

ABSTRAKSI

Perkembangan dunia komunikasi di Indonesia sudah semakin cepat.. Meningkatnya penggunaan aplikasi instant messaging sebagai sarana berkomunikasi didorong dengan kemudahan penggunaannya, biaya yang relatif murah, dan penggunaan yang efisien. Dengan banyaknya penggunaan aplikasi instant messaging, semakin besar pula kemungkinan penyadapan saat berkomunikasi. Masih ada kemungkinan semua pesan yang dikirimkan olehnya dapat terbaca oleh pihak lain. Hal ini akan membatasi bagaimana sikap dan perbuatan pengguna saat menggunakan aplikasi.

Maka dari itu, diperlukan sebuah aplikasi instant messaging yang dapat menjamin privasi saat berkomunikasi. Selain itu, protokol keamanan yang digunakan untuk menjamin privasi ini juga harus menggunakan protokol keamanan yang sudah terjamin dan memiliki standar. Sudah ada beberapa aplikasi yang mencoba menyelesaikan masalah privasi dan keamanan, namun dalam implementasinya masih sering ditemukan beberapa celah keamanan yang dapat menyebabkan kebocoran pesan saat berkomunikasi. Faktor utama dari munculnya celah keamanan ini adalah penggunaan protokol yang tidak memiliki standar dan banyaknya modifikasi protokol untuk memenuhi kebutuhan setiap aplikasi.

Untuk menambah keamanan saat berkomunikasi, dibuatlah aplikasi Secured Chatting berbasis web ini. Aplikasi ini menerapkan algoritma RSA dan AES yang sudah memiliki standar dan banyak digunakan pada dunia keamanan komputer. Implementasi kedua algoritma dilakukan pada data chatting antar kedua perangkat, sehingga server yang menyediakan aplikasi pun tidak dapat mengetahui apa isi percakapan tersebut.

Setelah melakukan uji coba pada aplikasi yang dibuat, ternyata aplikasi sudah dapat meningkatkan keamanan dan privasi komunikasi melalui enkripsi pesan. Semua pesan dalam jaringan sudah dalam bentuk ciphertext yang tidak dapat terbaca bahkan oleh server. Uji coba juga dilakukan terhadap tampilan, dan ditemukan bahwa aplikasi sudah cukup mudah digunakan.

Kata kunci : instant messaging, privasi, protokol keamanan.