Sensing as a service in Internet of Things: Efficient authentication and key agreement scheme. (2022) Journal of King Saud University - Computer and Information Sciences, 34 (8), pp. 5493-5509.
https://doi.org/10.1016/j.jksuci.2021.06.007

https://www.sciencedirect.com/science/article/pii/S1319157821001403/pdfft?md5=63f28da87839efa15369e46669b6a8aa&pid=1-s2.0-S1319157821001403-main.pdf

Authors: Atef Bentahar, Abdallah Meraoumia, Louardi Bradji, Hakim Bendjenna

Abstract

Internet of Things (IoT) sensing capabilities are now available as a public service. This new model, called sensing as a service (S2aaS), allows data owners to sell and/or exchange data with consumers interested in large open markets. However, the openness of the service industry makes the IoT-based S2aaS model more susceptible to malicious attacks. In this article, we propose a simple, efficient, and secure key agreement scheme for IoT-based S2aaS model. Users in the proposed system can securely and quickly access public services through a simple website rather than a traditional smart card. To simulate a real S2aaS environment, the cloud is treated as an untrusted node in the proposed method, and not all channels are secure. The fuzzy extractor and elliptic-curve Diffie–Hellman algorithms are used in conjunction with symmetric encryption and hash functions to establish a secure key agreement and data exchange session. In critical and frequent intervals, heavy processes are avoided. The proposed scheme's security has been informally analyzed and formally proven using the Automated Validation of Internet Security Protocols and Applications tool. The results show that our scheme satisfies the security requirements.