World Academy of Science, Engineering and Technology
International Journal of Computer and Systems Engineering
Vol:12, No:03, 2018

Open Science Index, Computer and Systems Engineering Vol:12, No:03, 2018 publications.waset.org/abstracts/91453.pdf

An Efficient and Provably Secure Three-Factor Authentication Scheme with Key Agreement

Authors : Mohan Ramasundaram, Amutha Prabakar Muniyandi

Abstract : Remote user authentication is one of the important tasks for any kind of remote server applications. Several remote authentication schemes are proposed by the researcher for Telecare Medicine Information System (TMIS). Most of the existing techniques have limitations, vulnerable to various kind attacks, lack of functionalities, information leakage, no perfect forward security and ineffectiveness. Authentication is a process of user verification mechanism for allows him to access the resources of a server. Nowadays, most of the remote authentication protocols are using two-factor authentications. We have made a survey of several remote authentication schemes using three factors and this survey shows that the most of the schemes are inefficient and subject to several attacks. We observed from the experimental evaluation; the proposed scheme is very secure against various known attacks that include replay attack, man-in-the-middle attack. Furthermore, the analysis based on the communication cost and computational cost estimation of the proposed scheme with related schemes shows that our proposed scheme is efficient.

Keywords : Telecare Medicine Information System, elliptic curve cryptography, three-factor, biometric, random oracle
Conference Title : ICCSAE 2018 : International Conference on Computer Science and Automation Engineering
Conference Location : Singapore, Singapore
Conference Dates : March 22-23, 2018