ABSTRAK

Mekanisme autentikasi konvensional memiliki berbagai kekurangan yang disebabkan oleh penyimpanan secret key secara statis. Physical Unclonable Function (PUF) memungkinkan adanya secret key secara dinamis, mengatasi kekurangan pada pendekatan konvensional. Namun, meskipun respon PUF (secret key) dapat dihasilkan secara dinamis, PUF tersebut masih memiliki kerentanan terhadap berbagai jenis serangan. Pada penelitian sebelumnya, penggunaan secret key tambahan sebagai external noisy source telah dilakukan untuk mengurangi ketergantungan secret key hanya pada respon PUF. Tetapi, pada penelitian sebelumnya, tidak terdapat proses optimisasi respon PUF sehingga masih terdapat kerentanan terhadap serangan PUF. Selain itu, surveillance camera yang digunakan untuk mendapatkan gambar sebagai external noisy source, mengakibatkan adanya nilai t-bits pada kapabilitas Error Correction Code (ECC) yang tinggi. Penyerang dapat secara lebih mudah membuat gambar palsu karena perangkat IoT menggunakan nilai t-bits yang tinggi untuk mengkoreksi gambar selama fase reproduction (false positive). Penelitian ini mengusulkan perangkat IoT berbasis PUF dengan respon PUF yang telah dioptimalkan untuk meningkatkan kinerja sistem autentikasi, sekaligus terintegrasi dengan parameter lingkungan yang sifatnya dinamis (sebagai external noisy source) serta memiliki kemampuan koreksi kesalahan (ECC t-bits) yang lebih rendah, sehingga mengurangi kemungkinan adanya false positive. Metode optimisasi respon PUF melibatkan truncating atau uniforming bits. Metode uniforming bits menunjukkan hasil yang signifikan dengan nilai decidability sebesar 1.37 (untuk unoptimized respon PUF hanya bernilai 0.73) dengan nilai confusion matrix masing-masing 3.04%, 0.98%, 99.02%, dan 96.96% untuk FRR, FAR, TRR, dan TAR (nilai untuk unoptimized respon PUF sebesar 18.02%, 4.93%, 95.06%, dan 81.97%). Selain itu, karena penelitian ini menggunakan two-factor fuzzy commitment yang memanfaatkan two-factor noisy source berupa kombinasi dari internal & external noisy source, terlihat bahwa kombinasi two-factor noisy source tersebut juga memiliki nilai decidability yang lebih baik (hingga 1.56) dengan tetap menjaga kualitas confusion matrix. Penelitian ini berhasil menciptakan kapabilitas ECC dalam sistem two-factor fuzzy commitment yang hanya bernilai 9 bit (dibandingkan dengan penelitian sebelumnya yang mencapai 30 bit untuk mencapai KRR 100% secara keseluruhan dalam hal pengkoreksian noisy source asli). Ini menunjukkan koreksi secara granular dan pemisahan antara noisy source asli dan penyerang secara lebih jelas. Oleh karena itu, dapat disimpulkan bahwa hasil metode yang diusulkan lebih baik dibandingkan dengan penelitian sebelumnya, dikarenakan dapat membangun sistem otentikasi yang lebih kompleks bagi penyerang.

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