

PERANCANGAN SECURE SOFTWARE ENGINEERING SMS BANKING PADA ARSITEKTUR JARINGAN GSM

Fuad Nasher

Program Studi Teknik Informatika
Universitas Suryakencana
Fuad.nasher@gmail.com

Abstrak

Teknologi Aplikasi SMS Banking sebagai sarana layanan informasi dan layanan dasar telekomunikasi secara seluler, dapat memberikan informasi kepada seseorang atau sekelompok orang yang membutuhkannya termasuk layanan kepada Nasabah yaitu berupa Informasi saldo, suku bunga dan transaksi perbankan lainnya melalui jalur elektronik dengan pemanfaatan fasilitas SMS pada telepon seluler. Tujuannya memberikan kemudahan kepada nasabah dan meningkatkan mutu pelayanan secara maksimal. supaya dalam transaksi tidak terjadi kegagalan maka dibutuhkan suatu perancangan Sistem Keamanan yang handal. Adapun yang perlu diamankan dengan menganalisa risiko dan dampak adalah : keamanan server, keamanan sumber daya aset, dan keamanan akses data. Untuk terjaminnya confidentiality, Integrity, dan Availability.

Kata kunci: SMS banking, sistem keamanan, arsitektur

1. Pendahuluan

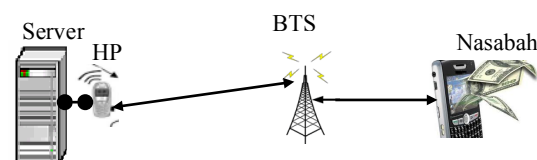
Kemajuan teknologi semakin membuat manusia mengharapkan komunikasi yang praktis, ekonomis dan realtime dalam memperoleh layanan informasi. Short Message Service (SMS) sebuah komunikasi yang menjadi pilihan masyarakat Indonesia saat ini. SMS adalah layanan dasar telekomunikasi seluler, yang tersedia pada jaringan GSM maupun CDMA. Layanan dasar SMS dapat digunakan pada semua jenis ponsel/HP (handphone) dengan terlebih dahulu mempergunakan SIM Card yang disediakan oleh operator telekomunikasi/service provider. SIM card akan otomatis menyediakan setting service center di ponsel tersebut sesuai dengan layanan yang diberikan oleh operator telekomunikasi. Ada 2 (dua) macam teknologi komunikasi jaringan seluler yang populer, yaitu GSM dan CDMA. Pembahasan ini akan fokus pada arsitektur jaringan GSM, hal ini karena layanan jaringan yang telah banyak digunakan.

Pemanfaatan SMS sebagai sarana layanan informasi dapat dibuat oleh sebuah sistem informasi, memberikan layanan kepada seseorang atau sekelompok orang yang membutuhkannya, termasuk para nasabah Bank yang menginginkan sebuah informasi perbankan dapat diperoleh dimanapun, mengingat hal tersebut pihak Bank berusaha memenuhi harapan para nasabahnya dengan memanfaatkan teknologi aplikasi SMS Banking.

Secara umum SMS Banking harus dapat memberikan informasi dan layanan kepada Nasabah yaitu berupa Informasi saldo, suku bunga dan transaksi

perbankan lainnya melalui jalur elektronik dengan pemanfaatan fasilitas SMS pada telepon seluler. Tujuannya memberikan kemudahan kepada nasabah dan

meningkatkan mutu pelayanan. Secara sederhana dapat dilihat dari gambar dibawah ini:



Gambar 1 Arsitektur SMS Banking Sederhana

2. Requirement

Dalam memenuhi kebutuhan sistem informasi, proses mengumpulkan bahan informasi sebanyak-banyaknya baik dari pengguna maupun dalam lingkungan Bank menjadi hal wajib, data-data tersebut di dapat mulai dari wawancara dengan nasabah, mengamati, mempelajari laporan, formulir dan prosedur yang digunakan.

Dari hasil evaluasi kinerja sistem dan untuk meningkatkan pelayanan kepada nasabah bank, maka analisis desain ini akan fokus pada arsitektur jaringan GSM, hal ini karena layanan jaringan GSM ini yang banyak digunakan:

2.1 Identifikasi Masalah

- Adanya kebutuhan nasabah melakukan transaksi tanpa harus ke kantor Bank dan dapat di akses dari manapun..
- Kebutuhan keamanan atas data-data Nasabah
- Kebutuhan ketersediaan mendapatkan akses informasi

- Kebutuhan teknologi informasi dapat di akses melalui telepon seluler (HP).

2.2 Tujuan

- Memenuhi kebutuhan nasabah Bank
- Mempermudah transaksi nasabah
- Mempersingkat jarak
- Memberikan pelayanan maksimal demi meningkatkan minat pelanggan untuk menjadi nasabah Bank

2.3 Kegunaan

Rancangan Perangkat Lunak SMS Banking dibangun demi memberikan mutu pelayanan yang saat ini terus ditingkatkan yaitu dengan memberikan kemudahan kepada para nasabah sebagai konsumen bank dalam melakukan transaksi melalui berbagai perangkat dan media teknologi, yang dapat digunakan untuk:

- Cek saldo
- Cek kurs valuta asing
- Transfer dana
- Informasi saldo, mutasi rekening
- Cek tiga transaksi terakhir
- Cek tagihan mitra seperti listrik, mobile, asuransi dll
- Pembayaran tagihan mitra seperti listrik, mobile, asuransi dll
- Pembayaran kartu kredit
- Transfer antar rekening
- Pembelian (pulsa isi ulang)
- dll.

2.4 Kebutuhan Perangkat

Untuk bisa menjalankan SMS Banking, membutuhkan:

1. Server
Disarankan minimal RAM 4GB, minimal space hard disk 520 GB, minimum processor Seon, spec lebih tinggi akan lebih baik
2. Web Browser
Disarankan menggunakan Firefox, opera atau Google Chrome terbaru. Tidak disarankan menggunakan IE karena ada fitur AJAX yang terdapat di dalam SMS tidak bisa berjalan dengan baik.
3. Web Server dan PHP server
Anda bisa menggunakan XAMPP, AppServ atau WAMP versi terbaru
4. Database Oracle
Sebagai basisdata yang digunakan untuk menampung seluruh data Nasabah
5. Gammu

Gammu adalah SMS library untuk sending dan receiving SMS (included)

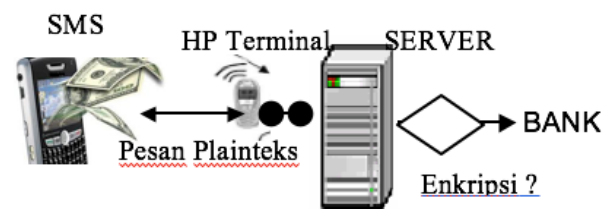
6. HP/Modem SMS

HP/Modem digunakan sebagai media untuk pengiriman dan penerimaan SMS. Sangat disarankan menggunakan modem Wavecom yang sudah teruji dengan baik. Untuk HP/modem merek lain sebaiknya diuji dulu kompatibilitasnya terhadap Gammu.

3. Desain

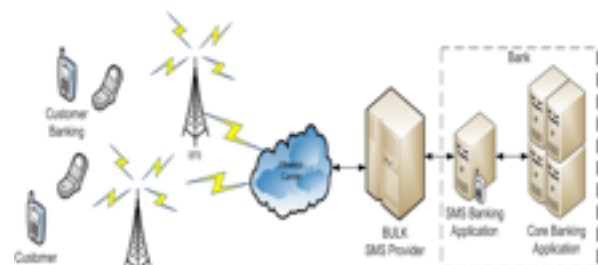
Cara mengoperasikan sistem teknologi informasi cukup dengan mengetikkan kode tertentu untuk melakukan transaksi dan dikirimkan melalui SMS. Saat SMS dikirimkan, pesan belum dienkripsi. Lalu SMS tersebut diterima oleh server, seperti SMS Gateway, kemudian oleh server diambil data yang dimaksud. Saat mencari dan mengambil data yang dibutuhkan data dienkripsi. Saat pengiriman data yang diminta oleh nasabah dapat dienkripsi terlebih dahulu atau tidak saat dikirimkan kembali, hal ini bergantung kepada kesepakatan antara developer dan pihak Bank.

Metode enkripsi yang akan dipilih disesuaikan kebutuhan pihak Bank, skema alur datanya sebagai berikut:



Gambar 2 Skema Sistem Sederhana

Penggunaan layanan SMS dari perbankan tidak terlepas dari adanya peran operator seluler. Operator seluler memberikan layanan SMS yang kemudian oleh pihak Bank dipergunakan untuk melakukan transaksi perbankan.



Gambar 3 Arsitektur SMS Banking

3.1 Skema Sistem

Skema sistem yang dikembangkan adalah pesan dikirim dengan SMS (melalui telepon atau aplikasi perangkat lunak) oleh pelanggan yang sudah terdaftar di sistem ke nomor khusus yang dipasang oleh pihak bank. Sinyal komunikasi ditransmisikan dari MS (Mobile Station) dan diterima oleh BTS

(Base Transceiver Station). Fungsi dari BTS adalah untuk menerima dan mentransmisikan sinyal menuju dan dari MS. BTS juga bertanggung jawab untuk mentranslasikan sinyal dalam bentuk format digital dan mentransferkannya pada BSC (Base Station Controller). BSC menyalurkan sinyal yang diterimanya ke MSC (Mobile Switching Center). Kemudian di balas secara otomatis oleh sistem (server) yang ada di bank untuk di informasikan ke nasabah. Untuk memperoleh informasi bisa berupa informasi saldo, suku bunga dan transaksi perbankan lainnya

3.2 Diagram Aktivitas User ke Sistem SMS Banking



Gambar 4 Arsitektur SMS Banking

Nasabah yang akan memanfaatkan aplikasi SMS Banking harus memenuhi Syarat-syaratnya dan dapat dilakukan melalui 2 Cara, adalah sbb:
Syarat-syaratnya:

- Nasabah Bank adalah pemilik rekening (perorangan) giro atau tabungan
- Pelanggan operator GSM
- Memiliki handphone GSM
- Menyetujui syarat dan ketentuan penggunaan layanan SMS Banking yang ada pada form aplikasi SMS Banking

Pendaftaran di kantor cabang (Costumer Service):

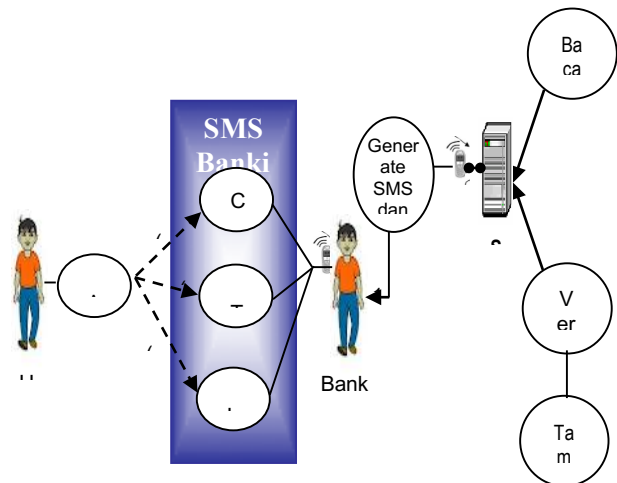
- Mengisi Formulir Aplikasi SMS Banking dan menandatangani
- Menunjukkan bukti diri (KTP/SIM/Paspor), Buku Tabungan atau Kartu ATM
- Data nasabah akan diproses dan disimpan dalam system SMS Banking

Pendaftaran di ATM:

- Dengan menggunakan Kartu ATM nasabah datang ke Mesin ATM di mana saja
- Masukkan Kartu ATM disertai dengan mengisi digit PIN Kartu ATM

- Tekan menu Registrasi e-Banking, Pendaftaran Awal, Masukkan no Handphone dan ikuti langkah selanjutnya.

3.3 Use-Case Diagram



Gambar 5 Use-Case Diagram

Pada use case diagram di atas di misalkan terdiri dari tiga aktor yang akan berperan di dalam sistem aplikasi ini sbb;

Aktor pertama user:

User adalah seluruh pengguna aplikasi, atau dalam contoh aplikasi SMS banking ini, adalah nasabah bank. User yang telah terdaftar dapat melakukan login dan menggunakan aplikasi ini untuk memeriksa jumlah saldo dan mengirimkan uang.

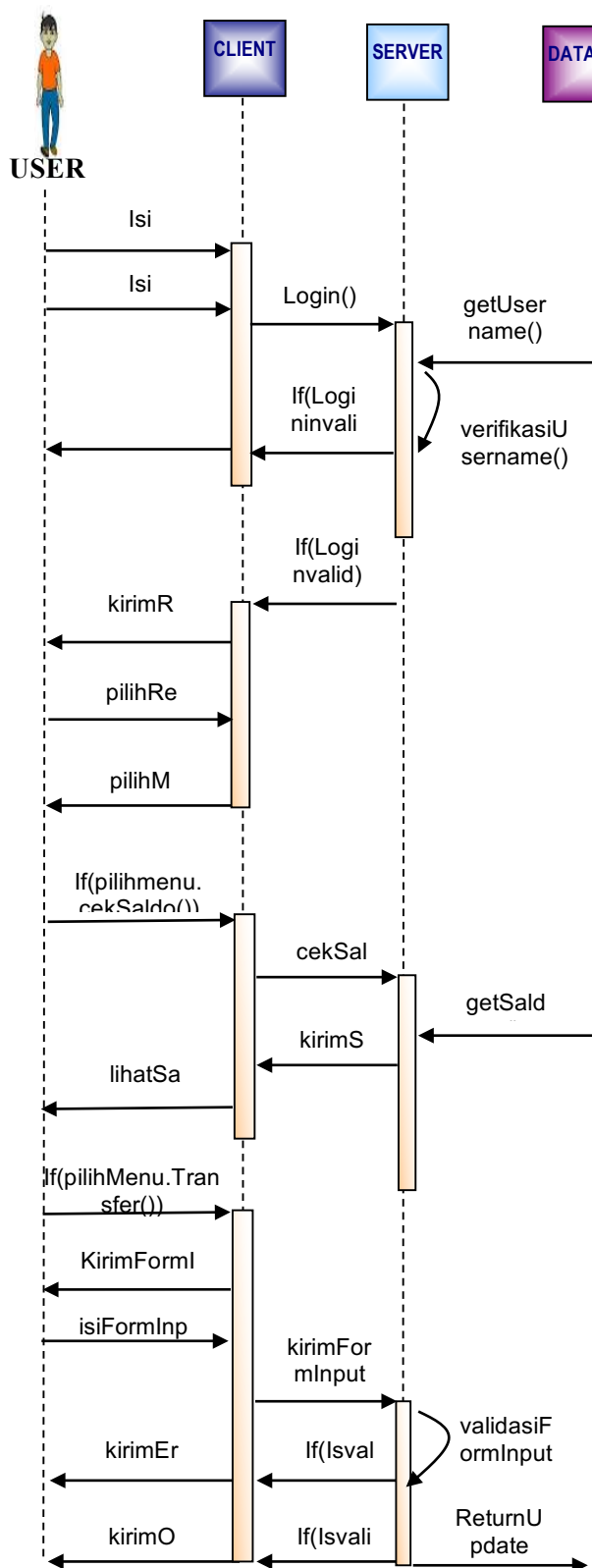
Aktor kedua Bank client:

Bank Client adalah Aktor kedua yang bertugas untuk memvalidasi apakah orang melakukan transaksi adalah orang yang berhak.

Aktor ketiga adalah server:

Antara Bank client dengan server akan terdapat proses generalisasi SMS. Di server, akan terdapat proses membaca pesan yang sudah terenkripsi oleh Bank client, verifikasi pesan atau data yang dimasukkan oleh user ke dalam Bank client lalu ke server. Setelah melakukan verifikasi, transaksi akan ditampilkan ke tujuan.

3.4 Sequence Diagram Aplikasi SMS Banking



Gambar 6 Sequence Diagram

Pergerakan sistem SMS Banking, dimulai pada saat user mengisi username dan password. Isi dari username dan password ini akan dikirimkan ke client, dari client proses login dilanjutkan ke dalam server. Di server, username dan password dari client lalu diverifikasi dengan data yang didapatkan server dari database. Jika data pada proses login yang dikirimkan ke server tidak

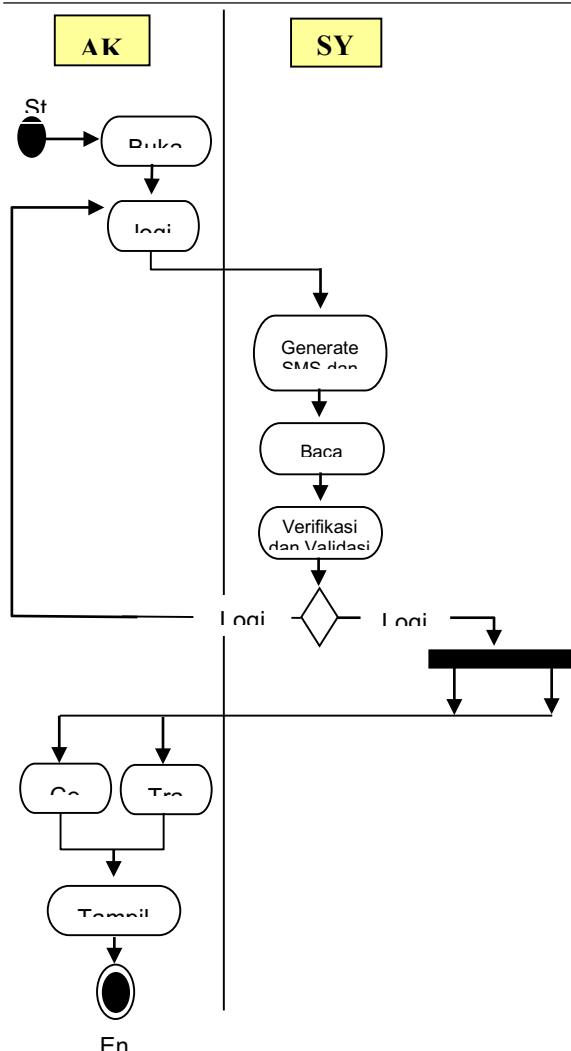
sesuai dengan data yang terdapat di database, maka client akan mengirimkan pesan error kepada user. Sedangkan, jika data pada proses login yang dikirimkan sesuai dengan data yang didapatkan server dari database, maka client akan meminta nomor rekening kepada user. User kemudian mengisi nomor rekening dan dikirimkan kembali ke client. Lalu, client mengirimkan kepada user pilihan menu fasilitas yang dapat digunakan yaitu cek saldo dan transfer.

Jika user memilih menu cek saldo, maka pilihan itu akan dikirimkan ke client kemudian diteruskan ke server. Di server permintaan menu cek saldo diterima, kemudian server mendapat data besar saldo yang diminta user dari database lalu dikirimkan ke client yang kemudian diteruskan ke user sebagai jawaban dari permintaan user di dalam menu.

Jika user memilih menu transfer, pilihan itu dikirimkan ke client. Lalu client mengirimkan kepada user FormInputTransfer. User akan mengisi FormInputTransfer. Form yang sudah terisi dikirimkan kembali kepada client dan diteruskan ke server. Data tersebut lalu divalidasi di dalam server. Jika data yang divalidasi sesuai maka client akan mengirimkan kepada user pesan "OK" sebagai keterangan bahwa proses transfer sukses dijalankan dan dikirimkan kembali ke database untuk memperbaharui data jumlah saldo. Sedangkan, jika data yang divalidasi tidak sesuai, maka client akan mengirimkan kepada user pesan "ERROR" sebagai keterangan bahwa proses transfer gagal dilaksanakan.

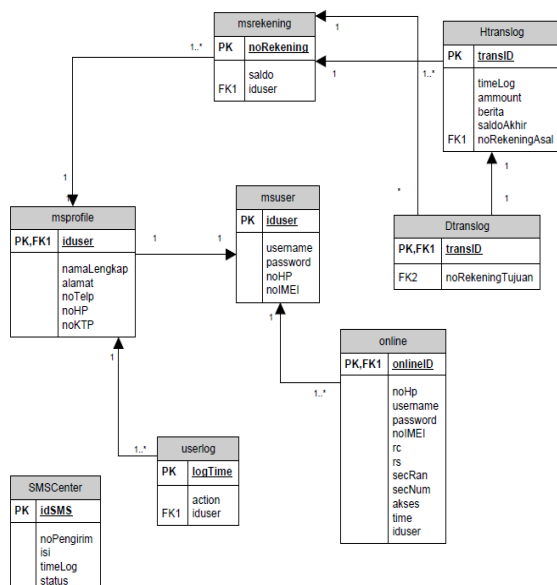
3.5 Activity Diagram

Activity diagram yang merefleksikan semua operasi menuju atau ada di sistem dan mengindikasikan semua kejadian yang menyebabkan transisi dari satu state ke state lainnya. Activity diagram tidak menggambarkan behavior internal sebuah sistem (interaksi antar subsistem) secara detail, tetapi lebih menggambarkan perusur dan jalur aktivitas dari level atas secara umum.



Gambar 7 Activity Diagram

3.6 Entity Relation Diagram (ERD)



Gambar 8 ERD

Tabel Rekening

Tabel Rekening adalah tabel yang menyediakan informasi sekaligus penyimpanan segala informasi tentang rekening bank dari nasabah.

Field	Type Data	Ukuran Field	Ket
noRekening	Varchar	10	
noPin	Int	5	
Saldo	Float	20	

Tabel Nasabah :

Tabel Nasabah adalah yang menyediakan informasi sekaligus penyimpanan segala informasi tentang data pribadi nasabah

Field	Type Data	Ukuran Field	Ket
noRekening	Varchar	10	
noPin	Int	5	
namalengkap	Varchar	75	
alamat	Varchar	150	
tempat_lahir	Varchar	30	
tanggal_lahir	Date	yyyy/mm/dd	
noHP	Int	20	

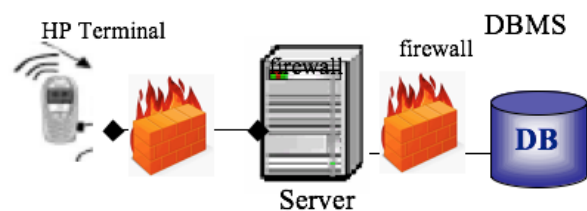
Tabel SMS Center :

Tabel SMS Center adalah yang menyediakan informasi sekaligus penyimpanan segala informasi tentang data SMS Nasabah.

Field	Type Data	Ukuran Field	Ket
idSMS	Varchar	12	
noPengirim	Varchar	12	
Isi	Varchar	250	
timeLog	Date/Time	30	
status	Varchar	10	

3.7 Rancangan Keamanan Sistem

3.7.1 Keamanan Server



Gambar 9 Rancangan Keamanan Server

Server yang disediakan dapat digunakan untuk setiap operator/pengguna jaringan yang ada di bank, setiap operator/pengguna yang akan memasuki file server harus menggunakan account masing-masing pengguna. Sedangkan file yang dapat disimpan dalam server adalah file yang penting dan digunakan untuk bekerja. Pada file server juga tersedia file yang dapat digunakan bersama dan untuk menggunakan folder ini telah disediakan account bersama.

3.7.2 Keamanan Sumber Daya Aset

	Jenis Ancaman	Current				
		Peluang	Konsekuensi	Jml Risiko	Nilai Risiko	
Langkah 1: Database, Informasi	Pencurian informasi rahasia yang berharga	3	3	9	Penting	Penerapan kebijakan dan informasi (Kriptografi) Pengaturan (user ID) atau cara untuk memberikan hak access
	Kehilangan kesempatan bisnis karena gangguan pelayanan	3	3	9	Penting	Menjamin kepastian bahwa orang yang berhak.
Langkah 2: Aplikasi, Sistem Operasi	Kerusakan pada sistem operasi atau aplikasi (Software tidak berfungsi dengan baik)	4	5	2	Penting	Pemasangan Firewall

kelemahan dalam software yang digunakan untuk mengelola data.

- Tindakan Pengamanan: Keamanan yang berhubungan dengan orang (nasabah) untuk mengurangi resiko pengunjung, dan profil resiko dari orang yang mempunyai akses (pekerja/pelanggan) harus diatur dengan berhati-hati untuk mengurangi kemungkinan adanya penyalahgunaan data.

• Keamanan dalam Administratif: termasuk prosedur yang digunakan untuk mengatur dan mengelola sistem keamanan, dan juga termasuk prosedur setelah serangan (post attack recovery).

- Keamanan Media yang digunakan untuk komunikasi, topologi dari jaringan yang dipakai
- Untuk semua layanan email dan web service dapat menggunakan keamanan jenis SSL.

Sedangkan untuk account dan password dapat menggunakan metode enkripsi

Quantitative Estimation:

- Tingkat risiko = asset x threat x vulnerability
- Tingkat risiko = 40 x 20 x 20 = 16000
- Dampak: jika di kalkulasikan dengan uang, kerugian tiap hari bisa mencapai Rp.160.000.000 (jika Tingkat resiko x 10000) itu berarti sangat tinggi sekali.

3.7.3 Keamanan Akses Data

Pengguna dalam sistem jaringan terdiri dari 2(dua) yaitu yang bersifat internal dan eksternal. Pengguna internal adalah pengguna yang ada dilingkungan bank, sedangkan pengguna eksternal adalah pengguna yang ada diluar lingkungan bank untuk melakukan transaksi dan keperluan lainnya terkait dengan sistem jaringan, sehingga hak aksesnya perlu diatur dalam sistem.

Dalam sistem jaringan komputer yang terdisiri banyak pengguna, diperlukan tingkat keamanan yang tinggi baik untuk hardware, software maupun pengguna. Berikut kebutuhan keamanan yang diperlukan :

Qualitative Estimation:

Account	Resiko	Dampak	Keputusan
Pengguna (Nasabah)	Tinggi	Tinggi	Perlu
Masy. Umum	Tinggi	Tinggi	Perlu
Admin SMS	Rendah	Rendah	Tidak
Operator SMS	Rendah	Tinggi	Perlu
Admin Bank	Tinggi	Tinggi	Perlu
Operator Bank	Rendah	Tinggi	Perlu
Programmer	Rendah	Rendah	Tidak

Access Control: terhadap User

- Nasabah
- Operator SMS
- Admin SMS
- Admin Bank
- Operator Bank
- Orang lain/Masy. umum

Setiap user yang terdaftar dalam sistem SMS Banking diberi otentifikasi berupa account dan password, hal ini terkait keamanan proses transaksi berkaitan dengan keaslian data pengguna.

Otorisasi:

- Pemberian Wewenang atau hak istimewa (priviledge) untuk setiap nasabah
- Kendali otorisasi (=kontrol akses) yang dibangun pada perangkat lunak untuk

- Keamanan yang bersifat fisik (physical security): termasuk akses orang ke gedung, peralatan, dan media yang digunakan.
- Keamanan dari data dan Aplikasi serta teknik komunikasi (communications). adalah

mengendalikan account nasabah dan bagaimana nasabah melakukannya.

- Sistem administrasi yang bertanggungjawab untuk memberikan hak akses dengan membuat account pengguna.

Perintah	Keterangan
CREATE	Menciptakan objek sehingga memungkinkan pengguna (Nasabah) untuk membuat objek tertentu yang dibuat
DROP	Menghapus database
INSERT	Mengijinkan pengguna (Nasabah) menambahkan data pada tabel
SELECT	Mengijinkan pengguna (Nasabah) mengambil data pada database
UPDATE	Mengijinkan pengguna (Nasabah) meng-ubah data pada tabel

User	CREA TE	INSE RT	SELE CT	UPDA TE	DRO P	Perintah Lainnya
Pengguna (Nasabah)	X	✓	✓	✓	X	X
Masy. Umum	X	X	X	X	X	X
Admin SMS	X	X	✓	X	X	X
Operator SMS	X	X	✓	X	X	X
Admin Bank	✓	✓	✓	X	X	X
Operator Bank	X	X	✓	X	X	X
Programmer	✓	✓	✓	✓	✓	✓

Keterangan: ✓ diberi wewenang dan hak istimewa
X tidak diberi wewenang

Otorisasi Admin terhadap DB

Tipe Admin	DB SMS Banking	DB Lain
1. Admin System (Superadmin)	✓	
2. Admin DBA	✓	✓
3. Admin Aplikasi Lain		✓

Keterangan: ✓ diberi wewenang dan hak istimewa

Otorisasi User (Pengguna) terhadap Data

Keterangan: ✓ diberi wewenang dan hak istimewa

Tipe User	Appl.	Data				Keterangan
		Edit	View	Del	Add	
1. Administrator	✓	✓	✓	✓	✓	Semua data
2. Pengguna (Nasabah)	✓	✓	✓	✓	✓	Data2 Bank. milik peserta
3. Operator	✓		✓			Semua data
4. Masyarakat Umum	✓					Data2 pengumuman

3.7.4 Identifikasi Ancaman

Merupakan kemungkinan-kemungkinan munculnya kejadian yang tidak diinginkan dan dapat membahayakan asset-asset berharga atau organisasi. Diantaranya:

Sumber Daya (Asset)	Bentuk Ancaman
Bersifat Fisik: Hardware Perangkat Jaringan Perangkat Komunikasi Data	Interruption Perangkat sistem menjadi rusak atau tidak tersedia. Serangan ditujukan kepada ketersediaan (availability) dari sistem. Pencurian perangkat keras komputer atau perangkat aringan Kerusakan pada komputer dan perangkat komunikasi jaringan Wiretapping Bencana alam
Logik: Aplikasi Sistem Operasi Data dan Informasi	Modification mengubah isi pesan dengan pesan-pesan yang merugikan pemilik account. (SMS spoofing) Kerusakan pada sistem operasi atau aplikasi (Software tidak berfungsi dengan baik) Virus Sniffing Denial Of Services

Kerentanan (Vulnerability)

Kerentanan (vulnerability) : Terhubungnya jaringan komputer ke internet membuka potensi adanya lubang keamanan (security hole). Sehingga bagaimana setiap organisasi dapat memastikan bahwa sistem informasi yang ada memiliki sistem pengamanan dan pengendalian yang memadai.

Usaha-usaha untuk mengurangi Kerentanan:

1. Perlu adanya prosedur – prosedur Keamanan yang dilakukan oleh perusahaan.

2. Melakukan Penerapan pengawasan dan kontrol melalui (countermeasure), yaitu:

- Pencegahan
- Deteksi
- Represif
- Evaluasi

Dampak Terhadap Sistem

Mengidentifikasi dan menghitung kerugian dampak yang ditimbulkan oleh peristiwa pengrusakan jika keamanan sistem di abaikan, serta tidak terjaminnya:

- confidentiality, usaha untuk menjaga informasi dari orang yang tidak berhak mengakses.,
- Integrity, bahwa informasi tidak boleh diubah tanpa seijin pemilik informasi.
- Availability, ketersediaan berhubungan dengan ketersediaan informasi ketika dibutuhkan.

Tabel Dampak yang ditimbulkan

Sumber Daya (Asset)	Bentuk Ancaman	Dampak yang Diperoleh
Bersifat Fisik: Hardware Peran perangkat Jaringan Peran perangkat Komunikasi Data	Interruption Perangkat sistem menjadi rusak atau tidak tersedia. Serangan ditujukan kepada ketersediaan (availability) dari sistem. Pencurian perangkat keras komputer atau perangkat jaringan Kerusakan pada komputer dan perangkat komunikasi jaringan Wiretapping Bencana alam	Kerusakan perangkat keras. Penyalahgunaan penggunaan komputer Terganggunya kestabilan system / pelayanan ke nasabah.
Logik : Aplikasi Sistem Operasi Data dan Informasi	Modification mengubah isi pesan dengan pesan-pesan yang merugikan pemilik account. (SMS spoofing) Kerusakan pada sistem operasi atau aplikasi (Software tidak berfungsi dengan baik) Virus Sniffing Denial Of Services	Penolakan terhadap sebuah aktivitas transaksi atau sebuah komunikasi baik secara sengaja maupun tidak disengaja. Pelanggaran atau penyalahgunaan wewenang legal Menghalangi seseorang dalam mengakses informasi, sumber, dan fasilitas-fasilitas lainnya

4. Kesimpulan

Berdasarkan kegiatan-kegiatan yang dilakukan dapat diambil kesimpulan sebagai berikut:

4.1 Short Message Service (SMS) sebuah komunikasi yang menjadi pilihan masyarakat Indonesia saat ini. SMS adalah layanan dasar telekomunikasi seluler, yang tersedia pada jaringan GSM maupun CDMA. Pemanfaatan SMS sebagai sarana layanan informasi dapat dibuat oleh sebuah sistem informasi, memberikan layanan kepada seseorang atau sekelompok orang yang membutuhkannya, termasuk para nasabah Bank menginginkan sebuah informasi perbankan yang dapat diperoleh dimanapun.

4.2 UML menggabungkan teknik-teknik terbaik dari data model (diagram hubungan entitas), model bisnis (aliran kerja), pemodelan objek, dan komponen model. Hal ini dapat digunakan dengan semua proses, sepanjang siklus hidup pengembangan perangkat lunak, dan teknologi implementasi yang berbeda.

4.3 Pengembangan sebuah sistem informasi, dengan memanfaatkan teknologi jaringan akan berdampak pada resiko yang akan diterima jika faktor keamanan tidak menjadi hal yang diperhatikan, penerapan teknologi keamanan sistem juga harus sesuai dengan kebutuhan dari sistem SMS-Banking yang akan dikembangkan, Algoritma kriptografi adalah pilihan dalam mengenkripsi sebuah pesan dan menyembunyikan bagian informasi yang penting seperti nomor seri transaksi, nomor PIN, ataupun nilai transfer transaksi.

4.4 Setelah semua analisa risiko dan dampak diperhatikan sistem juga harus dapat merecovery/ mereset dirinya secara otomatis jika terjadi kegagalan dengan mengembalikan basis data ke dalam keadaan yang dianggap benar.

5. Referensi

- [1] Denis Pankratov, Dmitri Kramarenko
- [2] (2004). SMS spoofing – Q&A with CCRC staff.
- [3] Luciana Spica Almilia, Antony Nova Giarta (2007). Perspektif Nasabah Perbankan atas kehadiran SMS banking dan WAP banking sebagai sistem informasi perbankan yang bernilai tambah.
- [4] Budiono (2008). Penerapan Tanda Tangan Digital Untuk Otentikasi SMSBanking.
- [5] Rinaldi Munir (2009). Kriptografi.
- [6] <http://lecturer.ukdw.ac.id/budsus/pemodelan/Modul2.pdf>
- [7] UML Specification version 1.1 (OMG document ad/97-08-11)
- [8] <http://people.inf.uajy.ac.id/~alex/project/CSharp/EHIS/Dokumentasi/SKPL-UseCase.pdf>