ABSTRACT

Security in network communication is a crucial aspect to ensure data confidentiality, integrity, and authentication. The Modified Otway-Rees and Needham-Schroeder protocols are designed to strengthen security in the key exchange and authentication process between communicating parties. However, the potential vulnerabilities in the design of these protocols require in-depth analysis to ensure their effectiveness. This research aims to analyze the security of both protocols using BAN (Burrows-Abadi-Needham) logic, a formal method aimed at evaluating security protocols. This approach starts by defining basic assumptions, translating protocol steps into BAN logic notation, and analyzing whether security goals such as confidentiality, authentication, and integrity can be achieved. After testing this protocol, it was found that this protocol is safe from basic threats that have been tested using a basic correction process using BAN logic.

Keyword: *Security protocols, Modified Otway-Rees, Modified Needham-Schroeder, key exchange, BAN logic, authentication*