikasi chatting berbasis web yang diuji melalui simulasi sistem [6], [7]. Sementara itu, untuk melakukan proses verifikasi terhadap kunci, akan digunakan metode SHA-256. Metode SHA-256 tergolong aman karena didesain sedemikian rupa sehingga tidak memungkinkan mendapatkan pesan yang berhubungan dengan *message digest* yang sama [8]. Dalam segi kekuatan keamanan, fungsi hash SHA256 dapat melakukan pengamanan lebih baik dibandingkan MD5. Dilihat dari hasil percobaan, nilai hash yang diproduksi oleh fungsi hash SHA256 lebih rumit dibandingkan dengan MD5, hal ini memungkinkan orang lain yang ingin mencuri data lebih kesulitan untuk memecahkan nilai hash SHA256 [9].

Oleh karena itu, penelitian ini berfokus pada perancangan dan evaluasi protokol keamanan komunikasi *chatting* berbasis *web* dengan menggunakan kombinasi algoritma ChaCha20 sebagai mekanisme enkripsi simetris dan Elliptic Curve Diffie-Hellman Ephemeral (ECDHE) sebagai mekanisme pertukaran kunci. Protokol keamanan yang dirancang diimplementasikan dan diuji melalui simulasi aplikasi chatting berbasis web untuk mengevaluasi efektivitasnya dalam menjaga kerahasiaan pesan serta mencegah serangan *eavesdropping*.

Berdasarkan uraian tersebut, maka akan dilakukan penelitian dengan judul "IMPLEMENTASI DAN EVALUASI PROTOKOL KEAMANAN CHATTING MENGGUNAKAN CHACHA20 DAN ECDHE UNTUK PENCEGAHAN EAVESDROPPING." Dengan demikian, penelitian ini diharapkan dapat memberikan

kontribusi akademik dalam pengembangan protokol keamanan komunikasi *chatting* berbasis *web* yang aman dan efisien.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, maka rumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Penerapan E2EE pada aplikasi *chatting* masih memiliki celah keamanan yang muncul akibat lemahnya mekanisme pertukaran kunci, manajemen sesi komunikasi (berupa parameter kunci yang selalu berbeda-beda dan ditentukan pada setiap proses *login* ke sistem), serta pemilihan algoritma kriptografi yang kurang tepat.
2. Masih terbatas penelitian yang secara spesifik mengevaluasi efektivitas kombinasi algoritma ChaCha20 dan Elliptic Curve Diffie-Hellman Ephemeral (ECDHE) dalam mencegah serangan *eavesdropping* pada skenario komunikasi *chatting*.

1.3 Tujuan

Berdasarkan rumusan masalah yang telah dipaparkan, tujuan dari penelitian ini adalah sebagai berikut:

1. Mengimplementasikan kombinasi algoritma ChaCha20 dan ECDHE untuk membentuk sebuah protokol komunikasi *end-to-end* yang aman pada aplikasi *chat*.
2. Mengevaluasi efektivitas kombinasi ChaCha20 dan ECDHE dalam menjaga kerahasiaan pesan dari serangan *eavesdropping* pada simulasi komunikasi *chatting* berbasis *web*.

1.4 Manfaat

Manfaat dari penelitian ini adalah:

1. Meningkatkan perlindungan privasi dan keamanan data dalam komunikasi digital, dengan menunjukkan bagaimana kombinasi algoritma tersebut mampu mencegah penyadapan pesan yang dapat mengancam informasi sensitif pengguna.
2. Menyediakan informasi hasil evaluasi mengenai efektivitas kombinasi algoritma ChaCha20 dan Elliptic Curve Diffie-Hellman Ephemeral (ECDHE) dalam mencegah serangan *eavesdropping* pada skenario komunikasi *chatting*.

1.5 Ruang Lingkup

Ruang lingkup penelitian ini mencakup:

1. Penelitian dilakukan pada simulasi aplikasi *chatting* berbasis *web* yang digunakan sebagai lingkungan uji untuk mengimplementasikan dan mengevaluasi protokol keamanan yang diusulkan. Platform berbasis web dipilih karena lebih mudah dikembangkan, mudah direplikasi, serta memungkinkan pengujian protokol secara terkontrol tanpa ketergantungan pada variasi perangkat keras tertentu. Oleh karena itu, hasil pengujian performa difokuskan sebagai indikator efisiensi relatif algoritma kriptografi yang digunakan, bukan sebagai representasi performa aplikasi chatting produksi pada platform tertentu.
2. Aplikasi yang dikembangkan berupa simulasi *chat* sederhana berbasis *web* yang hanya mendukung pengiriman pesan teks. Fitur seperti panggilan suara/video, maupun media tidak termasuk dalam cakupan penelitian. Penelitian ini tidak mencakup pengembangan aplikasi *chatting* siap pakai pada *platform* produksi tertentu.
3. Sistem mengimplementasikan ChaCha20 sebagai algoritma enkripsi simetris dan ECDHE sebagai mekanisme pertukaran kunci asimetris dengan dukungan *forward secrecy*. Sementara itu, untuk melakukan proses verifikasi kunci akan digunakan metode SHA-256.
4. Evaluasi keamanan difokuskan pada ketahanan sistem terhadap serangan *eavesdropping* pasif, yaitu ketidakmampuan pihak ketiga untuk membaca atau mendekripsi isi pesan yang berhasil disadap.
5. Evaluasi performa difokuskan pada proses kriptografi yang dilakukan oleh sistem, meliputi pengukuran latensi enkripsi/dekripsi, tanpa mempertimbangkan pengaruh kondisi jaringan eksternal secara mendalam.
6. Pengujian performa dilakukan menggunakan variasi ukuran pesan mulai dari 200 karakter hingga 1000 karakter dan berbagai ukuran *file* mulai dari 1 MB sampai 5 MB untuk menilai skalabilitas algoritma kriptografi yang digunakan.
7. Pengujian juga dilakukan dengan mengubah data yang dikirimkan dan melihat hasil yang diperoleh dari metode SHA-256 dan metode ChaCha20.
8. Penelitian ini dilakukan dengan asumsi bahwa lingkungan jaringan berada dalam kondisi stabil dan tidak terdapat eksploitasi terhadap sistem operasi maupun perangkat keras di luar konteks protokol keamanan yang diuji.
9. Penelitian ini tidak mengevaluasi mekanisme autentikasi pengguna maupun verifikasi identitas lanjutan. Evaluasi keamanan juga dibatasi pada skenario serangan *eavesdropping* yang telah ditentukan.