

RADIO FREQUENCY IDENTIFICATION

Tugas Proyek Mata Kuliah Keamanan Sistem Informasi

Oleh:

ERWIN

13200040



**DEPARTEMEN TEKNIK ELEKTRO
FAKULTAS TEKNOLOGI INDUSTRI
INSTITUT TEKNOLOGI BANDUNG**

2004

Abstrak

Pada era globalisasi keamanan informasi merupakan hal yang sangat penting. Sebuah sistem keamanan informasi harus memperhatikan tiga hal yaitu keamanan, autentikasi, dan integritas. Untuk mencapai tiga hal tersebut maka dibutuhkan sebuah sistem yang dapat melakukan identifikasi terhadap pengguna yang akan mengakses suatu informasi. Pada makalah ini penulis akan mengemukakan sebuah solusi identifikasi berbasis frekuensi radio.

Dalam beberapa tahun terakhir ini teknologi identifikasi berbasis frekuensi radio (*Radio Frequency Identification*) berkembang dengan pesat. Hal ini diakibatkan oleh beberapa hal, salah satu di antaranya kebutuhan yang besar dari aplikasi untuk konsumen dengan menggunakan teknologi ini.

Radio Frequency Identification (RFID) adalah teknologi *wireless* yang kompak yang berpotensi sangat besar untuk kemajuan perniagaan (*commerce*). RFID menggunakan chip yang dapat dideteksi pada range beberapa meter oleh pembaca RFID. RFID sebagai barcode generasi berikutnya dapat digunakan untuk otomatisasi inventory control, sehingga dapat mengurangi biaya dari pabrik ke distributor.

Tag RFID yang telah diperbaharui mempunyai beberapa keunggulan dibandingkan dengan teknologi identifikasi lainnya dan dapat juga digunakan untuk sistem keamanan. Tag RFID menawarkan solusi identifikasi dengan berbagai macam tingkat keamanan.

Pada makalah ini akan dibahas masalah identifikasi, overview mengenai RFID, cara kerja RFID, berbagai macam arsitektur RFID, dan aplikasinya dalam kehidupan sehari-hari.

Daftar Isi

Abstrak.....	i
Daftar Isi	ii
Daftar Gambar	iv
1. Pendahuluan.....	1
2. Identifikasi dan Autentifikasi.....	2
2.1. Identifikasi	2
2.2. Isu Kriptografi Dalam Identifikasi.....	3
2.3. Identifikasi dengan <i>Password</i> atau PIN.....	4
2.4. Autentifikasi dengan Pertanyaan dan Respon.....	5
3. Radio Frequency Identification (RFID).....	7
3.1. Overview RFID.....	7
3.2. Pembaca RFID	8
3.3. Tag RFID	9
3.4. Frekuensi Kerja RFID.....	10
3.5. Akurasi RFID.....	11
3.5.1. Akurasi Sistem RFID Frekuensi Rendah.....	11
3.5.2. Akurasi Sistem RFID Frekuensi Tinggi	12
3.6. Beberapa Arsitektur RFID Untuk Keamanan	13
3.6.1. Sistem Fixed Code	13
3.6.2. Sistem Rolling Code	13
3.6.3. Sistem Proteksi dengan <i>Password</i>	14
3.6.4. Sistem Kombinasi Rolling Code dan <i>Password</i>	14
3.7. <i>Crypto Transponder</i>	14
3.7.1. Digital Signature <i>Transponder</i>	14
3.7.2. Enkripsi.....	17
3.7.3. Rangkaian Supervision	18
4. Aplikasi RFID.....	19
4.1. Inventory Control.....	19
4.2. Transportasi.....	19
4.3. Keamanan dan Akses Kontrol	19
5. Kesimpulan	20

Daftar Pustaka.....21

Daftar Gambar

Gambar 1. Sistem RFID.....	8
Gambar 2. Sistem Crypto <i>Transponder</i>	15
Gambar 3. Digital Signature <i>Transponder</i>	16
Gambar 4. Diagram Blok Crypto <i>Transponder</i>	18

1. Pendahuluan

Pada era globalisasi keamanan informasi merupakan hal yang sangat penting. Sebuah sistem keamanan informasi harus memperhatikan tiga hal yaitu keamanan, autentifikasi, dan integritas. Untuk mencapai tiga hal tersebut maka dibutuhkan sebuah sistem yang dapat melakukan identifikasi terhadap pengguna yang akan mengakses suatu informasi.

Dalam beberapa tahun terakhir ini teknologi identifikasi berbasis frekuensi radio (*Radio Frequency Identification*) berkembang dengan pesat. Hal ini diakibatkan oleh beberapa hal, salah satu di antaranya kebutuhan yang besar dari aplikasi untuk konsumen dengan menggunakan teknologi ini.

Radio Frequency Identification (RFID) adalah teknologi *wireless* yang kompak. RFID berpotensi sangat besar untuk kemajuan perniagaan (*commerce*). RFID menggunakan chip yang dapat dideteksi pada range beberapa meter oleh pembaca RFID. Sebagai contoh RFID dapat menjadi barcode generasi berikutnya yang dapat digunakan untuk otomatisasi inventory control akan memberikan banyak kemudahan dan dapat mengurangi biaya dari pabrik ke distributor.

Tag RFID mempunyai beberapa keunggulan dibandingkan barcode. Barcode hanya mengidentifikasi tipe objek, tetapi RFID dapat membawa identitas tambahan yang unik, misalnya serial number yang dapat membedakan objek yang satu dari objek lain yang serupa. Sehingga informasi proses yang dialami dari sebuah objek yang menggunakan tag RFID dapat diperoleh dengan mudah. Selain itu RFID juga tidak memerlukan kontak langsung, dan sebuah *reader* RFID dapat membaca semua tag RFID yang berada pada daerah jangkauannya. Dengan cara ini maka waktu untuk inventory control dapat dihemat.

2. Identifikasi dan Autentifikasi

Pada era globalisasi ini isu keamanan informasi menjadi sangat penting. Pada saat ini hampir semua orang menyimpan informasi secara elektronik. Media penyimpanan informasi secara elektronik memiliki banyak keunggulan dibandingkan media lainnya, di antaranya: informasi elektronik lebih padat kapasitas penyimpanannya, informasi elektronik mudah dipindahkan, dan mudah untuk mengaksesnya. Tetapi di sisi lain, media informasi elektronik menimbulkan masalah baru dalam hal keamanan informasi, karena informasi elektronik lebih mudah dicuri, diubah, dan dirusak dibandingkan media lainnya. Oleh karena itu diperlukan layanan keamanan informasi untuk melindungi nilai dari informasi tersebut.

Keamanan informasi mempunyai fungsi untuk melindungi informasi dari usaha pencurian, penggantian, dan perusakan oleh pihak-pihak yang tidak punya hak akses terhadap informasi tersebut. Untuk itu diperlukan kemampuan identifikasi pengguna oleh sistem keamanan informasi, untuk mencegah pengaksesan informasi oleh pengguna yang tidak berhak.

Pada bab ini akan dibahas mengenai pertimbangan teknik yang dapat digunakan suatu sistem keamanan untuk dapat melakukan proses identifikasi dan dapat melakukan verifikasi bahwa suatu pihak adalah pengguna yang mempunyai hak akses terhadap suatu sistem. Dengan sistem ini maka tindakan penipuan dan imitasi terhadap sistem informasi elektronik dapat dicegah.

2.1. Identifikasi

Dari sisi sistem keamanan, hasil dari protokol autentifikasi adalah salah satu dari penerimaan identitas dari suatu pihak yang dikenal, atau penolakan identitas yang tidak dikenal. Secara lebih spesifik, tujuan dari protokol identifikasi adalah:

- Jika A berhasil melakukan autentifikasi identitasnya pada B, maka B akan melanjutkan protokol setelah menerima identitas A.
- *Transferability*: B tidak dapat menggunakan pertukaran identifikasi dengan A, untuk dapat melakukan imitasi A terhadap pihak ketiga C.
- *Impersonation*: Sangat kecilnya kemungkinan pihak C yang berbeda dari A, melakukan protokol identifikasi dengan B dan mengambil peran dari A, yang dapat menyebabkan B menerimanya sebagai identitas A.
- *Transferability* dan *Impersonation* berlaku untuk jumlah proses autentifikasi yang sangat banyak.

2.2. Isu Kriptografi Dalam Identifikasi

Dari sudut pandang kriptografi, masalah identifikasi meliputi dua tugas penting yaitu, melakukan identifikasi dan melakukan autentifikasi terhadap identitas. Beberapa jenis kriptografi yang dapat digunakan untuk sistem identifikasi di antaranya:

- **Pengetahuan**
Sistem identifikasi berdasarkan pengetahuan tentang suatu rahasia, misalnya *password* atau PIN (*Personal Identification Number*) untuk menunjukkan keabsahan identitas. Untuk beberapa aplikasi dengan keamanan yang tinggi, tidak diimplementasikan dengan sistem ini, karena level keamanannya yang tidak terlalu baik.
- **Biometric**
Sistem identifikasi berdasarkan atribut biologis, misalnya sidik jari, suara, retina, atau pengenalan wajah. Dengan salah satu dari atribut ini maka identitas seseorang dapat dilakukan.
- **Kepemilikan**
Identifikasi dengan berdasarkan kepemilikan suatu benda. Metoda ini adalah metoda yang umum dan masih akan digunakan secara luas pada masa yang akan datang. Hal ini dapat diimplementasikan dengan kepemilikan *magnetic card*, *smart card*, dan lain-lain.

Untuk pembahasan berikut akan digunakan istilah kunci untuk hal-hal yang dipergunakan untuk sistem identifikasi di atas. Semua sistem kriptografi yang dideskripsikan di atas merupakan prosedur autentifikasi statik. Autentifikasi statik artinya sistem keamanan dapat mengenali identitas dari kunci, tetapi kunci tidak dapat melakukan pengenalan terhadap sistem keamanan.

Prosedur autentifikasi mutual yang memungkinkan kunci untuk memastikan identitas sistem keamanan adalah salah satu fitur yang dapat menambah tingkat keamanan dari suatu sistem keamanan. Dengan prosedur ini maka rahasia yang hanya diketahui oleh kunci dan sistem keamanan yang sesuai tidak akan dikeluarkan oleh kunci kepada sistem lain.

Tingkat keamanan yang lebih tinggi dapat diperoleh dengan algoritma simetris yang dikenal dengan protokol pertanyaan dan jawaban (*challenge / response protocol*). Sistem keamanan akan memastikan identitas kunci dengan mengirimkan pertanyaan (*challenge*) dan kemudian akan memeriksa jawaban (*response*) dari kunci. Jawaban yang benar hanya akan diberikan oleh kunci jika sebuah rahasia diketahui oleh sistem keamanan dan kunci. Konsep ini mempunyai beberapa keunggulan, yaitu: pada penggunaan normal, rahasia tidak dipertukarkan, dan pertanyaan dan jawaban dapat bervariasi dari waktu ke waktu.

2.3. Identifikasi dengan Password atau PIN

Password konvensional melibatkan *password time-invariant* (tidak berubah menurut waktu). Ide dasar adalah sebuah *password* yang berasosiasi terhadap seorang pengguna terdiri dari kalimat terdiri dari 6 sampai 10 atau lebih karakter. Ini adalah rahasia yang diketahui oleh pengguna dan sistem.

PIN (*Personal Identification Number*) juga termasuk ke dalam kategori *password time-invariant*. PIN biasanya digunakan bersamaan dengan kepemilikan suatu

benda (*token*) misalnya *smart card*. Ini akan menyediakan level keamanan yang lebih baik karena orang lain tidak dapat memperoleh akses tanpa mengetahui PIN bila *token* ini hilang atau dicuri. Umumnya PIN dibuat pendek yaitu antara 4 sampai 8 digit. Untuk mencegah pencarian PIN secara acak (karena jumlah kemungkinan yang sedikit), maka diperlukan mekanisme tambahan, misalnya penguncian kartu pada ATM untuk kesalahan memasukkan PIN 3 kali berturut-turut.

Karena manusia sulit untuk mengingat kode rahasia yang cukup panjang untuk mendapatkan tingkat keamanan yang cukup tinggi, maka *Password* dan PIN tidak dapat dibuat panjang sehingga sistem autentifikasi keamanannya tidak cukup kuat.

2.4. Autentifikasi dengan Pertanyaan dan Respon

Ide dari protokol kriptografi dengan pertanyaan dan respon adalah sebuah entitas yang akan menunjukkan keabsahan identitasnya kepada entitas lain (sistem keamanan) dengan mendemonstrasikan rahasia dirinya kepada sistem keamanan, tanpa membuka rahasia kepada sistem keamanan tersebut, pada saat protokol sedang berlangsung. Hal ini dapat dilakukan dengan memberikan respon terhadap pertanyaan yang *time-variant* (berubah terhadap waktu), di mana respon bergantung pada rahasia entitas tersebut dan pertanyaan yang diberikan. Pertanyaan umumnya berupa sebuah bilangan yang dipilih salah satu entitas secara acak dan rahasia. Walaupun jalur komunikasi disadap pada saat protokol berlangsung, respon dari sebuah proses identifikasi tidak akan memberikan informasi yang berguna untuk identifikasi selanjutnya.

Parameter *time-invariant* dapat digunakan pada protokol identifikasi untuk mencegah terjadinya perulangan. Parameter ini umumnya disebut sebagai *unique number* atau *nonce*. *Nonce* adalah nilai yang digunakan tidak lebih dari satu kali, untuk penggunaan yang sama. Hal ini dilakukan untuk mencegah pengulangan yang dapat dideteksi.

Bilangan acak dapat digunakan dalam mekanisme pertanyaan respon, untuk memberikan keunikan dan mencegah perulangan. Bilangan acak juga menyediakan sistem yang tidak dapat diprediksi.

Istilah bilangan acak, yang digunakan dalam konteks protokol identifikasi dan autentikasi, melibatkan bilangan *pseudorandom* yang tidak terprediksi. Bilangan *pseudorandom* adalah bilangan yang seolah-olah acak, tapi sebenarnya ada perulangannya dengan periode perulangan yang sangat panjang.

3. Radio Frequency Identification (RFID)

3.1. Overview RFID

RFID adalah proses identifikasi seseorang atau objek dengan menggunakan frekuensi transmisi radio. RFID menggunakan frekuensi radio untuk membaca informasi dari sebuah devais kecil yang disebut tag atau *transponder* (*Transmitter* + *Responder*). Tag RFID akan mengenali diri sendiri ketika mendeteksi sinyal dari devais yang kompatibel, yaitu pembaca RFID (*RFID Reader*).

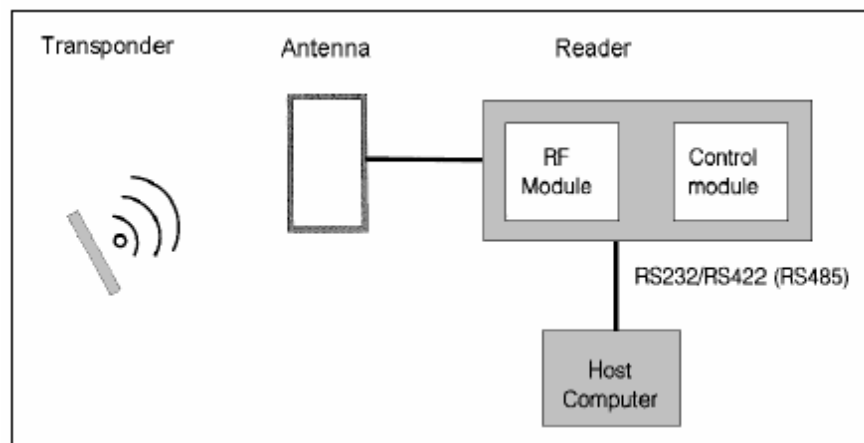
RFID adalah teknologi identifikasi yang fleksibel, mudah digunakan, dan sangat cocok untuk operasi otomatis. RFID mengkombinasikan keunggulan yang tidak tersedia pada teknologi identifikasi yang lain. RFID dapat disediakan dalam devais yang hanya dapat dibaca saja (*Read Only*) atau dapat dibaca dan ditulis (*Read/Write*), tidak memerlukan kontak langsung maupun jalur cahaya untuk dapat beroperasi, dapat berfungsi pada berbagai variasi kondisi lingkungan, dan menyediakan tingkat integritas data yang tinggi. Sebagai tambahan, karena teknologi ini sulit untuk dipalsukan, maka RFID dapat menyediakan tingkat keamanan yang tinggi.

Pada sistem RFID umumnya, tag atau *transponder* ditempelkan pada suatu objek. Setiap tag membawa dapat membawa informasi yang unik, di antaranya: serial number, model, warna, tempat perakitan, dan data lain dari objek tersebut. Ketika tag ini melalui medan yang dihasilkan oleh pembaca RFID yang kompatibel, tag akan mentransmisikan informasi yang ada pada tag kepada pembaca RFID, sehingga proses identifikasi objek dapat dilakukan.

Sistem RFID terdiri dari empat komponen, di antaranya seperti dapat dilihat pada gambar 1:

- Tag: Ini adalah devais yang menyimpan informasi untuk identifikasi objek. Tag RFID sering juga disebut sebagai *transponder*.

- Antena: untuk mentransmisikan sinyal frekuensi radio antara pembaca RFID dengan tag RFID.
- Pembaca RFID: adalah devais yang kompatibel dengan tag RFID yang akan berkomunikasi secara *wireless* dengan tag.
- Software Aplikasi: adalah aplikasi pada sebuah workstation atau PC yang dapat membaca data dari tag melalui pembaca RFID. Baik tag dan pembaca RFID diperlengkapi dengan antena sehingga dapat menerima dan memancarkan gelombang elektromagnetik.



Gambar 1. Sistem RFID

3.2. Pembaca RFID

Sebuah pembaca RFID harus menyelesaikan dua buah tugas, yaitu:

- Menerima perintah dari software aplikasi
- Berkomunikasi dengan tag RFID

Pembaca RFID adalah merupakan penghubung antara software aplikasi dengan antena yang akan meradiasikan gelombang radio ke tag RFID. Gelombang radio yang diemisikan oleh antena berpropagasi pada ruangan di sekitarnya. Akibatnya data dapat berpindah secara *wireless* ke tag RFID yang berada berdekatan dengan antena.

3.3. Tag RFID

Tag RFID adalah devais yang dibuat dari rangkaian elektronika dan antena yang terintegrasi di dalam rangkaian tersebut. Rangkaian elektronik dari tag RFID umumnya memiliki memori sehingga tag ini mempunyai kemampuan untuk menyimpan data. Memori pada tag secara dibagi menjadi sel-sel. Beberapa sel menyimpan data *Read Only*, misalnya *serial number* yang unik yang disimpan pada saat tag tersebut diproduksi. Sel lain pada RFID mungkin juga dapat ditulis dan dibaca secara berulang.

Berdasarkan catu daya tag, tag RFID dapat digolongkan menjadi:

- Tag Aktif: yaitu tag yang catu dayanya diperoleh dari batere, sehingga akan mengurangi daya yang diperlukan oleh pembaca RFID dan tag dapat mengirimkan informasi dalam jarak yang lebih jauh. Kelemahan dari tipe tag ini adalah harganya yang mahal dan ukurannya yang lebih besar karena lebih kompleks. Semakin banyak fungsi yang dapat dilakukan oleh tag RFID maka rangkaiannya akan semakin kompleks dan ukurannya akan semakin besar.
- Tag Pasif: yaitu tag yang catu dayanya diperoleh dari medan yang dihasilkan oleh pembaca RFID. Rangkaiannya lebih sederhana, harganya jauh lebih murah, ukurannya kecil, dan lebih ringan. Kelemahannya adalah tag hanya dapat mengirimkan informasi dalam jarak yang dekat dan pembaca RFID harus menyediakan daya tambahan untuk tag RFID.

Tag RFID telah sering dipertimbangkan untuk digunakan sebagai barcode pada masa yang akan datang. Pembacaan informasi pada tag RFID tidak memerlukan kontak sama sekali. Karena kemampuan rangkaian terintegrasi yang modern, maka tag RFID dapat menyimpan jauh lebih banyak informasi dibandingkan dengan barcode.

Pada tabel 1 diilustrasikan perbedaan utama antara teknologi barcode dengan RFID.

Sistem	Barcode	RFID
Transmisi data	Optik	Elektromagnetik
Ukuran data	1 – 100 byte	128 – 8096 byte
Modifikasi data	Tidak bisa	Bisa
Posisi pembawa data	Kontak cahaya	Tanpa kontak
Jarak Komunikasi	Beberapa meter	Dari cm sampai meter
Supseptibilitas Lingkungan	Debu	Dapat diabaikan
Pembacaan jamak	Tidak bisa	Bisa

Tabel 1. Perbandingan Teknologi Barcode dengan RFID

Fitur pembacaan jamak pada teknologi RFID sering disebut sebagai anti collision.

3.4. Frekuensi Kerja RFID

Faktor penting yang harus diperhatikan dalam RFID adalah frekuensi kerja dari sistem RFID. Ini adalah frekuensi yang digunakan untuk komunikasi *wireless* antara pembaca RFID dengan tag RFID.

Ada beberapa band frekuensi yang digunakan untuk sistem RFID. Pemilihan dari frekuensi kerja sistem RFID akan mempengaruhi jarak komunikasi, interferensi dengan frekuensi sistem radio lain, kecepatan komunikasi data, dan ukuran antena. Untuk frekuensi yang rendah umumnya digunakan tag pasif, dan untuk frekuensi tinggi digunakan tag aktif.

Pada frekuensi rendah, tag pasif tidak dapat mentransmisikan data dengan jarak yang jauh, karena keterbatasan daya yang diperoleh dari medan elektromagnetik. Akan tetapi komunikasi tetap dapat dilakukan tanpa kontak langsung. Pada kasus

ini hal yang perlu mendapatkan perhatian adalah tag pasif harus terletak jauh dari objek logam, karena logam secara signifikan mengurangi fluks dari medan magnet. Akibatnya tag RFID tidak bekerja dengan baik, karena tag tidak menerima daya minimum untuk dapat bekerja.

Pada frekuensi tinggi, jarak komunikasi antara tag aktif dengan pembaca RFID dapat lebih jauh, tetapi masih terbatas oleh daya yang ada. Sinyal elektromagnetik pada frekuensi tinggi juga mendapatkan pelemahan (atenuasi) ketika tag tertutupi oleh es atau air. Pada kondisi terburuk, tag yang tertutup oleh logam tidak terdeteksi oleh pembaca RFID.

Ukuran antena yang harus digunakan untuk transmisi data bergantung dari panjang gelombang elektromagnetik. Untuk frekuensi yang rendah, maka antena harus dibuat dengan ukuran yang lebih besar dibandingkan dengan RFID dengan frekuensi tinggi.

3.5. Akurasi RFID

Akurasi RFID dapat didefinisikan sebagai tingkat keberhasilan pembaca RFID melakukan identifikasi sebuah tag yang berada pada area kerjanya. Keberhasilan dari proses identifikasi sangat dipengaruhi oleh beberapa batasan fisik, yaitu:

- Posisi antena pada pembaca RFID
- Karakteristik dari material lingkungan yang mencakup sistem RFID
- Batasan catu daya
- Frekuensi kerja sistem RFID

3.5.1. Akurasi Sistem RFID Frekuensi Rendah

Pada frekuensi rendah, contohnya pada frekuensi 13,56 MHz, komunikasi frekuensi radio antara tag dengan pembaca RFID sangat bergantung pada daya yang diterima tag dari antena yang terhubung dengan pembaca RFID. Pada ruang

bebas, intensitas dari medan magnet yang diemisikan oleh antena berkurang terdapat jarak, maka terdapat batas jarak di mana tag tidak aktif, dan komunikasi frekuensi radio tidak dapat terjadi. Pengurangan ukuran tag akan mengurangi juga batas jarak.

Komunikasi radio berkurang jika medan magnet harus menembus material yang mengurangi daya elektromagnetik, contohnya pada kasus objek dengan bahan logam. Tag RFID tidak akan terdeteksi ketika diletakkan di dalam logam, karena material logam akan meredam fluks magnet yang melalui tag secara drastis.

Orientasi dari tag sangat penting dan dapat menyebabkan medan magnet bervariasi. Jika orientasi tag RFID sejajar dengan arah propagasi energi, maka fluks adalah nol dan komunikasi radio frekuensi tidak akan terjadi walaupun jarak antara antena dan tag sangat dekat.

3.5.2. Akurasi Sistem RFID Frekuensi Tinggi

Pada frekuensi tinggi, performansi dari sistem RFID sangat bergantung pada lingkungan di mana komunikasi di antara tag dan pembaca RFID terjadi. Pada jarak tanpa hambatan proses identifikasi dapat terjadi pada jarak pada orde 10 meter. Tetapi bila ada hambatan maka jarak ini akan berkurang secara drastis.

Pada frekuensi tinggi, tag RFID bekerja secara aktif dengan daya dari baterai. Akurasi dari tag RFID dapat berkurang karena kekurangan daya.

Akurasi dari sistem RFID pada umumnya sangat bergantung dari lingkungan di mana sistem RFID dioperasikan. Tantangan desain sistem RFID adalah melakukan desain infrastruktur RFID di antara lingkungan yang kurang bersahabat yang telah dijelaskan sebelumnya.

3.6. Beberapa Arsitektur RFID Untuk Keamanan

Untuk penggunaan RFID untuk aplikasi sistem keamanan, terdapat beberapa macam arsitektur yang dapat digunakan.

3.6.1. Sistem Fixed Code

Sistem ini merupakan sistem paling sederhana yang paling sering digunakan. Kode tetap yang tersimpan di tag RFID dibaca dan dibandingkan dengan kode yang tersimpan database. Untuk keperluan ini dapat digunakan tag RFID yang hanya dapat ditulis satu kali saja dan belum diprogram sama sekali. User dapat memprogram sendiri tag tersebut. Kelemahannya adalah user dapat membuat *copy* dari tag RFID yang tidak dapat dibedakan oleh sistem keamanan. Tersedia pula tag RFID yang hanya dapat dibaca, dan telah diprogram pada proses produksi dengan nomor identifikasi yang unik. Sistem ini tidak memungkinkan pembuatan *copy* dari tag RFID. Sistem yang sederhana ini tingkat keamanannya paling rendah.

3.6.2. Sistem Rolling Code

Beroperasi dengan cara sama dengan sistem *Fixed Code*, akan tetapi kode rahasia pada tag RFID hanya berlaku pada periode waktu tertentu. Pembaca RFID pada sistem ini harus mempunyai kemampuan untuk menulis tag RFID. Tag RFID yang digunakan harus dapat diprogram berkali-kali. Jadinya setiap terjadi proses identifikasi maka sistem keamanan akan mengubah kode rahasia yang ada pada tag RFID, dan akan menggunakan kode rahasia tersebut untuk proses identifikasi selanjutnya.

Sistem ini memberikan tingkat keamanan yang lebih baik, tetapi yang harus dipertimbangkan adalah proses sinkronisasi kode rahasia.

3.6.3. Sistem Proteksi dengan Password

Sistem autentikasi mutual yang sederhana dapat disediakan oleh sistem RFID dengan proteksi *password*. Data rahasia pada tag RFID hanya akan ditransmisikan setelah Pembaca RFID mengirimkan data berupa *password* yang sesuai untuk dapat membuktikan keabsahan pembaca RFID. Panjang dari *password* dapat bervariasi disesuaikan dengan kebutuhan tingkat keamanan.

Password biasanya ditransmisikan dalam plain text. Waktu untuk menduga *password* bervariasi antar beberapa menit sampai beberapa tahun bergantung dari panjang dari *password*.

Untuk sistem keamanan dengan banyak pengguna dengan *password* berbeda, memiliki keterbatasan yaitu yaitu total waktu komunikasi yang sangat lama, karena pembaca RFID harus menduga *password* dari database yang tersedia.

3.6.4. Sistem Kombinasi Rolling Code dan Password

Merupakan sistem gabungan dengan fasilitas kode rahasia berubah-ubah dan *password* untuk melindungi kode rahasia yang tersimpan dalam tag RFID. Isu yang kritis dari sistem ini adalah waktu komunikasi dan sinkronisasi *password*. Dengan sistem ini akan memberikan tingkat keamanan yang tinggi.

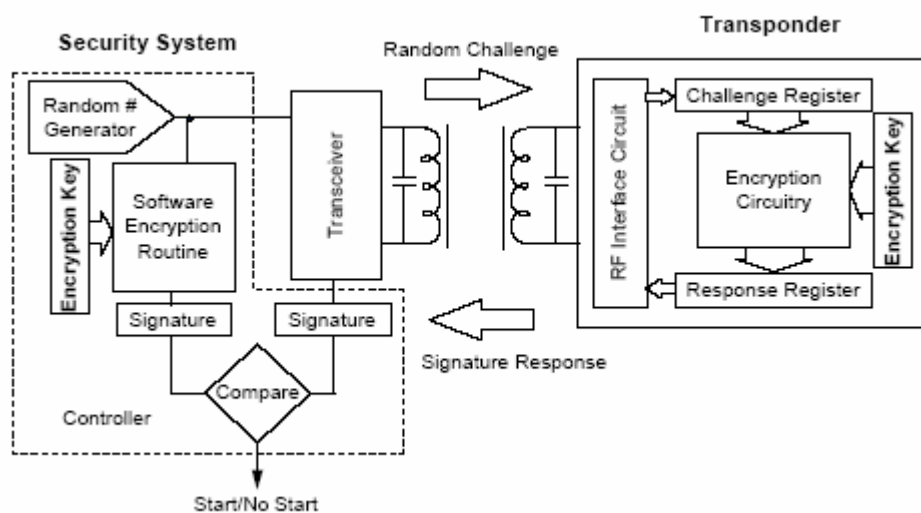
3.7. Crypto Transponder

3.7.1. Digital Signature Transponder

Digital Signature *Transponder* adalah devais crypto yang menggunakan sistem pertanyaan dan jawaban. Ini adalah merupakan generasi kedua dari tag RFID yang khusus digunakan untuk sistem keamanan, di mana hanya sebuah kunci yang dapat mengakses sistem kewanaman tersebut. Sistem ini contohnya dapat diaplikasikan pada sistem pengamanan mobil. Pada saat inisialisasi, sistem

keamanan dan *transponder* bertukar kunci enkripsi rahasia. Kunci ini tidak dapat dibaca, hanya respon *transponder* terhadap pertanyaan yang dikirimkan sistem keamanan yang dapat dibaca.

Pada aplikasinya, sistem keamanan mengirimkan sejumlah bit bilangan acak (pertanyaan) kepada *transponder* menggunakan *Pulse Width Modulation*. Pada *transponder* pertanyaan tersebut dimasukkan ke dalam register pertanyaan. Untuk waktu yang singkat, energi disediakan oleh sistem keamanan dan rangkaian logika enkripsi akan menghasilkan respon (signature). Pada gambar 2 dapat dilihat sistem *Crypto Transponder*.



Gambar 2. Sistem *Crypto Transponder*

Respon R adalah fungsi dari kunci enkripsi K_e , *challenge* $RAND$, dan algoritma kriptografi F_c .

$$R = f(F_c, RAND, K_e)$$

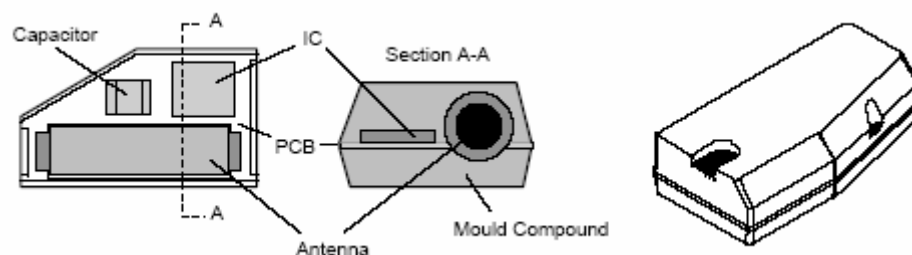
Respon dikembalikan ke sistem keamanan dengan menggunakan *Frequency Shift Keying* (FSK).

Sistem keamanan menghitung respon yang diharapkan dengan menggunakan algoritma yang sama dan kunci enkripsi yang sama dan membandingkan respon yang diterima dari *transponder* dengan hasil perhitungan. Hasil perhitungan dari respon yang diharapkan dapat selesai bersamaan dengan komunikasi antara *transponder* dengan sistem keamanan atau setelah menerima respon dari *transponder*. Jika hasilnya sama, maka informasi akan dikirimkan ke komputer manajemen.

Keunggulan dari sistem ini adalah sebagai berikut:

- Respon berbeda pada setiap waktu, bergantung dari pertanyaan (*challenge*). Akibatnya proses autentifikasi adalah dinamis.
- Tidak ada bagian dari kunci enkripsi yang dikirimkan setelah inisialisasi.
- Kunci enkripsi tidak dapat dibaca.
- *Transponder* tidak dapat diduplikasi.
- Kunci enkripsi dapat dikunci atau diubah jika diinginkan dengan melakukan inisialisasi ulang.

Transponder merupakan devais logika yang kompleks dan sistem yang didesain untuk beroperasi pada daya sangat rendah. Gambar dari *transponder* ini dapat dilihat pada gambar 3.



Gambar 3. Digital Signature *Transponder*

3.7.2. Enkripsi

Semua algoritma enkripsi secara teoritis dapat dipecahkan. Sebuah algoritma enkripsi dikatakan aman jika waktu untuk memecahkannya dibutuhkan waktu sangat lama.

Terdapat beberapa metoda penyerangan terhadap enkripsi yaitu:

- *Scanning*

Adalah pendekatan paling sederhana di mana penyerang mengirimkan respon random terhadap setiap *challenge* yang dihasilkan sistem keamanan. Waktu rata-rata untuk sukses dirumuskan menjadi:

$$t_s = R \times 2^{(rb-1)}$$

di mana rb adalah panjang respon dalam bit, dan R adalah waktu perulangan sistem keamanan dalam detik. Misalkan saja waktu perulangan adalah 200 ms dan panjang respon 24 bit, maka waktu rata-rata untuk membobol sistem keamanan itu adalah 19,4 hari.

- *Dictionary Attack*

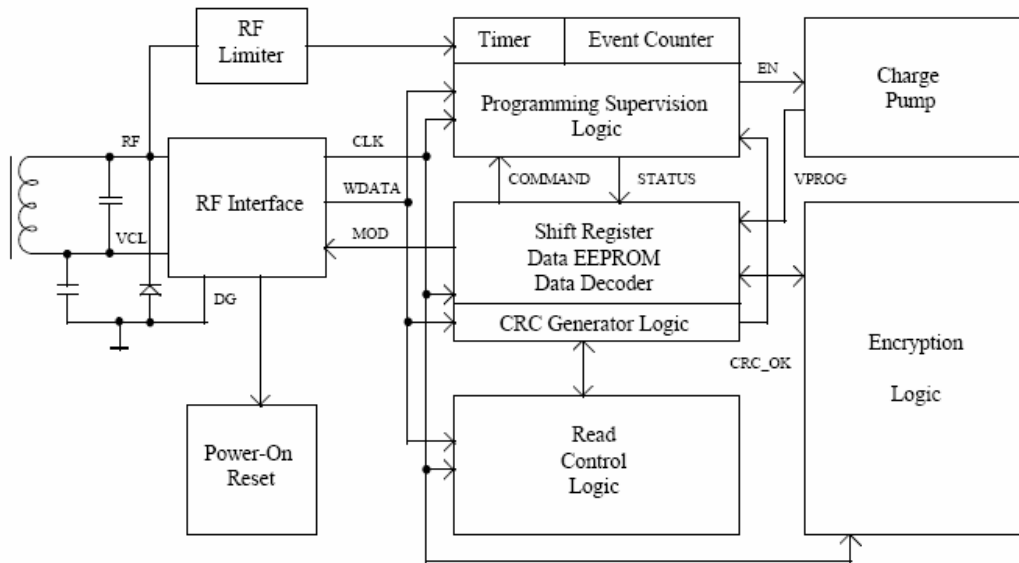
Merupakan pendekatan penyerangan yang kompleks di mana pihak penyerang membuat *dictionary*, dan respon disesuaikan dengan *challenge* dan *dictionary* yang diupdate setiap respon diberikan.

- *Cryptoanalysis*

Menggunakan pengetahuan dari algoritma. Penyerang mencoba untuk mencari solusi matematika dari masalah untuk mencari kunci enkripsi dengan jumlah terbatas pasangan *challenge* dan respon. Cara ini sangat sulit sekali dilakukan.

3.7.3. Rangkaian Supervision

Rangkaian ini digunakan untuk meyakinkan reliabilitas dalam aplikasi. Misalnya untuk eksekusi pemrograman *transponder*, penggunaan CRC untuk melakukan pemeriksaan terhadap command, data dan address yang diterima pada fasa penulisan *transponder*. Pada gambar 4 dapat dilihat blok diagram dari *transponder crypto*.



Gambar 4. Diagram Blok Crypto Transponder

4. Aplikasi RFID

Pada bab sebelumnya dibahas mengenai beberapa tipe sistem RFID, dan perkembangannya. Penggunaan RFID dengan berbagai macam arsitektur, dapat diimplementasikan dalam berbagai macam aplikasi.

4.1. Inventory Control

Sistem penanganan barang pada proses manufaktur dan distribusi yang efisien dan hemat waktu, dapat disediakan dengan sistem identifikasi yang cepat dan aman. Hal ini dapat dengan mudah direalisasikan dengan RFID, karena tidak memerlukan kontak langsung, maupun kontak optik. Dengan tambahan fitur anticollision sejumlah barang dapat diperiksa secara bersamaan. Pada aplikasi ini masalah lingkungan dan kecepatan merupakan peranan yang penting.

4.2. Transportasi

Kenyamanan dan efisiensi waktu menjadi tawaran yang menarik untuk penggunaan RFID pada bidang transportasi, di mana penggunaan sistem identifikasi yang cepat diperlukan. Contohnya adalah penggunaan tag RFID untuk menandai bawaan penumpang, dan pengganti tiket sehingga dapat mencegah antrian yang panjang

4.3. Keamanan dan Akses Kontrol

Contoh aplikasi pada bidang ini adalah sistem keamanan pada mobil, atau fasilitas tertentu, di mana untuk aplikasi ini diperlukan keamanan dengan level yang tinggi dan tidak mudah ditiru. Untuk kebutuhan ini dapat direalisasikan dengan generasi kedua tag RFID yaitu Digital Signature *Transponder*.

5. Kesimpulan

RFID merupakan teknologi yang masih baru, dan akan terus berkembang. Seiring dengan kemajuan teknologi rangkaian terintegrasi, maka dapat dipastikan bahwa harga tag RFID dapat ditekan sangat murah. Kebutuhan akan tag RFID juga akan bertambah di waktu yang akan datang, karena kebutuhan akan proses yang berhubungan dengan identifikasi dan keamanan yang lebih nyaman, efisien, dan hemat waktu.

Perkembangan teknologi RFID terus dilakukan secara terus-menerus untuk perbaikan performa RFID, sehingga dapat menangani lebih banyak masalah anticollision, dapat beroperasi dengan daya yang rendah.

Daftar Pustaka

- [1] Menezes A.: Handbook of Applied Cryptography, CRC Press (1996), bab 10
- [2] ---: RFID White Paper, Allied Bussiness Intelligence, 2002
- [3] d'Hont S.: The Cutting Edge of RFID Technology and Applications for Manufacturing and Distribution, Texas Instrument TIRIS
- [4] Das Raghu: RFID Explained, Free IDTechEx White Paper, 2004
- [5] ---: Securing RFID Value Chain, RSA Security