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

Muhammad Kenshin Himura Mahmuddin, 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. .....Times of the pandemic have underlined the importance of software applications based on text, audio, and video messaging in society. Among the instant messaging applications widely used in Indonesia are Discord and LINE. Those two applications by default do not implement complete and comprehensive secure communication protocols for data that are in-transit. Some other applications have already implemented such protocols, with Signal and WhatsApp being the most popular among those that implement secure communication by default. However, both Signal and WhatsApp use a centralized architecture for their protocol, where all communication relies on centralized servers controlled by a single central authority. As such, users are ”forced” to trust and rely on those central servers that they have no control over. With such concerns in mind, this research attempts to introduce an instant messaging application that is end-to-end

encrypted with the XMPP protocol in addition to using OMEMO encryption scheme. XMPP is an instant messaging protocol that is selected due to its decentralized nature and the lack of need to rely on any central authority. The XMPP protocol can run on top of TCP or QUIC. For the purposes of this research, the implemented application supports XMPP connections utilizing either TCP or QUIC. On top of that, support for voice and video calls is also implemented with WebRTC and the Jingle extension as it is expected for instant messaging applications to have such a call feature. Two main aspects are evaluated in the implemented system, which are latency and resource usage. This research nds that the latency performance of the XMPP network is adequate, but an increase of latency is identi ed in cases where clients concurrently send each other messages. Furthermore, there is no signi cant performance difference between the use of XMPP on QUIC and TCP. This research also nds that the addition of OMEMO encryption compromises the latency performance of the application signi cantly, but as a result, any intermediary server or proxy can no longer read the contents of messages. The evaluation of the voice and video call features shows that the latency performance is satisfactory for a real-time application. A comparative test is also conducted between connections that utilize a relay server and those that do not, with there being no signi cant performance difference. However, this connection burdens additional load onto the relay server.