# KEAMANAN TRANSAKSI E-COMMERCE DENGAN MENGGUNAKAN SMS

**Hidayatulah Himawan**
Jurusan Teknik Informatika UPN "Veteran" Yogyakarta
Jl. Tambakbayan 2, Babarsari, 55281, Telp (0274) 485323
Email : himawan@if.upnyk.ac.id

**Abstrak**
*Pengguna transaksi online atau e-commerce semakin meningkat dari waktu ke waktu. Salah satu bentuk perlindungan pada transaksi e-commerce pada saat ini dapat dilakukan dengan melakukan konfirmasi transaksi melalui sms. Namun ada beberapa resiko atau kerugian jika kita menggunakan sms untuk konfirmasi transaksi pada e-commerce. Termasuk didalamnya pemberian informasi dan data pengguna yang akan di konfirmasi kebenaran datanya pada bagian akhir transaksi melalui authentifikasi pengguna. Meskipun teknologi enkripsi menawarkan hal tersebut, namun pemberian keamanan transaksi pada e-commerce adalah suatu pilihan untuk digunakan, atau bahkan sama sekali tidak digunakan. Hal ini disebabkan banyaknya merchants atau toko yang merasa tidak memerlukan suatu system keamanan yang baik. Sejak sistem keamanan melindungi data dan informasi yang akan dikirimkan pada transaksi, banyak toko atau merchants yang mengakses data-data penting seperti informasi pada kartu kredit atau kartu debit. Penyimpanan data kartu kredit atau debit yang tidak terenkripsi dengan baik, akan memberikan resiko yang tinggi terhadap pencurian atau bahkan penggunaan data-data yang tidak pada tempatnya.*

***Kata kunci** : Keamanan E-Commerce, Mobile, Internet Payment Protocol, Short Message Service.*

## 1. PENDAHULUAN

Teknologi bukan merupakan "barang" yang asing lagi bagi tiap orang. Setiap kegiatan dan aktifitas yang dijalankan pasti selalu berhubungan dengan teknologi. Banyak teknologi yang kurang dimanfaatkan oleh masyarakat. Namun ketika teknologi itu dimanfaatkan, banyak pula akibat yang kurang baik yang bisa didapatkan oleh pengguna. Salah satunya adalah internet. Internet sudah merupakan kebutuhan sehari-hari bagi setiap orang. Memang internet belum menjangkau seluruh wilayah Indonesia, namun dengan jumlah pengguna yang semakin meningkat dari waktu ke waktu, menjadikan internet sebagai hal yang sangat dibutuhkan dalam kehidupan sehari-hari. Perkembangan teknologi telekomunikasi dan komputer menyebabkan terjadinya perubahan kultur kita sehari-hari. Dalam era yang disebut "*information age*" ini, media elektronik menjadi salah satu media andalan untuk melakukan komunikasi dan bisnis.

Salah satu aktifitas komunikasi dan bisnis pada dunia internet adalah melakukan transaksi perdagangan. Pada umumnya para pelaku bisnis memanfaatkan teknologi yang dapat diandalkan (*reliable*) dalam fungsi dan pengelolaannya. Sehingga transaksi yang dijalankan akan sangat berpengaruh terhadap aplikasi bisnis yang dijalankan. Selain itu, teknologi bisnis yang dapat terjangkau (*affordable*) oleh semua pengguna internet akan membantu bisnis yang dijalankan. Dengan kata lain para pelaku bisnis harus memiliki suatu sistem yang canggih, yang dapat mengatur aliran informasi, baik sesama internal organisasi atau manajemen perusahaan maupun dari kalangan eksternal yang merupakan konsumen yang akan kita raih. Sehingga dukungan teknologi baik dari perangkat keras *(hardware)* maupun perangkat lunak *(software)* sangat dibutuhkan. Selain itu ada tiga faktor yang juga harus kita perhatikan untuk membangun sistem penjualan online (e-commerce), yaitu variability, visibility dan velocity.

Untuk mengimplementasikan e-commerce tersedia suatu aturan dalam infrastruktur yang akan dijalankan. Yaitu infrastruktur sistem distribusi yang akan dijalankan (*flow of good*), infrastruktur pembayaran (*flow of money*), dan infrastruktur sistem informasi yang akan diterapkan (*flow of information*). Ketiga infrastruktur ini dapat mengakomodir semua kebutuhan yang akan dijalankan. Terutama untuk menjaga fungsi kepercayaan yang diberikan oleh para konsumen.

Untuk itulah, penelitian ini lebih memperhatikan aspek keamanan (*security*) yang harus diberikan kepada para konsumen. Salah satu konsep yang diberikan adalah dengan memberikan verifikasi data transaksi melalui pelayanan pesan singkat atau yang biasa dikenal oleh masyarakat umum dengan SMS. Sistem ini memberikan data dan authentivikasi pembayaran melalui ponsel yang dimiliki oleh konsumen. Dan tentu saja, pelayanan yang diberikan adalah terhadap pengguna atau konsumen (*user*) yang sudah terdaftar pada suatu (*merchants*) atau toko *online*.

## 2. E-COMMERCE

Mengimplementasikan *e-commerce* tidaklah mudah. Hal ini dikarenakan banyaknya faktor – faktor yang mempengaruhi sistem penjualan tersebut. Selain itu teknologi yang digunakan adalah teknologi yang terbaru. Ada beberapa jenis bisnis transaksi *online* yang biasa kita kenal pada dunia internet. Yaitu :

a. *Bussiness to Bussiness* (B2B)
   B2B biasanya menggunakan mekanisme *electronic data interchange* (EDI). Namun disayangkan bahwa pada saat ini masih banyak standar EDI yang sering digunakan oleh para retailer menyulitkan interkomunikasi ketika hal ini diaplikasikan oleh para pelaku bisnis. Standart yang ada pada saat ini antara lain : EDIFACT, ANSI X.12, SPEC 2000, CII, IEF dan lain sebagainya.
   Pendekatan lain yang sering digunakan dalam standarisasi pengiriman data adalah dengan menggunakan *Extensible Markup Language* (XML) yang dikembangkan oleh *World Wide Web Consortium* (W3C). XML menyimpan struktur dan jenis elemen data di dalam dokumennya dalam bentuk tags seperti HTML tags sehingga sangat efektif digunakan untuk sistem yang berbeda.

b. *Bussiness to Consumer* (B2C)
   B2C memiliki permasalahan yang berbeda. Mekanisme untuk mendekati konsumen menggunakan bermacam-macam pendekatan seperti menggunakan "*electronic shopping mall*" atau menggunakan konsep portal. *Electronic shopping mall* menggunakan web site untuk menjajakan produk dan servis yang akan diberikan. Dimana para retailer menyediakan katalog produk yang akan ditawarkan. Sehingga para konsumen dapat melihat produk-produk yang ditawarkan tanpa adanya batasan ruang dan waktu. Sehingga kapanpun dan dimanapun konsumen ingin melakukan transaksi, maka hal tersebut dapat dijalankan.

c. *Consumer to Consumer* (C2C)
   C2C dijalankan atas dasar kesepakatan antar konsumen dalam melaksanakan transaksi. Hal ini dapat terjadi lebih karena rasa *trust* atau kepercayaan yang diberikan oleh para rekan bisnis. Sehingga konsep C2C akan sangat tergantung pada komitmen yang diberikan oleh tiap komponen yang terlibat.

## 3. ARSITEKTUR SHORT MESSAGE SERVICE (SMS)

Saat ini siapa yang tidak pernah mengenal istilah *Short Message Service* atau SMS. Hampir setiap orang pasti pernah mendengar atau bahkan terlibat sebagai pengguna (*user*) SMS. Sehingga wajar kalau SMS dapat kita kembangkan tidak hanya berfungsi sebagai pengirim pesan, namun bisa juga digunakan untuk fungsi-fungsi pendukunglainnya, terutama dalam transaksi e-commerce.

Short Message Service adalah salah satu tipe *instant message* (IM) atau pesan singkat yang memungkinkan para pengguna (*user*) untuk bertukar pesan singkat kapanpun dan dimanapun. SMS dihantarkan pada *channel signal* GSM (*Global System for Mobile Communication*) pada spesifikasi teknis ETSI. SMS diaktifkan oleh ETSI dan dijalankan di *scope* 3GPP. SMS juga digunakan pada teknologi GPRS dan CDMA.

SMS yang dikirim oleh *handphone* dengan format tertentu diterima oleh SMS Gateway pada penyedia jasa aplikasi. Kemudian, SMS Gateway tersebut mengkonversi format pada data SMS tadi menjadi *text* yang lebih mudah diproses oleh pelanggannya. Biasanya, format ini berbentuk *script* sederhana pada aplikasi web seperti PHP, ASP atau XML. Kemudian pelanggan memproses *message* tersebut untuk melakukan *query* pada *database* tertentu. Hasil dari *query* tersebut dikirimkan menuju SMS Gateway dan diteruskan pada *handphone* pengirim SMS dengan format yang telah dirubah menjadi format SMS. SMS menjamin pengiriman pesan akan sampai oleh jaringan, sehingga jika terjadi kegagalan pesan atau biasa tertulis "message can not send" maka pesan tersebut akan disimpan terlebih dahulu oleh dijaringan, dan ketika jaringan sudah memiliki koneksi yang baik, pesan tersebut akan dapat diteruskan kepada nomer tujuan. Pengiriman paket SMS bersifat *out of band* atau yang biasa kita sebut dengan *bandwith* rendah. Sehingga tidak mengganggu gelombang elektronik lainnya.

SMS dimaksudkan untuk menjadi alat pertukaran informasi antara dua *mobile subscriber*. Elemen-elemen utama pada arsitektur SMS terdiri dari :

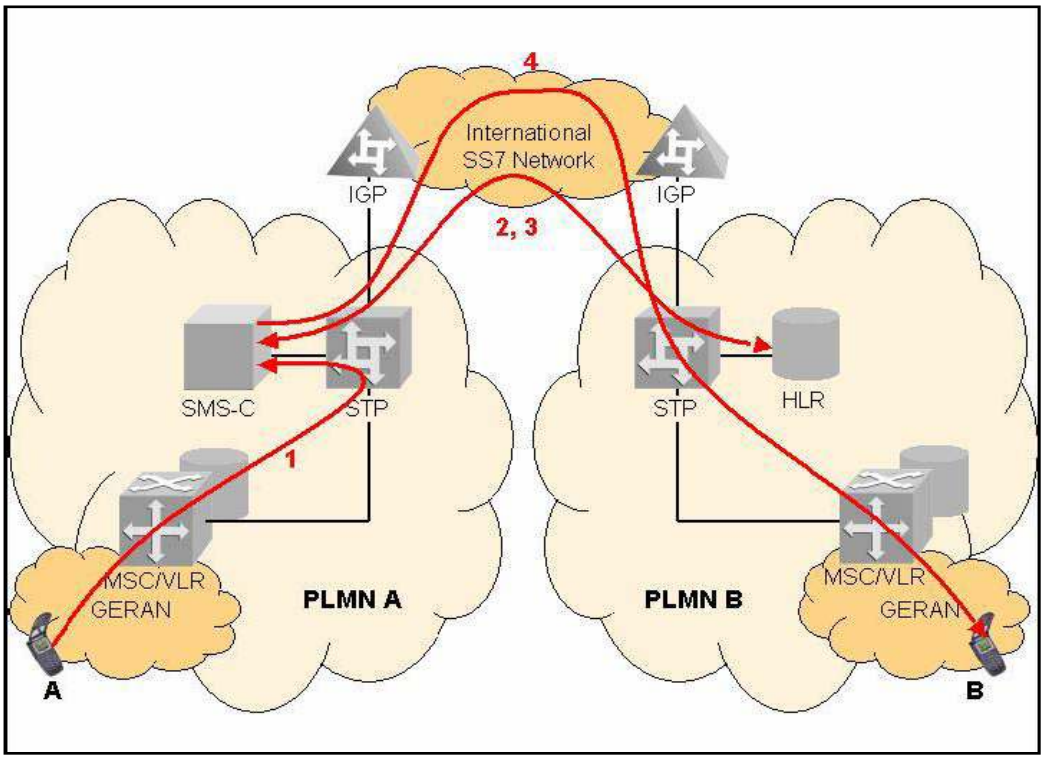
a. *Short Message Entity* (SME)
   *Short Message Entity* (SME) adalah elemen yang dapat mengirim atau menerima pesan singkat. SME dapat berupa software aplikasi pada mobile handset, dapat juga berupa perangkat facsimile, perangkat telex, remote internet server, dll.
   Sebuah SME dapat berupa server yang terkoneksi dengan SMS centre secara langsung atau melalui gateway. Dikenal juga External SME (ESME) yang merepresentasikan sebuah WAP proxy/server, Email Gateway atau Voice Mail server.

b. SMS *Service Centre* (SMSC)
SMS Service Centre (SMSC) memegang peran kunci dalam arsitektur SMS. Fungsi utama SMSC adalah menyampaikan pesan singkat antara SME dengan MS, juga menyimpan dan meneruskan pesan singkat (menyimpan pesan jika penerima SME tidak tersedia). SMSC dapat terintegrasi sebagai bagian dari mobile network (cth: terintegrasi dengan MSC) atau sebagai entitas network independen.

c. Email Gateway yang terkoneksi dengan elemen-elemen pada GSM sebagai *channel* penghantar.

Pada pengiriman SMS ini, banyak elemen yang terlibat dan harus trkoneksi dengan baik. Hal ini untuk menjaga agar konektifitas pada proses pengiriman SMS dapat berjalan dengan sempurna.

Gambar berikut ini menunjukkan dua GSM network dan komponen yang menyampaikan pesan dari end user A ke end user B :




**Gambar 1. Susunan Jaringan dan Aliran Message**

Dari gambar tersebut dapat kita lihat bahwa end user A mengirim SMS. Dimana SMS tersebut dikirim melalui MSC/VLR ke SMSC di PLMN (*Public Land Moile Network*) A. Ini merupakan sebuah pesan MAP "forward SM", termasuk nomor MSISDN asal A dan MSISDN tujuan B.

Selanjutnya, Karena end user B berada di PLMN B, SMSC harus merouting informasi dari HLR PLMN B. Untuk melakukannya, SMSC mengirim MAP "send routing info for SM" dengan nomor MSISDN B.

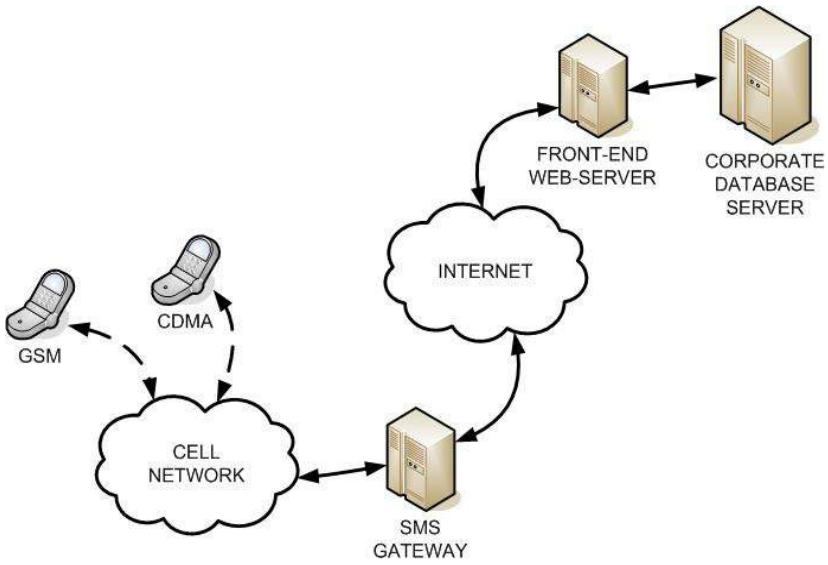
Setelah proses peroutingan selesai, maka HLR mengirim kembali IMSI dari end user B dan VLR nya. Sehingga pesan tersebut dapat diproses. Dan SMSC mengirim SMS sebagai MAP message melalui MSC/VLR ke end user B.

Konsep pengiriman SMS tersebut akan menjadi dasar keaman yang akan dibentuk pada transaksi e-commerce. Hal ini perlu diketahui agar konsep yang dibentuk tidak menyimpang dari aturan yang telah ditetapkan. Dimana proses pengiriman tersebut dapat menjadi acuan agar tingkat keamaman yang diinginkan oleh konsumen dan retailer agar tetap dapat terjaga.

Untuk mengenal lebih jauh tentang konsep yang terdapat pada SMS, ada beberapa beberapa basic feature pada SMS, seperti :

1. *Message Submission and Delivery*
   Terdiri dari message sending dan message delivery. Pada message sending, pesan dikirm dari MS ke SMSC, dialamatkan ke SME lain sebagai mobile user lain atau host internet. Originator (asal) SME menentukan validity period dari pesan tersebut, pesan yang sudah tidak valid lagi akan dihapus oleh SMSC sepanjang pengiriman pesan. Fitur ini dikenal sebagai Short Message-Mobile Originated (SM-MO).
   Pada message delivery, pesan disampaikan oleh SMSC ke MS. Dikenal sebagai Short Message Mobile Terminated (SM-MT). SM-MO dan SM-MT dapat dikirim / diterima saat voice call atau koneksi data sedang berlangsung. Pada GSM pesan dikirim pada channel SDCCH/SACCH, pada GPRS pesan dikirim pada channel PDTCH.
2. *Status Report*
   SME asal (originator) meminta status report pada pengiriman pesan singkat ke SME penerima (recipient). Status report memberikan indikasi pada user asal apakah pesan terkirim dengan sukses atau tidak kepada SME penerima.
3. *Reply Path*
   Replay Path dapat diatur oleh SME asal (atau SMSC serving) untuk mengindikasikan bahwa SMSC serving dan mampu untuk menghandle secara langsung reply dari SME penerima.
4. *Addressing Mode*
   Addressing mode menggunakan MSISDN pada format [ITU-E.164]. Email address ditentukan oleh IETF pada format [RFC-2822] atau operator specific numbering.
5. *Validity Period*
   Pesan originator dimungkinkan untuk menentukan validity period sebuah pesan. Validity period ini menentukan batas waktu sebuah pesan harus dikirim sebelum akhirnya dihilangkan oleh jaringan.

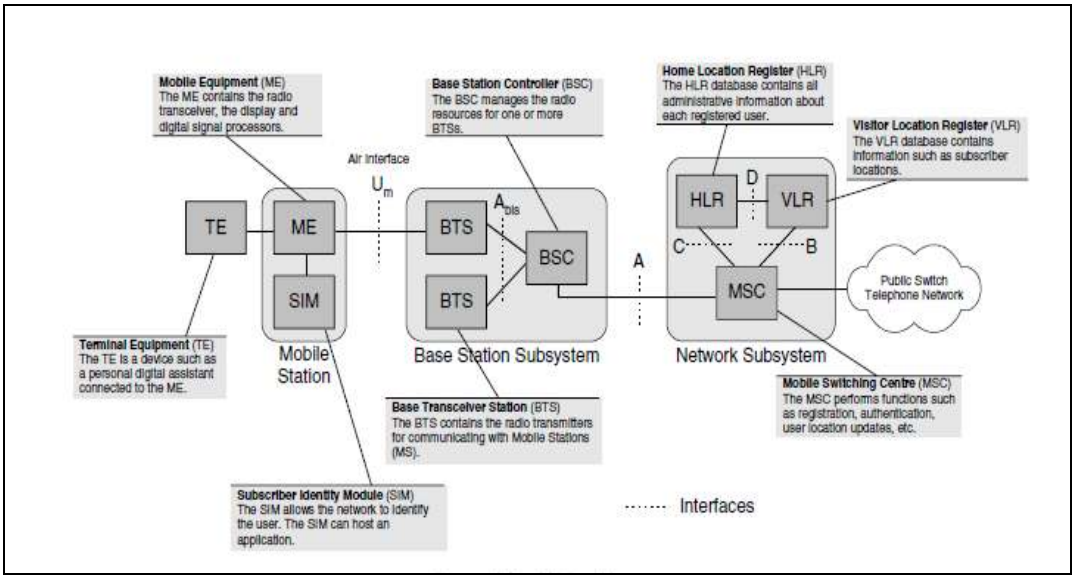
Namun pada konsep pengiriman SMS dalam proses transaksi e-commerce, ada beberapa hal yang harus kita perhatikan, agar tingkat keamanan yang dihasilkan lebih maksimal. Untuk lebih memberikan gambaran secara sederhana akan diberikan pada gambar 2.




**Gambar 2**. Arsitektur Pengiriman SMS pada Transaksi Online

## 4. GLOBAL SYSTEM FOR MOBILE COMMUNICATION (GSM)

Arsitektur GSM dalam mendukung transaksi bisnis online dapat kita lihat pada gambar 3. Dimana jaringan GSM tersebut terdiri atas tiga subsistem. Yaitu Base Station Sub System (BSS), Network Sub System (NSS) dan Operation Sub System (OSS). Namun pada penelitian ini, kami lebih memberikan penilaian pada BSS dan NSS.




**Gambar 3**. Arsitektur GSM

Adapun unsur – unsur BSS dan NSS adalah sebagai berikut :

a. *Mobile Station* (MS)

Mobile Station (MS) adalah perangkat yang mengirim dan menerima signal radio dalam melaksanakan transaksi bisnis online. MS dapat berupa *mobile handset* yang biasa kita sebut dengan *handphone* atau *Personal Digital Assistant* (PDA). Produk-produk tersebut tentu saja harus bisa mendukung teknologi yang akan dijalankan. MS terdiri dari *Mobile Equipment* (ME) *dan Subscriber Identity Module* (SIM). ME berisi *transceiver* radio, *display* dan *Digital Signal Processor*. SIM digunakan agar *network* dapat mengenali *user*. Sehingga ketika konfirmasi dan authentifikasi data akan diberikan, dapat diterima dengan baik.

b. *Base Transceiver Station* (BTS)

Base transceiver Station (BTS) berfungsi sebagai interface komunikasi semua MS yang aktif dan berada dalam coverage area BTS tersebut. Di dalamnya termasuk modulasi signal, demodulasi, equalize signal dan error coding. Beberapa BTS terhubung pada satu Base Station Controller (BSC). Satu BTS biasanya mampu menghandle 20-40 komunikasi serentak.

c. *Base Station Controller* (BSC)

BSC berfungsi mengatur konkesi BTS-BTS yang berada dalam kendalinya. Fungsi tersebut memungkinkan operasi seperti handover, cell site configuration, management of radio resources dan menyetel power level dari frekuensi radio BTS. Pada jaringan GSM BSC mengatur lebih dari 70 BTS.

d. *Mobile Switching Centre* (MSC) dan *Visitor Location Register* (VLR)

Mobile Switching Centre (MSC) melakukan fungsi registrasi, authentikasi, update lokasi user, billing service dan sebagai interface dengan jaringan lain. Selain itu MSC juga bertanggung jawab untuk call set-up, release dan routing.

Visitor Location Register (VLR) berisi informasi dinamis tentang user yang terkoneksi dengan mobile network termasuk lokasi user tersebut. VLR biasanya terintegrasi dengan MSC.

Melalui MSC, mobile network terhubung dengan jaringan lain seperti PSTN (Public Switched Telephone Network), ISDN (Integrated Service Digital Network), CSPDN (Circuit Switched Public Data Network) dan PSPDN (Packet Switched Public Data Network).

e. *Home Location Register* (HLR)

Home Location Register (HLR) adalah elemen jaringan yang berisi detil dari setiap subscriber. Sebuah HLR biasanya mampu mengatur ratusan bahkan ribuan subscriber.

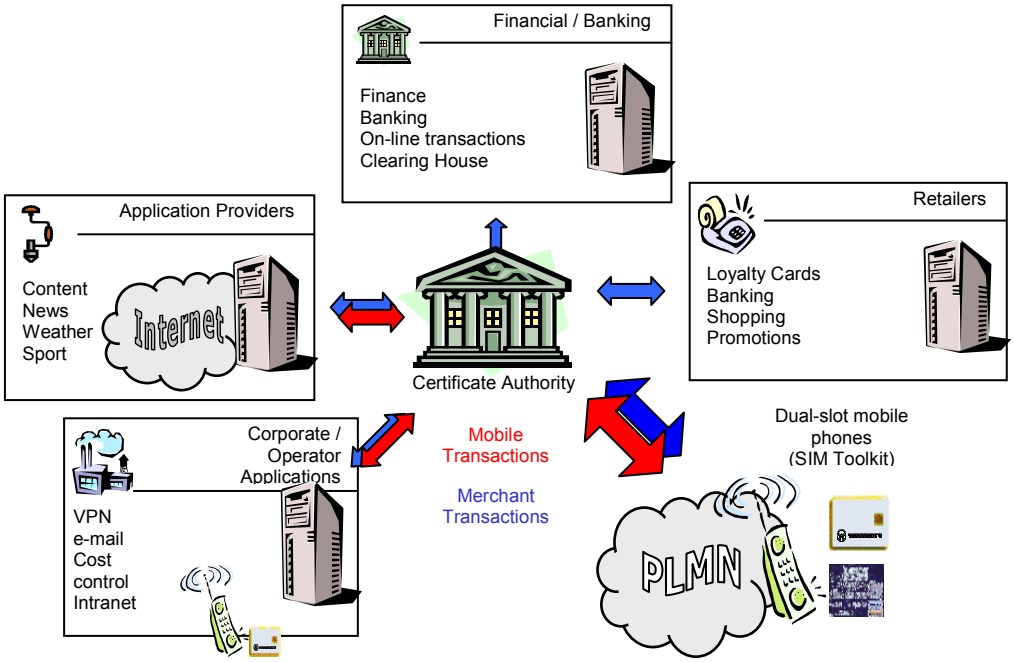
Pada jaringan GSM, signaling berbasis pada protokol Signaling System Number 7 (SS7). Penggunaan SS7 dilengkapi dengan penggunaan protokol Mobile Application Part (MAP). MAP digunakan untuk pertukaran informasi lokasi dan subscriber antara HLR dan elemen jaringan lainnya seerti MSC.

Untuk setiap subscriber, HLR mengatur pemetaan antara International Mobile Subscriber Identity (IMSI) dan Mobile Station ISDN Number (MSISDN).

Untuk alasan keamanan, IMSI jarang ditaransmisikan melalui perantara radio dan hanya dikenali pada jaringan GSM yang ditentukan. IMSI menggunakan format [ITU-E.212]. Tidak seperti IMSI, MSISDN mengidentifikasi subscriber di luar jaringan GSM, MSISDN menggunakan format [ITU-E.164].

## 5. E-COMMERCE MENGGUNAKAN 3G

Pada konsep jaringan 3G, model dan sistem transaksi e-commerce yang terbentuk melibatkan banyak komponen atau pihak. Mulai dari pihak *financial* atau pihak bank yang menerima pembayaran, pihak *retailers*, pihak *application providers* hingga pihak *corporate* dan konsumen yang melaksanakan transaksi dengan melibatkan pihak ke tiga (*certificate*) sebagai bagian untuk menjaga kepercayaan (*trust*) antar penjual dan pembeli. Komunikasi yang terjadi melibatkan dua jenis komponen, yaitu komunikasi melalui *mobile transaction* dan komunikasi *merchant transaction*. Pada komunikasi *mobile transaction*, komunikasi terjadi antara pihak *application providers*, *corporate* dan konsumen. Sedangkan pada pihak *merchants transaction* pihak yang terlibatkan adalah semua komponen unsur di dalam transaksi *e-commerce*.




**Gambar 4.** Transaksi e-commerce Menggunakan Mobile Transaction

## 6. KEAMANAN E-COMMERCE DAN GSM

Keterbatasan keamanan pada GSM sebagai teknologi carrier SMS menjadi salah satu ancaman keamanan pada SMS. Terdapat cara-cara untuk menguping pada GSM call. Call ini hanya dienkripsi dan didekripsi antara BTS dan MS, elemen jaringan yang lain hampir tidak terproteksi sama sekali. Jika seorang penyusup mempunyai akses ke jaringan SS7, yang digunakan oleh operator GSM, semua call dan trafik *signaling* nyaris tidak terproteksi. Seorang penyusup juga mungkin mendapatkan akses ke HLR, yang menyimpan semua informasi *subscriber*, walaupun biasanya diproteksi dengan baik tetapi menjadi tantangan tersendiri bagi penyusup.

Cara lain untuk menyusup pada GSM call adalah dengan mencari tahu *secret key* dari subscriber, yang merupakan basis keamanan GSM. Keterbatasan keamanan pada GSM membuat teknologi *carrier* ini mudah untuk di *snooping* dan *interception*. Penyerangan *Snooping* biasanya dilakukan pada perangkat jaringan di *elemen store* dan *forward*. Sedangkan *Interception* biasanya masuk melalui udara dan jaringan kabel.

Sehingga secara umum, keamanan merupakan salah satu komponen yang sangat diperlukan dalam mengaplikasikan e-commerce. Ada banyak teknologi yang bisa diterapkan dalam menjaga keamanan dalam bertransaksi e-commerce. Salah satu bentuk usaha untuk menjaga keamanan, dapat dilakukan melalui beberapa cara, yaitu dengan menggunakan teknologi kriptografi.

Teknologi kriptografi menjelaskan bagaimana mengamankan data dengan menggunakan enkripsi. Berbagai sistem sudah dikembangkan seperti sistem *private key* dan *public key*. Penguasaan algoritma-algoritma populer digunakan untuk mengamankan data juga sangat penting. Contoh algoritma ini antara lain DES, IDEA, RC5, RSA

dan ECC (Ellliptic Curve Cryptography. Salah satu masalah dalam mengamankan enkripsi adalah bagaimana memastikan bahwa hanya sang penerima yang dapat mengakses data. Anda dapat menggembok data dan mengirimkannya bersama kuncinya ke alamat tujuan, tetapi bagaimana memastikan kunci itu tidak dicuri orang di tengah jalan? Salah satu cara untuk memecahkannya adalah bahwa si penerima yang mengirimkan gemboknya, tetapi tidak mengirimkan kuncinya. Anda menggembok data dengan gembok yang dikirim olehnya dan mengirimkannya. Si penerima kemudian akan membukanya dengan kunci miliknya yang tidak pernah dikirimkannya ke siapa-siapa. Kini masalahnya bila data yang digembok itu dicuri orang, tetapi dengan enkripsi yang kompleks akan sangat sulit bagi orang itu untuk mengakses data yanmg sudah digembok itu.

Sehingga bentuk keamanan yang dibentuk dapat menjadikan transaksi mealui e-commerce lebih aman dan terkendali tanpa rasa takut akan bocornya informasi yang dikirimkan oleh konsumen.

## 7. ANCAMAN KEAMANAN SMS

SMS Spoofing adalah pengiriman sms dimana nomor pengirim yang tertera bukanlah nomor pengirim yang sebenarnya. Mekanisme SMS Spoofing ini dimungkinkan karena lemahnya proteksi koneksi SMSC-gateway. Penyusup dapat merekam login dan pasword dari pesan yang berasal dari SMS gateway menuju SMSC. Walaupun tak terlalu mudah namun ini dapat dilakukan dalam beberapa kasus.

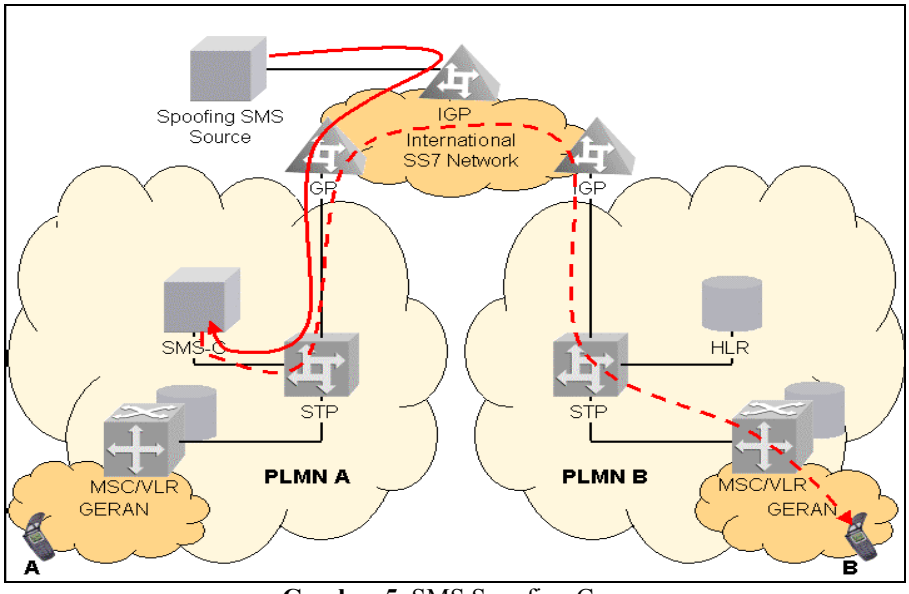
Dalam hal ini penyusup mengatur sebuah gateway palsu yang berlaku seperti gateway sesungguhnya. Gateway palsu ini dapat mengirim semua jenis pesan pendek kepada user MS melalui SMSC. Pada teknik spoofing ini pesan dikirim dengan memanipulasi nomor MSISDN asal (originate) pada field yang disediakan sehingga pesan akan tampak datang dari nomor pengirim lainnya.

Kemungkinan spoofing yang lain adalah dengan membuat simulator SMSC yang berlaku seperti SMSC asli. Dengan cara ini gateway akan kebanjiran pesan, sebagai contoh aplikasi bank menggunakan gateway dapat dengan mudah diperoleh informasi account bahkan dapat digunakan untuk transaksi bank tanpa proses authorisasi.

Sehingga data-data yang terkirim akan dapat terbaca dan berasal dari orang yang tidak kita kenal. orang-orang yang tidak bertanggung jawab ini dapat memanipulasi data pengiriman. Kalau terjadi pada transaksi e-commerce, maka banyak pihak yang akan dirugikan. Terlebih ketika pengiriman data yang dilakukan adalah pengiriman nomer-nomer atau *identification number* (ID) yang menjadi kunci utama dalam transaksi pembayaran.

Bentuk kepedulian terhadap komponen atau unsur untuk menjaga authentifikasi data haruslah di utamakan. Banyak pihak yang terlibat dalam pengiriman data-data konsumen. Mulai dari pihak merchant yang bertanggung jawab terhadap pengolahan data transaksi, hingga pihak penjual yang menjadi pintu utama di mulainya transaksi. Unsur-unsur tersebut harus dapat dijaga kerahasiaanya. Karena dari beberapa kasus yang terjadi, kebocoran bukan terjadi karena sistem yang berjalan, namun diindikasikan melibatkan unsur-unsur atau komponen-komponen yang tidak bertanggung jawab dengan menjual data atau informasi yang terdapat pada kartu kredit. Sehingga transaksi-transaksi yang dilakukan dapat terjadi karena adanya informasi data palsu yang diberikan kepada pihak *merchants*.

Berikut ini gambar kasus spoofing pada infrastruktur selular provider :




**Gambar 5**. SMS Spoofing Case

Pada gambar di atas SMS yang dikirim ke SMSC telah dimanipulasi nomor MSISDN-A nya. Sehingga "SMS Spoofing Source" menirukan end user A, mengirim sebuah pesan ke end user lain di PLMN B. Selanjutnya "SMS Spoofing Source" adalah sistem yang memiliki spesifikasi aplikasi SS7. Menggunakan nomor MSISDN-A asli atau palsu dan alamat VLR dan atau SCCP asal (originate). Dan hal ini berakibat pada banyaknya informasi- infor masi yang diberikan namun oleh pihak-pihak yang tidak bertanggung jawab.

Dampaknya pada operator jaringan adalah mengalami kerugian dalam hal pendapatan, karena user spoofing ini tidak dapat ditagih biaya ketika menggunakan nomor MSISDN palsu dan operator diwajibkan membayar operator PLMN B untuk penyerahan SMS.

## 8. AUTHENTIFIKASI

Beberapa aspek keamanan yang harus diperhatikan oleh tiap unsur yang terlibat dalam transaksi e-comerce adalah sebagai berikut :

a. *Privacy*. Hal ini menjadi aspek terpenting dalam konsep keamanan pada e-commerce. Privacy data atau informasi harus diberikan. Agar tiap komponen yang terlibat tidak merasa dirugikan oleh unsur yang lain.
b. *Integrity*. Integritas yang terbentuk harus saling memiliki komitmen. Sehingga data-data yang diberikan akan dapat terjaga tanpa adanya kebocoran data kepada pihak-pihak yang tidak bertanggung jawab.
*c. Authentivication.* Authentivikasi data harus dijaga dengan baik. Agar pengiriman dan konfirmasi transaksi data yang dilakukan dapat terjaga dengan aman.
*d. Availibility.* Ketersediaan data dan informasi harus diberikan dengan baik. Agar tiap komponen dan unsur yang terlibat dapat dilihat kemungkinan dan efektifitas yang akan terjadi pada transaksi.
*e. Access control.* Akses dan pengamanan yang dilakukan harus terpusat. Hal ini untuk mengurangi intervensi data dan informasi dari pihak luar. Agar terjadinya kehilangan informasi atau tersebarnya data-data penting kepada pihak-pihak yang tidak bertanggung jawab dapat dikurangi. Sehingga keamanan data dan transaksi yang terjadi akan tetap dapat terjaga.

Beberapa aspek keamanan tersebut, harus dapat di analisa terhadap resiko–resiko yang mungkin akan di hadapi. Hal ini difungsikan sebagai upaya untuk menentukan aset dan resiko yang akan datang. Dari analisa resiko tersebut, kita harus dapat membuat rencana dan strategi terhadap keamanan yang akan di jalankan. Tentu saja sumber dana yang di butuhkan harus dapat di alokasikan oleh unsur – unsur yang terlibat. Kebijakan pelaksanaan sistem keamanan dan penerapan sistem informasi yang baik akan menggunakan banyak sumber daya dan dana. Namun hal ini akan membawa dampak kepercayaan yang tinggi terhadap transaksi yang dilakukan oleh para konsumen.

## 9. KESIMPULAN

Dengan adanya perkembangan teknologi yang semakin pesat, dengan melibatkan banyaknya unsur yang menjadi pemain di dalam teknologi tersebut, maka sistem keamanan pada transaksi e-commerce dengan menggunakan SMS sebagai unsur pendukung, perlu adanya perhatian yang lebih dari berbagai komponen yang ada. Diantaranya :

a. Dibutuhkannya kerjasama industri atau ruang lingkup bisnis , perhuruan tinggi dan pemerintah untuk menghasilkan suatu sistem dan aturan yang tepat.
b. Pengembangan sumber daya yang terlibat harus dapat menunjang kebutuhan sistem yang akan dijalankan.

## 10. DAFTAR PUSTAKA

Budi Raharjo, 2000, *Keamanan dalam Electronic Commerce*, Jakarta

Deris Setiawan, 2002, *E-Commerce*, Jakarta.

Efraim Turban, Ephrain Mclean, James Watherbe, 2001, *Information Technology For Management*, John Wiley & Sons Inc.

Ekawati Prihatini, 2006, *Aspek Keamanan pada Jalur Komunikasi Short Message Servive*, Bandung.

ETSI, 2001, *Digital Cellular Telecomunications System, (Phase 2+); Security Aspects (GSM 02.09 version 8.0.1)*, European Telecomunications Standards Institution.

Indira Fajar Putri dkk, *Aplikasi eSMSis Sebagai IT dalam Sistem Informasi Bisnis*, Malang .

Safri Lubis, 2008, *Mengenal Lebih Dekat Mobile Commerce*, Jakarta.

Uke Kurniawan Usman, 2000, *3G Network*, Jakarta

V. Hassler , 2001, Security Fundamentals for e-Commerce, Artech House.

Vorapranee Khu-Smith, Chris j Mitchell, 2002, *Using GSM to Enhance E-Commerce Security*, Information Security Group, United Kingdom.

http://www.linuxindo.com

http://www.asp.co.id

http://www.goechi.com