

STUDI MENGENAI ASPEK PRIVASI PADA SISTEM RFID

DEDI SUPRIATNA
23205321

Sekolah Teknik Elektro Dan Informatika
Institut Teknologi Bandung
Januari 2007

Abstrak

RFID (*Radio-Frequency IDentification*) merupakan sebuah teknologi *compact wireless* yang diunggulkan untuk mentransformasi dunia komersial. Sebagai suksesor dari barcode, RFID dapat melakukan kontrol otomatis untuk banyak hal. Sistem-sistem RFID menawarkan peningkatan efisiensi dalam pengendalian inventaris (*inventory control*), logistik dan manajemen rantai *supply* (*supply chain management*).

Oleh karena itu, terdapat kepentingan yang besar pada *enterprise* maupun agen-agen pemerintah untuk secara intensif mempercayakan pada sistem ini, khususnya para peritel dan para pembuat produk *consumer* yang besar. Sasaran jangka panjang organisasi-organisasi tersebut adalah mengintegrasikan RFID pada level ritel.

Adopsi yang meluas dari RFID telah memunculkan kekhawatiran akan persoalan keamanan dan *privasi* pada para konsumen dan masyarakat umum. Berdasarkan kenyataan tersebut di atas, dilakukan studi mengenai aspek *privasi* pada sistem-sistem RFID. Studi tersebut akan membahas identifikasi masalah, solusi-solusi yang sudah pernah ditawarkan serta pemilihan solusi yang tepat berdasarkan solusi-solusi yang sudah pernah ditawarkan.

I. Pendahuluan

RFID merupakan sebuah teknologi *compact wireless* yang diunggulkan untuk mentransformasi dunia komersial. RFID adalah sebuah teknologi yang memanfaatkan frekuensi radio untuk identifikasi otomatis terhadap obyek-obyek atau manusia. Kenyataan bahwa manusia amat terampil dalam mengidentifikasi obyek-obyek dalam kondisi lingkungan yang berbeda-beda menjadi motivasi dari teknologi ini. Sebagai contoh, seseorang yang mengantuk dapat dengan mudah mengambil secangkir kopi di atas meja sarapan yang berantakan di pagi hari. Sementara itu komputer sangatlah lemah dalam melakukan tugas-tugas demikian. RFID dapat dipandang sebagai suatu cara untuk pelabelan obyek-obyek secara eksplisit untuk memfasilitasi “persepsi” mereka dengan menggunakan peralatan-peralatan komputer.^[3] Menurut^[2], RFID adalah teknologi penangkapan data yang dapat digunakan secara elektronik untuk mengidentifikasi, melacak dan menyimpan informasi yang tersimpan dalam *tag* RFID.

Perhatian terhadap RFID dalam lingkungan media massa maupun akademis yang populer, telah meningkat dalam beberapa tahun ini. Salah satu buktinya adalah usaha dari organisasi-organisasi yang besar seperti Wal-Mart, Procter and Gamble, dan Departemen Pertahanan Amerika Serikat untuk menggunakan RFID sebagai suatu alat untuk mengontrol secara otomatis terhadap rantai supply mereka. Harga *tag* yang menurun dan standarisasi yang dinamis telah menyebabkan kita berada pada ambang ledakan penggunaan RFID.^[3]

Para pengamat RFID menganggap RFID sebagai suksesor dari *barcode* optik yang banyak dicetak pada barang-barang dagangan dengan dua keunggulan pembeda^[3] :

- 1) **Identifikasi yang unik** : Sebuah *barcode* mengindikasikan tipe obyek tempat ia dicetak, misalnya “Ini adalah sebatang coklat merek ABC dengan kadar 70% dan berat 100 gram”. Sebuah *tag* RFID selangkah lebih maju dengan mengemisikan sebuah nomor seri unik di antara jutaan obyek yang identik, sehingga ia dapat mengindikasikan “Ini adalah sebatang coklat merek ABC dengan kadar 70% dan berat 100 gram, nomor seri 897348738” *Identifier* yang unik dalam RFID dapat berperan sebagai pointer terhadap entri basis data yang menyimpan banyak histori transaksi untuk item-item individu.
- 2) **Otomasi** : Barkode di-*scan* secara optik, memerlukan kontak *line-of-sight* dengan *reader*, dan tentu saja peletakan fisik yang tepat dari obyek yang di-*scan*. Kecuali pada lingkungan yang benar-benar terkontrol, *scanning* terhadap *barcode* memerlukan campur tangan manusia, sebaliknya *tag-tag* RFID dapat dibaca tanpa kontak *line-of-sight* dan tanpa penempatan yang presisi. *Reader* RFID dapat melakukan *scan* terhadap *tag-tag* sebanyak ratusan perdetik.

Sebagai suksesor dari *barcode*, RFID dapat melakukan kontrol otomatis untuk banyak hal. Sistem-sistem RFID menawarkan peningkatan efisiensi dalam pengendalian inventaris (*inventory control*), logistik dan manajemen rantai *supply* (*supply chain management*).

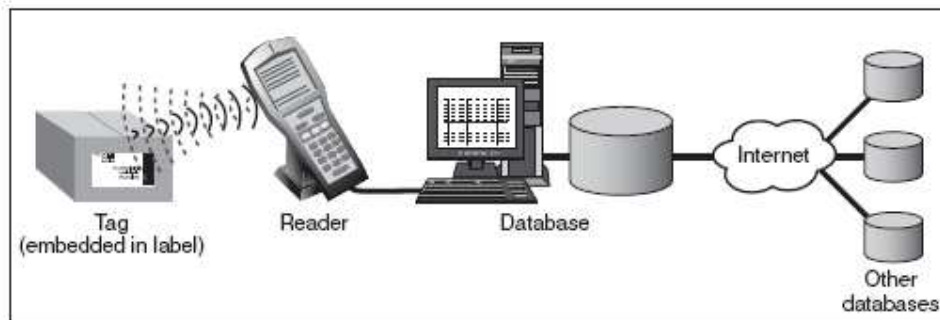
Menurut^[1], sistem RFID meraih popularitas, juga nama buruknya, dalam tahun-tahun ini. Kekuatan pengendali di balik perkembangan yang cepat dari teknologi RFID adalah munculnya *pervasive commerce*, kadang-kadang disebut revolusi diam-diam. *Pervasive commerce* menggunakan teknologi seperti peralatan lacak (*tracking*) dan label pintar yang ditanamkan pada sensor-sensor pentransmisi dan *reader* cerdas untuk mentransmisikan informasi tentang area-area kunci di mana konsumen tinggal dan bekerja untuk sistem pemrosesan data. Untuk mengumpulkan data ini, para peritel dapat memilih dari sekian banyak pilihan.

Sebagai suatu sistem yang mentransmisikan data unik, terbuka banyak celah privasi yang dapat menimbulkan kekhawatiran di berbagai kalangan. Isu privasi banyak dimunculkan oleh para pemerhati RFID seiring dengan semakin populernya teknologi RFID akhir-akhir ini. Studi ini akan membahas isu-isu privasi tersebut.

II. Tinjauan tentang Sistem RFID

2.1 Komponen-komponen Utama Sistem RFID

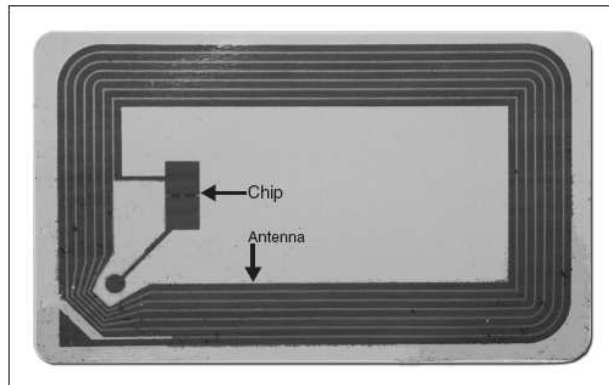
Secara garis besar sebuah sistem RFID terdiri atas tiga komponen utama, yaitu *tag*, *reader* dan basis data (Gambar 1). Secara ringkas, mekanisme kerja yang terjadi dalam sebuah sistem RFID adalah bahwa sebuah *reader* frekuensi radio melakukan *scanning* terhadap data yang tersimpan dalam *tag*, kemudian mengirimkan informasi tersebut ke sebuah basis data yang menyimpan data yang terkandung dalam *tag* tersebut.^[2]



Gambar 1 Komponen utama sistem RFID^[2].

Sistem RFID merupakan suatu tipe sistem identifikasi otomatis yang bertujuan untuk memungkinkan data ditransmisikan oleh peralatan *portable* yang disebut *tag*, yang dibaca oleh suatu *reader* RFID dan diproses menurut kebutuhan dari aplikasi tertentu. Data yang ditransmisikan oleh *tag* dapat menyediakan informasi identifikasi atau lokasi, atau hal-hal khusus tentang produk-produk bertag, seperti harga, warna, tanggal pembelian dan lain-lain. Penggunaan RFID dalam aplikasi-aplikasi pelacakan dan akses pertama kali muncul pada tahun 1980an. RFID segera mendapat perhatian karena kemampuannya untuk melacak obyek-obyek bergerak. Seiring semakin canggihnya teknologi, semakin meluas pula penggunaan *tag* RFID.^[1]

Sebuah *tag* RFID atau *transponder*, terdiri atas sebuah mikro (*microchip*) dan sebuah antena (Gambar 2). *Chip* mikro itu sendiri dapat berukuran sekecil butiran pasir, seukuran 0.4 mm^[3]. *Chip* tersebut menyimpan nomor seri yang unik atau informasi lainnya tergantung kepada tipe memorinya. Tipe memori itu sendiri dapat *read-only*, *read-write*, atau *write-once-read-many*. Antena yang terpasang pada chip mikro mengirimkan informasi dari chip ke *reader*. Biasanya rentang pembacaan diindikasikan dengan besarnya antena. Antena yang lebih besar mengindikasikan rentang pembacaan yang lebih jauh. *Tag* tersebut terpasang atau tertanam dalam obyek yang akan diidentifikasi. *Tag* dapat discan dengan *reader* bergerak maupun stasioner menggunakan gelombang radio.^[2]



Gambar 2 *Tag* RFID^[2].

Tag RFID sangat bervariasi dalam hal bentuk dan ukuran. Sebagian *tag* mudah ditandai, misalnya *tag* anti-pencurian yang terbuat dari plastik keras yang dipasang pada barang-barang di toko. *Tag* untuk tracking hewan yang ditanam di bawah kulit berukuran tidak lebih besar dari bagian lancip dari ujung pensil. Bahkan ada *tag* yang lebih kecil lagi yang telah dikembangkan untuk ditanam di dalam serat kertas uang.^[1]

Tag versi paling sederhana adalah *tag* pasif, yaitu *tag* yang tidak memiliki catu daya sendiri serta tidak dapat menginisiasi komunikasi dengan *reader*. Sebagai gantinya, *tag* merespon emisi frekuensi radio dan menurunkan dayanya dari gelombang-gelombang energi yang dipancarkan oleh *reader*. Sebuah *tag* pasif minimum mengandung sebuah indentifier unik dari sebuah item yang dipasang *tag* tersebut. Data tambahan dimungkinkan untuk ditambahkan pada *tag*, tergantung kepada kapasitas penyimpanannya.^[2]

Dalam keadaan yang sempurna, sebuah *tag* dapat dibaca dari jarak sekitar 10 hingga 20 kaki. *Tag* pasif dapat beroperasi pada frekuensi rendah (*low frequency*, LF), frekuensi tinggi (*high frequency*, HF), frekuensi ultra tinggi (*ultrahigh frequency*, UHF), atau gelombang mikro (*microwave*). Contoh aplikasi *tag* pasif adalah pada pas transit, pas masuk gedung, barang-barang konsumsi.^[2]

Harga *tag* pasif lebih murah dibandingkan harga versi lainnya. Perkembangan *tag* murah ini telah menciptakan revolusi dalam adopsi RFID dan memungkinkan penggunaannya dalam skala yang luas baik oleh organisasi-organisasi pemerintah maupun industri.^[2]

Tag semipasif adalah versi *tag* yang memiliki catu daya sendiri (baterai) tetapi tidak dapat menginisiasi komunikasi dengan *reader*. Dalam hal ini baterai digunakan oleh *tag* sebagai catu daya untuk melakukan fungsi yang lain seperti pemantauan keadaan lingkungan dan mencatu bagian elektronik internal *tag*, serta untuk memfasilitasi penyimpanan informasi. *Tag* versi ini tidak secara aktif memancarkan sinyal ke *reader*. Sebagian *tag* semipasif tetap dorman hingga menerima sinyal dari *reader*. *Tag* semi pasif dapat dihubungkan dengan sensor untuk menyimpan informasi untuk peralatan keamanan kontainer.^[2]

Tag aktif adalah *tag* yang selain memiliki antena dan chip juga memiliki catu daya dan pemancar serta mengirimkan sinyal kontinyu. *Tag* versi ini biasanya memiliki kemampuan baca tulis, dalam hal ini data *tag* dapat ditulis ulang dan/atau

dimodifikasi. *Tag* aktif dapat menginisiasi komunikasi dan dapat berkomunikasi pada jarak yang lebih jauh, hingga 750 kaki, tergantung kepada daya baterainya. Harga *tag* ini merupakan yang paling mahal dibandingkan dengan versi lainnya.^[2]

Tabel 1 Karakteristik umum *tag* RFID^[2].

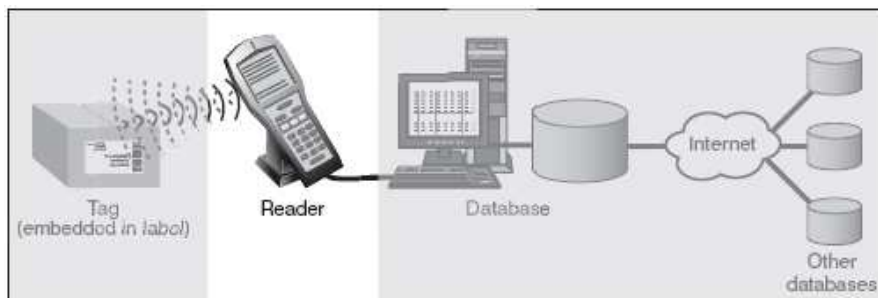
| | <i>Tag</i> pasif | <i>Tag</i> semipasif | <i>Tag</i> aktif |
|-----------------|---------------------------------|-------------------------|-------------------------|
| Catu daya | eksternal (dari <i>reader</i>) | baterai internal | baterai internal |
| Rentang baca | dapat mencapai 20 kaki | dapat mencapai 100 kaki | dapat mencapai 750 kaki |
| Tipe memori | umumnya read-only | read-write | read-write |
| Harga | \$.20 hingga beberapa dolar | \$2 hingga \$10 | \$20 atau lebih |
| Usia <i>tag</i> | dapat mencapai 20 tahun | 2 sampai 7 tahun | 5 sampai 10 tahun |

Seperti telah disinggung di atas bahwa *tag* memiliki tipe memori yang bervariasi yang meliputi *read-only*, *read/write*, dan *write-once read-many*. *Tag read-only* memiliki kapasitas memori minimal (biasanya kurang dari 64 bit) dan mengandung data yang terprogram permanen sehingga tidak dapat diubah. Informasi yang terkandung di dalam *tag* seperti ini terutama adalah informasi identifikasi item. *Tag* dengan tipe memori seperti ini telah banyak digunakan di perpustakaan dan toko persewaan video. *Tag* pasif biasanya memiliki tipe memori seperti ini.^[2]

Pada *tag* dengan tipe memori *read/write*, data dapat dimutakhirkan jika diperlukan. Sebagai konsekuensinya kapasitas memorinya lebih besar dan harganya lebih mahal dibandingkan *tag read-only*. *Tag* seperti ini biasanya digunakan ketika data yang tersimpan didalamnya perlu pemutakhiran seiring dengan daur hidup produk, misalnya di pabrik.^[2]

Tag dengan tipe memori *write-once read-many* memungkinkan informasi disimpan sekali, tetapi tidak membolehkan perubahan berikutnya terhadap data. *Tag* tipe ini memiliki fitur keamanan *read-only* dengan menambahkan fungsionalitas tambahan dari *tag read/write*.^[2]

Untuk berfungsinya sistem RFID diperlukan sebuah *reader* atau alat *scanning device* yang dapat membaca *tag* dengan benar dan mengkomunikasikan hasilnya ke suatu basis data (Gambar 3).

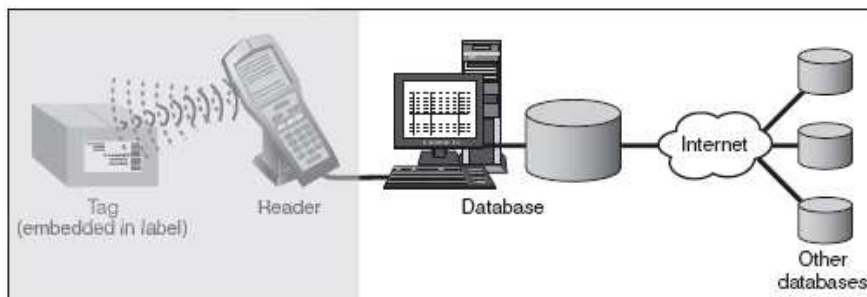


Gambar 3 *Reader* RFID^[2].

Sebuah *reader* menggunakan antenanya sendiri untuk berkomunikasi dengan *tag*. Ketika *reader* memancarkan gelombang radio, seluruh *tag* yang dirancang pada

frekuensi tersebut serta berada pada rentang bacanya akan memberikan respon. Sebuah *reader* juga dapat berkomunikasi dengan *tag* tanpa *line of sight* langsung, tergantung kepada frekuensi radio dan tipe *tag* (aktif, pasif atau semipasif) yang digunakan. *Reader* dapat memproses banyak item sekaligus. Menurut bentuknya, *reader* dapat berupa *reader* bergerak seperti peralatan genggam, atau stasioner seperti peralatan *point-of-sale* di supermarket. *Reader* dibedakan berdasarkan kapasitas penyimpanannya, kemampuan pemrosesannya, serta frekuensi yang dapat dibacanya.^[2]

Basis data merupakan sebuah sistem informasi logistik pada posisi back-end yang bekerja melacak dan menyimpan informasi tentang item bertag. (Gambar 4). Informasi yang tersimpan dalam basis data dapat terdiri dari *identifier* item, deskripsi, pembuat, pergerakan dan lokasinya. Tipe informasi yang disimpan dalam basis data dapat bervariasi tergantung kepada aplikasinya. Sebagai contoh, data yang disimpan pada sistem pembayaran tol akan berbeda dengan yang disimpan pada rantai *supply*. Basis data juga dapat dihubungkan dengan jaringan lainnya seperti *local area network* (LAN) yang dapat menghubungkan basis data ke Internet. Konektivitas seperti ini memungkinkan *sharing* data tidak hanya pada lingkup basis data lokal.^[2]



Gambar 4 Basis data pada sistem RFID^[2].

2.2 Frekuensi Radio sebagai Karakteristik Operasi Sistem RFID^[2]

Pemilihan frekuensi radio merupakan kunci karakteristik operasi sistem RFID. Frekuensi sebagian besar ditentukan oleh kecepatan komunikasi dan jarak baca terhadap *tag*. Secara umum tingginya frekuensi mengindikasikan jauhnya jarak baca. Frekuensi yang lebih tinggi mengindikasikan jarak baca yang lebih jauh. Pemilihan tipe frekuensi juga dapat ditentukan oleh tipe aplikasinya. Aplikasi tertentu lebih cocok untuk salah satu tipe frekuensi dibandingkan dengan tipe lainnya karena gelombang radio memiliki perilaku yang berbeda-beda menurut frekuensinya. Sebagai contoh, gelombang LF memiliki kemampuan penetrasi terhadap dinding tembok yang lebih baik dibandingkan dengan gelombang dengan frekuensi yang lebih tinggi, tetapi frekuensi yang lebih tinggi memiliki laju data (*data rate*) yang lebih cepat.

Di Amerika Serikat, *Federal Communications Commission* (FCC) mengatur alokasi band frekuensi untuk penggunaan komersial, sementara *National Telecommunications and Information Administration* (NTIA) mengatur spektrum

pada negara bagian. Sistem RFID menggunakan rentang frekuensi yang tak berlisensi dan diklasifikasikan sebagai peralatan *industrialscientific-medical* atau peralatan berjarak pendek (*short-range device*) yang diizinkan oleh FCC. Peralatan yang beroperasi pada bandwidth ini tidak menyebabkan interferensi yang membahayakan dan harus menerima interferensi yang diterima. FCC juga mengatur batas daya spesifik yang berasosiasi dengan masing-masing frekuensi. Kombinasi dari level-level frekuensi dan daya yang dibolehkan menentukan rentang fungsional dari suatu aplikasi tertentu seperti keluaran daya dari *reader*.

Berikut ini adalah empat frekuensi utama yang digunakan oleh sistem RFID : (1) LF, (2) HF, (3) UHF, dan (4) gelombang mikro.

- 1) Band LF berkisar dari 125 kilohertz (KHz) hingga 134 KHz. Band ini paling sesuai untuk penggunaan jarak pendek (*short-range*) seperti sistem antipencurian, identifikasi hewan dan sistem kunci mobil.
- 2) Band HF beroperasi pada 13.56 megahertz (MHz). Frekuensi ini memungkinkan akurasi yang lebih baik dalam jarak tiga kaki dan karena itu dapat mereduksi risiko kesalahan pembacaan *tag*. Sebagai konsekuensinya band ini lebih cocok untuk pembacaan pada tingkat item (*item-level reading*). *Tag* pasif dengan frekuensi 13.56 MHz dapat dibaca dengan laju 10 to 100 *tag* perdetik pada jarak tiga kaki atau kurang. *Tag* RFID HF digunakan untuk pelacakan barang-barang di perpustakaan, toko buku, kontrol akses gedung, pelacakan bagasi pesawat terbang, pelacakan item pakaian.
- 3) *Tag* dengan band UHF beroperasi di sekitar 900 MHz dan dapat dibaca dari jarak yang lebih jauh dari *tag* HF, berkisar dari 3 hingga 15 kaki. *Tag* ini lebih sensitif terhadap faktor-faktor lingkungan daripada *tag-tag* yang beroperasi pada frekuensi lainnya. Band 900 MHz muncul sebagai band yang lebih disukai untuk aplikasi rantai *supply* disebabkan laju dan rentang bacanya. *Tag* UHF pasif dapat dibaca dengan laju sekitar 100 hingga 1.000 *tag* perdetik. *Tag* ini umumnya digunakan pada pelacakan kontainer, truk, trailer, terminal peti kemas, serta telah diadopsi oleh peritel besar dan Departemen Pertahanan Amerika Serikat. Sebagai tambahan, di Amerika Serikat, band MHz digunakan untuk mengidentifikasi isi kontainer dalam area komersial dan industri untuk meningkatkan ketepatan waktu dan akurasi transmisi data. Menurut FCC penggunaan semacam itu menguntungkan perusahaan pengapalan komersial dan memberikan manfaat keamanan yang signifikan dengan dimungkinkannya seluruh isi kontainer teridentifikasi dengan mudah dan cepat serta dengan dapat diidentifikasinya kerusakan selama pengapalan.
- 4) *Tag* yang beroperasi pada frekuensi gelombang mikro, biasanya 2.45 dan 5.8 gigahertz (GHz), mengalami lebih banyak pantulan gelombang radio dari obyek-obyek di dekatnya yang dapat mengganggu kemampuan *reader* untuk berkomunikasi dengan *tag*. *Tag* RFID gelombang mikro biasanya digunakan untuk manajemen rantai *supply*.

Tabel 2 Frekuensi RFID yang umum beroperasi pada *tag* pasif^[2].

| Gelombang | Frekuensi | Rentang dan laju baca | Contoh penggunaan |
|-----------------|--------------|---|---|
| LF | 125 KHz | ~1.5 kaki; kecepatan baca rendah | Access control, animal tracking, point of sale applications |
| HF | 13.56 MHz | ~3 kaki; kecepatan baca sedang | Access control, smart cards, item-level tracking |
| UHF | 860-930 MHz | up to 15 kaki; kecepatan baca tinggi | Pallet tracking, supply chain management |
| Gelombang mikro | 2.45/5.8 GHz | ~3 kaki; kecepatan baca tinggi | Supply chain management |

2.3 Kategori Sistem RFID

Secara kasar sistem-sistem RFID dapat dikelompokkan menjadi empat kategori sebagai berikut^[1].

- 1) Sistem EAS (*Electronic Article Surveillance*) : Umumnya digunakan pada toko-toko untuk menyensor ada tidaknya suatu item. Produk-produk diberi *tag* dan *reader* berantena besar ditempatkan di masing-masing pintu keluar toko untuk mendeteksi pengambilan item secara tidak sah.
- 2) Sistem *Portable Data Capture* : dicirikan oleh penggunaan *reader* RFID yang portabel yang memungkinkan sistem ini digunakan dalam seting yang bervariasi.
- 3) Sistem *Networked* : dicirikan oleh posisi *reader* yang tetap yang terhubung secara langsung ke suatu sistem manajemen informasi terpusat, sementara transponder berada pada orang atau item-item yang dapat dipindahkan.
- 4) Sistem *Positioning* : Digunakan untuk identifikasi lokasi item-item atau kendaraan.

2.4 Pemanfaatan Teknologi RFID

Jika di masa lalu barcode telah menjadi cara utama untuk pelacakan produk, kini sistem RFID menjadi teknologi pilihan untuk tracking manusia, hewan peliharaan, produk, bahkan kendaraan. Salah satu alasannya adalah kemampuan baca tulis dari sistem RFID aktif memungkinkan penggunaan aplikasi interaktif. Selain itu, *tag* juga dapat dibaca dari jarak jauh dan melalui berbagai substansi seperti salju, asap, es, atau cat di mana barcode telah terbukti tidak dapat digunakan.^[1]

Gagasan untuk menggunakan teknologi RFID akhir-akhir ini merebak, baik di kalangan agen-agen pemerintah maupun perusahaan. Tabel 3 memperlihatkan penggunaan/rencana penggunaan RFID oleh agen-agen pemerintah Amerika Serikat. Berikut ini adalah beberapa contoh nyata agenda berbagai organisasi pemerintah maupun perusahaan dalam rencananya untuk mengimplementasikan teknologi RFID sebagaimana diuraikan oleh^[1].

- 1) Pelacakan pakaian : Produsen pakaian Benetton merencanakan untuk memasang *tag* RFID di dalam item-item ritel. Peralatan yang ditanam tersebut memungkinkan Benetton untuk melacak individu-individu dan barang inventaris yang mereka miliki dengan me-*link*-kan nama konsumen

dan informasi kartu kredit dengan nomor seri pada suatu item pakaian. Demikian juga Marks & Spencer, salah satu peritel terbesar di Inggris, mengumumkan untuk memulai memasang *tag* pada item-item pakaian dengan *tag* UHF mulai musim gugur 2003. *Tag* UHF adalah teknologi RFID generasi baru yang menyediakan kecepatan transfer data yang cepat dan rentang baca yang lebih jauh. Marks & Spencer telah secara ekstensif menggunakan peralatan tracking pada divisi penjualan makanannya.

- 2) Pelacakan barang dagangan dalam kemasan : Gillette, Wal-Mart, dan Tesco, rantai supermarket berbasis di Inggris, bergabung untuk menguji rak-rak yang dapat melacak secara real-time terhadap barang-barang dalam toko. “Rak-rak pintar” akan dapat membaca gelombang frekuensi radio yang diemisikan oleh *chip* mikro yang ditanam dalam jutaan silet dan produk-produk lainnya. Wal-Mart merencanakan untuk menguji rak Gillette diawali di toko yang berlokasi di Brockton. Jika sukses, Wal-Mart juga merencanakan untuk bergabung dengan Procter & Gamble untuk menguji hal serupa pada produk-produk kosmetik dan telah mendukung 100 *top suppliernya* untuk menggunakan pelacak barang nirkabel pada 2005. Para eksekutif Wal-Mart mengatakan bahwa perusahaan hanya akan menggunakan *chips* RFID untuk melacak barang dagangan dan akan melepasnya jika sudah dibeli.
- 3) Pelacakan ban : pembuat ban Michelin baru-baru ini memulai pengujian sistem identifikasi ban dengan frekuensi radio untuk ban mobil penumpang dan truk kecil. Transponder RFID dipasang di dalam ban dan menyimpan informasi identifikasi yang dapat diasosiasikan dengan nomor identifikasi kendaraan.
- 4) Pelacakan uang : Bank Sentral Eropa melaju dengan rencananya untuk menanamkan *tag* RFID setipis rambut manusia di dalam serat uang kertas Euro pada tahun 2005 meskipun menuai banyak protes. *Tag-tag* tersebut memungkinkan uang untuk mencatat informasi tentang setiap transaksi. Pemerintah dan agen-agen peradilan menyambut teknologi tersebut sebagai cara untuk mencegah pencucian uang, transaksi pasar gelap dan bahkan permintaan kuitansi kosong dari koruptor.
- 5) Pelacakan pasien dan orang : Rumah Sakit Alexandra di Singapura belum lama ini menerapkan sistem tracking di bagian gawat daruratnya karena sadar akan kekuatiran wabah Severe Acute Respiratory Syndrome (SARS). Dengan sistem ini seluruh pasien, pengunjung dan karyawan yang memasuki rumah sakit diberi sebuah kartu yang ditanami *chip* RFID. Kartu dibaca oleh sensor yang dipasang di langit-langit yang mencatat secara tepat waktu masuk dan keluarnya seseorang. Informasi ini tersimpan dalam komputer selama 21 hari. Teknologi ini juga memungkinkan untuk dengan segera melacak orang-orang yang pernah kontak dengan seorang penderita SARS.
- 6) Sistem pembayaran : Pada tahun 1997, ExxonMobil mengembangkan aplikasi pembayaran nirkabel yang diberi nama Speedpass. Sejak itu enam juta konsumen dapat melakukan pembayaran dengan cara ini pada 7.500 lokasi *Speedpass-enabled*. Sekarang, banyak merchant dan peritel mencari

cara untuk mengimplementasikan sistem pembayaran nirkabel RF. Sony dan Philips menjadi pendahulu. Kedua korporasi ini akan segera memulai melakukan uji lapangan terhadap sebuah sistem RFID yang disebut *Near Field Communication* (NFC), yang akan memungkinkan komunikasi RFID di antara PC, komputer genggam dan peralatan elektronik lainnya. Kedua perusahaan tersebut menggambarkan bahwa para konsumen akan masuk ke dalam portal mereka dengan melakukan swiping terhadap smart card mereka – yang ditaman dengan RFID Sony atau Philips – yang akan dibaca oleh *reader* RFID yang dipasang pada port USB di komputer. Di waktu selanjutnya, konsumen akan dapat belanja *online*, misalnya untuk tiket pertunjukan lokal. Mereka dapat melakukan pembayaran tiket *online*, mendownloadnya melalui PC dan kemudian mentransmisikannya melalui teknologi NFC ke *tag* RFID pada HP mereka. Selanjutnya pada saat pertunjukan, dengan mendekatkan HP mereka ke *reader* RFID di pintu masuk, mereka akan diperbolehkan masuk secara otomatis.

Saat ini *tag* RFID belum digunakan secara luas pada barang-barang konsumsi karena harga *tag* yang dianggap masih mahal. Namun, seiring usaha perusahaan-perusahaan untuk memperbaiki cara pelacakan produk dan melihat profil konsumen, peningkatan permintaan dan produksi teknologi RFID akan membawa pada penurunan harga. Pengembangan teknologi RFID yang ada telah menghasilkan sistem-sistem dengan kapasitas memori yang lebih besar, rentang pembacaan yang lebih lebar dan pemrosesan yang lebih cepat. Sebagai respon terhadap hal tersebut, pasar *tag* RFID mengalami ledakan, diproyeksikan mencapai \$10 miliar pertahun dalam dekade ini.^[1]

Para pakar industri memperkirakan bahwa beberapa tahun yang akan datang akan terdapat titik-titik RFID dalam rentang yang luas, bahkan beberapa sistem yang benar-benar terintegrasi pun diluncurkan. Beberapa korporasi telah terdaftar dan bergerak maju dengan rencana penanaman *tag* RFID dalam produk-produknya. Akhir-akhir ini, Microsoft Corporation mengumumkan rencana mengembangkan perangkat lunak yang memungkinkan retailer, pembuat, dan distributor untuk menggunakan *tag* RFID untuk melakukan tracking barang-barang di dalam toko dan pabrik sebagaimana program-program yang dirancang khusus untuk menggunakan teknologi *tagging* retail baru.^[1]

Berikut ini adalah contoh kemungkinan pemanfaatan RFID di masa yang akan datang^[3].

- 1) **Mesin cerdas:** *Tag-tag* RFID, misalnya pada garmen dan kemasan makanan, dapat dimanfaatkan untuk menjadikan peralatan rumah tangga bekerja lebih cerdas, misalnya mesin cuci dapat mengenali adanya kain-kain yang halus di dalamnya sehingga dapat memilih siklus pencucian secara otomatis untuk mencegah robek. Contoh lain, referigerator dapat memberikan peringatan ketika di dalamnya terdapat bahan makanan yang kadaluarsa atau ketika bahan makanan tertentu hampir habis, atau bahkan dapat mentransmisikan daftar pesanan ke layanan antaran.
- 2) **Belanja :** Pada toko ritel, pembeli dapat melakukan *check out* dengan mendorong kereta belanjanya melewati terminal *point-of-sale*. Terminal ini

secara otomatis akan menghitung item-itemnya, menghitung jumlah harga dan bahkan mungkin membebaskan *tagihan* pada peralatan pembayaran RFID-enabled milik pelanggan dan mengirimkan tanda terimanya lewat ponselnya. *Tag-tag* RFID dapat berlaku sebagai indeks pada *record* pembayaran di basis data dan membantu penjual untuk melacak asal-usul item-item yang rusak atau terkontaminasi.

- 3) **Obyek-obyek interaktif** : Pelanggan dapat berinteraksi dengan obyek-obyek bertag RFID melalui ponselnya (sebagian ponsel telah memiliki *reader* RFID). Seorang penggemar film bioskop dapat melakukan *scan* terhadap poster film untuk menampilkan jam tayang pada ponselnya. Dengan cara yang mirip, seorang calon pembeli furnitur dapat memperoleh informasi tentang pembuatnya melalui ponselnya yang dapat membaca *tag* RFID yang dipasang pada furnitur tersebut.
- 4) **Observasi medis** : Riset di Intel dan Universitas Washington meneliti RFID untuk memfasilitasi observasi medis dan petunjuk pulang bagi para manula. Salah satu hasil penelitian tersebut adalah lemari obat yang dipasang RFID dapat membantu memeriksa ketepatan waktu penggunaan obat. Lebih umum lagi, pemanfaatan RFID menjanjikan manfaat yang sangat besar bagi pihak rumah sakit.

Tabel 3 Penggunaan/rencana penggunaan RFID pada pemerintah Amerika Serikat^[2].

| Agen | Aplikasi |
|---|---|
| Department of Defense | Logistics support |
| | Tracking shipments |
| Department of Energy | Detection of prohibited articles |
| | Tracking the movement of materials |
| Department of Health and Human Services | Physical access control |
| Department of Homeland Security | Border control, immigration and customs (U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT)) |
| | Location system |
| | Smart containers |
| | Tracking and identification of assets |
| | Tracking and identification for use in monitoring weapons |
| | Tracking and identification of baggage on flights |
| Department of Labor | Tracking and locating case files |
| Department of State | Electronic passport |
| Department of Transportation | Electronic screening |
| Department of the Treasury | Physical and logical access control |
| | Records management (tracking documents) |
| Department of Veterans Affairs | Audible prescription reading |
| | Tracking and routing carriers along conveyor lines |
| Environmental Protection Agency | Tracking radioactive materials |
| General Services Administration | Distribution process |
| | Identification of contents of shipments |
| | Tracking assets |
| | Tracking of evidence and artifacts |
| National Aeronautics and Space Administration | Hazardous material management |
| Social Security Administration | Warehouse management |

III. Masalah Privasi pada Sistem RFID

RFID memunculkan dua kekhawatiran utama bagi para pengguna, yaitu pelacakan tersembunyi (*clandestine tracking*) dan pengumpulan data secara diam-diam (*clandestine inventorying*). *Tag* RFID merespon interogasi *reader* tanpa memberitahu pemilik atau pembawanya. Karena itu jika berada pada rentang pembacaan *reader*, *scanning* diam-diam (*clandestine scanning*) pun mengancam.^[3]

Ancaman terhadap privasi muncul ketika sebuah nomor seri *tag* dikombinasikan dengan informasi pribadi, sebagai contoh, ketika seorang konsumen membayar dengan kartu kredit, toko yang melayaninya dapat membuat *link* antara identitas konsumen tersebut dengan nomor seri *tag* yang ada padanya. Penjual kemudian dapat mengidentifikasi profil konsumen menggunakan jaringan *reader-reader* RFID, baik di dalam toko maupun di luar.^[3]

Tag-tag tertentu, khususnya *tag* EPC, selain menyimpan nomor seri juga menyimpan informasi tentang item-item yang dipasangnya, biasanya berupa informasi tentang pabrik pembuatnya, serta kode produk. Oleh karena itu orang yang membawa *tag* EPC dapat mengalami *clandestine inventorying*. Sebuah *reader* secara diam-diam dapat dapat menentukan obyek-obyek yang dibawa seseorang dan memanen informasi pribadi penting, misalnya jenis obat yang sedang dibawanya sehingga dapat diketahui penyakit yang dideritanya, *loyalty card* yang dibawanya sehingga dapat diketahui tempat langganan belanjanya, ukuran bajunya, kesukaan aksesorisnya, dan lain-lain. Gambar 5 mengilustrasikan potensi ancaman privasi yang mungkin mengancam seorang konsumen.^[3]



Gambar 5 Ilustrasi potensi ancaman privasi pada konsumen^[3].

Sekarang masalah *clandestine tracking* dan *clandestine inventorying* masih merupakan kekhawatiran yang terbatas karena infrastruktur RFID masih terbatas dan terpisah-pisah, namun begitu RFID merajalela hampir dapat dipastikan bahwa masalah privasi akan menjadi masalah yang lebih serius.^[3]

Sistem-sistem RFID ini memungkinkan pemilik bisnis untuk memiliki akses *real-time* terhadap informasi barang-barang inventarisnya. Teknologi RFID juga

memungkinkan para peritel dan korporasi untuk mengintip kehidupan para konsumen. Produk-produk yang ditanami *tag* RFID dapat terus-menerus mentransmisikan informasi yang memancar dari *identifier electronic product code* (EPC) untuk menginformasikan tentang item itu sendiri, seperti status konsumsi atau kesegaran produk, bahkan juga dapat melakukan *link* informasi produk dengan konsumen tertentu.^[2]

Informasi yang kompleks ini sangat bernilai – dan lebih mencakup – dibandingkan data apapun yang dapat diperoleh dari *scanning* pada barcode, atau bahkan *loyalty card*. Sering kali kartu pembeli melakukan *link* konsumen pada belanjanya, tetapi informasi yang terbatas ini hanya memberi peritel gambaran yang dangkal tentang kecenderungan belanja konsumen di toko tersebut. Sebaliknya, sistem RFID memungkinkan obyek-obyek bertag untuk berkomunikasi dengan *reader* elektronik selama masa hidup produk – sejak produksi hingga dibuang – memberi peritel gambaran yang jelas tentang cara dan perilaku belanja konsumen.^[2]

3.1 Isu Privasi yang Menyelimuti Penggunaan RFID

Sementara raksasa-raksasa korporat mengunggulkan kelebihan teknologi RFID, para pemerhati kebebasan sipil memperingatkan bahwa kemampuan melacak orang, produk, kendaraan dan bahkan uang akan menciptakan dunia Orweli di mana para penegak hukum dan peritel penasaran dapat dengan mudah membaca isi tas tangan seseorang (dengan memasang *reader* RFID di dekatnya) yang mungkin tidak disadari oleh yang bersangkutan. Kekhawatiran tersebut bukan tanpa alasan. Saat ini, sebagian *reader* RFID memiliki kapasitas untuk membaca dan ditransmisikan oleh berbagai macam *tag* RFID. Ini berarti bahwa jika seseorang memasuki toko dengan membawa beberapa *tag* RFID (misalnya yang ada pada baju atau kartu dalam dompet) salah satu *reader* RFID dapat membaca data yang diemisikan oleh seluruh *tag* dan sinyalnya direlay oleh produk-produk dalam toko. Kapasitas ini memungkinkan peritel yang menggunakan *reader* RFID untuk mengkompilasi profil yang lebih lengkap dari pembeli dibandingkan dengan yang mungkin diperoleh dari *scanning* terhadap *barcode* dari barang-barang belanjaan konsumen.^[1]

Menyadari akan hal-hal tersebut di atas, banyak pihak mengangkat isu kekhawatiran tersebut ke permukaan. Pengumuman rencana penggunaan teknologi RFID oleh berbagai perusahaan maupun agen pemerintah sering menuai kritik dari para pemerhati privasi. Ketika Benetton mengumumkan rencana untuk memasang *tag* RFID pada pakaian produksinya para pemerhati memperingatkan potensi penyalahgunaan dari sistem semacam itu dan Benetton pun setuju untuk menundanya. Keputusan Wal-Mart untuk mengimplementasikan teknologi RFID untuk pelacakan barang dagangan dalam kemasan menimbulkan kekhawatiran jika hal tersebut akan mendorong penyebaran *tag* dalam kemasan barang dagangan ke mana-mana, meskipun pihak eksekutif perusahaan menyatakan akan mencopot *tag* dari barang yang sudah dibeli. Pada rencana penanaman *tag* RFID pada ban oleh Michelin, para kritikus berargumen bahwa *tag-tag* tersebut akhirnya dapat memberitahukan ke mana dan kapan kendaraan suatu kendaraan pergi. Demikian juga dengan rencana penanaman *tag* RFID pada uang kertas Euro banyak pihak mengkhawatirkan jika teknologi tersebut dapat mengeliminir anonimitas perolehan uang.^[1]

Batasan dan sifat alamiah dari isu privasi terkait dengan penggunaan RFID di kalangan pemerintahan maupun komersial tergantung kepada maksud spesifik penggunaannya. Sebagai contoh, penggunaan teknologi ini untuk pengontrolan barang inventaris umum tidak akan menimbulkan banyak kekhawatiran privasi. Lain halnya dengan penggunaan RFID oleh pemerintah untuk melacak gerakan dari perjalanan orang-orang di wilayah suatu negara, hal ini akan membangkitkan kekhawatiran dari pihak-pihak yang terkena dampaknya. Isu privasi terkait dengan implementasi RFID meliputi pemberitahuan mengenai keberadaan atau penggunaan teknologi tersebut, pelacakan gerakan-gerakan individu, profiling kebiasaan, selera atau kesukaan individu, serta kemungkinan penggunaan sekunder dari informasi.^[2]

- 1) **Pemberitahuan.** Masyarakat mungkin tidak menyadari bahwa teknologi ini sedang digunakan jika mereka tidak diberitahu bahwa alat tersebut digunakan. Demikian juga para konsumen, mereka mungkin tidak menyadari bahwa *tag-tag* RFID dipasang pada item-item yang sedang mereka cari atau beli, atau barang-barang yang sudah dibelinya sedang *discan* jika tidak diberi tahu.^[2]
- 2) **Pelacakan.** Pelacakan adalah pencarian lokasi secara *real-time* atau mendekati *real-time*, di mana pergerakan seseorang diikuti oleh scanning RFID. Laporan-laporan media massa menguraikan kekhawatiran tentang cara-cara di mana anonimitas tampaknya terancam oleh pelacakan lokasi. Banyak kelompok kebebasan sipil menguatirkan aplikasi teknologi ini untuk pelacakan gerakan masyarakat, seperti di lokasi sekolah umum, dan menyebabkan kehilangan anonimitas di tempat-tempat umum. Sebagai tambahan, survey publik periodik telah menunjukkan ketidakpercayaan yang nyata akan kemampuan potensial dari pemerintah untuk memantau gerakan-gerakan maupun transaksi-transaksi masyarakat. Tiga agen di Amerika Serikat juga mengindikasikan bahwa penggunaan teknologi ini dapat memungkinkan pelacakan gerakan para buruh.^[2]
- 3) **Profiling.** *Profiling* adalah rekonstruksi dari pergerakan-pergerakan atau transaksi-transaksi seseorang dalam periode tertentu, biasanya digunakan untuk menggali sesuatu tentang kebiasaan, selera atau kesukaan seseorang. Oleh karena *tag* berisi *identifier* yang unik maka sekali suatu item bertag diasosiasikan dengan individu tertentu, informasi yang dapat mengidentifikasi secara pribadi pun dapat diperoleh dan kemudian dapat digabungkan untuk mengembangkan profil individu tersebut. Baik pelacakan maupun *profiling* tracking dapat mengganggu privasi dan anonimitas seseorang.^[2]
- 4) **Pemakaian sekunder.** Selain dari isu-isu tentang pemakaian terencana dari informasi yang didapat dari sistem RFID, terdapat juga kekhawatiran tentang kemungkinan organisasi-organisasi dapat mengembangkan penggunaan sekunder terhadap informasi tersebut, yaitu bahwa informasi sebenarnya dikumpulkan untuk suatu tujuan kemudian pada kesempatan tertentu juga dimanfaatkan untuk keperluan lainnya. Hal ini diistilahkan sebagai penyelewengan misi atau fungsi ("*mission-*" atau "*function-creep*"). Sebagai contoh histori *Social Security Number* (SSN) memberikan banyak bukti tentang bagaimana suatu *identifier* yang dikembangkan untuk tujuan khusus

telah menjadi basis dari banyak fungsi yang lain, baik oleh pemerintah maupun nonpemerintah. Pemakaian sekunder dari SSN telah menjadi masalah, bukan karena kontrol teknis, melainkan karena perubahan kebijakan dan prioritas-prioritas administratif.^[2]

Adopsi yang luas dari teknologi ini dapat memberikan andil peningkatan terjadinya isu-isu privasi tersebut. Seperti telah disebutkan bahwa *tag* dapat dibaca oleh sembarang *reader* kompatibel. Jika *reader* dan *tag* menyebar di mana-mana maka item-item bertag yang dibawa oleh seseorang dapat discan tanpa disadarinya. Selanjutnya, meningkatnya jumlah *reader* dapat membuka lebih banyak peluang bagi data untuk dikumpulkan dan digabungkan. Seiring pertumbuhan penggunaan teknologi, para konsumen pun mengangkat kekuatirannya tentang apakah data yang dikumpulkan dapat menunjukkan informasi pribadi semisal kecenderungan penyakit atau histori kesehatan pribadi serta apakah penggunaan informasi ini dapat menyebabkan penolakan jaminan asuransi atau penolakan lamaran kerja. Sebagai contoh, penggunaan teknologi RFID untuk melacak tindakan medis telah membangkitkan banyak kontroversi. Selain itu, tiga agen di Amerika Serikat mengangkat isu tentang perlindungan data pribadi seperti kelahiran dan biometrik yang tersimpan dalam *tag*.^[2]

3.2 Rentang Baca sebagai Celah Privasi

Menurut^[3], rentang baca *tag* merupakan suatu faktor penting dalam pembahasan mengenai privasi. Ada empat rentang yang perlu diperhatikan sebagai berikut.

- 1) **Rentang baca nominal** : standar-standar dan spesifikasi-spesifikasi produk RFID umumnya mengindikasikan rentang baca pada operasi *tag* yang diinginkan. Rentang ini merepresentasikan jarak maksimum di mana sebuah *reader* yang beroperasi dengan antena dan keluaran daya biasa dapat melakukan scan dengan benar terhadap *tag*. Sebagai contoh, ISO 14443 menspesifikasikan rentang baca nominal untuk *smartcard* yang *contactless*.
- 2) **Rentang scanning nakal** : Rentang scanning nakal adalah rentang maksimum di mana sebuah *reader* dapat mencatu dan membaca sebuah *tag*. Rentang *reader* sensitif yang dilengkapi dengan antena yang kuat atau *antenna array* dapat memperluas rentang baca nominal. Keluaran daya yang besar dapat mengamplifikasi rentang baca. *Reader* nakal dapat mengeluarkan daya melebihi batas legal. Sebagai contoh *reader* dengan catu daya baterai berpotensi melakukan *scan* terhadap *tag* ISO 14443 pada rentang 50 cm, yaitu sejauh lima kali rentang baca nominal.
- 3) **Rentang tag-to-reader eavesdropping** : Keterbatasan rentang baca untuk RFID pasif terutama dihasilkan dari kebutuhan *reader* untuk mencatu *tag*. Sekali *reader* mencatu *tag*, sebuah *reader* lain dapat memantau emisi *tag* yang dihasilkan tanpa memancarkan sinyal sendiri sehingga *reader* tersebut dapat menguping. Jarak maksimum dari *reader* lain tersebut dapat melebihi rentang *scanning* nakal.
- 4) **Rentang reader-to-tag eavesdropping** : Pada sebagian protokol RFID, sebuah *reader* mentransmisikan informasi *tag-specific* ke *tag*. Oleh karena *reader* mentransmisi dengan daya yang lebih besar daripada *tag*, maka

dimungkinkan untuk terjadinya pengupingan (*eavesdropping*) pada jarak yang jauh melebihi jarak komunikasi *tag-to-reader*.

IV. Solusi-solusi yang Ditawarkan

Babian ini akan membahas pendekatan-pendekatan perlindungan privasi pada *Tag* dasar, berdasarkan asumsi bahwa tag-tag yang paling banyak beredar, baik sekarang maupun di waktu yang akan datang adalah tag dasar.

Tag dasar adalah *tag* hanya mampu melakukan operasi-operasi dasar. Dilihat dari sisi keamanan, *tag* dasar berarti *tag* yang miskin dengan sumberdaya untuk melakukan operasi-operasi kriptografi. Menurut^[3], masalah harga menjadi pertimbangan utama pemilihan *tag* pada umumnya. Karena *tag* dasar harganya lebih murah dibandingkan *tag* yang dapat melakukan kriptografi, maka *tag* jenis inilah yang banyak digunakan. Ada beberapa pendekatan yang diusulkan untuk mengatasi masalah privasi konsumen berkaitan dengan penggunaan *tag* dasar sebagai berikut.

4.1 “Killing” and “Sleeping”

Tag EPC menggunakan cara sederhana untuk melindungi privasi konsumen, yaitu mematikan *tag*. Ketika sebuah *tag* EPC menerima perintah “*kill*” dari *reader*, ia merender dirinya sendiri untuk tidak beroperasi secara permanen. Untuk mencegah deaktivasi sembarangan terhadap *tag*, perintah *kill* dilindungi dengan PIN. Untuk mematikan *tag*, *reader* juga harus mentransmisikan PIN *tag*-specific (panjangnya 32 bit untuk standar EPC kelas 1 generasi 2). Karena *tag* yang sudah mati tidak dapat “bercerita” apapun, mematikan *tag* merupakan cara yang sangat efektif untuk ukuran privasi.^[3]

Meskipun mematikan *tag* dapat melindungi privasi secara efektif, tetapi di sisi lain cara ini mengeliminasi seluruh manfaat RFID pascabayar bagi konsumen. Pengembalian barang rusak, mesin cerdas, bantuan bagi manula serta sistem-sistem bermanfaat lainnya sebagaimana telah diuraikan sebelumnya tidak dapat bekerja dengan *tag* yang sudah dimatikan. Karena alasan ini kiranya penting untuk mencari pendekatan lain yang lebih seimbang daripada mematikan *tag*.^[3]

Pendekatan “*sleep*” dapat menjadi cara yang lebih seimbang dibandingkan dengan pendekatan “*kill*”. Pada pendekatan ini *tag* diinaktifkan untuk sementara waktu. Konsep pendekatan ini sederhana, namun akan sulit dalam praktiknya. Jelasnya, *tag* tidur tidak dapat memberikan perlindungan privasi jika sembarang *reader* dapat membangunkannya. Oleh karena itu, sebagian dari kontrol akses diperlukan untuk membangunkan *tag*. Kontrol akses ini dapat diambil dari PIN *tag*. Untuk membangunkan dan menidurkan *tag*, *reader* harus mentransmisikan PIN ini. Inti dari sistem semacam adalah bahwa konsumen harus mengelola PIN untuk *tag*nya.^[3]

4.2 Pendekatan renaming

Meskipun *identifier* yang diemisikan oleh *tag* RFID tidak memiliki arti intrinsik tetapi masih memungkinkan pelacakan. Untuk alasan ini, sekedar mengenkripsi *identifier tag* saja tidak menyelesaikan masalah privasi. *Identifier* terenkripsi itu sendiri hanyalah sebuah *meta-identifier* yang bersifat statis dan karenanya mungkin untuk pelacakan seperti nomor seri lainnya. Untuk mencegah pelacakan *tag* RFID *identifier tag* perlu disembunyikan atau diganti antar waktu.^[3]

4.2.1 Relabeling

Beberapa gagasan mengenai mekanisme *relabeling* telah usulan. Sarma, Weis, dan Engels (SWE) mengusulkan gagasan penghapusan *identifier* unik dalam *tag* di *point-of-sale* untuk mengatasi persoalan pelacakan dengan menyisakan *identifier* tipe produk (data *barcode* tradisional) untuk penggunaan di kemudian waktu. Inoue dan Yasuura (IY) mengusulkan agar konsumen diberi alat untuk melabel ulang *tag* dengan *identifier* baru tetapi *identifier tag* lama masih memungkinkan untuk diaktifkan kembali untuk penggunaan umum di kemudian waktu, semacam daur ulang. Sebagai sebuah mekanisme fisik untuk mengadopsi ide SWE, IY juga menggali ide pemisahan *identifier* tipe produk dan *identifier* unik melalui dua *tag* RFID. Dengan mengelupas salah satu dari kedua *tag* tersebut konsumen dapat mereduksi granularitas data *tag*. Karjoth dan Moskowitz memperluas gagasan ini dengan mengusulkan cara agar pengguna dapat mengganti *tag* secara fisik untuk membatasi emisi datanya dan memperoleh konformasi fisik dari pergantian tersebut. Untuk mengatasi *clandestine scanning* terhadap buku perpustakaan, Good et al. mengusulkan gagasan pelabelan ulang *tag* dengan *identifier* acak pada *checkout*.^[3]

Kekurangan pendekatan-pendekatan di atas ini adalah jelas. Penghapusan *identifier* unik tidak mengeliminasi ancaman *clandestine inventorying*, juga tidak cukup mengeliminasi ancaman pelacakan. Meskipun *tag* hanya mengemisikan informasi tipe produk tetapi *tag* tersebut masih dapat diidentifikasi secara unik dalam konstelasi. Penggunaan *identifier* acak pada kode produk menyelesaikan persoalan *inventorying*, tetapi tidak menyelesaikan persoalan pelacakan. Untuk mencegah pelacakan *identifier* harus sesering diperbarui.^[3]

4.2.2 Kriptografi minimalis

Juels mengusulkan sistem minimalis di mana setiap *tag* menyimpan sedikit koleksi *pseudonym*. *Tag* merotasi *pseudonym-pseudonym* tersebut kemudian merilis *pseudonym* yang berbeda untuk masing-masing *query reader*. *Reader* yang diberi kewenangan dapat menyimpan seluruh *pseudonym* dan karenanya dapat mengidentifikasi *tag* secara konsisten, tetapi *reader* yang tidak diberi kewenangan karena tidak memiliki pengetahuan tentang seluruh *pseudonym*, tidak dapat melakukan korelasi terhadap kenampakan yang berbeda dari sebuah *tag* yang sama. Untuk mencegah pencurian seluruh *pseudonym* oleh pihak musuh melalui interogasi *rapid-fire*, Juels mengusulkan agar *tag* menyumbat emisi datanya, misalnya dengan memperlambat responnya ketika terjadi *query* yang terlalu cepat. Sebagai pengembangan dari sistem dasar, pembaca-pembaca valid dapat merefresh *pseudonym tag*. Skema minimalis menawarkan resistansi terhadap spionase korporat seperti *clandestine scanning* terhadap stok produk pada lingkungan ritel.^[3]

4.2.3 Enkripsi ulang

Juels dan Pappu (JP) memperhatikan persoalan khusus dari perlindungan privasi konsumen untuk uang kertas dengan RFID. Skema yang diusulkan melibatkan sistem kriptografi kunci publik dengan satu pasangan kunci, yaitu kunci publik PK dan kunci privat SK yang ditangani oleh agen penegak hukum yang tepat. Sebuah *tag* RFID dalam sistem JP menyimpan satu *identifier* unik S, yaitu nomor seri uang. S dienkripsi dengan PK menghasilkan *ciphertext* C, kemudian *tag* RFID mengemisikan

C. Hanya agen penegak hukum sebagai pemroses kunci privat SK yang dapat mendekripsi C dan mendapatkan nomor seri S. ^[3]

Untuk menangani ancaman pelacakan, JP mengusulkan agar ciphertext C dienkripsi ulang secara periodik. JP menggambarkan sebuah sistem di mana toko-toko dan bank-bank memagari reader-reader yang mengenkripsi ulang dengan PK. Properti-properti aljabar dari kriptosistem El Gamal kriptosistem memungkinkan *ciphertext* C ditransformasikan menjadi sesuatu yang baru. Untuk mencegah enkripsi ulang secara sembarangan oleh pihak-pihak yang jahat, JP mengusulkan agar uang kertas dilengkapi dengan kunci akses tulis optik karena untuk mengenkripsi ulang suatu ciphertext, suatu *reader* harus melakukan *scan* terhadap kunci ini. ^[3]

Untuk beberapa persektif, seperti kebutuhan akan *reader* pengenkripsi ulang, sistem JP tampaknya sangat merepotkan, tetapi sistem ini membantu memperkenalkan prinsip bahwa kriptografi dapat meningkatkan privasi *tag* RFID, bahkan ketika *tag*. Model JP memiliki keterbatasan, di antaranya bahwa pengupingan *reader* pengenkripsi ulang pada sistem JP dapat menurunkan privasi. ^[3]

4.2.4 Enkripsi ulang universal

Sistem JP bergantung pada pasangan kunci tunggal dan universal (SK,PK). Jika untuk suatu sistem moneter yang menyatu sepasang kunci mungkin sudah mencukupi, maka untuk sebuah sistem RFID umum tentu saja diperlukan banyak pasangan kunci. Akan tetapi ekstensi JP yang sederhana untuk melipatgandakan pasangan kunci (SK1, PK1), (SK2, PK2), . . . (SKn, PKn) dapat mengurangi privasi sistem. Untuk mengenkripsi ulang sebuah *ciphertext* C, perlu diketahui dengan kunci publik PK_i yang mana C dienkripsi. Informasi tersebut berpotensi sensitif terhadap privasi. Golle et al. mengatasi kelemahan JP dengan mengusulkan suatu kriptosistem sederhana yang memungkinkan kriptosistem yang memungkinkan enkripsi ulang terhadap *ciphertext* tanpa mengetahui kunci publik sebelumnya. *without knowledge of the corresponding public key*. Sistem tersebut disebut *enkripsi ulang universal*, melibatkan sebuah ekstensi terhadap kriptosistem El Gamal yang menggandakan ukuran ciphertext. ^[3]

Sistem Golle et al. memiliki kelemahan keamanan yang serious, yaitu tidak dapat mempertahankan integritas. Sebagai perlawanan terhadap enkripsi ulang *ciphertext*, pihak musuh dapat mengganti keseluruhan *chipertext* yang baru dengan cara mengubah *plaintext* asalnya. Ateniese, Camenisch, dan de Medeiros melengkapi solusi terhadap masalah ini dengan mendasarkan pada pasangan-pasangan bilinear alam kriptosistem kurva eliptik. Mereka mengusulkan suatu skema enkripsi ulang universal di mana sebuah ciphertext dapat ditandatangani secara digital oleh penguasa pusat sehingga memungkinkan siapapun untuk memverifikasi keaslian plaintext yang berasosiasi dengannya, yaitu *tag identifier*. Skema Ateniese et al. menjaga fitur-fitur enkripsi ulang universal biasa dalam perlindungan privasi. Akan tetapi skema ini tidak memiliki ketahanan terhadap *swapping*, yaitu sebuah serangan di mana musuh mempertukarkan dua ciphertexts yang valid melalui *tag -tag* RFID. Pertahanan yang efektif terhadap serangan *swapping* masih menjadi permasalahan riset. ^[3]

4.3 Pendekatan *proxy*

Para konsumen mungkin lebih suka membawa peralatan pelindung privasi sendiri daripada menggantungkan diri pada *reader* RFID publik untuk memperkuat perlindungan privasinya. Seperti telah disebutkan, sebagian ponsel telah memiliki fungsionalitas RFID serta dimungkinkan bahwa ponsel mendukung perlindungan privasi yang canggih. Para peneliti telah mengusulkan beberapa sistem di jalur ini.^[3]

- 1) Floerkemeier, Schneider dan Langheinrich mengusulkan dan menguraikan secara sebuah prototipe “*Tag Watchdog*,” yang pada dasarnya adalah suatu sistem audit untuk privasi RFID. *Tag Watchdog* memantau *scanning* terhadap *tag-tag* RFID dan mengumpulkan informasi dari *reader*.^[3]
- 2) Rieback, Crispo dan Tanenbaum, serta Juels, Syverson dan Bailey^[4] mengusulkan peralatan yang sangat mirip yang disebut berturut-turut “RFID Guardian” (disingkat Guardian) dan “RFID Enhancer Proxy” (REP). Suatu Guardian bertindak sebagai petunjuk *firewall* RFID pribadi. Guardian memperantarai permintaan *reader* terhadap *tag*; dipandang dengan cara lain, Guardian secara selektif mensimulasikan *tag-tag* di bawah kontrolnya. Sebagai suatu alat dengan catu daya yang tinggi, sebuah Guardian dapat mengimplementasikan kebijakan-kebijakan privasi yang lebih baik serta dapat menggunakan kanal lain selain RFID (misalnya GPS atau koneksi Internet) untuk memberikan suplemen data. Sebagai contoh, sebuah Guardian dapat mengimplementasikan kebijakan seperti ini :

“*Tag* saya hanya dapat *discan* dalam jarak 30m dari rumah saya (sebagaimana ditentukan oleh GPS), atau di toko yang mengkompensasi *scanning tag* dengan kupon diskon 10%.”^[3]

4.4 Pengukuran jarak

Sumberdaya dasar dari *tag* dasar RFID memerlukan penggalian skema privasi yang murah, protokol tingkat tinggi atau mengembangkan protokol-protokol pada tingkat yang lebih rendah. Fishkin, Roy dan Jiang (FRJ) mendemonstrasikan bahwa rasio *signal-to-noise* dari sinyal *reader* pada suatu sistem RFID menghasilkan ukuran kasar tentang jarak antara sebuah *reader* dengan sebuah *tag*. Mereka mengasumsikan bahwa dengan tambahan sirkuit yang murah sebuah *tag* dapat mencapai ukuran kasar jarak *reader* penginterogasi. FRJ mengusulkan agar jarak ini berfungsi sebagai ukuran kepercayaan. Sebagai contoh, ketika *discan* dari jarak jauh sebuah *tag* mungkin merilis informasi umum (“Aku dipasang pada sebuah botol air mineral”), tetapi pada jarak dekat ia merilis informasi yang lebih spesifik, seperti *identifier* yang unik.^[3]

4.5 *Blocking*

Juels, Rivest dan Szydlo (JRS) mengusulkan skema perlindungan privasi yang mereka sebut *blocking*. Skema tersebut didasarkan pada penggabungan ke dalam *tag-tag* dari bit yang dapat dimodifikasi yang disebut bit privasi. Bit privasi ‘0’ menandakan *tag* dapat *discan* dengan *scanning* publik, sedangkan bit ‘1’ menandakan *tag* sebagai privat. JRS memperkenalkan ruang *identifier* dengan bit ‘1’ di awal sebagai zona *privasi*. Suatu *tag blocker* adalah sebuah *tag* RFID khusus yang mencegah *scanning* yang tidak dikehendaki pada *tag-tag* yang memasuki zona privasi.^[3]

Konsep *blocking* memiliki kekurangan. Pada transmisi yang tidak reliabel, *tag* pemblok yang posisinya sudah benar pun dapat gagal.^[3]

4.5.1 *Soft blocking*

Juels dan Brainard (JB) mengusulkan varian dari *blocking* yang disebut *soft blocking*. Sebuah *tag soft blocker* hanya mengemisikan sebuah pernyataan yang padat, misalnya “Jangan *scan tag* yang bit privasinya hidup”. JB mengusulkan *readers* menginterpretasikan kebijakan seperti itu dalam perangkat lunak *Soft blocking* tergantung kepada *auditing* dari konfigurasi *reader* untuk mendukung mesin. Oleh karena emisi *reader* dapat mengalami pemantauan maka dimungkinkan untuk membangun suatu alat audit yang mendeteksi *readers* yang melanggar kebijakan *tag*. Dibandingkan dengan skema *blocking* JRS yang kurang memiliki jaminan teknis, *soft blocking* memiliki keunggulan tertentu, misalnya jika pada *blocking* JRS “opt-out,”, *soft blocking* mendukung kebijakan “opt-in”. Salah satu skema yang diusulkan JB sama sekali tidak melibatkan *tag* pemblok eksplisit melainkan tergantung pada audit itu sendiri. Pendekatan yang sangat sederhana ini memiliki defisiensi teknis yang jelas, tetapi ini mungkin merupakan bentuk paling praktis untuk *blocking*.^[3]

4.5.2 *Trusted computing*

Molnar, Soppera, and Wagner (MSW) secara ringkas menguraikan pendekatan alternatif untuk mendukung kebijakan privasi seperti yang bergantung pada bit-bit privasi. Mereka menjelaskan bagaimana *readers* yang dilengkapi dengan modul-modul platform terpercaya (*Trusted Platform Module*, TPM) dapat mendukung *tag* kebijakan privasi secara internal. *Reader* seperti ini dapat membangkitkan konfirmasi yang dapat diverifikasi dari luar.^[3]

MSW mencatat bahwa *reader* ThingMagic Mercury 4 yang telah tersedia secara komersial menyertakan prosesor XScale 2 dengan sebuah TPM. Meskipun pendekatan MSW tidak diarahkan untuk permasalahan *readers* nakal, tetapi pendekatan ini dapat memfasilitasi atau komplemen terhadap bentuk-bentuk perlindungan privasi.^[3]

4.6 Legislasi

Sejak awal, privasi RFID telah menarik perhatian intensif dari para pembuat keputusan dan para legislator. Komisi Perdagangan Federal Amerika Serikat (*Federal Trade Commission*, FTC) telah mengeluarkan sebuah laporan yang mengungkapkan pengaruh RFID pada konsumen yang menekankan pada privasi tetapi belum menyatakan maksud untuk mengeluarkan regulasi. EPCglobal Inc. telah menerbitkan petunjuk bagi para anggotanya tentang privasi EPC untuk produk-produk konsumsi. Petunjuk ini menggarisbawahi pendidikan konsumen tentang kehadiran dan fungsi *tag* EPC dan petunjuk cara pencopotan atau mematakannya. Kebijakan publik tentang RFID tampaknya sulit untuk dibuat karena *tag-tag* RFID pada dasarnya tidak memiliki kontrol akses. Kerjasama teknolog dengan legislator adalah penting untuk memperkuat pencapaian privasi RFID yang baik.^[3]

V. Kesimpulan

Kepentingan organisasi-organisasi, baik perusahaan maupun agen pemerintah untuk melakukan pemantauan yang cepat dan tepat dengan memanfaatkan teknologi RFID melahirkan benturan kepentingan dengan masyarakat atau konsumen. Kemudahan yang diperoleh oleh perusahaan maupun agen pemerintah tersebut tidak jarang menjadi ancaman terhadap privasi bagi berbagai pihak.

Masalah privasi yang diangkat sebagai isu pada pemanfaatan sistem RFID secara garis besar meliputi pentingnya pemberian informasi tentang pemakaian teknologi RFID, pelacakan (*tracking*), pengembangan profil (*profilng*), dan pemakaian sekunder terhadap informasi hasil *scanning* dengan RFID. Dua hal yang menjadi kekhawatiran utama bagi konsumen dan masyarakat adalah pelacakan tersembunyi (*clandestine tracking*) dan pengumpulan data secara diam-diam (*clandestine inventorying*). Kedua hal tersebut sangat dimungkinkan karena *tag* RFID tidak pernah memberitahu pemilik atau pembawanya dalam responnya terhadap interogasi dari *reader*. Bentuk ancaman yang diakibatkan oleh hal-hal tersebut antara lain kehilangan anonimitas dan tersebarnya data pribadi yang seharusnya dijaga kerahasiaannya yang tidak jarang dapat mengakibatkan berkurang atau bahkan hilangnya daya terima pihak lain terhadap yang bersangkutan.

Hal yang khas pada sistem RFID adalah bahwa pada dasarnya *tag* RFID tidak memiliki kontrol akses sehingga sembarang *reader* dapat menginterogasinya. Kenyataan ini menyulitkan untuk mencari pendekatan yang paling tepat dalam rangka melindungi privasi. Beberapa pendekatan telah diusulkan oleh para peneliti, baik melalui pendekatan perangkat keras, perangkat lunak, maupun pendekatan regulasi. Bentuk-bentuk pendekatan tersebut yaitu mematikan atau menonaktifkan sementara; *renaming* dengan beberapa skemanya yaitu *relabeling*, kriptografi minimalis, enkripsi ulang, dan enkripsi ulang universal; pendekatan proxy; pengukuran jarak; *blocking* yang terdiri dari *soft blocking* dan *trusted computing*; serta pendekatan legislasi. Masing-masing pendekatan perangkat keras maupun perangkat lunak masih memiliki sisi-sisi kelemahan, atau dengan kata lain belum ada satu pendekatan pun yang dapat memenuhi semua kepentingan, sementara pada pendekatan legislasi, kebijakan publik tentang RFID juga sulit untuk dibuat.

DAFTAR PUSTAKA

- [1] _____ (), Radio Frequency Identification (RFID) Systems, <http://www.epic.org/privacy/rfid/>, 1 Oktober 2006, 09.00 WIB
- [2] United States Government Accountability Office (2005), *Information Security : Radio Frequency Identification Technology in the Federal Government*, <http://www.gao.gov/new.items/d05551.pdf>, 1 Oktober 2006, 09.00 WIB
- [3] Ari Juels (2005), *RFID Security and Privacy: A Research Survey*, http://www.rsasecurity.com/rsalabs/staff/bios/ajuels/publications/pdfs/rfid_survey_28_09_05.pdf, 2 Oktober 2006, 15.23 WIB

- [4] Ari Juels and Paul Syverson and Dan Bailey, *High-Power Proxies for Enhancing RFID Privacy and Utility*,
<http://www.rsasecurity.com/rsalabs/staff/bios/ajuels/publications/pdfs/RFIDREP2.pdf>, 2 Oktober 2006, 15.23 WIB
- [5] Ari Juels and Stephen A. Weis (2006), *Defining Strong Privacy for RFID*,
http://www.rsasecurity.com/rsalabs/staff/bios/ajuels/publications/rfid_privacy/rfidprivacy.pdf, 2 Oktober 2006, 15.23 WIB