Abstrak

Seiring dengan berkembangnya teknologi berbasiskan internet protokol memberikan dampak pada semakin beragamnya layanan yang di-*deliver* melalui jaringan internet. Dengan tuntutan tersebut diharapkan terdapat teknologi yang dapat mengitegrasikan berbagai layanan. Oleh karena itu, IMS muncul sebagai sebuah arsitektur yang menjanjikan untuk dapat mengintegrasikan berbagai layanan multimedia dalam satu *platform* saja.

Pesan yang dilewatkan pada arsitektur IMS mungkin terdapat data yang harus diberikan perlindungan lebih terhadap kerahasiaannya. Pada pengerjaan tugas akhir ini, diterapkan salah satu protokol keamanan TLS server *authentication* pada Gm Interface IMS dengan layanan *instant messaging*. Kemudian dilihat pengaruhnya terhadap keamanan data *register* dan waktu tambahan yang dibutuhkan untuk proses keamanan. *Software* yang digunakan adalah openimscore, boghe IMS client, openssl dan wireshark.

Dari hasil pengujian yang dilakukan diperoleh hasil TLS server *authentication* melakukan keamanan berupa pesan terenkripsi dari data *register* hingga pembentukan sesi antara kedua *client*. Kemudian waktu yang dibutuhkan untuk *register* melalui TLS lebih lama dibandingkan tanpa TLS karena terdapat proses tambahan berupa TLS *handshaking* dan enkripsi, dekripsi dari pesan *register*.

Kata kunci : Gm *Interface* IMS, TLS server *authentication, Ciphertext, Plaintext*.