BAB I. PENDAHULUAN

1.1. Latar Belakang

Dalam era digital saat ini, perkembangan teknologi Near Field Communication (NFC) telah merambah ke berbagai aspek kehidupan, termasuk penggunaannya dalam kartu pintar [1]. Teknologi NFC memungkinkan pengguna untuk melakukan transaksi dengan cepat dan mudah hanya dengan menempelkan kartu ke pembaca (reader), tanpa memerlukan tindakan tambahan yang rumit. Kemampuan ini telah membuat kartu NFC semakin populer dan digunakan secara luas dalam berbagai aplikasi, mulai dari pembayaran transportasi publik, akses kontrol, event acara, dan lain-lain

Salah satu implementasi kartu NFC yang umum adalah Kartu Tanda Mahasiswa (KTM) di lingkungan kampus. KTM tidak hanya berfungsi sebagai identitas mahasiswa, tetapi juga digunakan untuk mengakses fasilitas kampus, melakukan absensi, dan berbagai aktivitas lainnya. KTM menggunakan kartu NFC bertipe Mifare Classic 1K buatan NXP yang mempunyai frekuensi 13,56 MHz dengan kapasitas memori 1KB [3]. Kartu ini mempunyai jarak baca hingga 100mm. Dengan spesifikasi tersebut membuat kartu ini sangat banyak digunakan [1].

Namun, pada saat ini terdapat jasa untuk duplikasi KTM yang menjadi ancaman serius terhadap keamanan dan integritas data mahasiswa. Selain itu, praktik duplikasi ini juga dapat dimanfaatkan oleh pihak yang tidak berwenang untuk mendapatkan akses ilegal ke fasilitas kampus atau bahkan melakukan pencurian identitas mahasiswa. Untuk itu, diperlukan penerapan teknologi keamanan yang kuat dan efektif untuk menghindari ancaman tersebut.

Teknologi yang dimaksud adalah enkripsi data yang terdapat pada KTM. Data yang tidak terenkripsi saat ini dapat secara langsung untuk diakses sehingga dapat mengancam aspek keamanan *confidentiality* atau informasi data pribadi mahasiswa. Akibatnya data ini dapat disalahgunakan seseorang untuk mencuri data, mengakses fasilitas kampus secara ilegal, dan lain-lain.

Data yang terenkripsi saja belum cukup untuk mencegah duplikasi kartu. Jika data terenkripsi hanya statis dan tidak berubah-ubah, maka dengan duplikasi saja tanpa mengetahui isi data pada kartu masih dapat dilakukan untuk mengakses fasilitas kampus secara ilegal. Untuk itu dibutuhkan sistem autentikasi tambahan yang dapat memverifikasi keaslian kartu dan mengubah data pada kartu secara dinamis setiap kali kartu terbaca pada *reader*. Sehingga kartu yang

terduplikasi tidak dapat digunakan.

Penelitian ini berfokus pada penerapan enkripsi RSA [4] dan sistem autentikasi Rolling Code [5] Hash SHA256 pada KTM. Enkripsi RSA digunakan untuk melindungi data yang ada di dalam KTM sehingga tidak dapat diakses secara langsung oleh pihak yang tidak berwenang [4]. Sementara itu, sistem autentikasi Rolling Code Hash digunakan untuk memverifikasi keaslian KTM secara dinamis, dengan nilai hash yang berubah setiap kali kartu digunakan [6].

Implementasi teknologi ini juga harus mempertimbangkan kompleksitas komputasi dan efisiensi *resource* yang dipakai. Jika proses tersebut tidak dipertimbangkan, maka teknologi tersebut telah menghilangkan karakteristik kartu NFC itu sendiri yaitu proses transaksi yang cepat.

Implementasi teknologi ini diharapkan dapat mengurangi risiko duplikasi KTM dan melindungi integritas data mahasiswa dengan mempertimbangkan kompleksitas komputasi dan efisiensi penggunaan *resource*. Dengan adanya langkah-langkah keamanan yang kuat, diharapkan KTM dapat digunakan dengan lebih aman dan efisien dalam lingkungan kampus yang semakin terhubung secara digital.

1.2. Perumusan Masalah

Berdasarkan latar belakang yang telah dibahas sebelumnya, rumusan masalah yang dibahas adalah sebagai berikut:

1. Bagaimana metode penerapan enkripsi RSA untuk melindungi data pada KTM guna menghindari akses ilegal oleh pihak lain?
2. Bagaimana penerapan Rolling Code Hash SHA256 sebagai sistem autentikasi untuk verifikasi keaslian KTM?
3. Apakah penerapan enkripsi RSA dan rolling code pada KTM menyebabkan peningkatan beban komputasi dan penggunaan *resource* yang signifikan?

1.3. Tujuan

Tujuan yang dicapai dari penelitian yang dilakukan adalah sebagai berikut:

1. Menerapkan metode enkripsi RSA untuk melindungi data pada KTM guna menghindari akses ilegal oleh pihak lain.
2. Menerapkan *rolling code* hash SHA256 sebagai sistem autentikasi untuk verifikasi keaslian KTM.

3. Mengevaluasi beban komputasi dan efisiensi penggunaan *resource* penerapan enkripsi RSA dan *rolling code* pada KTM.

1.4. Batasan Masalah

1. Jenis kartu yang digunakan adalah *Mifare Classic 1K* yang merupakan jenis kartu KTM yang digunakan saat ini.
2. Sistem Rolling Code memungkinkan hanya terdapat satu kartu saja yang dapat diterima oleh sistem.
3. Penelitian ini terbatas pada penerapan RSA sebagai perlindungan data dengan mempertimbangkan waktu komputasinya dan *resource* yang tersedia.

1.5. Metodologi Penelitian

Berikut tahapan metodologi yang spesifik untuk menyelesaikan penelitian mengenai penerapan enkripsi data RSA dan sistem autentikasi rolling code hash SHA256 pada kartu tanda mahasiswa.

1.5.1. Identifikasi Masalah

Tahap ini melibatkan identifikasi terhadap kerentanan keamanan yang terdapat pada kartu tanda mahasiswa (KTM) saat ini. Fokus masalah dari penelitian ini adalah kartu tanda mahasiswa saat ini sangat mudah untuk diduplikasi. Tujuan dari penelitian ini adalah meningkatkan keamanan KTM dengan menerapkan enkripsi RSA dan sistem autentikasi *rolling code* hash SHA256.

1.5.2. Studi Literatur

Tahap ini melibatkan studi literatur yang mencakup tentang keamanan yang terdapat dalam RFID *(Radio Frequency Identification)* atau NFC *(Near Field Communications)*, seperti desain keamanan RFID/NFC, enkripsi data khususnya RSA, sistem OTP *(One-Time Password)*, *rolling code*, dll.

1.5.3. Perancangan Sistem

Tahap ini melibatkan perancangan sistem keamanan kartu yang mencakup:

1. Perancangan perangkat-perangkat yang dibutuhkan seperti perangkat baca/tulis ke kartu mahasiswa.

2. Perancangan server untuk mengimplementasikan enkripsi RSA dan *rolling code* hash SHA256.
3. Perancangan perangkat-perangkat pendukung lainnya seperti penghubung antara device baca/tulis dan server, dll.

1.5.4. Implementasi

Tahap ini melibatkan implementasi dari rancangan sistem yang telah dibuat sebelumnya. Perangkat digunakan untuk membaca dan menulis data ke kartu mahasiswa. Data ini mencakup *random shared key* dan data lainnya yang dihasilkan dan di-enkripsi menggunakan RSA oleh server.

1.5.5. Evaluasi

Tahap ini melibatkan evaluasi terhadap sistem yang telah dibuat dan memastikan bahwa:

1. Sistem enkripsi RSA dan rolling code hash SHA256 dapat meningkatkan keamanan data kartu mahasiswa dengan salah satunya mencegah duplikasi kartu mahasiswa.
2. Sistem yang diterapkan tidak memiliki beban komputasi yang lama dan berat sehingga mengganggu kenyamanan mahasiswa ketika menggunakan kartu.

Berdasarkan hasil evaluasi ini sehingga dapat disusun kesimpulan mengenai kemungkinan keberhasilan penerapan enkripsi RSA dan sistem rolling code hash SHA256 pada kartu tanda mahasiswa.