DESAIN DAN IMPLEMENTASI MOBILE PAYMENT SYSTEM DENGAN TEKNIK SET DAN SOCKET J2ME

Desrienaldo[1], Agus Virgono[2], Gunawan Adi[3]

[1]Teknik Telekomunikasi, Fakultas Teknik Elektro, Universitas Telkom

Abstrak

Tugas akhir ini mengimplementasikan sistem Mobile Payment pada Mobile device menggunakan J2ME. Sistem ini merupakan solusi bagi mobilitas user yang menjadi masalah dalam transaksi jual-beli. Sistem ini dibuat dengan tidak mengabaikan faktor keamanan transaksi, biaya transaksi, dan performansinya. Teknik SET, yang sudah terbukti handal dalam mengamankan transaksi elektronik pada aplikasi fix internet digunakan untuk menjamin keamanan dalam sistem ini. Namun teknik ini mengalami modifikasi Karena keterbatasan Mobile device yang belum bisa menyamai perangkat fix. Pengiriman data menggunakan teknologi GPRS, pertukaran data menggunakan teknik socket TCP.

Aplikasi Mobile Payment ini akan diimplementasikan pada emulator dan Mobile device. Pengimplementasian pada Mobile device digunakan untuk mengukur parameter expected behaviour dan keamanan dari segi keaslian server. Pengimplementasian pada Mobile device digunakan untuk mengukur performansi dari segi end-to-end delay nya.

Dari hasil pengujian yang dilakukan, teryata system dapat membedakan server palsu dan asli menggunakan SET. Dari segi performansi end-to-end delay/RTT masih berada dalam range yang ditolerir dari GPRS Indosat M3 untuk pengujian sebanyak 5 kali. RTT yang di butuhkan sebelum sesi terbentuk berkisar 10 kali lebih lama dibandingkan setela sesi terbantuk.

Kata Kunci : Kata kunci : Mobile Payment, J2ME, SET, Teknik socket

Abstract

This final project Implement a Mobile Payment system into Mobile device that is developed with J2ME. This system is solution for mobility that become problem in trading transaction. This system focuses for how secure, price, and performance is it. The famous SET technic securing internet electronic transaction had part in building this system. But the complex SET unable to build this system because of limited function of Mobile device, so SET is modificated. Data communication in this system is managed by socket programming technic and use GPRS.

Mobile payment system has been implementing on wireless emulator and Mobile device. Mobile payment system wich planted in mobile Device suppose to know the expected behaviour and system security that knowing the coect server.

System testing shows the system could idrrentify both the fake server and the right server. Five sample of testing shows that the performance of Mobile Payment system stay in the right range of end-to-end delay from indosat M3. It also show the different between the delayed of starting session is ten times than running session.

Keywords :

BAB I
PENDAHULUAN

1.1 Latar belakang

Manusia menginginkan kemudahan karena mobilitas mereka yang meningkat. Seandainya bisa mereka ingin melakukan apa saja menggunakan perangkat *payment*, termasuk pembayaran atas pembelian mereka. *Mobile Payment System* merupakan salah satu pilihan dalam kemdahan bertransaksi.

Untuk menjamin keamanan banyak metode yang digunakan untuk *electronic transaction* (transaksi elektronik), diantaranya HTTPS, SSH, STUNEL, dan SET. SET merupakan metode yang masih baru dan memiliki kamanan yang kuat. SET menggunakan kriptografi kunci *hybrid* yaitu menggunakan enkripsi asimetrik sebagai sarana pertukaran kunci dan enkripsi simetrik untuk sesi transaksi.

Di dalam SET terdapat beberapa algoritma kriptografi yang digunakan diantaranya RSA, fungsi hash (MD5 atau SHA1), RC4. dalam penelitian ini fungsi hash yang di gunakan adalah MD5. Pemilihan MD5 sebagai fungsi hash yang digunakan dan tidak memilih SHA1 karena outputan dari MD5 dua kali lebih kecil dari SHA1. hal ini berhubungan dengan keterbatasan memori mobile device.

Untuk itu penulis berusaha membuat aplikasi *Mobile Payment* menggunakan teknik SET yang sebenarnya sudah berkembang di luar negeri, akan tetapi belum dimanfaatkan sepenuhnya di Indonesia.

1.2 Tujuan Penelitian

Tujuan yang ingin dicapai dari Tugas Akhir ini adalah :

1. Mengimplementasikan beberapa algoritma kriptografi, yaitu fungsi hash satu arah MD5, enkripsi asimetrik RSA, dan enkripsi simetrik RC4 dalam teknik SET menjadi sistem *Mobile Payment* kedalam program aplikasi berbasis J2ME.
2. Menganalisa aplikasi *Mobile Payment* ini dari segi keamanan dari segi keaslian *server* yang dihubungi dengan parameter valid atau tidak valid, pengujian terhadap *expected behaviour* dari sistem dan *end to end* delaynya (dengan environment yang ditentukan sebelumnya) dengan parameter waktu milidetik.

1.3 Rumusan Masalah

Tugas akhir ini membahas perihal *Desain dan Implementasi Mobile Payment Sistem dengan Socket J2ME*. Hal ini penulis kembangkan didasari pada beberapa hal, diantaranya :

1. Bagaimana *Mobile Payment* memberikan solusi transaksi jual-beli yang aman, cepat, mudah, murah, dimana saja dan kapan saja.
2. Bagaimana mengimplementasikan teknologi SET dalam aplikasi MIDlet, karena telah di *support* pada MIDP 2.0.

1.4 Batasan Masalah

Agar pembahasan masalah yang dilakukan pada penerapan Desain dan Implementasi *Mobile Payment* dengan *Socket* J2ME tidak menyimpang dari tujuan yang telah ditetapkan, maka batasan yang dipakai dalam penulisan dari tugas akhir ini adalah :

1. Algoritma enkripsi yang digunakan adalah Rivest-Shamir-Adleman (RSA) dan RC4.
2. Algoritma Digital Fingerprint atau Message Digest atau Hash Function yang digunakan adalah MD5.
3. Teknologi pengiriman paket yang digunakan adalah teknologi GPRS.
4. Pembangunan aplikasi *client* pada *Mobile Payment system* ini difokuskan pada *payment phone* dan PDA yang sudah Java embeded.
5. Pembangunan aplikasi *server* yang melayani permintaan dari *client* (*payment phone*) dibangun berbasiskan Java (J2SE) dan database MySql.

1.5 Metodologi Penelitian

Langkah-langkah yang akan ditempuh dalam menyelesaikan Tugas Akhir ini adalah :

1. **Studi literature**; dilakukan dengan mengkaji teori–teori dasar dan teori pendukung yang tersedia dalam buku dan sumber-sumber referensi yang sesuai dengan penulisan tugas akhir. Hal ini bertujuan untuk mempelajari dasar–dasar teknologi J2ME, algoritma-algoritma yang dipakai, cara melakukan koneksi dengan *socket* dari *client* ke *server*. Selain itu

dilakukan dengan melakukan kajian ke laboratorium yang bersangkutan untuk bertanya dan memahami tentang konsep *socket programming* pada J2ME dan J2SE sebagai dasar pembangunan teknologi *Mobile Payment*. Menanyakan kepada Pembimbing Tugas Akhir dalam menyelesaikan Tugas Akhir ini.

2. **Desain sistem**; Sistem *Mobile Payment* didesain menggunakan protocol centric baik pada *client* maupun *prototype server*nya. Desain sistem digunakan sebagai pedoman pembuatan aplikasi *Mobile Payment*. Sehingga data yang diperoleh dapat dipertanggung-jawabkan berdasarkan desain sistemnya.
3. **Implementasi**; *Client* dari aplikasi *Mobile Payment* ini diimplementasikan menggunakan J2ME, sedangkan *server*nya menggunakan J2SE. Aplikasi didesain sebagai tool untuk dianalisa dan diuji dari end to end delay, keamanan dan *expected behaviour* sistem.

1.6 Sistematika Penulisan

Dalam pembuatan tugas akhir ini, penulis menggunakan sistematika penulisan sebagai berikut :

BAB I Pendahuluan

Dalam bagian ini diuraikan tentang latar belakang tujuan penulisan, ruang lingkup masalah, tujuan penelitian, pembatasan masalah, metode penyelesaian masalah, serta teori penunjang.

BAB II Teori Penunjang

Berisi mengenai overview J2ME, konsep dasar dari SET pada J2ME dan J2SE. serta teknologi GPRS.

BAB III Desain dan Perancangan Sistem

Berisi tentang perancangan terhadap proses aplikasi *Mobile Payment* dengan *socket* pada J2ME dalam perangkat *payment phone* yang Java embeded. Terdapat dua garis besar rancangan, yaitu perancangan pemodelan aplikasi dan perancangan modul komunikasi.

BAB IV Implementasi dan Analisa

Pengujian dilakukan terhadap *expected behaviour* dari *system* (respon yang diinginkan oleh sistem). Setelah dilakukan pengujian maka akan dianalisa dari aspek end to end delaynya (*client – server – client*) dan keamanannya. Pengujian dianalisa pada *client* (*payment phone*) dan *prototype server*.

BAB V Penutup

Berisi tentang kesimpulan dan saran tentang *Mobile Payment* yang telah diiimplementasikan.

BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

- Dari segi *expected behaviour* respon sistem telah berjalan dengan benar kecuali pada proses ganti *password*
- Dari segi keamanan sistem menjamin user dapat mengetahui *server* yang benar
- Dari segi performansi untuk *environment* yang telah ditentukan sebelumnya, RTT sistem masih tergolong baik karena masih dalam range yang ditolerir dari GPRS Indosat M3. Range RTT terdapat pada referensi [12]
- Saat peak time waktu yang dibutuhkan sedikit lebih lama dibanding saat off peak, walau selisihnya tidak besar
- *RTT* yang dibutuhkan sebelum sesi SET terbentuk kurang lebih sepuluh kali lebih lama dibanding dengan setelah sesi terbentuk

5.2 Saran

- Satu *user* hanya bisa login pada satu *mobile device* dalam satu waktu. Hal ini dapat direalisasikan dengan membuat satu tabel pada *database* Edopayment yang dapat menunjukkan status *user*. Dengan demikian user yang *online* dapat diketahui dan tidak diperkenalkan *login* pada *device* lain.
- Menu dibuat dinamis sehingga jika ada perubahan layanan *client* dapat secara otomatis bersinkronisasi dengan *server*.
- Untuk pengembangan selanjutnya dapat diarahkan kepada security *server*.

DAFTAR PUSTAKA

[1] [MIDP 2.0] *Payment Information Device Profile 2.0*, Java Community, JSR 118, 2002, Internet: http://www.jcp.org

[2] Sankar, Ravi Chilamkurti. *Internet*

[3] Handout by Forum Nokia. Version 1.0; Maret 8, 2004. *MIDP 2.0 : "Introduction to Using Sockets and Datagrams".*

[4] Irvan, Dedy 2002. "*Teknologi dan Cara Kerja GPRS"*. Dalam Chip (Computer and Communication) Oktober 2002. Jakarta.

[5] Knudsen. Jonathan, "*Wireless Java : Developing with J2ME second edition",* Appress, 2003.

[6] *Kuliah Berseri J2ME*, 2003, Internet : http://www.ilmukomputer.com

[7] Mahmud .H, Qusay. April 2003, "*J2ME Low-Level Network Programming with MIDP 2.0*." Artikel. Internet : http://developers.sun.com

[8] *"The Java™ Tutorial"*. Internet: http://java.sun.com/docs/books/tutorial.

[9] Team, GSM. 2003. "*Modul Open Mind Wireless Technology and Applications"*. Bandung: *Payment* Communication Laboratory, STT Telkom.

[10] Wicaksono. Ady, "Pemrograman aplikasi *Wireless* dengan Java", Elexmedia Computindo, Jakarta, 2002.

[11] *JSSE Reference Guide for the JDK 5_0*, 2004, Internet: http://java.sun.com/j2se/1.5.0/docs/guide/security/jsse/JSSERefGuide.html

[12] Haryadi, Sigit. Rodiati, Yati. Suryana, Joko." *Analisis Perbandingan Kinerja Teoritis dan Praktek GPRS"*, 2005, Internet: http://telecom.ee.itb.ac.id/~sigit/FullPaperSNI2004_Sigit%20H%20Analisis%20kinerja%20GPRS_.pdf