

Abstrak

Kartu tanda mahasiswa (KTM) saat ini masih rentan terhadap tindakan kecurangan dan pemalsuan, termasuk serangan *replay attack*. KTM memiliki beberapa fungsi, seperti memberikan akses masuk dan keluar area parkir, gedung kuliah, perpustakaan, serta sistem kehadiran mahasiswa. Serangan *replay attack* memungkinkan penyerang memalsukan kehadiran mahasiswa dan mengakses fasilitas kampus secara tidak sah. Oleh karena itu, tujuan utama dari Tugas Akhir ini adalah meningkatkan keamanan KTM dengan mengimplementasikan sistem keamanan berbasis enkripsi *Advanced Encryption Standard* (AES) dan *rolling code* yang dapat mencegah *replay attack*. Metode yang digunakan meliputi enkripsi data pada KTM menggunakan algoritma AES-128 dan penerapan *rolling code* pada sistem keamanan KTM. Hasil pengujian menunjukkan bahwa implementasi sistem keamanan berbasis enkripsi AES-128 dan *rolling code* pada KTM dapat meningkatkan keamanan dan keaslian KTM serta mencegah tindakan kecurangan dan pemalsuan, termasuk penyalinan KTM. Dengan demikian, Tugas Akhir ini memberikan solusi untuk meningkatkan keamanan KTM dan memberikan manfaat signifikan bagi pengguna KTM.

Kata kunci : Replay Attack, Radio Frequency Identification, Advanced Encryption Standard, Near Field Communication, Rolling code.