Title: Fuzzy Extractor-Based Key Agreement for Internet of Things.
Conference title: 020 1st International Conference on Communications, Control Systems and Signal Processing (CCSSP).
URL : https://doi.org/10.1109/CCSSP49278.2020.9151574 .

Authors:

Atef Bentahar; Abdallah Meraoumia; Hakim Bendjenna; Salim Chitroub; Abdelhakim Zeroual

Abstract

The emergence of the Internet of Things with its constraints obliges researchers in this field to find light and accurate solutions to secure the data exchange. This document presents secure authentication using biometrics coupled with an effective key agreement scheme to save time and energy. In our scheme, the agreed key is used to encrypt transmission data between different IoT actors. While the fuzzy extractor based on the fuzzy vault principle, is used as authentication and as key agreement scheme. Besides, our system incorporates the Reed Solomon and Hamming codes to give some tolerance to errors. The experimental results have been discussed according to several recognition rates and computation times. Indeed, the recognition rate results have been compared to other works to validate our system. Also, we clarify how our system resists to specific transmission attacks without affecting lightness and accuracy.