SECURITY STUDIES CONFERENCE

2ND WORLD CONFERENCE ON SECURITY STUDIES

06-08 June 2025 Brussels, Belgium

Identity Authentication and Key Agreement Mechanism In E-Health Environment with FDO Protocol Integration

Chih-Yao Hsu,Kuo-Hsuan Huang, Chung-Yen Wu

Department of Computer Science and Engineering, Tatung University, Taiwan

Abstract

E-health environment identity authentication and key agreement mechanism with FDO protocol integration E-health concepts and Internet of Things (IoT) devices are becoming more and more popular in healthcare environments today, minimizing the physical distance between physicians and patients and providing real-time monitoring and timely medical treatment. However, it is obvious that the E-health environment involves the transmission of private and sensitive information about patient's physiological conditions and related prescriptions between various networks and the Internet of Things (IoT). Therefore, it is increasingly important to securely and reliably transmit the data and verify the validity of the identities of the transmitting parties to resist hacking attacks. In this paper, we attempt to utilize the Fido Device Onboard (FDO) protocol's features such as device-enabled auto-online service, device ownership record chain, and support for various identity authentication and data encryption mechanisms, and replace the roles of the Sensor and the medical server in the previous literature on identity authentication and key exchange mechanisms in E-health environments with those of the FDO device and the DMS management platform. The roles of Sensor and medical server in other literature on identity authentication and key exchange mechanisms in E-health environment are replaced by FDO devices and DMS management platforms, and the overall security, advantages and disadvantages of the proposed mechanisms are analyzed.

Keywords: DMS; Internet of Things (IoT); medical; sensor; wireless body area networks (WBANs)