

Abstract

Along with the development of Internet protocol-based technologies have an impact on escalation in diversity and delivering services over the Internet network. it is expected to have technology that can integrate a variety of services. Therefore, IMS emerged as a promising architecture to be able to integrate various multimedia services into one platform only.

The message which is passed to the IMS architecture may contain data that should be given more protection of confidentiality. In this final project, will be applied one of security protocol in TLS authentication server on IMS Gm Interface with instant messaging services. Then it will be seen the influence given to the security register data and how much additional time used for security process. Software which is used openssl, boghe IMS client, openssl and wireshark

From testing result, it will give output about authentication server TLS provides message encryption from the register data to the establishment of session between two clients. Then the duration for TLS register is longer than register without TLS because there are additional process, that is TLS handshaking, encryption, decryption of register message.

Key words : Gm Interface IMS, TLS server authentication, Ciphertext, Plaintext.