# BAB I PENDAHULUAN

## 1.1 Latar belakang masalah

*Radio-frequency identification* (RFID) adalah penggunaan suatu objek yang diaplikasikan pada barang, hewan atau orang yang bertujuan untuk mengidentifikasi atau melacak menggunakan gelombang radio[1]. Penggunaan RFID semakin sering digunakan dalam kehidupan sehari - hari. Penggunaan yang paling umum diantaranya pada kartu mahasiswa, kartu transportasi, kartu tol atau kartu parkir. Pada beberapa kantor dan perusahaan RFID digunakan sebagai pembuka pintu untuk mengakses suatu ruangan. RFID dibagi 2 jenis yaitu RFID aktif dan pasif. RFID aktif memiliki sumber energi sendiri sedangkan RFID pasif bergantung pada sumber energi pembacanya. Keamanan RFID menjadi alasan utama dibuatnya tugas akhir ini. Dapat dibayangkan apa yang terjadi apabila sesorang dapat melakukan modifikasi pada isi RFID, maka orang tersebut dapat mengendarai alat transportasi secara gratis atau mengakses fasilitas khusus yang hanya dapat diakses orang tertentu[2].

*Near Field Communication* (NFC) [4] adalah suatu fitur komunikasi nirkabel yang menggunakan induksi magnet sehingga memungkinkan untuk komunikasi jarak dekat. Di Indonesia, penggunaan teknologi NFC belum terlalu banyak, sedangkan di luar negeri NFC merupakan fitur yang biasa digunakan untuk transaksi menggunakan telepon seluler (ponsel) sebagai pengganti kartu serta dapat digunakan untuk bertukar foto, video atau data. Pada beberapa ponsel, NFC dapat digunakan untuk membaca RFID pada kartu mahasiswa, kartu kredit atau kartu akses suatu tempat.

Dengan memanfaatkan fitur NFC pada ponsel, ada beberapa cara penyerangan yang bisa dilakukan peretas diantaranya adalah memodifikasi isi kartu serta melakukan *cloning* pada suatu kartu RFID. Baik melakukan modifikasi atau melakukan *cloning* dapat dilakukan jika sudah mengetahui *key*. Beberapa RFID jenis lama sudah diketahui *key* enkripsinya sehingga cukup mudah untuk melakukan modifikasi pada RFID tersebut.

Pada tugas akhir ini akan dilakukan eksploitasi teknik *cloning* dan modifikasi pada kartu mahasiswa Universitas Telkom. Percobaan dilakukan dengan cara membaca isi kartu mahasiswa dengan fitur NFC pada ponsel kemudian dicek jenis kartu serta enkripsinya. Kemudian isi kartu akan dipindahkan pada kartu RFID lain dan dicek apakah kartu tersebut dapat terbaca. Setelah penelitian selesai maka akan dicari solusi untuk mencegah terjadinya *Cloning* dan Modifikasi pada KTM.

## 1.2 Perumusan Masalah

Dalam tugas akhir ini akan dirumuskan beberapa permasalahan antara lain:

1. Cara membaca isi data dari kartu tanda mahasiswa dengan mudah.
2. Cara melakukan cloning pada kartu tanda mahasiswa menggunakan NFC.

## 1.3 Tujuan

Dalam tugas akhir ini terdapat 2 tujuan yang ingin dicapai di akhir penelitian, yaitu

1. Melakukan cloning pada kartu tanda mahasiswa Universitas Telkom.
2. Memodifikasi data dalam RFID.

## 1.4 Hipotesis

Kartu tanda mahasiswa Universitas Telkom tidak memiliki proteksi sehingga dapat dilakukan *cloning* dan modifikasi pada kartu tersebut.

## 1.5 Batasan Masalah

Dalam penulisan tugas akhir ini ada beberapa batasan masalah yang dibuat agar fokus untuk menyelesaikan permasalahan diantaranya adalah :

1. Teknik yang digunakan hanya teknik *cloning.*
2. Kartu RFID yang digunakan adalah kartu tanda mahasiswa Universitas Telkom.
3. Alat baca RFID adalah alat yang terdapat di kampus Universitas Telkom.
4. Ponsel yang digunakan adalah Google Nexus yang berbasis android dan memiliki fitur NFC.
5. Penelitian dilakukan hanya pada sisi pengguna RFID saja dan bukan pada sisi pengembang aplikasi RFID.

## 1.6 Metodologi Penelitian

Metode penelitian yang digunakan pada tugas akhir ini adalah metode penelitian kuantitatif. Metode penelitian kuantitatif adalah metode untuk melakukan percobaan pada suatu objek dengan teori yang sudah ada sebelumnya.

Untuk melakukan penelitian ini ada beberapa tahapan yang dilakukan agar berjalan dengan lancar adalah:

### 1. Studi Literatur

Pada proses ini akan didalami pengetahuan tentang RFID. Atribut yang terdapat pada RFID. Selain itu dilakukan pembelajaran tentang NFC serta bagaimana karakteristik NFC.

### 2. Pengumpulan Kebutuhan Sistem

Pada proses ini akan dikumpulkan alat alat yang menjadi kebutuhan dalam melakukan penelitian. Alat - alat yang dibutuhkan untuk melakukan penelitian ini adalah:

- Kartu tanda Mahasiswa (KTM)
- Ponsel Google Nexus yang dilengkapi dengan fitur NFC
- Aplikasi untuk membaca dan mengkloning RFID
- Kartu untuk *cloning* yang dapat dilakukan penulisan pada sektor 0.

**3. Pembacaan KTM**

Pada proses ini dilakukan pembacaan terhadap kartu KTM menggunakan ponsel. Hasil dari pembacaan yang diinginkan adalah data berupa:

- Tag ID dalam *Hexadecimal*
- Teknologi kartu
- Informasi memori
- Isi data RFID dalam *Hexadecimal*

**4. Analisis Kartu**

Pada proses ini dilakukan analisis terhadap data yang sudah didapatkan. Analisis yang dilakukan pertama kali adalah terhadap teknologi kartu. Dengan mendapatkan teknologi kartu maka bisa ditentukan bagaimana cara membaca tag serta isi data pada RFID. Analisis kedua adalah tag, yang hasilnya adalah kesimpulan apakah terdapat suatu proteksi pada RFID atau tidak. Apabila terdapat proteksi maka akan dicari apakah sudah terdapat solusi untuk memecahkannya atau tidak. Apabila belum, maka proses *cloning* dan modifikasi tidak dapat dilakukan dan langsung diambil kesimpulan. Apabila solusi dari proteksi sudah ada, maka akan dilakukan solusi itu untuk memecahkan proteksi kartu.

**5. Pencarian Kartu RFID Sejenis**

Pada proses ini akan dicari kartu RFID yang sejenis dengan KTM dari segi teknologi maupun chip. Pencarian ini diperkirakan memakan waktu 2 minggu untuk memesan barang dan menunggu barang datang

**6. Proses *Cloning* dan Modifikasi**

Pada proses ini setelah mendapatkan kartu yang sesuai dengan KTM maka dilakukan proses *cloning* KTM terhadap kartu lain. Pada proses *cloning* hal yang akan dikopikan ke kartu baru adalah

- Tag ID dalam *Hexadecimal*
- *Key A* dan *Key B*
- Isi data RFID dalam *Hexadecimal*

Setelah isi RFID dikopikan maka dilakukan uji coba apakah kartu baru terbaca oleh alat baca RFID atau tidak. Apabila terbaca maka akan dilihat apakah isi yang terbaca sudah sesuai

Proses modifikasi dilakukan dengan cara mengganti nilai atau isi dari data pada RFID menggunakan angka acak. Proses ini untuk membuktikan apakah RFID bisa ditulis ulang dan dilakukan perubahan isi data di dalamnya.

**7. Penarikan Kesimpulan**

Pada tahap ini dilakukan penarikan kesimpulan terhadap hasil uji coba. Isi dari kesimpulan menjawab hipotesa Kartu Tanda Mahasiswa Universitas Telkom tidak memiliki proteksi sehingga dapat dilakukan *cloning* dan modifikasi pada kartu tersebut

**8. Pembuatan Laporan**

Pada tahap ini dibuat laporan hasil dari penelitian yang sudah dilakukan. Laporan terdiri dari 5 bab dimulai dengan Pendahuluan, Tinjauan Pustaka, Rancangan Penelitian, Implementasi dan Analisis serta Kesimpulan dan Saran