Abstract
Website is one of the fastest-growing media. Many security methods are applied to secure data stored on a website, but from the user's perspective, carelessness can occur when accessing websites with the Hypertext Transfer Protocol Secure (HTTPS) protocol using a smartphone device. This carelessness can be the reason that all sensitive data can be accessed and provide an attack from attacker. One example of an attack that often occurs to users when accessing HTTPS websites is Man in the Middle (MITM) attack. MITM attacks serve as an intermediary between users and wifi with open security, one of the developments of MITM attacks is the MITM proxy. MITM proxies are capable of viewing network traffic as well as generating fake certificates when users access websites. Sensitive user data can be seen and obtained when the attack is carried out, but the attack that occurs causes anomalies in the Round Trip Time and Throughput values. In detecting attacks and anomalies that occur, the K-Nearest Neighbor (K-NN) algorithm can be used. It is hoped that the results from study can provide an overview about detection and MITM proxy attacks. From the results of the attacks, user-sensitive information such as usernames and passwords, are successfully obtained, and the results of attack detection tests using the K-NN algorithm had an accuracy value of 95.1% with an error rate of 4.9%.

Keywords: ***Security, Man-in-The-Middle, K-Nearest Neighbor Algorithm, Attack Detection.***