Implementasi dan evaluasi instant messaging serta Voice/Video over IP Terenkripsi End-to-End yang terdesentralisasi dengan XMPP/OMEMO dan WebRTC = Implementation and evaluation of secure decentralized instant messaging with VoIP Utilizing XMPP/OMEMO and WebRTC

Faris Haidar Zuhdi, author

Abstrak

Masa pandemi membuktikan pentingnya peran aplikasi komunikasi berbasis teks, audio, dan video di masyarakat. Contoh aplikasi instant messaging yang digunakan secara luas adalah Discord dan LINE. Namun, kedua aplikasi tersebut secara default belum mengadopsi protokol keamanan data yang sedang dalam proses pengiriman (in transit) secara sempurna dan menyeluruh. Contoh aplikasi yang sudah menerapkan hal tersebut adalah Signal dan WhatsApp. Kekurangan dari kedua aplikasi tersebut adalah digunakannya protokol yang tersentralisasi, di mana pesan harus berjalan melalui server-server yang dikontrol oleh satu pihak sehingga pengguna ”dipaksa” untuk memercayai dan bergantung pada server-server pusat tersebut. Dilatarbelakangi oleh permasalahan tersebut, penelitian ini memperkenalkan sebuah aplikasi Instant Messaging yang terenkripsi end-to-end menggunakan protokol XMPP dengan skema enkripsi OMEMO. Protokol XMPP adalah suatu protokol instant messaging yang dipilih karena tidak memerlukan adanya ketergantungan ke otoritas pusat manapun. Protokol XMPP dapat berjalan di atas TCP ataupun QUIC. Pada penelitian ini, aplikasi diimplementasikan sehingga mampu memulai koneksi XMPP menggunakan TCP atau QUIC. Selain itu ditambahkan juga tur voice and video call menggunakan WebRTC dan ekstensi Jingle karena kebanyakan aplikasi instant messaging memiliki tur ini. Dua aspek utama yang dievaluasi pada aplikasi hasil penelitian ini adalah latency dan resource usage. Penelitian ini menemukan bahwa performa latency pada jaringan XMPP cukup baik, tetapi terjadi peningkatan latency pada kasus ada banyak client yang saling mengirimkan pesan sekaligus pada waktu yang bersamaan. Selain itu, tidak ada perbedaan performa yang signi kan antara QUIC dan TCP pada XMPP. Penelitian ini juga menunjukkan bahwa implementasi OMEMO menyebabkan performa latency lebih buruk ketimbang tanpa adanya enkripsi end-to-end, tetapi server sudah tidak dapat lagi mengetahui isi dari pesan apapun yang dikomunikasikan antara client. Hasil evaluasi pada tur voice and video call menunjukan bahwa tur ini memiliki performa latency yang memuaskan untuk aplikasi real-time. Selain itu, dilakukan juga uji perbandingan latency dari koneksi yang menggunakan relay server dengan yang tidak dan ternyata tidak terjadi perbedaan performa yang signi kan. Namun, koneksi ini akan menjadi beban bagi relay server.