World Academy of Science, Engineering and Technology
International Journal of Computer and Systems Engineering
Vol:17, No:06, 2023

On the Design of a Secure Two-Party Authentication Scheme for Internet of Things Using Cancelable Biometrics and Physically Unclonable Functions

Authors : Behnam Zahednejad, Saeed Kosari

Abstract : Widespread deployment of Internet of Things (IoT) has raised security and privacy issues in this environment. Designing a secure two-factor authentication scheme between the user and server is still a challenging task. In this paper, we focus on Cancelable Biometric (CB) as an authentication factor in IoT. We show that previous CB-based scheme fail to provide real two-factor security, Perfect Forward Secrecy (PFS) and suffer database attacks and traceability of the user. Then we propose our improved scheme based on CB and Physically Unclonable Functions (PUF), which can provide real two-factor security, PFS, user's unlinkability, and resistance to database attack. In addition, Key Compromise Impersonation (KCI) resilience is achieved in our scheme. We also prove the security of our proposed scheme formally using both Real-Or-Random (RoR) model and the ProVerif analysis tool. For the usability of our scheme, we conducted a performance analysis and showed that our scheme has the least communication cost compared to the previous CB-based scheme. The computational cost of our scheme is also acceptable for the IoT environment.

Keywords : IoT, two-factor security, cancelable biometric, key compromise impersonation resilience, perfect forward secrecy, database attack, real-or-random model, ProVerif
Conference Title : ICICS 2023 : International Conference on Information and Communications Security
Conference Location : San Francisco, United States
Conference Dates : June 05-06, 2023