# Implementation of Mqtt Security with the Augpake Protocol to Prevent Man In The Middle Attacks

**Prabowo Nofieldi[1], Vera Suryani[2]**

**School of Computing, Telkom University, Bandung**

[1]prabowonofieldi@student.telkomuniversity.ac.id, [2]verasuryani@telkomuniversity.ac.id

**Abstract**

The implementation of MQTT has been widely used in the IoT (Internet of Things) area as a messaging transport protocol, where the MQTT process includes a lightweight protocol with low complexity, low power, and low foot printing in implementation. With the OASIS MQTT standard, the security provided is already able to maintain its security such as SLL/TSL which requires validation in its security. With the security provided, it can provide vulnerabilities and MITM (Man in The Middle) attacks on the MQTT protocol. In this paper the author focuses on the security of the MQTT protocol by implementing the AugPAKE method which in previous research has been carried out in the ubuntu 64bit virtual machine area and raspberry Pi 2 model B and the author wants to prove security in different OS areas, namely Windows OS and Kali Linux OS. as well as using the latest broker, namely Mosquitto v.2.1. In this paper the author will focus on maintaining the security of the MQTT Protocol by implementing the AugPAKEmethod on the Mosquitto v.2.1 as broker in the Windows OS and Kali Linux OS areas. By using the AugPAKE method, every process in the MQTT protocol does not require validation for its security and still maintains the security of the data sent.

Keywords: AugPAKE, MQTT, Man in The Middle, Internet of Things