ABSTRACT

The conventional approach to authentication mechanisms has several drawbacks since secrets are stored statically. Physical Unclonable Function (PUF) technology dynamically generates keys, overcoming this limitation. However, even though the PUF response (the secret key) is dynamically generated and can act as a "biometric" of the device, there are still vulnerabilities to certain types of attacks. In previous research, the use of an additional secret key as an external noisy source has been conducted to reduce dependence solely on the secret key originating from the PUF. However, in previous studies, there was no optimization process for the PUF's secret key, thus the vulnerability level to PUF attacks remained the same. Additionally, camera surveillance was used to obtain images as an external noisy source, leading to high t-bits Error Correction Code (ECC) capability. Attackers could more easily create rogue images since the IoT device implements high t-bits to correct images during the reproduction phase (false positives). This research presents PUF-based IoT device with an optimized PUF responses to enhance the system's security performance, along with dynamic environmental parameters (as an external noisy source) with lower t-bits ECC error correction capabilities, thus reducing the likelihood of false positives. The optimization method of PUF responses involves truncating or uniforming bits, where uniforming bits show significant results with a decidability value of 1.37 (unoptimized only valued at 0.73) with confusion matrix values of 3.04%, 0.98%, 99.02%, and 96.96% respectively for FRR, FAR, TRR, and TAR (unoptimized values at 18.02%, 4.93%, 95.06%, and 81.97%). Furthermore, because this research uses two-factor fuzzy commitment that utilizes two-factor noisy sources consisting of a combination of internal and external noisy sources, it is evident that the combined two-factor noisy sources also has a better decidability value (up to 1.56) while maintaining the quality of the confusion matrix values. Lastly, this research successfully creates the use of t-bits ECC capability in the two-factor fuzzy commitment system, which is only 9 bits (compared to previous work reaching up to 30 bits to achieve 100% KRR overall in genuine noisy sources). This demonstrates granular correction and separation between genuine and attacker noisy sources. Therefore, it can be concluded that the results of the proposed method are superior to previous works, as it establishes an authentication system that is more complex for attackers to breach.

Keywords: PUF, Internal & External Noisy Source, Two-Factor Fuzzy Commitment, Decidability, Confusion Matrix