Abstract

When sending a message from one device to another, the existing form of communication must be built properly so that the message conveyed arrives and there are no irregularities whatsoever. The threat contained in communication is that there are parties who are not responsible for sabotaging the path between the sender and receiver so that he is in the middle of the communication path between the sender and receiver. Dealing with this can be applied to checks for each message by authenticating data. The basic form of authentication utilizes the concept of zero knowledge proof. There are two parties involved as evidence and examiners in the form of authentication. This study focuses on the performance of authentication with zero knowledge proof and security of sending messages with AES. Testing gives results for low CPU and memory usage. It also makes it difficult for attackers with ciphertext message data.

Keywords: authentication protocol, data authentication, man-in-the-middle, zero-knowledge proof