SNATI
Seminar Nasional
Aplikasi Teknologi Informasi 2004
Yogyakarta, 19 Juni 2004

Aplikasi Pembayaran Jalan Tol dengan Smart Card Menggunakan Algoritma Enkripsi Idea dan 3DES: Studi Kasus pada PT. Citra Marga Nusaphala Persada

Elidjen, Hendy Budianto, Lilyawati Yohanes, Novianto Wibowo Nugroho
Universitas Bina Nusantara
Jl. K.H. Syahdan No.9 Kemanggisan Palmerah Jakarta Barat 11480
Telp. 021-5345830 Fax. 021-5300244
e-mail: elidjen@binus.ac.id, sphinxo@plasa.com, hendy@cbn.net.id, unythalia2@yahoo.com

Abstrak

Salah satu usaha pemerintah untuk mengatasi kemacetan adalah dengan membuat jalan tol, namun cara ini kurang efektif karena kemacetan masih terjadi akibat antrian yang panjang pada gerbang tol. Oleh sebab itu, penulis berusaha mencari solusi untuk membuat sistem baru yaitu dengan penggunaan smart card. Penggunaan smart card yang memiliki tingkat integritas, reliabilitas, dan keamanan yang tinggi diharapkan dapat dijadikan solusi untuk memecahkan semua masalah tersebut. Dalam penggunaan smart card ini, juga diperhatikan proses enkripsi pada penyimpanan data tersebut. Proses enkripsi ini bertujuan agar data yang tersimpan dalam smart card tersebut tidak dapat dimanipulasi oleh orang yang tidak bertanggung jawab. Sehingga dengan digunakannya sistem ini, selain dapat meminimalkan antrian dalam pembayaran tol, juga dapat menjaga data yang tersimpan dalam smartcard tersebut. Penulis membatasi ruang lingkupnya, yaitu data yang akan disimpan dalam smart card adalah nilai saldo, tanggal isi ulang, dan lokasi gerbang masuk tol untuk sistem tertutup. Semua data yang tersimpan dalam smart card tersebut akan dienkripsi. Aplikasi ini hanya digunakan untuk kartu pembayaran tol. Penulis tidak membahas masalah pengenalan golongan kendaraan. Sedangkan metodologi penelitian yang digunakan adalah dengan menganalisis sistem yang sudah ada, menyebarkan kuesionare, dan merancang sistem yang baru.

Kata kunci: enkripsi, IDEA, DES, smart card, jalan tol.

1. Pendahuluan

Transaksi yang terjadi dijalan tol sekarang ini berlangsung relatif agak lama karena petugas tol harus mengecek jenis kendaraan, asal kendaraan, menentukan tarifnya, dan menghitung uang kembaliannya dan juga bertambahnya jumlah kendaraan. Pengelola jalan tol sudah melakukan beberapa upaya untuk meningkatkan kecepatan transaksi pembayaran jalan tol dengan harapan panjangnya antrian dapat dikurangi dengan cara menyediakan jalur khusus uang pas (tanpa kembalian) dan menerbitkan karcis langanan. Hasil pembayaran pengguna jalan tol yang dikumpulkan oleh toll collector yang disetor ke kantor pusat harus dihitung terlebih dahulu oleh bagian keuangan. Hal ini tentu saja kurang praktis dan tidak efisien dari segi waktu. Demikian juga dengan karcis langganan, seorang pengemudi yang sering melewati jalan tol yang berbeda-beda harus membeli lebih dari satu jenis karcis langganan karena tarif tol di Jabotabek sangat beragam, tergantung dari ruas jalan yang dilewati dan golongan kendaraannya. Karcis langganan hanya dapat dibeli di beberapa kantor pengelola jalan tol.

Salah satu alternatif untuk memecahkan masalah-masalah dan keterbatasan tersebut, maka dapat digunakan smart card sebagai media pembayaran tol sehingga transaksi pembayaran di gerbang tol lebih cepat dan dapat mengurangi panjang antrian di gardu, kesalahan manusia dapat dikurangi, mengurangi waktu yang dibutuhkan untuk menyediakan dan menghitung uang kembalian, mengurangi waktu yang dibutuhkan untuk menghitung uang yang harus disetor ke kantor pusat, memudahkan pendataan pendapatan yang diperoleh, dan meningkatkan perolehan dana dari pengguna jalan tol lebih awal.

Tujuan penelitian merancang dan mengimplementasikan sistem informasi pembayaran jalan tol dengan smart card menggunakan algoritma IDEA dan 3DES yang dapat digunakan sebagai alternatif untuk mempercepat proses transaksi pembayaran jasa pemakaian jalan tol pada PT. Citra Marga Nusaphala Persada.

Penelitian ini dititikberatkan pada smart card dan enkripsi dengan algoritma IDEA dan 3DES yang dapat digunakan sebagai aplikasi pembayaran jalan tol dengan batasan: data yang akan disimpan dalam smart card adalah nilai saldo, tanggal isi ulang, dan lokasi gerbang masuk tol untuk sistem tertutup, data yang tersimpan dalam smart card akan dienkripsi, aplikasi hanya digunakan untuk kartu pembayaran tol yang ditujukan untuk kendaraan golongan 1 karena untuk pengenalan golongan dibutuhkan pembahasan tersendiri, dan aplikasi hanya dibuat untuk ruas jalan tol dalam kota dan ruas jalan tol T.B. Simatupang dan tidak membahas lebih lanjut mengenai cara penanganan uang dari setiap transaksi.

2. Smart Card

2.1 Pengertian Smart Card

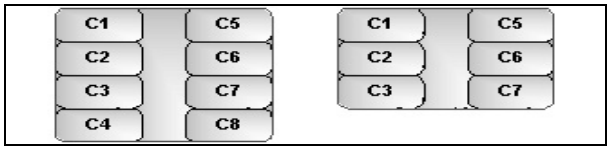
Pengertian smart card secara sederhana adalah sebuah kartu plastik yang pada umumnya seukuran kartu kredit dan mempunyai microchip di dalamnya, serta memenuhi standar ISO 7816. Microchip tersebut bisa berupa microprocessor yang dilengkapi dengan memori internal atau hanya berupa microchip memori saja. Smart card yang memiliki microprocessor dengan memori internal dapat diprogram untuk menjalankan suatu program dan menyimpan informasi. Tetapi harus diingat, bahwa brainnya berukuran sangat kecil sehingga kemampuan dari smart card jauh di bawah kemampuan komputer desktop.

2.2 Jenis Smart Card

Berdasarkan teknologinya, smart card dapat dibedakan menjadi 3 jenis, yaitu contact smart card, contactless smart card, dan hybrid smart card. Contact smart card memerlukan kontak fisik antara reader dengan kartu dimana kontak dilakukan dengan memasukan kartu ke dalam reader. Contactless smart cards tidak memerlukan kontak fisik dan komunikasi dilakukan via antenna dengan jangkauan yang bervariasi tergantung jenis kartu, ada yang mencapai jarak hingga 1 meter. Hybrid smart card adalah gabungan dari contact dan contactless smart card dalam satu kartu.

2.3 Komunikasi pada Smart Card

Semua komunikasi dari smart card menggunakan C7 contact, seperti kita lihat pada gambar 1. Dalam melakukan komunikasi, baik pihak kartu atau terminal (*card reader*) hanya satu pihak yang dapat berkomunikasi dalam satu waktu. Komunikasi ini biasa disebut dengan komunikasi half duplex. Komunikasi selalu diinisialisasi atau dimulai oleh terminal dimana hubungan relasi antara kartu dengan terminal hampir sama dengan client-server.



Gambar 1. Kontak elektrik smart card

Setelah kartu dimasukan ke dalam terminal, maka terminal akan mengaktifkannya dan melakukan power-on-reset. Kemudian kartu akan mengirimkan answer to reset (ATR) kepada terminal. ATR akan diterjemahkan, berbagai macam parameter akan diextract kemudian terminal akan mengsubmit initial instruction ke kartu. Kartu akan menggenerate reply dan mengirim balik ke terminal. Relasi client/server terus dilakukan sampai prosesnya selesai dan kartu dikeluarkan dari terminal.

2.3.1 *Smart Card Reader/Writer*

Smart card reader/writer adalah suatu antar muka untuk komunikasi antara kartu dengan komputer. Setiap tipe dari smart card mempunyai perintah dan protokol komunikasi yang berbeda. Antar muka antara smart card dan smart card reader mengikuti spesifikasi dari ISO 7816-3 dengan beberapa batasan atau penyempurnaan untuk meningkatkan fungsionalitas dari smart card reader/writer. Antar muka dari suatu smart card terdiri dari smart card power supply, pemilihan kartu, dan antar muka microcontroller.

2.3.2 Standar ISO 7816

Smart card telah distandarisasi baik kapabilitas fisiknya maupun command interface-nya. Standar dari command interface telah ditetapkan sedemikian rupa. Penamaan perintah-perintah dari suatu command sudah ditetapkan, sehingga para pengembang dapat dengan mudah membuatan aplikasinya. Begitu juga dengan interoperabilitas antara sistem yang berbeda. Standarisasi ini membuat perbedaan di antara produk-produk smart card yang ada, bukanlah penghalang dalam mengembangkan suatu aplikasi.

- ISO 7816-1: Atribut fisik

Memberikan standarisasi tentang karakteristik fisik dari Integrated Circuit Card (IC Card).

- ISO 7816-2: Menyatakan dimensi dan lokasi dari contacts.

Tabel 1. Fungsi kontak pada *smart card*

Contact	*Designation*	Kegunaan
C1	**Vcc**	Tempat penerimaan aliran listrik yang diberikan oleh *reader*
C2	**RST**	*Reset line*. Melalui jalur ini, IFD bisa memberi signal kepada *chip microprocessor smart card* untuk melakukan *reset sequence of instructions*
C3	**CLK**	*Clock signal line*, merupakan jalur untuk memasukan *clock signal* ke dalam *microprocessor chip*.
C4	**RFU**	Digunakan untuk beberapa tahun ke depan
C5	**GND**	*Ground line*, menyediakan *electrical ground* antara IFD dan ICC
C6	**Vpp**	Pemrograman koneksi listrik digunakan untuk memprogram EEPROM dari generasi pertama ICCs
C7	**I/O**	Masukan/keluaran yang menghasilkan komunikasi *half-duplex channel* antara *reader* dan *smart card*
C8	**RFU**	Digunakan untuk beberapa tahun ke depan.

- ISO 7816-3: Sinyal dan protokol
  Bagian ini menjelaskan tentang sinyal elektronik dan protokol transmisi dari Integrated Circuit Card.
- ISO 7816-4: Inter-industry commands for interchange
  - ✓ Isi dari suatu pesan, perintah dan respon, dikirimkan melalui suatu antar muka menuju kartu begitu pun sebaliknya.
  - ✓ Struktur dan isi dari byte yang telah dikirim kartu selama answer to reset.
  - ✓ Struktur dan metode akses file
  - ✓ Metode akses untuk algoritma yang digunakan oleh kartu.
- ISO 7816-5: Numbering system and registration procedure for application identifiers
  Menetapkan standarisasi untuk Application Identifiers (AIDs). AIDs mempunyai dua bagian. Yang pertama adalah Registered Application Provider Identifiers (RIDs) yang terdiri dari 5 byte, masing-masing vendor memiliki RID yang unik. Bagian kedua adalah panjang variabel yang terdiri dari 11 byte yang digunakan RIDs untuk identifikasi aplikasi yang spesifik.
- ISO 7816-6: Inter-industry data elements
  Menggambarkan aturan data yang dibutuhkan dalam beberapa aplikasi.
- ISO 7816-7: Inter-industry commands for Structured Card Query Language (SCQL)
  Menetapkan beberapa perintah untuk mengakses isi dari smart card dan struktur relasi database.

3. Kriptografi

3.1 Pengertian Kriptografi

Kriptografi adalah suatu ilmu ataupun seni mengamankan pesan dan dilakukan oleh cryptographer. Sedang cryptanalysis adalah suatu ilmu dan seni membuka (*breaking*). Kriptografi menghasilkan proteksi yang terintegrasi dan proteksi kerahasiaan. Selain itu juga menghasilkan teknologi key yang digunakan oleh komponen service keamanan yang lain seperti enkripsi, dekripsi, authentifikasi, digital signatures, dan signature verification. Suatu pesan yang telah dienkrip biasa disebut ciphers sedangkan pesan yang telah didekrip atau tidak dienkrip disebut plaintext.

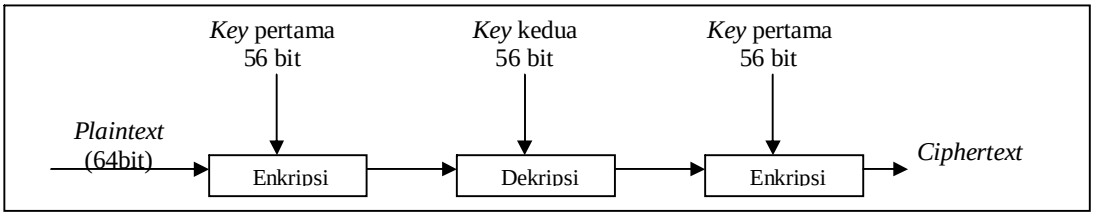
3.2 Kriptografi Secret - Key

Dalam beberapa algoritma enkripsi, encryption key dan decryption key yang digunakan adalah sama. Decryption key dapat dikalkulasikan dari encryption key dalam suatu useful time frame. Algoritma inilah yang disebut sebagai secret-key algorithms, private-key algorithms, atau symmetric algorithms. Dalam algoritma ini encryption key harus dirahasiakan. Selain itu juga diperlukan koordinasi antara sender dan receiver untuk mendistribusikan secret-key mereka. Ada tiga buah symmetric encryption algorithm yang akan dibahas yaitu DES, 3DES, dan IDEA.

3.3 Triple DES (3DES)

Dalam perkembangannya DES dianggap cukup rawan terhadap brute force attack, oleh karena itu dikembangkan alternative lain yang lebih aman. Triple DES dikembangkan oleh Tuchman untuk menggantikan DES. Sebenarnya dalam triple DES tidak ada perubahan algoritma yang signifikan. Melainkan hanya melakukan proses enkripsi, dekripsi, dan enkripsi lagi. Namun menggunakan dua buah key yang berbeda. Proses enkripsi dan dekripsi dalam triple DES sama dengan proses dalam DES. Detil dari triple DES dapat dilihat pada gambar

2.6. Pertama-tama plaintext dienkripsi dengan key yang pertama, lalu hasilnya didekripsi dengan key kedua. Hasil dari dekripsi ini selanjutnya dienkripsi kembali dengan key yang pertama, menghasilkan ciphertext.



Gambar 2. Proses Triple DES

Hingga saat ini, triple DES masih dianggap aman dan masih banyak digunakan dalam berbagai aplikasi.

3.4 IDEA (International Data Encryption Algorithm)

Algoritma IDEA berorientasi pada blok. Panjang blok data pada IDEA adalah 64 bit, dan mengunakan key sepanjang 128 bit. Artinya jika panjang data lebih dari 64 bit, maka data tersebut akan dibagi menjadi beberapa blok. Masing-masing sepanjang 64 bit dan selanjutnya masing-masing blok akan diproses sendiri-sendiri. Untuk proses dekripsi algoritma ini pada dasarnya adalah sama dengan proses enkripsi. Namun yang digunakan sebagai masukan adalah cihpertext. Selain itu ke 52 subkey yang digunakan juga berbeda. 52 subkey untuk proses dekripsi sebenarnya berasal dari penurunan 52 subkey enkripsi. Proses penurunannya adalah sebagai berikut.

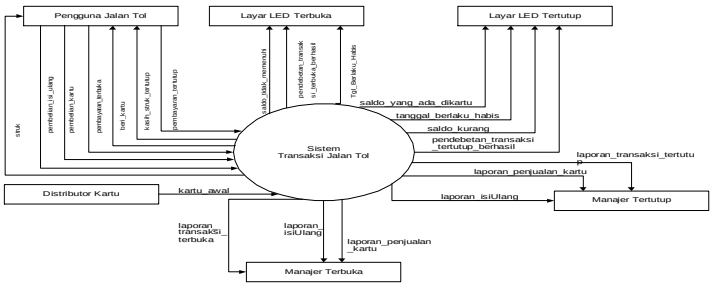
3.5 Fungsi Hash

Fungsi hash secara umum bisa digambarkan sebagai suatu fungsi yang menghasilkan sidik jari atau autentifikasi bagi suatu file, pesan, atau blok data lainnya. Nilai dari hash ini dihasilkan dari h = H(M). Dengan M sebagai pesan dengan panjang bebas, dan H(M) sebagai nilai hash yang memiliki panjang tetap.

4. Perancangan

Pihak pengelola jalan tol akan memperoleh dana dari pengguna jalan tol lebih awal. Sistem yang baru ini juga tetap mengakomodasi pembayaran dengan cara tunai.

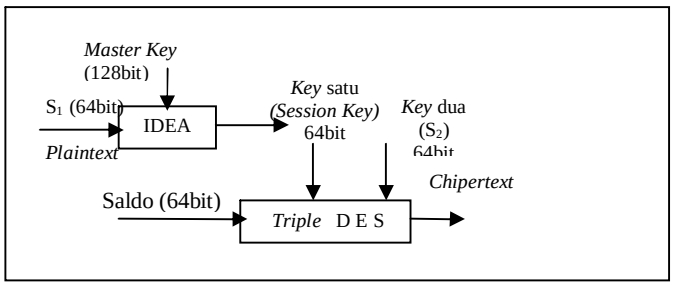
4.1 Diagram Aliran Data Sistem



Gambar 3. Diagram konteks (level 0) sistem yang diusulkan

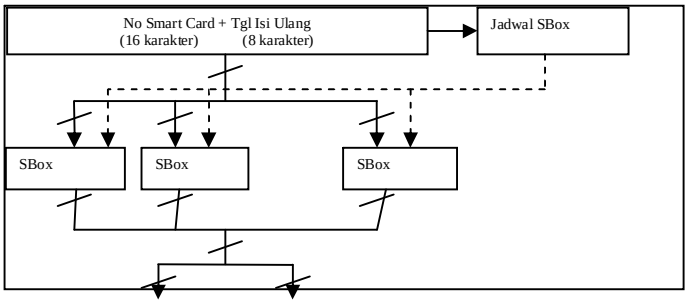
4.2 Algoritma Enkripsi yang Digunakan

Untuk mengurangi resiko serangan, maka digunakan *session key*. Sistem yang diusulkan, dirancang menggunakan kombinasi dari dua buah algoritma enkripsi yaitu Triple DES dan IDEA.



Gambar 4. Kombinasi algortima enkripsi IDEA dan DES

Seperti diilustrasikan pada gambar 4, nominal saldo akan dienkrip dengan algoritma Triple DES dengan menggunakan dua buah key. Key yang pertama merupakan session key yang didapat dari hasil enkripsi IDEA, sedang key yang kedua (S2) merupakan hasil dari Uniqe id generator. S1 yang merupakan masukan plaintext bagi IDEA, dan S2 yang merupakan key kedua bagi Triple DES, adalah hasil keluaran dari Uniqe id generator.



Gambar 5. Unique Id Generator

Uniqe id generator merupakan implementasi dari algoritma S-Box. Secara garis besar proses ini digambarkan pada gambar 5. Uniqe id generator memiliki masukan berupa 24 karakter dan keluaran 16 karakter. 24 Karakter ini diperoleh dari kombinasi identitas kartu (16 karakter) yang unik dan tanggal isi ulang kartu (6karakter). Dalam prosesnya, ke-24 karakter (192 bit) ini dibagi menjadi 32 segmen, masing-masing sepanjang 6 bit. Lalu masing-masing segmen di konversi menjadi 4 bit dengan mengunakan tabel S-Box.0 Sedangkan penjadwalan yang menentukan tabel S-Box mana yang akan dipakai, dirancang sedemikian rupa sehingga peluang terpilihnya masing-masing tabel adalah sama.

5. Implementasi dan Evaluasi

5.1 Cara Memperoleh Kartu

Kartu dapat dibeli di banyak tempat sesuai dengan tempat yang ditunjuk oleh pihak jalan tol. Pelanggan dapat langsung membeli tanpa harus memberikan informasi identitasnya kepada si penjual, dan dapat memilih jumlah saldo sebesar Rp. 100.000,00 atau Rp. 200.000,00. Setiap kartu yang dijual sudah terisi jumlah saldo dan mempunyai tanggal kadarluasa selama tiga bulan, dimana tanggal kadarluarsa terhitung sejak pertama kali kartu digunakan untuk pembayaran jalan tol.

5.2 Cara Transaksi dengan Sistem Baru

Di setiap gardu terdapat seorang petugas (toll collector), dimana harus melakukan login terlebih dahulu agar dapat memasuki sistem operasi. Kemudian petugas akan menjalankan sebuah program yang berfungsi melakukan proses transaksi di gerbang tol. Yang berhak untuk mengakses file tersebut hanya kepala shift. Apabila shift petugas sudah berakhir, maka petugas harus melakukan log out.

- Untuk sistem terbuka:
  - ✓ Bagi pengguna jalan tol yang memiliki kartu langganan.
    Setibanya di gardu masuk, pengguna harus memasukkan kartunya ke dalam reader. Kartu dapat dicabut dari reader apabila telah muncul informasi pada layar monitor. Informasi transaksi yang akan muncul di layar yaitu tarif yang didebet, dan sisa saldo. Jika saat pendebetan saldo yang ada di dalam kartu tidak mencukupi, maka akan tampil pesan di layar dan pengguna dapat melakukan pembayaran secara tunai.
  - ✓ Bagi pengguna jalan tol yang tidak memiliki kartu langganan.
    Setibanya di gardu masuk, maka pengguna bisa langsung membayar secara tunai, sesuai dengan tarif yang muncul di layar.
- Pencatatan Kejadian Penting:
  Pada sistem yang baru jika terjadi kejadian yang diluar dugaan, maka petugas gardu tol dapat memasukkanya kedalam sistem yang baru dengan mengetikkannya pada kolom kejadian.

5.3 Proses Isi Ulang Jumlah Saldo yang Ada di Kartu

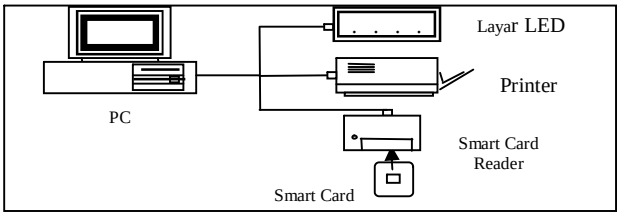
Untuk melakukan pengisian ulang jumlah saldo yang ada didalam kartu, dapat dilakukan di counter-counter yang telah ditentukan oleh pihak jalan tol. Yang berwenang untuk melayani pelanggan dalam melakukan proses ini hanya petugas tertentu saja, yang berasal dari pihak jalan tol. Petugas pertama kali harus melakukan log in terlebih dahulu untuk masuk ke dalam sistem operasi.

Jumlah saldo yang dapat dipilih oleh pelanggan tol antara lain: seratus ribu dan dua ratus ribu. Kartu akan dimasukkan ke dalam reader oleh petugas. Saldo yang tersisa di dalam kartu akan muncul di layar dan petugas akan menambah saldonya sesuai dengan permintaan pelanggan. Tanggal kadarluasa akan di update menjadi tiga bulan, terhitung dari tanggal saat pengisian. Kemudian jumlah saldo yang sudah terisi akan tampil di layar dan kartu dapat di cabut dari reader.

5.4 Proses Pemindahan Data Transaksi dan Pembuatan Laporan

Setelah selesai masa shiftnya, toll collector akan melakukan log out. Kepala shift akan masuk ke setiap gardu yang ada di gerbang tersebut dan melakukan log in, kemudian menjalankan modul pemindahan data transaksi. File transaksi dari setiap gardu akan digabung sesampainya di kantor pusat dan kemudian akan di simpan ke dalam database master.

Setelah semua data transaksi disimpan dalam database, maka dapat dilakukan pembuatan laporan. Laporan yang dihasilkan dapat berupa laporan transaksi harian, bulanan, atau tahunan. Juga bisa ditampilkan jumlah transaksi dari lokasi gardu tertentu, atau golongan kendaraan tertentu. Untuk laporan isi ulang, juga bisa ditampilkan berdasarkan lokasi isi ulang, dan jumlah nominal isi ulang. Untuk laporan penerbitan kartu, bisa ditampilkan data kartu yang pernah diterbitkan.



Gambar 6. Skema perangkat keras terminal tol sistem terbuka

5.5 Evaluasi Waktu Transaksi

Dalam melakukan evaluasi sistem yang diusulkan, kami melakukan pengujian terhadap waktu yang dibutuhkan dalam setiap transaksi sebanyak 30 kali untuk masing-masing aplikasi. Dalam pengujian tersebut, kami juga menyertakan smart card yang baru diterbitkan sebanyak 2 kali. Dan didapatkan hasil bahwa pada sistem yang diusulkan waktu rata-rata yang dibutuhkan pada transaksi gerbang tol sistem terbuka adalah 1,89 detik dan untuk kartu smart card baru membutuhkan waktu rata-rata 2,13 detik. Tingkat keberhasilan transaksi sebesar 100 %.

Sistem yang baru ini lebih cepat dibandingkan dengan transaksi dengan uang kembalian. Pada sistem yang lama waktu untuk transaksi dengan uang pas, adalah kurang lebih 1 detik. Sedangkan untuk transaksi dengan uang kembalian, membutuhkan waktu 3 sampai 6 detik.

5.6 Evaluasi Keamanan Data dalam Smart Card

Data nominal yang kami simpan di smart card diletakkan pada dua lokasi yang berbeda. Lokasi pertama yaitu account area dan lokasi kedua yaitu user file area. Data yang berada pada user file area akan dienkrip oleh sistem kami. Sedang data nominal yang ada di account area akan dienkripsi mengunakan fasilitas enkripsi dari smart card. Pada saat dilakukan transaksi, kedua data nominal tersebut akan dibandingkan sehingga diketahui apabila ada yang memanipulasi data dalam smart card tersebut.

Untuk meningkatkan keamanan data dalam smart card, kami menggunakan kombinasi dari dua buah algoritma enkripsi, yaitu IDEA dan 3DES. Selain itu juga digunakan session key yang berbeda untuk setiap kartu dan akan berubah-ubah setiap kali kartu diisi ulang. Sehingga dapat mengurangi kemungkinan manipulasi data oleh pihak-pihak yang tidak bertanggung jawab.

6. Kesimpulan dan Saran

Dari sistem yang dirancang, dapat disimpulkan bahwa:

a. Smart card dapat digunakan sebgai media kartu langganan jalan tol yang memiliki nilai lebih dibandingkan dengan sistem yang sedang berjalan.
b. Waktu transaksi dengan sistem yang baru lebih cepat dibandingkan dengan waktu transaksi pada sistem yang sedang berjalan pada keadaan tertentu.
c. Pengamanan yang dilakukan terhadap data nominal dalam smart card, mengakibatkan bertambahnya waktu transaksi yang dibutuhkan.
d. Kombinasi dua algoritma enkripsi dan penerapan session key, akan meningkatkan keamanan data dalam smart card.

Dari hasil evaluasi, ternyata smart card yang digunakan membutuhkan waktu rata-rata 1,33 detik sampai dengan 2,49 detik. Salah satu penyebab lamanya waktu transaksi dalam smart card adalah waktu untuk pemasukan kartu ke dalam smart card reader, maka untuk pengembangan lebih lanjut disarankan untuk:

a. Menggunakan smart card yang berjenis contactless
b. Menggunakan smart card yang ditujukan khusus untuk proses transaksi cepat.
c. Menggunakan teknologi pengenalan pola dalam pengenalan golongan kendaraan secara otomatis.
d. Menggunakan jaringan yang menghubungkan seluruh lokasi gerbang

Daftar Pustaka

Connolly, Thomas M. et al (2001). Database Systems: A Practical Approach to Design, Implementation, and Management. Third edition. Pearson Addison Wesley.

Doffell, Bonett. Contactless Technology for Secure Physical Access: Technology and Standards Choices (2002)
http://www.smartcardalliance.org/alliance_activities/Contactless_Technology_whitepaper.cfm.

Katz, Jeff. et al. A Smart Cards and Biometrics in Privacy-Sensitive Secure Personal Identification Systems. Smart Card Alliance (2002).

Petri, Steve, An Introduction to Smart Cards (2003)
http://www.sspsolutions.com/solutions/whitepapers/introduction_to_smartcards.htm

Pressman, Roger S. (2001). Software Engineering :A Practitioner Approach. Fifth Edition. McGraw Hill, Singapore.

Stalling, William. (1999). Cryptography and Network Security : Principles and Practice. Prentice Hall International, Inc. New Jersey, USA.