Cross-SN: a lightweight authentication scheme for a multi-server platform using IoT-based wireless medical sensor network

Several wireless devices and applications can be connected through wireless communication technologies to exchange data in future intelligent health systems (e.g., the Internet of Medical Things (IoMT)). Smart healthcare requires ample bandwidth, reliable and effective communications networks, energy-efficient operations, and quality of service support (QoS). Healthcare service providers host multi-servers to ensure seamless services are provided to the end-users. By supporting a multi-server environment, healthcare medical sensors produce many data transmitted via servers, which is impossible in a single-server architecture. To ensure data security, secure online communication must be considered since the transmitted data are sensitive. Hence, the adversary may try to interrupt the transmission and drop or modify the message. Many researchers have proposed an authentication scheme to secure the data, but the schemes are vulnerable to specific attacks (modification attacks, replay attacks, server spoofing attacks, Man-in-the middle (MiTM) attacks, etc.). However, the absence of an authentication scheme that supports a multi-server security in such a comprehensive development in a distributed server is still an issue. In this paper, a secure authentication scheme using wireless medical sensor networks for a multi-server environment is proposed (Cross-SN). The scheme is implemented with a smart card, password, and user identity. Elliptic curve cryptography is utilized in the scheme, and Burrows–Abadi–Needham (BAN) logic is utilized to secure mutual authentication and to analyse the proposed scheme's security. It offers adequate protection against replies, impersonation, and privileged insider attacks and secure communication in multi-server parties that communicate with each other.

Keyword: Authentication; Security; WSN; Multi-server environment; WMSN