IMPLEMENTASI APLIKASI ANTI SPAMMING SMS DALAM MENANGGULANGI SMS PENIPUAN DAN FRAUD BILLING SMS TELKOM FLEXI

TESIS

oleh :

BENNY SUSATYO

0606003215

MANAJEMEN TELEKOMUNIKASI
PROGRAM STUDI TEKNIK ELEKTRO
PROGRAM PASCA SARJANA BIDANG ILMU TEKNIK
UNIVERSITAS INDONESIA
2007

PERNYATAAN KEASLIAN

Saya yang bertandatangan dibawah ini, menyatakan dengan sesungguhnya bahwa tesis dengan judul :

IMPLEMENTASI APLIKASI ANTI SPAMMING SMS DALAM MENANGGULANGI SMS PENIPUAN DAN FRAUD BILLING SMS TELKOM FLEXI

yang saya buat ini adalah hasil karya saya sendiri, dan bukan merupakan duplikasi, serta tidak mengutip sebagian atau seluruh karya orang lain, kecuali yang telah disebutkan sumbernya dan sesuai dengan batasan serta tata cara pengutipan. Apabila didapati pelanggaran atas pernyataan saya ini, maka saya bersedia menerima sanksi sesuai peraturan yang berlaku.

Jakarta, Desember 2007

BENNY SUSATYO

NPM. 0606003215

LEMBAR PENGESAHAN

Tesis dengan judul :

IMPLEMENTASI APLIKASI ANTI SPAMMING SMS DALAM MENANGGULANGI SMS PENIPUAN DAN FRAUD BILLING SMS TELKOM FLEXI

dibuat untuk melengkapi sebagai persyaratan kurikulum program Magister Bidang Ilmu Teknik Universitas Indonesia guna memperoleh gelar Magister Teknik pada Program Pascasarjana Program Studi Teknik Elektro. Tesis ini telah diujikan pada sidang ujian tesis pada tanggal 27 Desember 2007 dan dinyatakan memenuhi syarat/sah sebagai tesis pada Departemen Elektro Fakultas Teknik Universitas Indonesia.

Jakarta, Desember 2007

Dosen Pembimbing

Ir. MUHAMAD ASVIAL, MSc., Ph.D.

NIP. 132 094 574

KATA PENGANTAR

Dengan mengucapkan puji syukur atas kehadirat Allah Yang Maha Besar yang senantiasa melimpahkan karunia rahmat, hidayah, innayah, dan barokah-Nya sehingga penulis diberikan kemudahan dan kesehatan dalam menyusun dan menyelesaikan pembuatan tesis ini tepat pada waktunya.

Tesis yang berjudul " **Implementasi aplikasi anti spamming SMS dalam menanggulangi SMS penipuan dan fraud billing SMS Telkom Flexi**" disusun untuk melengkapi persyaratan kelulusan pendidikan Pascasarjana pada jurusan Teknik Elektro Kekhususan Manajemen Telekomunikasi Fakultas Teknik, Universitas Indonesia.

Dalam kesempatan kali ini penulis ingin mengucapkan terima kasih dan apresiasi yang tinggi kepada :

1. Bapak Ir. Muhamad Asvial, Msc., Ph.D. Selaku Pembimbing Tesis yang sangat responsif dan efektif dalam memberikan arahan, bimbingan, dan nasihat kepada penulis selama desain, penyusunan, pembuatan, hingga terselesaikannya hasil tesis ini.
2. Bapak Ir. Gunawan Wibisono, MSc., Ph.D. Selaku Pembimbing Akademik yang memudahkan penulis untuk merealisasikan percepatan masa perkuliahan selama 3 (tiga) semester.
3. Seluruh dosen, karyawan, dan civitas akademika yang berada di lingkungan Teknik Elektro Universitas Indonesia di Salemba dan Depok yang banyak membantu penulis selama kegiatan perkuliahan dilaksanakan.

Jakarta, Desember 2007

BENNY SUSATYO

Benny Susatyo
NPM 0606003215
Departemen Teknik Elektro

Dosen Pembimbing
Ir. Muhamad Asvial, MSc., Ph.D.

IMPLEMENTASI APLIKASI ANTI SPAMMING SMS DALAM MENANGGULANGI SMS PENIPUAN DAN FRAUD BILLING SMS TELKOM FLEXI

ABSTRAK

Bagi para pengguna teknologi seluler dan *fix wireless*, penggunaan *service* SMS sudah menjadi kebutuhan utama setelah *voice*. Pesatnya pertumbuhan jumlah pengguna SMS khususnya di Telkom Flexi, dari satu sisi membawa masalah bagi operator, yaitu maraknya aksi penipuan yang dilancarkan melalui media SMS. Disamping menduduki kanal signaling operator yang jumlahnya terbatas, penipuan yang menggunakan nomor pengirim *postpaid*, secara langsung menimbulkan *fraud* tersendiri dari sisi *billing*. SMSC sebagai sentral SMS sudah sangat mendesak untuk segera melengkapi fiturnya dengan sistem sekuriti tambahan seperti aplikasi anti spamming yang dapat melakukan *parsing*, *checking*, dan *blocking* yang dapat menekan *spamming* SMS tersebut. Perumusan masalah, desain aplikasi, pembuatan aplikasi, analisis, serta evaluasi terhadap hasil *anti spamming* ini akan penulis bahas pada penulisan tesis ini. Diharapkan dari implementasi *anti spamming* ini dapat menurunkan frekuensi SMS penipuan dan menurunkan *fraud billing* SMS Telkom Flexi.

Kata kunci : Anti Spamming SMS, SMS Penipuan, Fraud Billing SMS

Benny Susatyo
NPM 0606003215
Electrical Engineering Department

Counsellor
Ir. Muhamad Asvial, MSc., Ph.D.

THE IMPLEMENTATION OF ANTI SPAMMING SMS APPLICATION TO PREVENT SMS CRIMINAL DECEPTION AND SMS BILLING FRAUD IN TELKOM FLEXI

ABSTRACT

For cellular and fix wireless users, SMS service has been the main needs after Voice. The fast growth of SMS users especially in Telkom Flexi, in one side has created one problem for operator, that is the increasing number of criminal deception via SMS. Besides using the limited number of operator signalling canals, the criminal deception using the post-paid number will effect directly on billing fraud. This is about time that SMSC as SMS Center to provide the features with additional security system as anti spamming that performs parsing, checking, and blocking on the said SMS spamming. The objective, application design, application making, analysis and evaluation on the anti spamming effect will be described in detail in this thesis. It is hoped that this anti spamming implementation can decrease the numbers of the SMS criminal deception and SMS billing fraud in Telkom Flexi.

Key Word : Anti Spamming SMS, SMS Criminal, SMS Billing Fraud

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR SINGKATAN

3GPP	*3rd Generation Partnership Project*
3GPP2	*3rd Generation Partnership Project 2*
ANSI	*American National Standards Institute*
BSC	*Base Station Controller*
BTS	*Base Tranceiver Station*
CDMA	*Code Division Multiple Access*
CDR	*Call Data Recording*
Divre II	*Divisi Regional II*
ESME	*External Short Message Entity*
ETSI	*European Telecommunications Standards Institute*
FTP	*File Transfer Protocol*
GSM	*Global System for subscriber Mobile*
HLR	*Home Location Register*
HP-UX	*Hewlett Packcard Unix*
IS-41	*Interim Standard 41*
IPS	*Intrution Prevention System*
MDN	*Mobile Directory Number*
MIN	*Mobile Identification Numbe*r
MAP	*Mobile Application Protocol*
MS	*Mobile Subscriber*
MSC	*Mobile Switching Center*
NE	*Network Elemen*
OLO	*Operasi Lintas Operator*
OS	*Operating System*
PSTN	*Public Switched Telephone Network*
RF	*Radio Frequency*
SMS	*Short Message System*
SDL	*Signalling Data Link*
SLC	*Signalling Link Code*
SQL	*Standardized query language for requesting info from a database*
SMDPP	*Short Message Delivery Point to Point*
SMPP34	*Short Message Peer to Peer Version 3.4*
SMPPGW	*Short Message Peer to Peer Version 3.4 Gateway*
SMSC	*Short Message Service Center*
SMTE	*Short Message Terminal Equipment*
SS7	*Signaling No.7*
SSF	*Satuan Sambungan Flexi*
SWOT	*Strength Weakness Opportunity Threath*
TCP/IP	*Transfer Control Protocol*
TDM	*Time Division Multiplexing*
TIA/EIA	*Telecommunications Industry Association/ Electrical Industries Association*
WAP	*Wireless Application Protocol*
WIN	*Wireless Intellegence Network*

BAB I

PENDAHULUAN

1.1 LATAR BELAKANG

Salah satu laporan resmi dari perusahaan seluler terbesar di Indonesia PT. Telkomsel menunjukan bahwa pada bulan Juni tahun 2006, trafik SMS *outgoing* dari *home country* Telkomsel sudah yang mencapai sekitar 3 Milyar SMS per bulan [1]. Dengan kata lain Telkomsel dapat meraup pendapatan sekitar 100 juta SMS per hari. Demikian halnya dengan PT Telkom yang memiliki *brand* produk Flexi yang telah menguasai 65% pangsa pasar CDMA dengan jumlah 5 juta pelanggan aktif di seluruh Indonesia [2]. SMS Flexi juga sudah menjadi bisnis besar mengingat tren pertumbuhannya yang terus naik.

Teknologi SMS saat ini sudah menjadi teknologi yang mapan, hal tersebut terlihat dari terimplementasikannya aplikasi SMS pada seluruh *mobile subcriber* dalam *platform* teknologi GSM maupun CDMA di seluruh dunia oleh para *vendor handset* [3]. Dengan begitu pesatnya perkembangan teknologi telekomunikasi khususnya dalam bisnis SMS para operator seperti memegang pisau tajam bermata dua, dimana selain dapat meraup keuntungan besar namun ada pula sisi *fraud* yang timbul dari bisnis SMS ini dalam bentuk *fraud* pada *billing collection*.

Bentuk penipuan lewat *spaming* SMS adalah salah satu penyebab utama timbulnya *fraud* pada *billing collection* dari bisnis SMS yaitu hilangnya peluang pendapatan yang disebabkan tidak tertagihnya piutang dari nomor-nomor *postpaid* yang melakukan *spamming* SMS tersebut. Dari berbagai laporan kejadian yang terjadi di *back room* Telkom Flexi, baik yang sempat diberitakan media maupun tidak, sudah banyak korban dari *spamming* SMS yang mengandung unsur penipuan. Mulai dari ibu-ibu rumah tangga, pembantu, supir, anak sekolah, mahasiswa, dosen, karyawan, karyawati beberapa pejabat publik, anggota kepolisian, anggota TNI, bahkan juga pula anggota DPR-RI yang pernah menjadi korban penipuan SMS ini.

Usaha untuk mengatasi cara-cara penipuan yang sangat halus dan menggiurkan ini mau tidak mau diperlukan suatu kepedulian nyata dari operator telekomunikasi dalam hal ini Telkom Flexi dalam rangka memutuskan rantai penipuan SMS ini.

Banyaknya aplikasi SMS yang dijual bebas dipasaran yang mampu mengirimkan SMS lewat *personal computer* yang terhubung ke *handphone* memungkinkan SMS dikirimkan ke ribuan nomor dalam waktu beberapa menit saja. Dan nomor *postpaid* yang menjadi pengirim SMS akan melakukan pengiriman SMS sebanyak-banyaknya untuk mengemplang kemudian hari.

Sebelum ada aplikasi *anti spamming* penanganan nomor-nomor yang melakukan penipuan melalui SMS dilakukan secara manual. Eksekusi SMS *spamming* diawali dahulu dengan komplain pelanggan dari *call center* 147 atau *helpdesk* terhadap nomor *spamming*. Kemudian teknisi SMS disisi *backroom* akan menindaklanjutinya dengan proses pengecekan secara manual secara bertahap sampai terbukti pelanggan tersebut terindikasikan melakukan penipuan SMS. Contoh-contoh kalimat seperti *"Selamat anda memenangkan undian/quiz dst ", "Kepada pelanggan yth, selamat anda telah memenangkan dst",* dsb. *Content* SMS tersebut cukup menjadi bukti kuat untuk mengelompokan nomor tersebut kedalam daftar nomor-nomor *blacklist.* Dilanjutkan dengan proses *blocking* nomor secara manual, dan hasilnya dikonfirmasi ulang ke *call center* 147 atau *helpdesk* sebagai antisipasi jika ada permintaan buka *blokir* kembali fitur SMS terhadap nomor-nomor yang sudah terindikasi penipuan tersebut dikemudian hari.

Penanganan SMS penipuan secara manual ini memiliki beberapa kekurangan disisi penanganannya, diantaranya adalah :

- tidak *real time* sehingga mungkin saja sudah jatuh korban.
- waktu penanganan relatif lama dan membutuhkan koordinasi dengan berbagai pihak yaitu pelanggan yang melaporkan, petugas *call center* 147 atau *helpdesk* Telkom Flexi, teknisi SMS, teknisi HLR terkait, klarifikasi ulang nomor *blacklist* tersebut ke *helpdesk* Telkom Flexi.
- tercecernya data-data nomor dari dokumentasi pemblokiran yang dilakuakn secara manual, dan
- belum terintegrasi dengan node SMSC lainnya di Telkom Flexi.

Akibat lain dari *spamming* SMS ini adalah timbulnya kerugian dari sisi operator diantaranya adalah :

- *resource network*, dimana *spamming* SMS jika didiamkan saja akan terus menduduki kanal operator yang terbatas dan mahal, terbatas pada sisi kanal RF *(carrier)*, kanal signaling di MSC, kanal *signalling* di HLR (SDL/SLC), kanal SMS internal, maupun kanal SMS lintas operator.
- *resouce disk*, pada *network* terkait yang dilewati *spamming* SMS.
- pendudukan *buffer* di SMSC dan SMSC *Gateway*.
- 99,99% biaya pemakaian SMS *spamming* tidak pernah bisa tertagih oleh Telkom dan menjadi *fraud* pada *billing collection*.

Dalam penelitian ini penulis akan membahas tentang permasalahan timbulnya *fraud* pada *billing collection postpaid* SMS, mendesain mekanisme dan algoritma aplikasi *anti spamming*. Pembuatan aplikasi *anti spamming*, analisa, serta evaluasi hasil dari implementasi aplikasi *anti spamming* di *network* SMS Telkom Flexi akan dilanjutkan pada tesis, yang akan penulis kerjakan sepenuhnya. Dari implementasi ini diharapkan dapat menurunkan frekuensi SMS penipuan dan menurunkan *fraud billing* SMS Telkom Flexi.

Hipotesis awal adalah perlunya dibuat suatu mekanisme baru untuk membendung *spamming* SMS dengan sebuah aplikasi yang dinamakan *anti spamming* SMS yang dapat melakukan proses *parsing, checking, bloking, dan blacklist* terhadap nomor-nomor yang melakukan *spamming* secara *realtime* dan terintegrasi.

1.2 PERUMUSAN MASALAH

Tumbuhnya trafik SMS ternyata diikuti dengan tumbuhnya trafik *spamming* SMS yang muncul tanpa terkendali pada jaringan SMS flexi sehingga menimbulkan dampak timbulnya *fraud billing* SMS yang tidak terkendali. Untuk itu diperlukan usaha untuk menekan timbulnya *fraud* pada *billing collection* SMS di jaringan SMS Telkom Flexi di kemudian hari.

1.3 TUJUAN PENELITIAN

Adapun tujuan dari penelitian ini adalah mengidentifikasi dan mencari solusi permasalahan mendasar yang mengakibatkan *fraud billing* SMS akibat trafik *spamming* SMS dengan melakukan langkah-langkah membuat aplikasi sekuriti tambahan di SMS *Center* aplikasi *anti spamming* SMS di jaringan SMS Telkom Flexi

1.4 BATASAN MASALAH

Ruang lingkup dan batasan masalah dari penelitian ini adalah :

a. Kajian hanya dilakukan pada layanan SMS yang pengirimnya berasal dari nomor *postpaid* Flexi, tidak pada unit lain, dan operator lain.
b. Data laporan bulanan *usage* SMS Flexi untuk analisa data, diambil pada saat sebelum implementasi, dan sesudah implementasi.
c. Bahasa pemrograman yang dipergunakan berbeda-beda disesuaikan dengan ketersediaan bahasa pemrograman di setiap perangkat yang berkaitan dalam pembangunan aplikasi *anti spamming* ini.
d. Pengaruh aplikasi ini terhadap layanan SMS Telkom Flexi hasilnya akan ditinjau dari sisi penurunan presentase SMS penipuan, dan menurunnya *fraud* pendapatan pelanggan *postpaid* yang diakibatkan dari *service* SMS.
e. Aspek hukum tidak dimasukan dalam pembahasan materi.

1.5 METODE PENELITIAN

Mengingat masih sedikitnya kajian seputar *anti spamming* dalam dunia telekomunikasi khususnya tentang SMS, maka metode yang akan digunakan adalah metode *action research* (penelitian tindakan) yaitu metode penelitian yang dikembangkan bersama-sama antara peneliti dan *decision maker* tentang *variable-variable* yang dapat dimanipulasikan dan dapat segera digunakan untuk menentukan kebijakan, dimana peneliti dan *decision maker* bersama-sama menentukan masalah, membuat desain serta mengimplementasikan program-program tersebut.

Ciri utama dari penelitian tindakan adalah untuk memperoleh penemuan yang signifikan secara operasional sehingga dapat digunakan ketika kebijakan

dilaksanakan. Penelitian tindakan mengadakan rangka kerja penelitian empiris yang didasarkan pada observasi objektif pada masa sekarang untuk memecahkan masalah-masalah baru, serta praktis dan aktual dalam kegiatan-kegiatan kerja. Karena itu, penelitian tindakan mempunya sifat lebih *flexible*, dapat mengorbankan kepentingan kontrol demi adanya inovasi dan bekerja dengan *on the spot experimentation*. Penelitian tindakan bertujuan memberikan penemuan-penemuan yang praktis, sehingga kurang memberikan kontribusi terhadap ilmu pengetahuan.

Langkah-langkah yang akan dilakukan antara lain :

a. Merumuskan masalah dengan melakukan langkah :
   - Menganalisa faktor-faktor yang berpengaruh pada *spamming* SMS dan *fraud*.

b. Mengumpulkan data dengan melakukan langkah :
   - Menganalisa data historis komplen penipuan, historis *fraud* pada *billing collection* lewat data *usage* SMS diatas satu juta rupiah.

c. Mendesain aplikasi sekuriti tambahan dengan melakukan langkah :
   - Melakukan analisa SWOT.
   - Menganalisa rencana pembuatan aplikasi dan investasi perangkat.
   - Membuat algoritma pemrograman.

d. Implementasi aplikasi dengan melakukan langkah :
   - Instalasi *hardware* dan *software* Aplikasi
   - Pengetesan program aplikasi berupa pengetesan algoritma dan *load server* perangkat terkait.
   - Implementasi aplikasi pada seluruh *netwok* elemen terkait.

e. Analisis hasil implementasi dengan melakukan langkah :
   - Evaluasi penurunan SMS penipuan.
   - Evaluasi penurunan *fraud billing* SMS.

1.6 SISTEMATIKA PENELITIAN

BAB I PENDAHULUAN

Berisi latar belakang, perumusan masalah, tujuan penelitian, batasan masalah, metode penelitian, dan sistematika penelitian.

BAB II SHORT MESSAGE SERVICE DAN KONDISI EKSISTING

Berisi teori mengenai *short message service* dan analisa kondisi eksisting.

BAB III PERANCANGAN SISTEM DAN ALGORITMA ANTI SPAMMING SMS

Pada bab ini akan dijelaskan perancangan sistem dan algoritma aplikasi *anti spamming* SMS di *network* Telkom Flexi.

BAB IV HASIL IMPLEMENTASI DAN ANALISA

Bab ini ditunjukan hasil implementasi aplikasi *anti spamming* dan analisa performansi disisi perangkat, laporan SMS penipuan dari *customer care*, dan data *fraud billing* divre II.

BAB V KESIMPULAN

Bab ini merupakan penutup dalam pembahasan tesis.

BAB II
SHORT MESSAGE SERVICE DAN KONDISI EKSISTING

2.1 SHORT MESSAGE SERVICE

SMS pada CDMA 2000-1X merujuk kepada referensi 3GPP2 C.S0015-A ver 1.0 tanggal 11 Januari 2002 berbasis pada TIA/EIA 637B yang membahas pengiriman informasi dalam bentuk *text* dan *alphanumeric* untuk *paging, messaging,* dan *voice mail notification.*

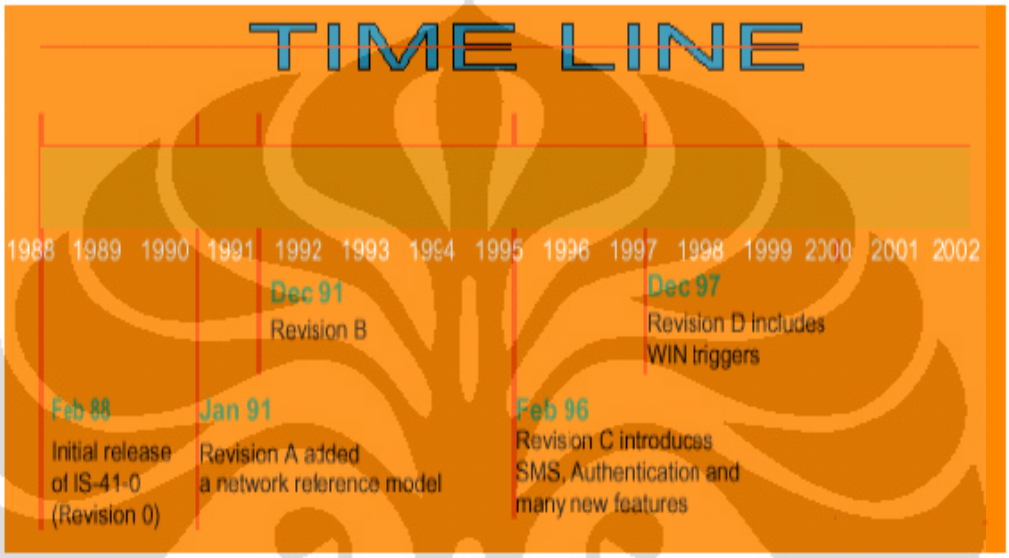
TIA/EIA adalah *Electrical Industries Association/Telecommunications Industry Association* merupakan salah satu standar international yang menjelaskan cara-cara dan prosedur interkoneksi yang harus dilakukan oleh perangkat selular berbasis radio dalam berinteraksi dengan perangkat selular lainnya yang berbeda.

IS-41 (ANSI-41) adalah salah satu standar internasional yang mengatur proses identifikasi dan authentikasi *users,* serta *routing calls* pada jaringan selular. standar ini juga mendefinisikan bagaimana *users* dapat diidentifikasi dan memungkinkan *users* dapat melakukan komunikasi dalam posisi *roaming* di jaringan selular yang berbeda.

Pada TIA/EIA/IS-41 *revision* D menjelaskan tentang hal-hal berikut ini :

- *Correction of some technical errors and the reformatting of the standard into ANSI format*
- *Released in successive phases, not all at once*
- *Reflects a shared industry interest to support government mandates (e.g. portability, E911).*
- *Meet the unique challenges of the evolving international market*
- *Definition for WIN Phase 1 (IS-771)b and WIN Phase 2 (IS-826)*

Berikut gambar 2.1 dibawah ini menjelaskan rentang periode revisi IS-41 dalam bentuk *time line* sampai pada revisi ke IS-41D yang sudah mengenali komunikasi *messaging* SMS pada jaringan selular, serta beberapa authentikasi baru dan fitur-fitur baru termasuk cara interkoneksi dengan perangkat *charging* WIN (*Wireless Intelligence Network*) pada authentikasi terkait.

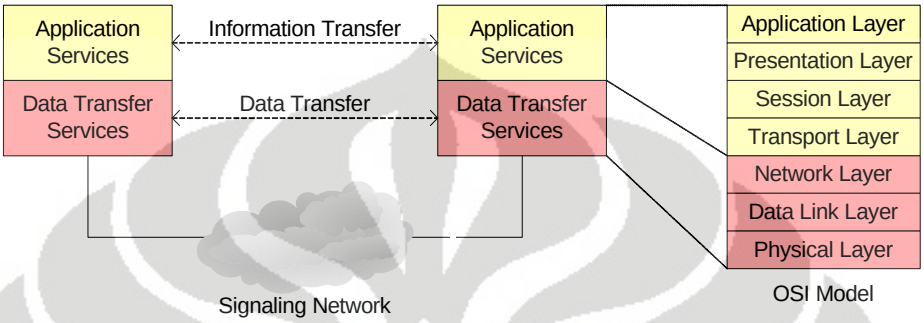


Gambar 2.1. Time Line TIA/EIA [3]

Beberapa contoh fitur-fitur baru pada TIA/EIA IS-41 *revision* D meliputi :

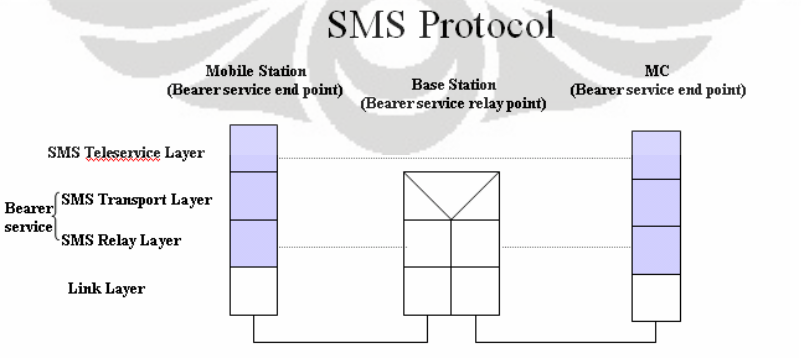
- *AuthenticationDirective*
- *AuthenticationFailureReport*
- *AuthenticationRequest*
- *AuthenticationStatusReport*
- *BaseStationChallenge*
- *CountRequest*
- *FeatureRequest*
- *FlashRequest*
- *InformationDirective*
- *InformationForward*
- *InterSystemPage*
- *InterSystemPage2*
- *InterSystemSetup*
- *LocationRequest*
- *OriginationRequest*
- *QualificationRequest*
- *RedirectionDirective*
- *RegistrationNotification*
- *RemoteFeatureControlRequest*
- *Authentication*
- *Basic Feature Processing*
- *MS Inactivity Reporting*

Gambar 2.2 adalah TIA/EIA IS-41 *signalling protocol achitecture* yang memiliki yang mengatur proses signaling didalamnya berkaitan dengan *information transfer* dan *data transfer* yang secara keseluruhan berkaitan pada aplikasi *messaging* pada jaringan selular yang berbeda.



Gambar 2.2. TIA/EIA-41 Signalling Protocol Architecture [3]

SMS *Teleservice* menyediakan *priority level, future delivery time, message expiration interval, future delivery time, message expiration interval,* dan *broadcast message* pada sisi *paging channel*. *Bearer service* memiliki fungsi untuk men*delivery message* antara MSC dan *mobile subscriber*, kemudian dalam menjalankan fungsinya *protocol bearer service* dibagi menjadi *transport* dan *relay layer*.



Gambar 2.3. SMS Protocol pada MS, BSS, MSC [3]

Gambar 2.3 diatas menjelaskan bahwa *Transport layer* merupakan *layer* terbesar dalam *bearer service*, karena *layer* ini memiliki tugas untuk me*manage end to end delivery message* dan meneruskan *message* yang dikirimkan atau diterima dari *transport layer* ke *layer* dibawahnya yaitu *relay layer*. *Transport layer* juga melakukan proses interpretasi tujuan, menambahkan *ruting info*, dan mem*forward delivery message* ke *relay layer*. *Relay layer* menyediakan *interfacing* antara *transport layer* ke *link layer* untuk membawa trafik *short message*, diantaranya adalah melanjutkan trafik dengan memberi alamat *ruting* ke MSC tujuan, menerima tugas dari *transport layer message* dan men*deliver message* tersebut ke tujuan yang ditentukan, menyediakan fungsi *error* untuk *transport layer* ketika *message* tidak dapat diteruskan ke tujuan, dan menerima *message* beserta *forward message* tersebut ke *transport layer*.

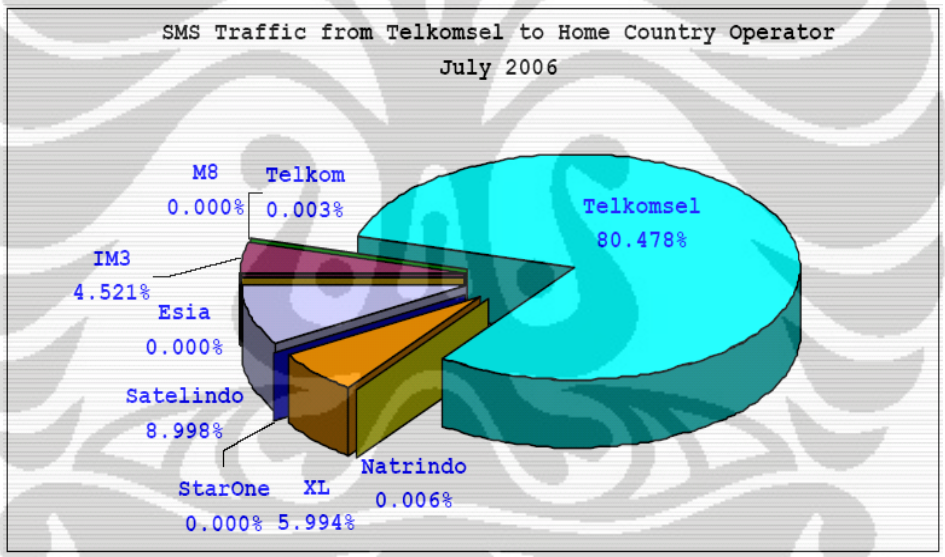
Pengunaan SMS pada awalnya bertujuan untuk dilakukannya pertukaran informasi dalam jumlah yang terbatas diantara dua pelanggan saja. Keterbatasan kapasitas SMS ini menjadi kelemahan utama SMS yang justru membatasi dirinya dengan perkembangan aplikasi selular lainnya seperti *download ringtone, download gambar*, dsb, sehingga aplikasi SMS mau tidak mau harus memisahkan diri dengan aplikasi baru lainnya yang mulai berkembang seperti MMS dan EMS.

Contoh penggunaan SMS pada aplikasi konsumen diantaranya adalah *service* SMS antara *person to person*, *information services*, *content service*, *download service*, dan *chat application*. Para konsumen dapat mengakses berbagai layanan-layanan tersebut untuk meng-*customize handset* mereka, baik untuk menerima informasi dari *remote server*, atau pertukaran pesan singkat antara rekan. Contoh penggunaan SMS pada aplikasi perusahaan diantaranya adalah *service vehicle positioning*, dan *remote monitoring*. Dan operator yang meyediakan layanan SMS, pada prinsipnya operator tersebut akan membangun suatu *network* SMS untuk mendukung suatu perangkat SMS *Center*, SMS *Center* dapat diklasifikasikan dengan SMSC *Core*, dan SMSC *Gateway*, serta beberapa aplikasi lainnya yang berkaitan dengan layanan SMS seperti *Message Waiting Indicator*, WAP *Push*, dan fitur-fitur lainya seperti *message submission* dan *message delivery, status report, reply path, addressing mode*, dan *validity period*.

2.2. KONDISI EKSISTING

Short Message Service (SMS) adalah sebuah layanan dasar yang memungkinkan pertukaran pesan pendek melalui *text* antar pelanggan, trial pertama kali pesan pendek melalui *text* ini terjadi pada tahun 1992 yang dilakukan pada operator jaringan GSM *Vodafone* di Inggris yang dilewatkan pada kanal *signalling*. Semenjak *trial* SMS tersebut sukses dilanjutkan dengan *lounching* komersial pertama kali *service* SMS pada tanggal 3 Desember 1992, trafik pemakaian SMS diseluruh dunia terus naik secara menakjubkan sampai dengan saat ini.

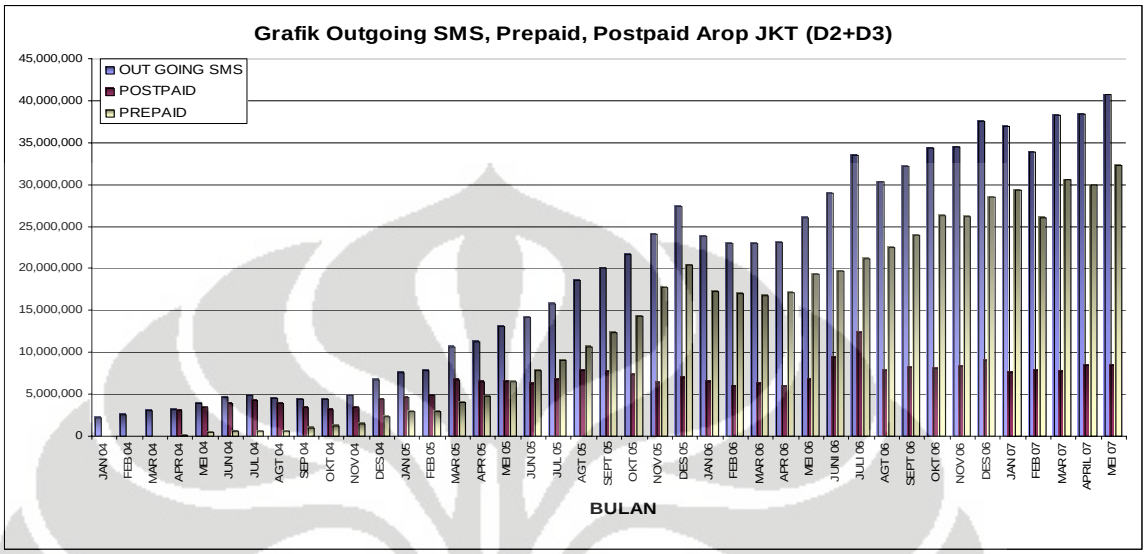
Berikut trafik SMS di PT. Telkomsel sebagai *leader* trafik SMS di Indonesia, pada bulan Juni 2006 sebagai berikut :



Gambar 2.4. Trafik Outgoing SMS dari Telkomsel [1]

Gambar 2.4 diatas terlihat bahwa dari perhitungan Telkomsel trafik *outgoing* yang menuju Telkom adalah sebesar 0.003%. Jika angka tersebut dikaitkan dengan data trafik dari sisi Telkom Flexi maka akan ditemukan jumlah total trafik SMS *outgoing* dari Telkomsel secara keseluruhan sudah mencapai lebih dari 100 juta SMS perhari [1].

Berikut trafik SMS di PT. Telkom Divisi Fix Wireless Area Divisi Jakarta yang membawahi Divisi Regional II dan III, selama periode 2004 sampai dengan 2007 sebagai berikut :

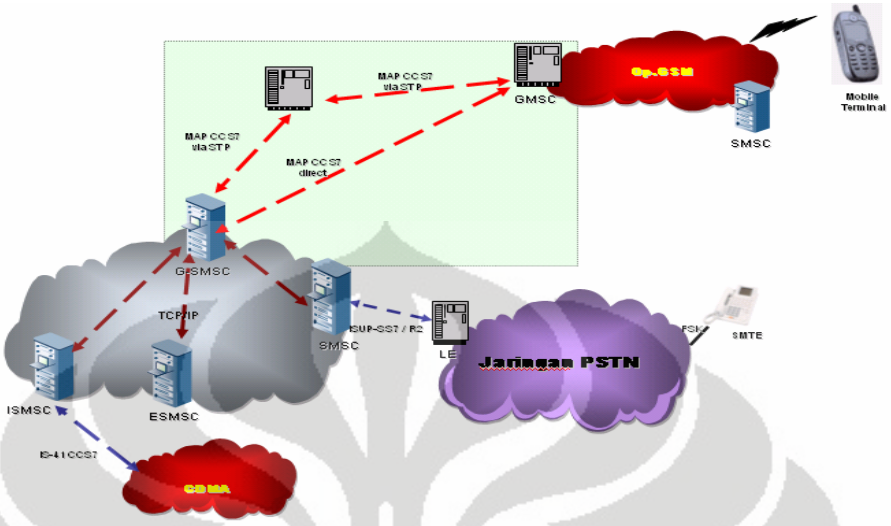


Gambar 2.5. Trafik Outgoing SMS dari Telkom Flexi Area Jakarta [3]

Trafik pada gambar 2.5 diatas menunjukan bahwa perkembangan pengguna SMS di Telkom Flexi masih terus tumbuh. Ditambah pula dengan sudah adanya teknologi signaling yang memungkinkan pertukaran SMS dilakukan pada *platform* teknologi yang berbeda baik dari GSM atau ke CDMA dan sebaliknya. Hal ini membuat trafik SMS menjadi semakin meningkat. Dalam GSM *phase-1* ETSI *technical spesification*, disebutkan bahwa SMS memungkinkan *mobile subscriber* dapat berkomunikasi dengan berbagai jaringan operator untuk melakukan pertukaran SMS. Strandarisasi yang dikeluarkan oleh ETSI saat ini juga sudah dimasukan dalam 3GPP *standart*, sehingga SMS yang pada awalnya lahir didalam jaringan GSM, saat ini sudah dapat digunakan pada jaringan CDMA dengan 3GPP2 *standard* [3].

Interfacing pertukaran SMS antara jaringan GSM dan CDMA dapat dimungkinkan dengan mengunakan perangkat berbasis TDM/SS7 yang menggunakan protokol MAP *(Mobile Application Part)* pada POI *(Point of Interconnection)* di SMSC *gateway* masing-masing operator, seperti yang

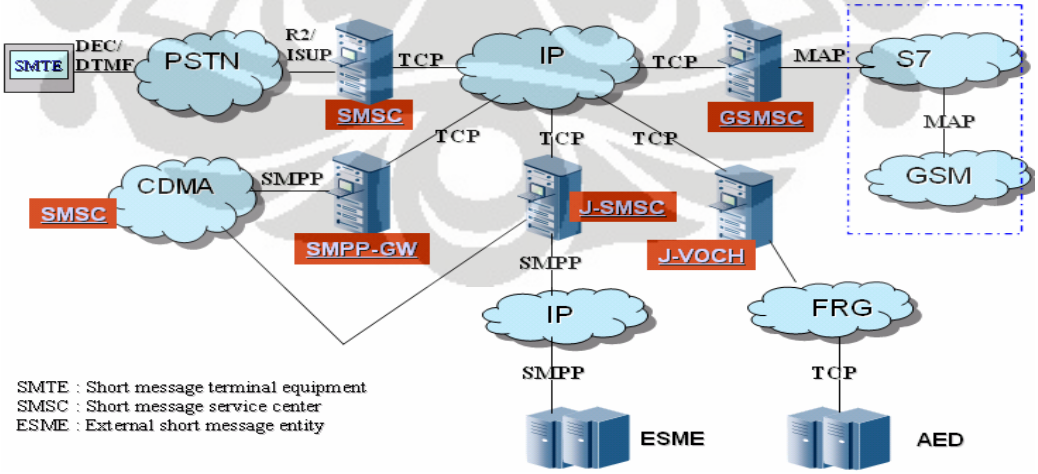
ditunjukan pada gambar 2.6 konfigurasi interkoneksi jaringan antara GSM dan CDMA dengan protokol MAP berikut ini :



Gambar 2.6. Konfigurasi SS7 MAP [4]

2.2.1. KONFIGURASI SMS FLEXI

Berikut adalah konfigurasi jaringan SMS di Telkom Flexi yang meliputi *node element*, protokol yang digunakan, media *transport*, dan interkoneksinya seperti ditunjukan pada gambar 2.7 berikut ini :



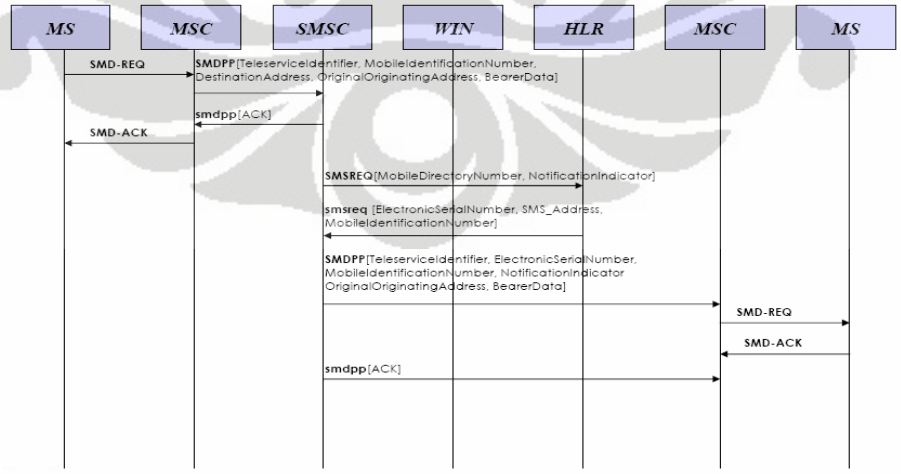
Gambar 2.7. Konfigurasi SMS di Telkom Flexi [4]

Dimana terdapat dua basis *signaling* yang digunakan dalam interaksi jaringan SMS internal Telkom Flexi yaitu SS7 *base* dan TCP/IP *base*. *Signalling* SS7 *base* digunakan pada interkoneksi antara SMSC dan jaringan CDMA yang meliputi MS (*mobile subscriber*), BTS (*Base Transceiver Station*), BSC (*Base Station Controller*), MSC (*Mobile Switch Center*), dan HLR (*Home Location Register*) dengan protocol IS-41, dan antara GSMSC dan jaringan GSM dengan protokol MAP. TCP/IP *base* digunakan pada interkoneksi antara SMSC dan SMS *Gateway* dengan protokol SMPP (*short message peer to peer*) versi 3.4.

Pada akhir tahun 2007 ini pula sedang dikerjakan *project* penambahan 2 *node* SMSC baru dan melakukan *upgrade signaling transport* dari sebelumnya SS7 *base* ke teknologi *Sigtran base* pada beberapa *node* SMSC yang mampu mengusung *signaling over* IP.

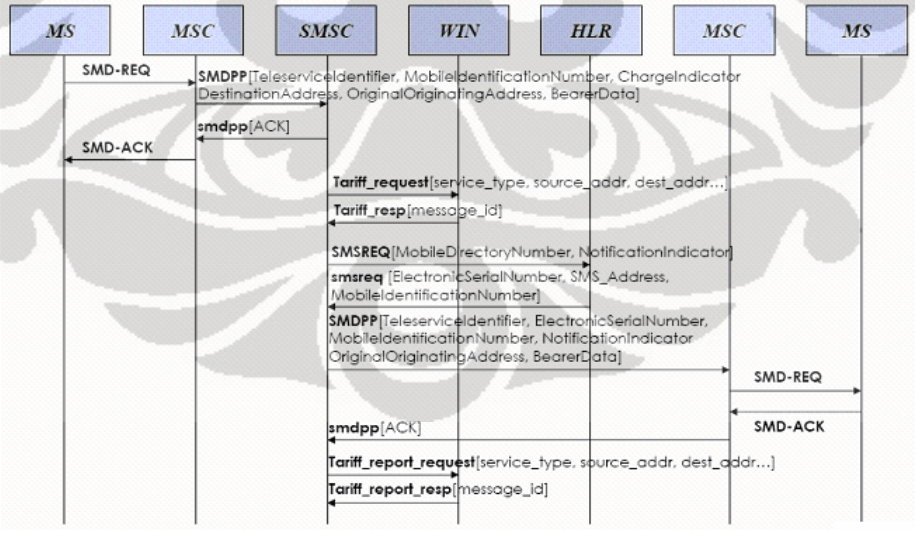
2.2.2. FLOW SMS PADA NETWORK FLEXI

Berikut adalah beberapa *flow* signaling SMS pada jaringan Telkom Flexi secara *end-to-end* yang meliputi *flow* signaling dari MS (*mobile subscriber*) dan antar perangkat SMS terkait dan perangkat *core* jaringan CDMA. Contoh pada gambar 2.8 menunjukan bagaimana *flow* yang terjadi pada saat MS melakukan proses pengiriman SMS sebagai berikut :



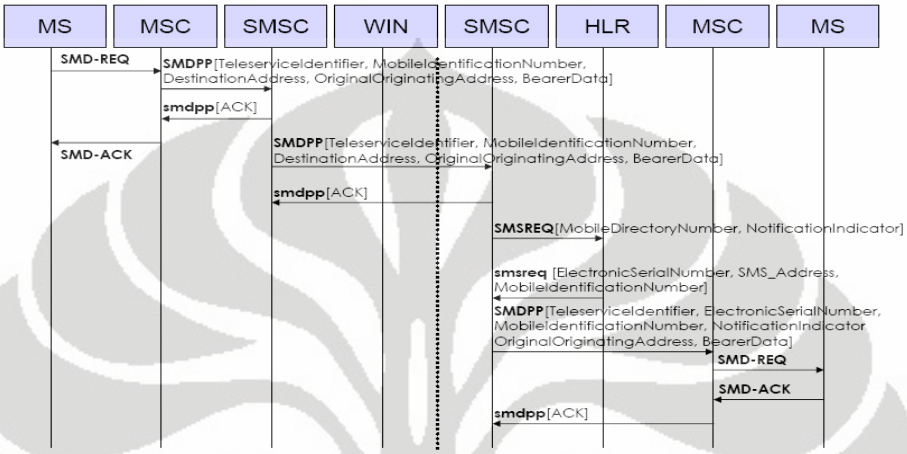
Gambar 2.8. Flow SMS From MS (Postpaid) to MS [4]

Penjelasan *flow* diatas adalah jika MS mengetik tombol SEND untuk melakukan pengiriman SMS, maka *handset* MS akan mengirimkan signaling SMDPP-*Request* (*Short Message Delivery Point to Point Request*) yang akan disalurkan oleh kanal BTS dan BSC menuju MSC terdekat kemudian oleh MSC akan dikenali ada permintaan *service non voice* dari MS berupa SMS dan selanjutnya melanjutkan proses SMDPP-*Request* tersebut ke SMSC. SMSC sebagai *short message center* akan menerima SMDPP-*Request* yang disampaikan dan mengirimkan balasan SMDPP-*Request ack* ke MSC sebagai tanda SMDPP-*Request* sudah diterima, kemudian MSC akan menginformasikan ke MS bahwa SMS telah diterima oleh SMSC. SMSC akan melanjutkan proses dengan melakukan pengecekan ke database pelanggan yang dituju di HLR (*home location register*) terkait dan jika kondisi MS tujuan normal secara *service* dan *handset* MS tujuan terdeteksi hidup. Maka SMSC akan mengirimkan SMDPP ke MSC terkait, dan MSC tersebut akan melanjutkan sampai MS tujuan, dan setelah SMDPP diterima oleh MS tujuan, maka MSC akan mengirimkan balasan bahwa SMDPP sudah sampai MS dan transaksi ditutup. Serta SMS akan di *drop* dari *buffer message* di SMSC.



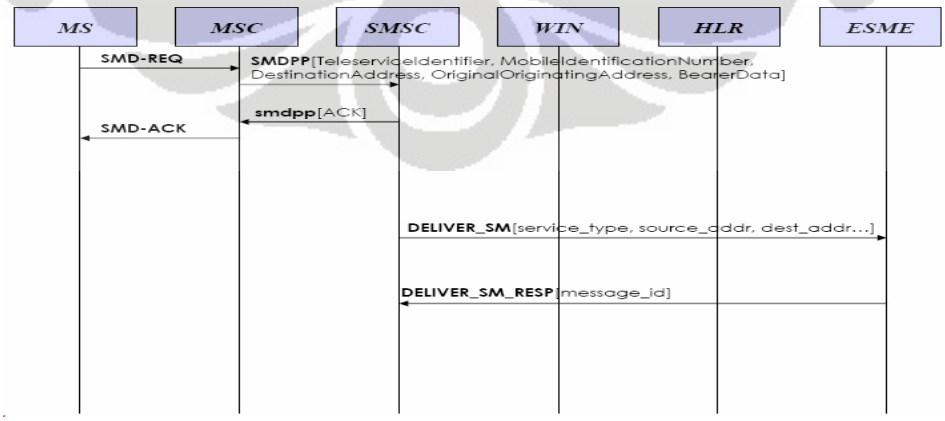
Gambar 2.9. Flow SMS From MS (Prepaid) to MS [4]

Penjelasan gambar 2.9 diatas hampir sama dengan penjelasan gambar 2.8 sebelumnya, namun ada tambahan *flow signalling* ke WIN untuk permintaan cek pulsa dalam bentuk *tariff request* sebelum SMS di *deliver* ke MS disebabkan jenis pelanggan yang mengirimkan SMS dikategorikan sebagai pelanggan *prepaid*.



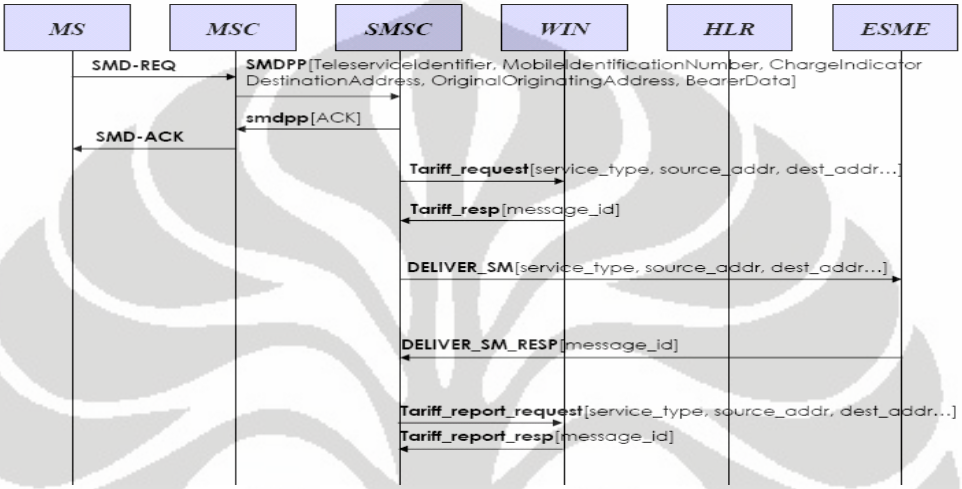
Gambar 2.10. Flow SMS From MS(Postpaid) to MS (One more SMSC) [4]

Penjelasan gambar 2.10 adalah flow SMS jika ada pengiriman SMS yang melalui 2 (dua) buah *node* SMSC atau lebih, dimana SMSC pertama yang menerima SMS akan langsung mengirimkan ke SMSC tujuan dan SMSC terakhir yang akan men*deliver* SMS ke MS dan jika MS pengirim kategori *postpaid*, maka *flow tariff request* ke WIN akan di *bypass*.



Gambar 2.11. Flow SMS From MS(Postpaid) to ESME [4]

Penjelasan gambar 2.11 adalah *flow* SMS dari SMSC awal menuju ESME *client* yang dapat berupa CP, PSTN, dan OLO dimana bentuk transaksi menuju ESME dilakukan pada *mode* transmisi TCP/IP. Sehingga fungsi SMSC juga dapat menkonversikan *signalling* SMS dari bentuk TDM *based* menjadi TCP/IP *based* dan sebaliknya. Jika MS pengirim kategori *postpaid* maka flow ke WIN di *bypass*.



Gambar 2.12. Flow SMS From MS(Prepaid) to ESME [4]

Penjelasan gambar 2.12 adalah mirip dengan penjelasan dari gambar 2.11 sebelumnya bahwa *flow* SMS dari SMSC awal menuju ke ESME *client* yang dapat berupa CP, PSTN, dan OLO bentuk transaksi menuju ESME dilakukan pada *mode* transmisi TCP/IP. Sehingga fungsi SMSC juga dapat menkonversikan *signalling* SMS dari bentuk TDM *based* menjadi TCP/IP *based* dan sebaliknya. namun perbedaan ada pada *tariff request* ke WIN karena MS pengirim kategori *prepaid*.

2.2.3. CDR FORMAT SMSC

Dibawah ini adalah format CDR (*Call Data Record*) pada SMSC Telkom Flexi yang akan terkait langsung dengan aplikasi *anti spamming* SMS yang akan dikembangkan pada tesis berikut ini :

Tabel 2.1. Format CDR SMSC [4]

A	B	C	D	E	F	G	H	I	J	K	L	M

Field	Field Name	Length(byte)	Total length(byte)
A	Message Type Indicator	2	2
B	Calling Address	20	22
C	Called Address	20	42
D	Submit Time	12	54
E	Delivery Time	12	66
F	Attempt Count	3	69
G	Success/Fail	1	70
H	Prepaid/Postpaid	5	75
I	FailReason	5	80
J	Delivery Report Message Flag	1	81
K	Message Identifier	8	89
L	Calling Mobile Identification Number	10	99
M	Called Mobile Identification Number	10	108

Setiap transaksi SMS yang masuk ke SMSC akan dicatat status transaksinya baik *delivery* SMS yang sukses maupun yang gagal kedalam *database* internal dan selanjutnya akan dibuatkan CDR. Setiap 1 (satu) transaksi SMS akan dibuat 1 (satu) baris CDR dalam bentuk kode-kode sebanyak 108 karakter. Setiap kode CDR tersebut memiliki informasi tertentu dan baru dapat diartikan setelah membandingkannya dengan dokumentasi format CDR yang telah ditentukan pada table 2.1.

a. Message Type Indicator

From \ To	MSC	GW	Premium	SMSC	ESME	Type
MSC	11	12	13	14	15	Outgoing
GW	21	00	00	22	00	Incoming (Free of charge)
Premium	31	00	00	32	00	Incoming
SMSC	41	42	43	00	44	Transit (Calling Routing)
ESME	51	00	00	52	00	Incoming

a.1. *Outgoing case*

11- *Outgoing (From MSC to MSC)*
12- *Outgoing (From MSC to GW)*
13- *Outgoing (From MSC to Premium)*
14- *Outgoing (From MSC to SMSC)*
15- *Outgoing (From MSC to ESME)*

a.2. *Incoming case*

21- *Incoming (From GW to MSC) – Free of charge*
22- *Incoming (From GW to SMSC)*
31- *Incoming (From Premium to MSC)*
32- *Incoming (From Premium to SMSC)*
51- *Incoming (From ESME to MSC)*
52- *Incoming (From ESME to SMSC)*

a.3. *Transit case*

41- *transit (From SMSC to MSC) - Calling Routing*
42- *transit (From SMSC to GW) - Calling Routing*
43- *transit (From SMSC to Premium) - Calling Routing*
44- *transit (From SMSC to ESME) - Calling Routing*

b. *Calling Address (Originating Address)*

Value	*Description*
Space	*Nothing*
others	*Calling number digit*

c. *Called Address (MDN)*

Value	*Description*
Space	*Nothing*
Others	*Called Number digit*

d. *Submit Time*

Value	*Description*
YYMMDDhhmmss	*Submit time*

(YY=year, MM=month, DD=day, hh=hour, mm=minute, ss=second)

e. *Delivery Time*

Value	*Description*
YYMMDDhhmmss	*Delivery time*

(YY=year, MM=month, DD=day, hh=hour, mm=minute, ss=second)

f. Attempt Count

Value	*Description*
Digit	*Attempt Counts*

g. Success/Fail Status

Value	*Description*
1	*Success*
0	*Fail*

h. Prepaid/Postpaid

Value	*Description*
00000	*Postpaid Subscriber*
00001	*Prepaid Subscriber*

i. Fail Reason : Set last Fail Reason Code

Value	*Description*
Digit	*Fail Reason Code*

If RETRY event is occurred, fail reason code is replaced old fail-reason by the last fail-reason.

j. Delivery Report Status

Value	*Description*
0	*Message*
1	*Delivery Report*

k. Message Identification

Value	*Description*
xxxxxxxx	*Message Indentifier is ID message combine using numeric and hexadecimal in 8 character.*

l. Calling Mobile Identification Number

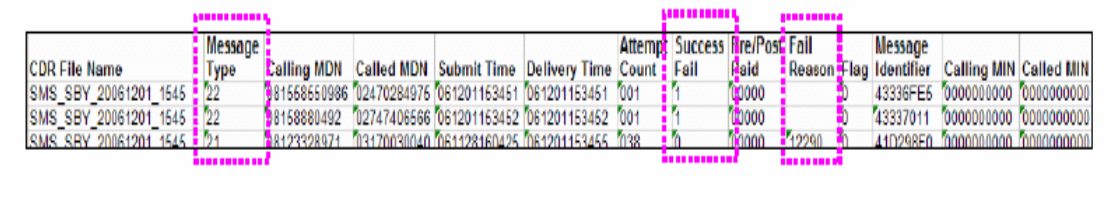
Value	*Description*
xxxxxxxx	*Calling MIN as A number*

m. Called Mobile Identification Number

Value	*Description*
xxxxxxxx	*Called MIN as B number*

Berikut contoh format CDR SMS Flexi dari penjelasan diatas sebagai berikut

Tabel 2.2 Contoh format CDR SMS Flexi [4]



CDR File Name	Message Type	Calling MDN	Called MDN	Submit Time	Delivery Time	Attempt Count	Success Fail	Pre/Post Paid	Fail Reason	Flag	Message Identifier	Calling MIN	Called MIN
SMS_SBY_20061201_1545	22	081558660986	02470284976	061201163451	061201153451	001	1	00000		0	43336FE5	0000000000	0000000000
SMS_SBY_20061201_1545	22	08158880492	02747406566	061201163452	061201153452	001	1	00000		0	43337011	0000000000	0000000000
SMS_SBY_20061201_1545	21	08123328971	03170030040	061128160425	061201153455	038	0	00000	12290	0	41D298E0	0000000000	0000000000

Penjelasan dari contoh CDR diatas adalah sebagai berikut :

- Kolom pertama CDR *File Name* SMS_SBY_20061201_1545 adalah CDR dari mesin SMSC lokasi Surabaya yang diambil dari transaksi SMS tahun 2006 bulan 12 tanggal 01 pukul 15 menit 45.
- Kolom kedua *message type* 22 adalah transaksi SMS berasal dari *Gateway* GSM menuju ke SMSC Surabaya berupa *incoming* SMS.
- Kolom ketiga *calling* MDN 081558660986 adalah nomor pengirim dari GSM Indosat.
- Kolom keempat *called* MDN 02470284976 adalah nomor penerima flexi yang berada di kode area 024 Semarang.
- Kolom kelima *submit time* 061201153451 adalah waktu diterimanya SMS dari nomor *calling* MDN pada SMSC Surabaya pada tahun 2006 bulan 12 tanggal 01 jam 15 menit 34 dan detik ke 51.
- Kolom keenam *delivery time* 061201153451 adalah waktu dikirimkannya SMS tersebut ke *called* MDN pada tahun 2006 bulan 12 tanggal 01 pukul 15 menit 34 dan detik ke 51.
- Kolom ketujuh *attempt count* 001 adalah satu kali proses *sending* oleh SMSC, SMS tersebut berhasil di *forward* oleh SMSC Surabaya ke *called* MDN
- Kolom kedelapan *success/fail* 1 adalah status SMS tersebut berhasil tidaknya terkirim ke *called* MDN.
- Kolom kesembilan *Prepaid/Postpaid* 00000 adalah status *calling* MDN yang dinyatakan sebagai *postpaid*.
- Kolom kesepuluh *fail reason* kosong adalah status kegagalan pengiriman SMS ke *called* MDN dimana terlihat bahwa tidak ada status *fail reason*.

- Kolom kesebelas *flag delivery report* menunjukan bahwa SMS tersebut adalah berbentuk *message* bukan berbentuk SMS *delivery report*.
- Kolom kedua belas *message identifier* adalah *MessageID* SMS yang bersifat unik yang diproduksi oleh SMSC dalam bentuk *hexadecimal*.
- Kolom ketiga belas *calling* MIN adalah fasilitas tambahan yang dipersiapkan untuk *charging* SMS Flexi Combo.
- Kolom keempatbelas *called* MIN adalah fasilitas yang dipersiapkan untuk *charging* SMS Flexi Combo.

BAB III
PERANCANGAN SISTEM DAN ALGORITMA

ANTI SPAMMING SMS

3.1. DATA SEBELUM IMPLEMENTASI

3.1.1. DATA COMPLAIN HANDLING

Berikut adalah data *complain handling* yang masuk di *helpdesk* Telkom Flexi Area Divisi Jakarta yang menerima keluhan dari para pelanggan Telkom Flexi yang berada dalam wilayah layanan divre II Jakarta, Bogor, Depok, Tangerang, Bekasi dan sekitarnya serta eskalasi *complain* dari *Call Center* 147 selama periode bulan Juni 2007 sebagai berikut dibawah ini :

Tabel 3.1. Rekap Complain Handling Divre II Juni 2007 [22]

NO	URAIAN	DIVRE-II
1	Pengaduan Proses Aktivasi	5485
2	Pengaduan RUIM	5156
3	Pengaduan Gangguan Network	4854
4	Pengaduan Buka Tutup Isoliran	141
5	Pengaduan Tagihan/Billing	10
6	Pengaduan Fitur TELKOMFlexi	272
7	Pengaduan Akses TELKOMFlexi (Dial)	2029
8	Pengaduan SMS	1584
9	Pengaduan pulsa / voucher	935
10	Pengaduan product Flexi	6871
11	Lain-lain	67
	JUMLAH	27404

Dari tabel 3.1 diatas selama bulan Juni 2007 ada sebanyak 27.404 pengaduan yang berasal dari pelanggan divre II dengan jumlah pengaduan tentang SMS mencapai 1.584 pengaduan atau 5,78% dari keseluruhan pengaduan.

3.1.2. DATA PENGADUAN SMS

Rincian detil pengaduan SMS yang berasal dari para pelanggan Divre II dapat dilihat pada tabel 3.2 dibawah ini :

Tabel 3.2. Rekap Pengaduan SMS Divre II Juni 2007 [22]

NO	PENGADUAN SMS	DIVRE II
1	SMS berulang	678
2	SMS rusak/cacat	98
3	SMS Penipuan	71
4	SMS tidak sampai	29
5	SMS content	323
6	SMS Provisioning Combo	385
	JUMLAH	**1584**

Dari tabel 3.2 diatas total pengaduan SMS yang berjumlah 1.584, sebanyak 71 pengaduan atau 4,48 % adalah pengaduan mengenai SMS penipuan.

Dari informasi pelanggan yang melaporkan tentang pengaduan SMS penipuan tersebut *helpdesk* mendata nomor-nomor yang melakukan indikasi SMS penipuan dan berikut adalah asal usul pengirim SMS penipuan berasal dari nomor Flexi dan OLO seperti ditunjukan dalam tabel 3.3 dibawah ini :

Tabel 3.3. Rekap Data Penipuan SMS Divre II Juni 2007 [22]

NO	PENGIRIM SMS PENIPUAN	DIVRE II
1	Dari Internal Flexi	65
2	Dari External Flexi	6
	JUMLAH	**71**

Kemudian diperoleh informasi lanjutan bahwa dari 71 pengaduan SMS penipuan tersebut 91,55% berasal dari nomor Flexi dan sisanya 8,45% berasal dari nomor operator lain. Proses *cross check* dilanjutkan lagi dengan membandingkan dengan data SMSC maka didapatlah kombinasi nomor dan isi *content* SMS yang membuktikan bahwa nomor-nomor yang diadukan oleh pelanggan tersebut adalah benar-benar merupakan *content* SMS penipuan.

3.1.3. DATA CONTENT SMS

Berikut adalah data hasil pengecekan dari sisi SMS *Center* terhadap nomor-nomor yang melakukan SMS penipuan seperti yang dilaporkan oleh pelanggan dapat ditunjukan pada Tabel 3.4 dibawah ini :

Tabel 3.4. Nomor-Nomor Pengirim SMS Penipuan dan Content SMS [22]

No	FLEXI	CONTENT SMS
1	02168606912	Halo TELKOMSEL nomor simPATI Anda sbg Peraih GEBYAR HADIAH'TELKOMSELpoin'Hub Call Center : 021-70302367Pengirim:777
2	02170297542	Plgn Yth no sim card anda mendp,kan HADIAH TELKOMSEL poinU/info,sgr,hub:0817790896KABAG PROMOSI PT.TELKOMSEL
3	02170297659	Selamat!!No'SimCard Anda telahmemenangkan!!TELKOMSELpointhp.2006,HarapHub Call Center:021-6855 8185021-6855 8187Pengirim:777
4	02170297662	Plg yth.Selamat!No'Flexi anda tlh men-dpt hadiahmelalui programRegistrasi telkomU/info harap hub:021-6850 4973021-9383 5758pengirim:4444
5	02170302686	Plgn Yth no sim card anda men-dpt,kan HADIAHTELKOMSELpoinU/info,sgr,hub:021-30678465KABAG-PROMOSIPT.TELKOMSELPengirim: 222
6	02168611143	Pemberitahuan: No'simPATI'Anda meraih,Hadiah Rp.18'juta"Dari KUIS-KDI'3'Hub Sekretariat(TPI) 021-70634518 021-93684029pengirim:+6288
7	02170297663	Plgn yth,Selamat No'Flexi Anda!!! Meraih "UNDIAN" Melalui program Registrasi "flexi" U/info harap hub:021-68080464021-68142933Pengirim:4444
8	02168650126	Selamat, No.FlexiAnda, berhasilmdpt-kan undianmelalui Programregistrasi Flexi"U/info harap hub:(021-98019747)(021-68634457)Pengirim:4444
9	02170297663	Plgn yth,Selamat No'Flexi Anda!!! Meraih "UNDIAN" Melalui program Registrasi "flexi" U/info harap hub:021-68080464021-68142933Pengirim:4444
10	02168620934	Pelanggan YTH,No.FLEXI ANDA..!!!mendptkan undianmelalui ProgramRegistrasi Flexi,Utk info hub:021-6854-9927021-6865-9939Pengirim:4444
11	02170297705	Plgn YTH ! No.HpAnda Sbg PeraihMega Bonus dariTELKOMSEL POINCek tunai Rp35jtU/ Info Hubungi :021-93082447021-68637247Pengirim:777
12	02170297674	Plgn YTH ! No.HPAnda Sbg PeraihMega Bonus dariTELKOMSEL POINCek tunai Rp.25jtHub. Call Center:021-93834857021-70297674Pengirim:777
13	02170297681	SELAMAT!! andamen-dpt"GRANDPRIZE"_simPATIRp.45juta dari:PT.TELKOMSELHub; Call Center:021 6867 7414021 6864 6927Pengirim:777
14	02170302353	SELAMAT!! andamen-dpt"GRANDPRIZE"_simPATIRp.45juta dari:PT.TELKOMSELHub; Call Center:021 6864 6927021 6867 7414Pengirim:777
15	02170310465	SELAMAT!! andamen-dpt"GRANDPRIZE"_simPATIRp.45juta dari:PT.TELKOMSELHub; Call Center:021 6867 7414021 6864 6927Pengirim:777
16	02168723830	Selamat,No.SimCard Anda telahMeraih UNDIANTELKOMSELpoin u/info sgr HUB: TELKOMSEL 021-9308 3997 021-9288 3447 Pengirim:222
17	02168723831	Selamat,No.SimCard Anda telahMeraih UNDIANTELKOMSELpoin u/info sgr HUB: TELKOMSEL 021-9351 3497 021-9351 3498 Pengirim:222
18	02168723832	Selamat,No.SimCard Anda telahMeraih UNDIANTELKOMSELpoin u/info sgr HUB: TELKOMSEL 021-9351 3497 021-9351 3498 Pengirim:222
19	02168723849	Selamat,SIM CARD Anda mendptkan DANA Rp.35juta Dr.KDI-3 Kontes Dangdut TPI Silahkan HUB: 02198012887 085880742562 02168723849
20	02168620936	Plgn Yth no sim card anda men-dpt,kan HADIAHTELKOMSELpoinU/info,sgr,hub:021-30643696KABAG-PROMOSIPT.TELKOMSELPengirim:222
21	02168620684	Plng Yth: No sim Card anda meraih Hadiah TelkomselPoint Thn.2006Untuk informasiHub,Call Center:021-93886515021-93397295Pengirim:777
22	02170755336	Selamat! No'simCard anda telahmen-dpt hadiahGRAND PRIZE drMobile 8 u/ infoHub Call Center:021-9336 4291021-9336 5992Pengirim:6868
23	02170310468	Pelanggan Yth.No' Flexi anda!!men-dpt hadiahmelalui programRegistrasi flexi.U/info harap hub:021-6850 4973021-9383 5758Pengirim:4444
24	02168723846	Plgn Yth,No.SIM CARD,anda meraih Gebyar "POIN HADIAH",dr TELKOMSEL.Hrp, Hub Call Center: (021) 68525853 (021) 68525854 Pengirim:222
25	02168723827	Plgn Yth,No.SIM CARD,anda meraih Gebyar "POIN HADIAH",dr TELKOMSEL.Hrp, Hub Call Center: (021) 68525853 (021) 68525854 Pengirim:222
26	02170310472	Plg Yth, No.Flexianda terpilih sbgPemenang undianMelalui programregistrasi Flexi.U/info harap hub:(021)68549927(021)68659939Pengirim:4444
27	02170310469	Plgn TELKOMflexiNo.CDMA anda sbgPeraih NOMINASIHADIAH TAHAPANPT.TELKOMflexiHub Call Center :021 70302366021 Pengirim:8888
28	02170308440	Plgn TELKOMflexiNo.CDMA anda sbgPeraih NOMINASI HADIAH TAHAPAN "PT.TELKOMflexi" Hub Call Center :021-70302366021-70302367Pengirim:8888
29	02168620936	Plgn Yth no sim card anda men-dpt,kan HADIAHTELKOMSELpoinU/info,sgr,hub:021-30643696KABAG-PROMOSIPT.TELKOMSELPengirim:222
30	02170308107	Selamat,No.Sim Card Anda telah Meraih UNDIAN TELKOMSELpoin u/info sgr HUB: TELKOMSEL 021-9288 3447 021-9308 3997 Pengirim: +222
31	02170308110	Plgn YTH: No.HP Anda Sbg Peraih Mega Bonus Dari TELKOMSELpoin Cek Tunai Rp25jt Hub.Call Center: 021-68602577 021-30618794 Pengirim: +777
32	02170298915	Pelanggan YthNo,Flexi anda!!menang undianMelalui programRegistrasi flexi.U/Ket harap hub:021-93394357021-93389457Pengirim:4444
33	02170298914	Pelanggan YthNo,Flexi anda!!menang undianMelalui programRegistrasi flexi.U/Ket harap hub:021-93394357021-93389457Pengirim:4444
34	02170331401	Selamat,No.SimCard Anda telahMeraih UNDIANTELKOMSELpoin u/info sgr HUB: TELKOMSEL 021-6864 8567 021-6864 1625 Pengirim:222
35	02170331402	Halo TELKOMSEL nomor simPATI Anda sbg Peraih'TELKOMSELpoin'Cek Tunai 25 jutaHub Call Center : 021-70302366021-70302367Pengirim:777
36	02170331405	Pemberitahuan: No'simPATI'Anda meraih,Hadiah Rp.18'juta"Dari KUIS-KDI'3'Hub Sekretariat(TPI) 021-70634518 021-93684029pengirim:+6288
37	02170331408	Plg yth.Selamat!No'Flexi anda tlhmen-dpt hadiahmelalui programRegistrasi telkomU/info harap hub:021-9383 5758021-9322 0257pengirim:4444
38	02170331416	Halo TELKOMSEL nomor simPATI Anda sbg Peraih'TELKOMSELpoin'Cek Tunai 25 jutaHub Call

		Center : 021-70300967021-70302367Pengirim:777
39	02168608245	Plgn YTH ! No.HpAnda Sbg PeraihMega Bonus dariTELKOMSEL POINCek tunai Rp35jtU/ Info Hubungi :021-6862960708521327026 7Pengirim:+777
40	02170308115	Selamat,No.Sim Card Anda telah Meraih UNDIAN TELKOMSELpoin u/info sgr HUB: TELKOMSEL 021-9308 3997 021-9288 3447 Pengirim: 222
41	02170276917	SELAMAT!! Anda men-dpt" Grand Prize"simPATI" Rp.45 jt dari:PT. TELKOMSELpoin Hub;Call Center: 021 6867 7414 021 6864 6927 Pengirim: 777
42	02170276918	SELAMAT!! anda men-dpt"GRAND PRIZE"_simPATI JITU Rp. 45jt dr PT.TELKOMSEL Hub Call Center: 021 930 66552 021 930 66553 Pengirim: +777
43	02170276921	SELAMAT! Anda men-dpt"GRAND PRIZE"_simPATI JITU.Rp,45jt dr PT.TELKOMSEL Hub; Call Center: 021-30612648 021-30612649 Pengirim: +777
44	02170297078	Pemberitahuan: No'simPATI'Anda meraih,Hadiah Rp.18'juta"Dari KUIS-KDI'3'Hub Sekretariat(TPI) 021-70634518 021-93684029 pengirim: +6288
45	02170298913	Selamat! No.Flexi anda telah meme- nangkan GRAND PRIZE.Rp.21jt, dr Telkom Flexi" hrp Hub, Call Center: (021-68628679) (021-68651839) From: TELKOM
46	02170331396	Plgn YTH ! No.HP Anda Sbg Peraih Mega Bonus dari TELKOMSEL POIN Cek tunai Rp.25jt Hub. Call Center: 021-93834857 021-70331396 Pengirim: +777
47	02170331417	Slamat,SIM CARD Anda mendptkan DANA Rp.35juta Dr.KUIS KDI-3 kontes Dangdut TPI.Silahkan HUB 02198012887 085880742562 Pengirim: 6288
48	02170348023	Selamat ! Anda "memenangkan" GEBYAR HADIAH TELKOMSELpoin Priode thp ke-2 Edisi thn - 2006 Rp.35jt+Pls.1jt Hub Call Center: 021-68242847
49	02170331397	Selamat! No.HP Anda mendapat Bonus Rp.25 jt Dari KDI Kontes Dangdut TPI.Hub: Sekretariat KDI3 021-70302257 085213156627 Pengirim: +6288
50	02170331410	Plgn/Yth!"Anda mendpt undian <simPATI"Jitu> :Rp.25juta,dari TELKOMSELpoin Utk/Info, hub Call Center :021-68455747 Pengirim: TELKOMSEL
51	02170308121	Selamat,No.Sim Card Anda telah Meraih UNDIAN TELKOMSELpoin u/info sgr HUB: TELKOMSEL 021-9351 3497 021-9351 3498 Pengirim: 222
52	02170276917	SELAMAT!! Anda men-dpt" Grand Prize"simPATI" Rp.45 jt dari:PT. TELKOMSELpoin Hub;Call Center: 021 6867 7414 021 6864 6927 Pengirim: 777
53	02170348686	Plng Yth: No sim Card anda meraih Hadiah Telkomsel Point Thn.2006 Untuk informasi Hub,Call Center: 021-93886515 021-93397295 Pengirim: 777
54	02170331405	Pemberitahuan: No'simPATI'Anda meraih,Hadiah Rp.18'juta"Dari KUIS-KDI'3'Hub Sekretariat(TPI) 021-70634518 021-93684029 pengirim: +6288
55	02170276917	SELAMAT!! Anda men-dpt" Grand Prize"simPATI" Rp.45 jt dari:PT. TELKOMSELpoin Hub;Call Center: 021 6867 7414 021 6864 6927 Pengirim: 777
56	02170331215	SELAMAT!! Anda men-dpt" Grand Prize"simPATI" Rp.45 jt dari:PT. TELKOMSELpoin Hub;Call Center: 021 6867 7414 021 6864 6927 Pengirim: 777
57	02170276918	SELAMAT!! anda men-dpt"GRAND PRIZE"_simPATI JITU Rp. 45jt dr PT.TELKOMSEL Hub Call Center: 021 930 66552 021 930 66553 Pengirim: +777
58	02170332114	Plgn YTH: No.HP Anda Sbg Peraih Mega Bonus Dari TELKOMSELpoin Cek Tunai Rp25jt Hub.Call Center: 021-68602577 021-30618794 Pengirim: +777
59	02170331396	Plgn YTH ! No.HP Anda Sbg Peraih Mega Bonus dari TELKOMSEL POIN Cek tunai Rp.25jt Hub. Call Center: 021-93834857 021-70331396 Pengirim: +777
60	02170276918	SELAMAT!! anda men-dpt"GRAND PRIZE"_simPATI JITU Rp. 45jt dr PT.TELKOMSEL Hub Call Center: 021 930 66552 021 930 66553 Pengirim: +777
61	02170331396	SELAMAT!! anda men-dpt"GRAND PRIZE"_simPATI JITU Rp. 45jt dr PT.TELKOMSEL Hub Call Center: 021 930 66552 021 930 66553 Pengirim: +777
62	02170276921	SELAMAT! Anda men-dpt"GRAND PRIZE"_simPATI JITU.Rp,45jt dr PT.TELKOMSEL Hub; Call Center: 021-30612648 021-30612649 Pengirim: +777
63	02170297672	Plgn YTH ! No.Hp Anda Sbg Peraih Mega Bonus dari TELKOMSEL POIN Cek tunai Rp35jt U/ Info Hubungi : 021-93082447 021-68628948 Pengirim: +777
64	02170331396	Plgn YTH ! No.HP Anda Sbg Peraih Mega Bonus dari TELKOMSEL POIN Cek tunai Rp.25jt Hub. Call Center: 021-93834857 021-70331396 Pengirim: +777
65	02170331412	Halo TELKOMSEL nomor simPATI Anda sbg Peraih 'TELKOMSELpoin' Cek Tunai 25 juta Hub Call Center : 021-70302366 021-70302367 Pengirim: 777
NO	**GSM**	**CONTENT SMS**
1	081322959471	SELAMAT!! andamen-dpt"GRANDPRIZE"§simPATIRp.45juta dari:PT.TELKOMSELHub; Call Center:021 6867 7417021 6867 7414Pengirim:777
2	081355564011	Plgn TELKOMflexiNo.CDMA anda sbgPeraih NOMINASIHADIAH TAHAPANPT.TELKOMflexiHub Call Center :021 70302366021 70302367Pengirim:8888
3	081322959471	(1/2)SELAMAT!! andamen-dpt"GRANDPRIZE"§simPATIRp.45juta dari:PT.TELKOMSELHub; Call Center:021 9355 4315021 6867 7414Pengirim:777
4	081381603759	Plng Yth:No.sim card anda meraih "GRAND PRIZE" kejutan bulanan, dr.TELKOM Flexi Hub.Call center:021-68540284021-68540285Pengirim:147
5	02193507415	Selamat! No.HP Anda mendapat Bonus Rp.25 jt Dari KDI Kontes Dangdut TPI.Hub: Sekretariat KDI3 085214023117 085213156627 Pengirim: +6288
6	02130619071	Pelanggan Yth No,Flexi anda!! menang undian Melalui program Registrasi flexi. U/Ket harap hub: 021-93394357 021-93389457 Pengirim: 4444

Terlihat dari tabel 3.4 bahwa isi *content* SMS diatas sudah sangat jelas menunjukan indikasi dan bukti yang kuat bahwa SMS tersebut dapat diketegorikan kedalam jenis SMS penipuan dan jika diamati kata-kata yang paling

sering muncul dalam *content* SMS penipuan maka dapat kita rangking jumlah *text*-nya dari yang paling sering digunakan dalam tabel 3.5 dibawah ini :

Tabel 3.5. Text Yang Sering Muncul Pada Content SMS Penipuan [18]

NO	TEXT SMS PENIPUAN	COUNT	SAMPLE	RATE(%)
1	Pengirim	68	71	95,77%
2	Anda	67	71	94,37%
3	Sim	42	71	59,15%
4	Call Center	38	71	53,52%
5	Selamat	32	71	45,07%
6	Yth	31	71	43,66%
7	Plg	26	71	36,62%
8	Plgn	23	71	32,39%
9	Peraih	18	71	25,35%
10	Meraih	18	71	25,35%
11	Undian	16	71	22,54%
12	Grand	16	71	22,54%
13	Prize	16	71	22,54%
14	Card	14	71	19,72%
15	Simcard	6	71	8,45%
16	Gebyar	4	71	5,63%
17	Plng	3	71	4,23%

Text yang sering digunakan oleh para *spammer* SMS penipuan ini sangat membantu penulis dalam melakukan perancangan desain aplikasi *anti spamming* SMS dimana *text-text* tersebut akan ditambahkan fitur *screening text.*

Penentuan *keyword* pada aplikasi *screening text* dilakukan dengan kriteria tertentu sebagai berikut :

- *Text* yang dimasukan ke dalam *list keyword* adalah *text* yang paling sering digunakan dalam *content* SMS penipuan, dan *screening text* minimal harus memenuhi 2 kombinasi *text* yang didefinisikan, jika hanya satu kombinasi maka SMS tidak akan diblokir.

- *Text* yang dimasukan ke dalam *list keyword* adalah *text* yang tidak lazim digunakan oleh pelanggan normal.

- *Text* yang tidak dimasukan ke dalam *list keyword* adalah *text* yang dinilai sering digunakan oleh pelanggan *non spamming* lainnya.

3.1.4. DATA BILLING DAN JUMLAH SPAM SMS

Dari ke-65 nomor *spamming* yang berasal dari nomor Flexi dilanjutkan dengan *cross check* terhadap data tunggakan *billing* dan data SMSC maka diperoleh kombinasi antara nomor *spamming*, jumlah tunggakan SMS dan jumlah *Spam* SMS yang dikirimkan oleh para *spammer* seperti ditunjukan pada tabel 3.6 berikut ini :

Tabel 3.6. Jumlah Tunggakan SMS dan Jumlah SMS Spam Penipuan [21]

No	FLEXI	TUNGGAKAN SMS (RP)	JUMLAH SPAM (SMS)
1	02168606912	1.444.225	29.474
2	02170297542	3.268.503	66.704
3	02170297659	6.498.524	132.623
4	02170297662	3.925.278	80.108
5	02170302686	3.578.480	73.030
6	02168611143	6.714.906	137.039
7	02170297663	1.917.629	39.135
8	02168650126	2.186.348	44.619
9	02170297663	1.917.629	39.135
10	02168620934	1.591.275	32.475
11	02170297705	1.894.709	38.668
12	02170297674	2.852.270	58.210
13	02170297681	2.561.470	52.275
14	02170302353	3.897.836	79.548
15	02170310465	24.774.865	505.609
16	02168723830	3.589.560	73.256
17	02168723831	2.227.770	45.465
18	02168723832	2.222.058	45.348
19	02168723849	5.513.635	112.523
20	02168620936	4.993.818	101.915
21	02168620684	4.189.938	85.509
22	02170755336	1.855.319	37.864
23	02170310468	21.871.279	446.353
24	02168723846	1.923.927	39.264
25	02168723827	2.330.719	47.566
26	02170310472	17.950.552	366.338
27	02170310469	17.377.967	354.652
28	02170308440	13.563.918	276.815
29	02168620936	4.993.818	101.915
30	02170308107	4.049.679	82.647
31	02170308110	1.890.993	38.592
32	02170298915	1.212.888	24.753
33	02170298914	2.914.269	59.475
34	02170331401	3.860.497	78.786
35	02170331402	8.231.382	167.987
36	02170331405	1.931.270	39.414
37	02170331408	2.130.081	43.471
38	02170331416	8.643.087	176.390
39	02168608245	4.261.673	86.973
40	02170308115	2.494.337	50.905
41	02170276917	2.846.382	58.089
42	02170276918	2.888.273	58.944

43	02170276921	2.437.426	49.743
44	02170297078	1.082.266	22.087
45	02170298913	1.259.684	25.708
46	02170331396	1.862.804	38.016
47	02170331417	4.761.062	97.165
48	02170348023	5.715.532	116.644
49	02170331397	5.559.651	113.462
50	02170331410	1.681.800	34.322
51	02170308121	2.762.048	56.368
52	02170276917	2.846.382	58.089
53	02170348686	11.364.986	231.938
54	02170331405	1.931.270	39.414
55	02170276917	2.846.382	58.089
56	02170332115	4.430.505	90.418
57	02170276918	2.888.273	58.944
58	02170332114	3.967.827	80.976
59	02170331396	1.862.804	38.016
60	02170276918	2.888.273	58.944
61	02170331396	1.862.804	38.016
62	02170276921	2.437.426	49.743
63	02170297672	4.251.687	86.769
64	02170331396	1.862.804	38.016
65	02170331412	2.361.804	48.200
	JUMLAH	**295.908.536**	**6.038.950**

Dari tabel 3.6. diatas dapat diketahui bahwa semua nomor diatas menunggak pembayaran tagihan rekening telepon, dan jumlah keseluruhan tunggakan SMS yang berasal dari ke-65 nomor flexi tersebut adalah sebesar Rp. 295.908.536,- dan jumlah *spam* SMS yang berhasil dikirimkan oleh para *spammer* SMS ke jaringan SMS Telkom Flexi adalah sebanyak 6.038.950 SMS selama periode bulan Juni 2007.

Dari angka tersebut dapat diketahui besarnya nilai rata-rata, maximum, minimum tunggakan SMS dan jumlah SMS seperti ditunjukan pada tabel 3.7 berikut ini :

Tabel 3.7. Average, Maximum, Minimum Tunggakan SMS dan Spam SMS [21]

	TUNGGAKAN SMS	JUMLAH SPAM SMS
JUMLAH	295.908.536	6.038.950
AVERAGE	4.552.439	92.907
MAXIMUM	24.774.865	505.609
MINIMUM	1.082.266	22.087

Dari tabel 3.7 diatas dapat digambarkan bahwa *resources* jaringan Telkom Flexi yang jumlahnya terbatas dan seharusnya digunakan untuk kepentingan

bisnis perusahaan ternyata dipergunakan oleh para *spammer* SMS secara tidak bertanggung jawab.

Salah satu bentuk tidak bertanggung jawab adalah melakukan perbuatan yang disengaja dari para *spammer* dalam memanipulasi data registrasi pelanggan pada masa awal pendaftaran supaya identitasnya sulit dideteksi oleh Telkom jika terjadi proses penagihan *billing* pemakaian telepon di kemudian hari, diantaranya dengan menggunakan identitas palsu, alamat palsu dan sebagainya.

Kemudian dari ke-65 nomor pengirim SMS *spamming* di *cross check* dengan *database* pelanggan divre II ditemukan hasil bahwa ke-65 nomor tersebut 100% *postpaid*, berikut jumlah piutang perusahaan sebesar Rp. 295.908.536,- semuanya menjadi *fraud billing* dan tidak dapat dicairkan oleh manajemen Telkom.

Dari penjelasan diatas dapat diketahui bahwa walaupun jumlah keluhan SMS penipuan relatif kecil hanya sebesar 4,48% dari keseluruhan pengaduan SMS yang masuk selama bulan Juni 2007, namun jika ditelaah lebih lanjut keluhan yang jumlahnya sedikit tersebut ternyata cukup menggerogoti keuangan perusahaan berupa *bad debt* dalam pencairan piutang perusahaan yang mencapai Rp. 295.908.536,- dalam waktu sebulan saja.

3.2. ANALISA SWOT

Analisa SWOT adalah analisis situasi yang mengidentifikasi berbagai faktor secara sistematis untuk merumuskan strategi. Analisis ini didasarkan pada logika yang dapat memaksimalkan kekuatan (*Strenghts*) dan peluang (*Opportunities*) namun secara bersamaan dapat meminimalkan kelemahan (*Weaknesses*) dan ancaman (*Threats*). Proses pengambilan keputusan strategis selalu berkaitan dengan pengembangan misi, tujuan, strategi, dan kebijakan perusahaan saat ini dan proses penyusunan perencanaan strategis dilakukan melalui tiga tahap analisis yang meliputi tahap masukan, tahap analisis, dan tahap pengambilan keputusan.

3.2.1 TAHAP MASUKAN

Tahap ini masukan merupakan suatu kegiatan pengklasifikasian dan pra-analisis. Pada tahap ini data dapat dibedakan menjadi dua, yaitu data eksternal dan data internal. Berikut adalah resume hasil *questioner* penentuan faktor eksternal pada tabel 3.8 dimana *resume* berasal dari hasil questioner dengan responden sebanyak 12 (duabelas) orang yang dipilih oleh penulis secara cermat dari *level* manajemen di Telkom Flexi yang ada kaitannya dengan SMS *Spamming*, *Customer Service* dan *Fraud Billing* dengan hasil resume sebagai berikut :

Tabel 3.8. Resume Hasil Questioner Penentuan Faktor External [23]

NO	INDIKATOR/FAKTOR	JUMLAH RESPONDEN				TOT	IDX	BBT	RTG	BBT X RTG
		4	3	2	1					
A	**PELUANG**									
1	Meningkatkan pendapatan SMS	5	4	3	0	12	38	0,118	4	0,472
2	Pertumbuhan pelanggan TelkomFlexi	5	4	3	0	12	38	0,118	4	0,472
3	Investasi pada infrastruktur TelkomFlexi	3	4	3	2	12	32	0,099	3	0,298
4	Jumlah Pelanggan yang mencapai 5jt ssf	3	6	1	2	12	34	0,106	3	0,317
5	Operator FWA terbesar di Indonesia	4	5	1	2	12	35	0,109	3	0,326
B	**ANCAMAN**									
1	Maraknya Laporan tentang SMS penipuan	3	4	2	3	12	29	0,090	-2	-0,180
2	Citra perusahaan 'brand Flexi' menurun	3	6	1	2	12	26	0,081	-2	-0,161
3	Nomor whitelist banyak yang membayar	3	3	4	2	12	29	0,090	-3	-0,270
4	Rasa tidak nyaman bagi penerima SPAM	4	1	5	2	12	29	0,090	-3	-0,270
5	Muncul korban dari Spam SMS Penipuan	2	3	4	3	12	32	0,099	-3	-0,298
	TOTAL						**322**	**1,00**		**0,705**

Dari tabel 3.8 resume hasil *questioner* penentuan faktor external diatas diperoleh nilai dari aspek peluang dan ancaman adalah sebesar 0,705.

Kemudian dari nilai aspek kekuatan dan ancaman yang merupakan faktor internal *resume* hasilnya dapat dilihat pada tabel 3.9 berikut ini :

Tabel 3.9. Resume Hasil Questioner Penentuan Faktor Internal [23]

NO	INDIKATOR/FAKTOR	JUMLAH RESPONDEN				TOT	IDX	BBT	RTG	BBT X RTG
		4	3	2	1					
A	**KEKUATAN**									
1	SDM yang memiliki kompetensi	3	4	2	3	12	31	0,104	3	0,311
2	Dukungan Manajemen	2	6	2	2	12	32	0,107	3	0,321
3	Data pengirim nomor Spam	4	6	2	0	12	38	0,127	3	0,381
4	Performansi Perangkat memadai	3	5	4	0	12	35	0,117	3	0,351
5	Interoperability perangkat mendukung	3	3	5	1	12	32	0,107	2	0,214
B	**KELEMAHAN**									
1	Flexi Combo dengan nomor temporer	2	8	1	1	12	25	0,084	-2	-0,167
2	Cek manual isi content SMS	3	2	6	1	12	29	0,097	-3	-0,291
3	Jangkauan Flexi yang luas 200 kota	4	6	2	0	12	22	0,074	-2	-0,147
4	Sosialisasi akibat Spam masih kurang baik	4	1	5	2	12	29	0,097	-3	-0,291
5	Kerjasama dengan pihak berwajib kurang	3	4	5	0	12	26	0,087	-3	-0,261
	TOTAL						**299**	**1,00**		**0,421**

Dari tabel 3.9 *resume* hasil *questioner* penentuan faktor internal diatas diperoleh nilai dari aspek kekuatan dan kelemahan adalah sebesar 0,421.

Berikut adalah cara penghitungan nilai aspek internal dan eksternal dan penentuan nilai total (TOT), nilai *index* (IDX), nilai bobot (BBT) dan hasil *rating* (RTG) berdasarkan dari hasil survey sebagai berikut :

- Pada bagian faktor internal terdapat dua aspek yang ditinjau yaitu kekuatan dan kelemahan, sedangkan pada faktor eksternal terdapat dua aspek yang ditinjau yaitu peluang dan ancaman.
- Masing-masing aspek terdiri dari lima *point* yang harus dinilai oleh responden.
- Setiap *point* diberikan pilihan penilaian dari angka 1 sampai 4 (berdasarkan pada keterangan nilai survey), yang harus dipilih responden berdasarkan pendapatnya masing-masing.

- Pada aspek kekuatan *point* pertama “SDM yang memiliki kompetensi” didapat jumlah yang memilih angka 4 ada 3 orang, angka 3 ada 4 orang, angka 2 ada 2 orang, dan angka 1 ada 3 orang, sehingga hasilnya adalah : (4 x 3) + (3 x 4) + (2 x 2) + (1 x 3) = 31 angka ini merupakan nilai *index*. Rumus ini berlaku juga untuk aspek peluang.
- Pada aspek kelemahan dan ancaman ada sedikit perbedaan untuk menentukan nilai *index* yaitu dengan membalik pilihan penilaian untuk perhitungannya. Pada aspek kelemahan *point* pertama “Flexi Combo dengan nomor temporer” didapat jumlah yang memilih angka 4 ada 2 orang, angka 3 ada 8 orang, angka 2 ada 1 orang, angka 1 ada 1 orang sehingga hasilnya adalah : (1 x 2) + (2 x 8) + (3 x 1) + (4 x 1) = 25.
- Pada faktor internal seluruh nilai *index* dari aspek kekuatan dan kelemahan dijumlah sehingga didapat total nilai *index* yaitu 299. Begitu pula pada faktor eksternal seluruh nilai *index* dari aspek peluang dan ancaman dijumlah sehingga didapat total nilai *index* yaitu 322.
- Cara penentuan bobot faktor internal yaitu dengan membagi nilai *index* dengan total nilai *index*, missal pada aspek kekuatan *point* pertama didapat nilai index 31 maka bobotnya adalah : 31 / 299 = 0,104. Begitu seterusnya sampai 10 *point*. Total bobot pada faktor internal haruslah berjumlah 1. Hal ini berlaku juga pada cara penentuan bobot faktor eksternal.
- Cara penentuan rating dari masing-masing *point* adalah dengan memilih nilai terbanyak yang dipilih responden, missal aspek kekuatan *point* pertama yang paling banyak dipilih adalah nilai 3 maka *rating*nya adalah 3. Hal ini juga berlaku juga untuk aspek peluang.
- Maka nilai bobot x *rating* untuk aspek kekuatan *point* pertama adalah 0,104 x 3 = 0,311.
- Cara penentuan *rating* untuk kelemahan dan ancaman penilaiannya dibalik dan diberi tanda minus, misal yang terbanyak dipilih adalah 3 maka nilai *rating*nya adalah -2.
- Maka nilai bobot x *rating* untuk aspek kelemahan untuk aspek kelemahan *point* pertama adalah 0.084 x (-2) = -0,167.

- Nilai bobot x *rating* dijumlahkan seluruhnya (baik internal maupun eksternal), nilai inilah yang menjadi acuan pada matrik *Grand Strategy*.

3.2.2. TAHAP ANALISIS

Setelah mengumpulkan semua informasi yang berpengaruh dan diperoleh nilai faktor internal dan eksternal maka nilai tersebut akan dijadikan acuan penulis dalam matrik *Grand Strategy*. Namun sebelum itu bantuan model kuantitatif perumusan strategi matrik SWOT juga diperlukan untuk menentukan langkah-langkah strategi dalam mengatasi permasalahan *spamming* SMS tersebut seperti yang dijelaskan dalam matrik SWOT berikut ini :

Tabel 3.10. Matrik SWOT [23]

SW / OT	STRENGTH (S)	WEAKNESS (W)
	SDM yang memiliki kompetensi Dukungan Manajemen Data pengirim nomor Spam Performansi Perangkat memadai Interoperability perangkat mendukung	Flexi Combo dengan nomor temporer Cek manual isi content SMS Jangkauan layanan Flexi yang luas 200 kota Sosialisasi akibat Spam masih kurang baik Kerjasama dengan pihak berwajib kurang
OPPORTUNITY (O)	**STRATEGI SO**	**STRATEGI WO**
Meningkatkan pendapatan SMS Pertumbuhan pelanggan TelkomFlexi Investasi pada infrastruktur TelkomFlexi Jumlah Pelanggan yang mencapai 5jt ssf Operator FWA terbesar di Indonesia	Memacu terus pertumbuhan trafik SMS dan menekan SMS spamming dengan membuat mekanisme anti spam dengan ketersediaan perangkat dan dukungan dari manajemen	Sosialisasi kepada seluruh pelanggan akan bahaya laten spamming sms lewat channel divisi regional diseluruh Indonesia
THREATHS (T)	**STRATEGI ST**	**STRATEGI WT**
Maraknya Laporan SMS penipuan Citra perusahaan 'brand Flexi' menurun Nomor whitelist banyak yang membayar Rasa tidak nyaman bagi penerima SPAM Muncul korban dari Spam SMS Penipuan	Menjaga citra perusahaan dengan Mem-broadcast ke seluruh pelanggan secara periodik untuk mengabaikan SMS yang berindikasi penipuan	Melaporkan nomor spam kepada pihak berwajib dari perbuatan SMS penipuan dan membuat database blacklist dan Whitelist untuk keperluan internal

Strategi SO

Mendukung pertumbuhan trafik SMS Flexi diikuti dengan menekan seminimal mungkin pertumbuhan trafik SMS *spamming* yang tidak diharapkan terkait dengan semakin gencarnya investasi perusahaan dibidang infrastruktur

CDMA yang akan dibangun pada tahun mendatang yang didukung oleh gencarnya program-program marketing untuk mempertinggi jumlah pelanggan dengan mengembangkan mekanisme *anti spamming* SMS.

Strategi ST

Melaporkan nomor-nomor pengirim *spamming* SMS kepada pihak berwajib sebagai antisipasi hukum akibat dari perbuatan SMS penipuan dan membuat database *blacklist* dan *whitelist* untuk keperluan internal.

Strategi WO

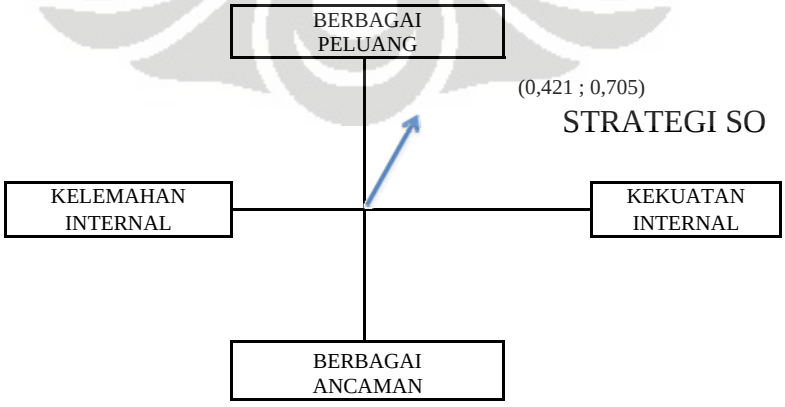
Penanganan terhadap SMS *spamming* masih belum ditangani dengan baik selama ini oleh perusahaan dan pemerintah sehingga diperlukan sosialisasi kepada para *customer* tentang bahaya laten dari SMS penipuan untuk menghindari hal-hal yang tidak diinginkan.

Strategi WT

Bekerja sama dengan pihak berwajib terhadap nomor-nomor yang melakukan *spamming* SMS penipuan dengan harapan pelakunya dapat dilacak keberadaannya, dapat tertangkap dan tidak terulangi lagi dikemudian hari.

3.2.3. TAHAP PENGAMBILAN KEPUTUSAN

Hasil perhitungan pada resume tahap masukan mengindikasikan bahwa strategi yang diambil adalah strategi SO (*Strength-Opportunity*) seperti ditunjukan pada gambar 3.1 dibawah ini :



Gambar 3.1. Matrik Grand Strategy [23]

Matrik *grand strategy* diatas menunjukan nilai yang dihasilkan berada pada kuadran I dimana sumbu x = 0,421 dan sumbu y = 0,705 hal ini merupakan situasi yang sangat menguntungkan karena perusahaan/manajemen yakin dan memiliki peluang serta kekuatan untuk menghadapi masalah yang ada. Sehingga strategi yang harus diterapkan dalam kondisi ini adalah mendukung strategi SO *Strength-Opportunity* (agresif).

Strategi SO yang akan dijalankan yaitu mendukung pertumbuhan trafik SMS Flexi diikuti dengan menekan seminimal mungkin pertumbuhan trafik SMS *spamming* yang tidak diharapkan, terkait dengan gencarnya investasi perusahaan dibidang infrastruktur Flexi pada tahun-tahun mendatang dan didukung dengan program-program *marketing* dalam rangka mempertinggi jumlah pelanggan Flexi dengan mengembangkan suatu mekanisme *anti spamming* SMS di jaringan SMS Telkom Flexi.

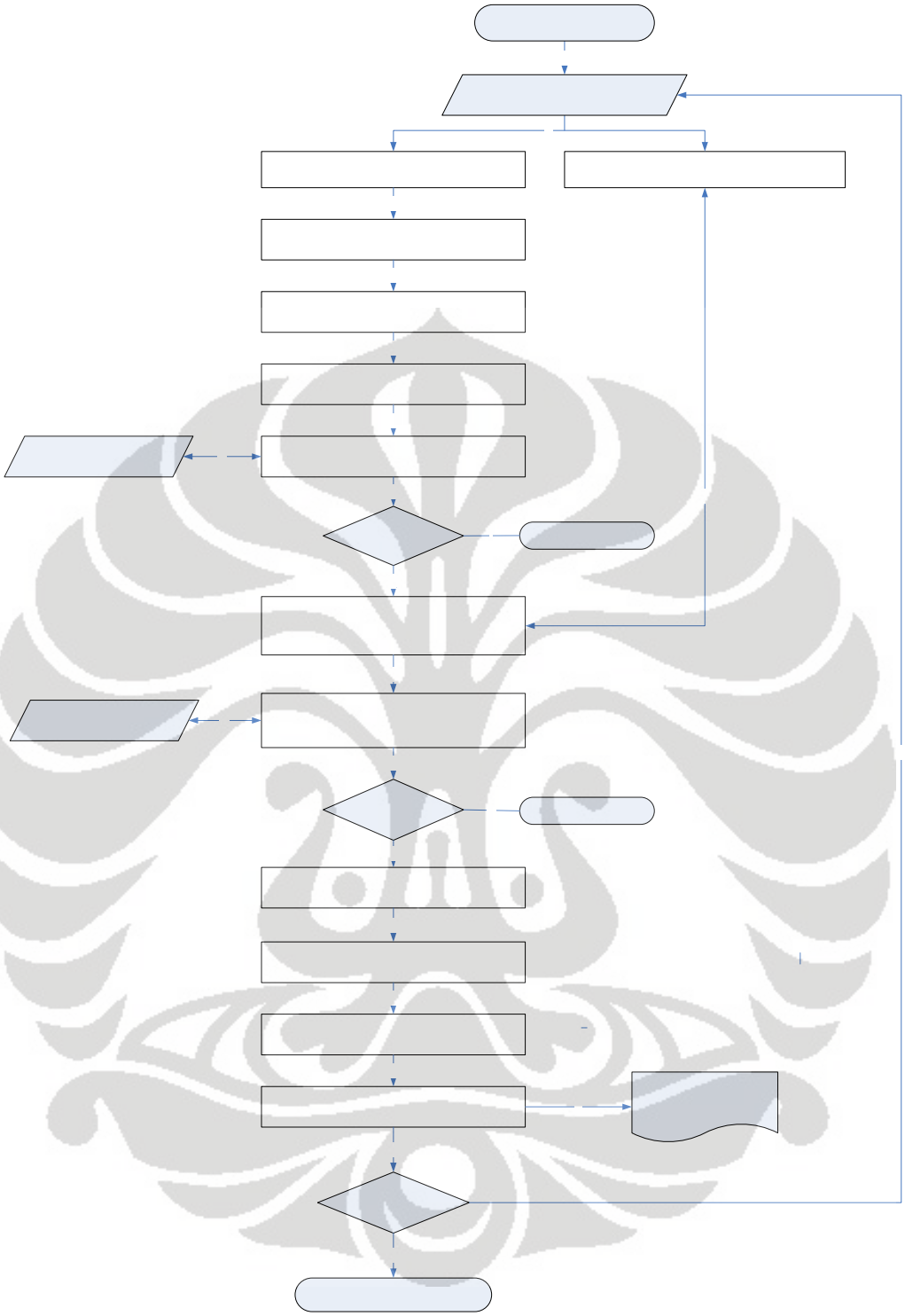
3.3. MODEL APLIKASI

Model aplikasi yang ditawarkan dan dibuat memiliki kombinasi *input* dan *output* sebanyak 12 (dua belas) langkah dari mulai *start* sampai dengan *stop*.

Secara umum model aplikasi *anti spamming* ini memiliki 2 (dua) kriteria inti sebagai berikut yaitu :

- Melakukan pengecekan jumlah frekuensi trafik *originating* SMS yang melebihi *threshold* yang ditentukan.
- Melakukan pengecekan *content* SMS dengan *keyword* yang telah didefinisikan.

Disamping itu model ini juga ada fitur *whitelist* untuk memberi izin kepada nomor-nomor yang telah didaftarkan oleh administrator SMSC untuk melakukan transaksi *spamming*.



Gambar 3.2. Model Aplikasi Anti Spamming SMS

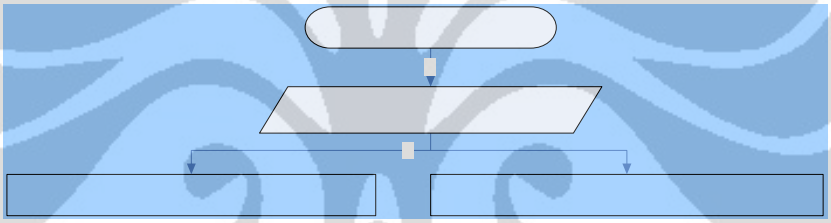
Model aplikasi yang ditawarkan dan dibuat memiliki kombinasi *input* dan *output* sebanyak 12 (dua belas) langkah dari mulai *start* sampai dengan *stop*.

Secara umum model aplikasi *anti spamming* ini memiliki 2 (dua) kriteria inti sebagai berikut yaitu :

- Melakukan pengecekan jumlah frekuensi trafik *originating* SMS yang melebihi *threshold* yang ditentukan.
- Melakukan pengecekan *content* SMS dengan *keyword* yang telah didefinisikan.

Disamping itu model ini juga ada fitur *whitelist* untuk memberi izin kepada nomor-nomor yang telah didaftarkan oleh administrator SMSC untuk melakukan transaksi *spamming*. Berikut dibawah ini adalah penjelasan langkah-langkah desain model aplikasi *anti spamming* SMS sebagai berikut :

3.3.1. LANGKAH KE-1

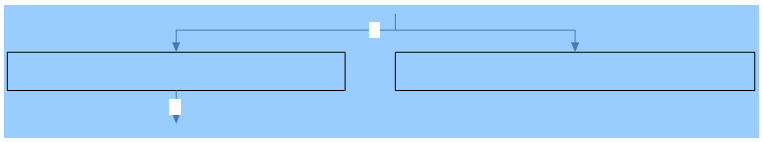


Gambar 3.3. Model Anti Spamming SMS Langkah ke-1 [18]

Aplikasi bekerja diawali dengan menjalankan program di internal proses SMS *Center* yang dibuat dalam bentuk *shell script* untuk melakukan proses pengambilan data CDR dan data *history Content* SMS. dan eksekusi dilaksanakan oleh *operating system* SMSC yang memiliki fungsi *crontab*.

Input	*File shell script* disimpan pada *crontab operating system* SMSC.
Proses	Melakukan kompresi *tar file* data CDR dan mengambil data *history content* SMS setengah jam terakhir.
Output	Data CDR dan data *content* SMS dalam bentuk kompresi.

3.3.2. LANGKAH KE-2

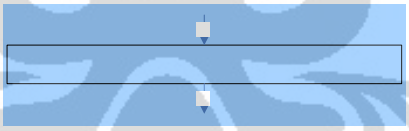


Gambar 3.4. Model Anti Spamming SMS Langkah ke-2 [18]

Data CDR diambil secara periodik setiap setengah jam dengan menggunakan kompresi *tar file*, dan data *content* SMS diambil secara periodik dari *table MySql* SMSC dengan FTP ke server aplikasi *anti spamming* SMS.

Input	Data CDR dan data *content* SMS dalam bentuk kompresi.
Proses	Mengumpulkan data CDR dan data *content* SMS dari seluruh SMSC dalam setengah jam terakhir dan digabungkan menjadi satu *file* kompresi.
Output	1. Data CDR dalam satu *file* kompresi. 2. Data *content history* SMS

3.3.3. LANGKAH KE-3

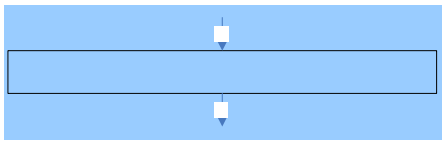


Gambar 3.5. Model Anti Spamming SMS Langkah ke-3 [18]

Data dalam bentuk kompresi diproses selanjutnya dikakukan dekompresi dan siap diparsing untuk mencari data yang perlukan dan menyisihkan data yang tidak diperlukan.

Input	Data CDR dan data *content* SMSC dalam satu file kompresi.
Proses	Dekompresi *tar file* dan *upload* data CDR ke Oracle menggunakan SQLloader ke Table Master dengan *parsing Message Identifier*, dan *Calling Mobile Identification Number*.
Output	Table SQL Master berisi data *Message Identifier* dan *Calling Mobile Identification Number*.

3.3.4. LANGKAH KE-4

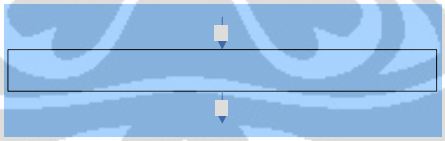


Gambar 3.6. Model Anti Spamming SMS Langkah ke-4 [18]

Proses didalam Oracle untuk mencari dan menghitung frekuensi kemunculan data *Calling Mobile Identification* Number. Dimana *Calling Mobile Identification Number* adalah identifikasi identik menghitung *usage* SMS Flexi Reguler dan Flexi Combo.

Input	Table SQL Master berisi data *Message Identifier* dan *Calling Mobile Identification Number*.
Proses	Menghitung frekuensi kemunculan *Calling Mobile Identification Number*, dan ke dalam *table query* baru.
Output	*Table query* yang berisikan 3 (dua) *field Message Identifier*, *Calling Mobile Identification Number*, dan Frekuensi.

3.3.5. LANGKAH KE-5

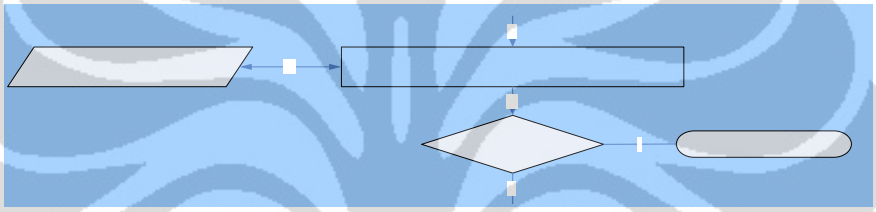


Gambar 3.7. Model Anti Spamming SMS Langkah ke-5 [18]

Proses didalam Oracle untuk mencari batas *threshold* frekuensi SMS *originating* yang diperbolehkan oleh aplikasi *anti spamming* SMS. Keputusan limit dan batas *threshold* ditentukan oleh Manajemen *fraud* di Telkom Flexi dan dapat di*setting* yaitu sebesar 150 SMS per setengah jam.

Input	*Table query* yang berisikan 3 (dua) *field Message Identifier, Calling Mobile Identification Number,* dan Frekuensi.
Proses	Ambil data *Calling Mobile Identification Number* yang frekuensinya melebihi batas *threshold* yang diizinkan ke *Table query* baru.
Output	*Table query* yang berisikan 2 (dua) *field Message Identifier,* dan *Calling Mobile Identification Number*.

3.3.6. LANGKAH KE-6

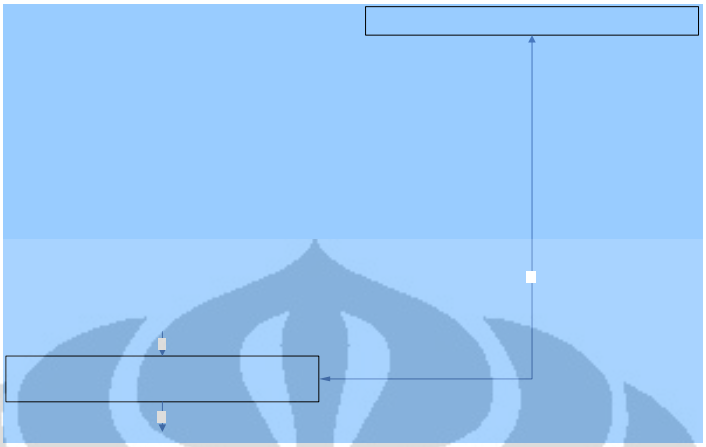


Gambar 3.8. Model Anti Spamming SMS Langkah ke-6 [18]

Proses didalam Oracle untuk melakukan *cross check* dan *filtering output* dari langkah ke-5 dengan data *whitelist*.

Input	1. *Table query* yang berisikan 2 (dua) *field Message Identifier,* dan *Calling Mobile Identification Number*. 2. Data *whitelist* berisikan data *Calling Mobile Identification Number* yang diizinkan untuk melakukan spamming melebihi batas *threshold* yang diizinkan.
Proses	Melakukan *comparing* terhadap 2 (dua) masukan dan melakukan proses internal untuk membuang data *Calling Mobile Identification* dari *Table query* yang sama dengan *list* pada *Whitelist*.
Output	*Table query* yang berisikan 2 (dua) *field Message Identifier,* dan *Calling Mobile Identification Number*.

3.3.7. LANGKAH KE-7

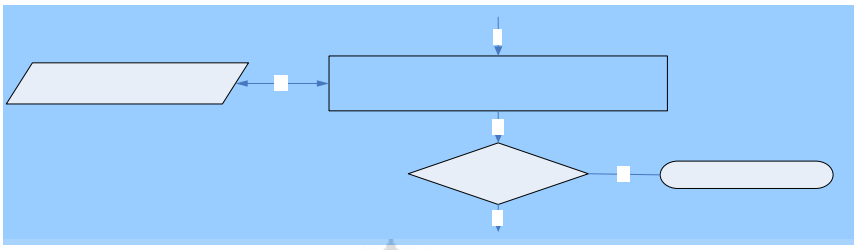


Gambar 3.9. Model Anti Spamming SMS Langkah ke-7 [18]

Proses mengambil data *content history* SMSC yang masih dalam bentuk *database* MySQL dan mengkonversi kedalam *database* Oracle, serta melakukan proses penggabungan nomor yang sudah terpilih dari langkah ke-6 dengan data *content* SMS.

Input	1. *Table query* yang berisikan 2 (dua) *field Message Identifier,* dan *Calling Mobile Identification Number*. 2. Data *content* SMS
Proses	Mengambil data *content* SMS dari *history* SMSC dengan mengacu pada *Table query* hasil langkah ke-6, serta melakukan penggabungan data *Calling Mobile Identification Number* dan *Message Content*.
Output	*Table query* yang berisikan 3 (tiga) *field Message Identifier, Calling Mobile Identification Number,* dan *Message Content.*

3.3.8. LANGKAH KE-8



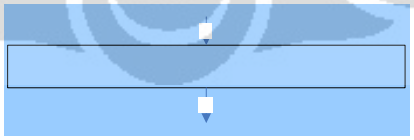
Gambar 3.10. Model Anti Spamming SMS Langkah ke-8 [18]

Proses *filtering content* SMS dengan menggunakan kata kunci / *keyword* yang sudah didefinisikan dengan melihat statistik *message content* penipuan yang paling sering dipergunakan oleh para *spammer* SMS penipuan.

Input	1. *Table query* yang berisikan 3 (tiga) *field Message Identifier, Calling Mobile Identification Number,* dan *Message Content.* 2. Data *keyword*
Proses	Melakukan proses pengecekan dengan membuang baris *Calling Mobile Identification Number*, dan *Message Content* yang tidak sesuai dengan kriteria *keyword.*
Output	*Table query* yang berisikan 3 (tiga) *field Message Identifier, Calling Mobile Identification Number*, dan *Message Content.*

KEYW

3.3.9. LANGKAH KE-9

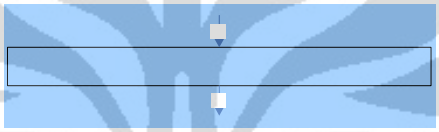


Gambar 3.11. Model Anti Spamming SMS Langkah ke-9 [18]

Proses didalam Oracle untuk mencari jumlah frekuensi SMS *originating* untuk kemudian akan dibandingkan dengan *threshold* yang diperbolehkan oleh aplikasi *anti spamming* SMS pada langkah berikutnya.

Input	Table query yang berisikan 3 (tiga) *field Message Identifier*, *Calling Mobile Identification Number*, dan *Message Content.*
Proses	Menghitung frekuensi kemunculan masing-masing *Calling Mobile Identification Number* kedalam *Table query* baru.
Output	*Table query* yang berisikan 3 (dua) *field Message Identifier*, *Calling Mobile Identification Number*, dan Frekuensi.

3.3.10. LANGKAH KE-10

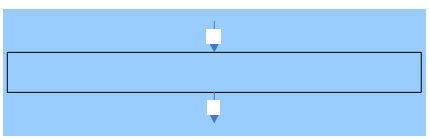


Gambar 3.12. Model Anti Spamming SMS Langkah ke-10 [18]

Proses didalam Oracle untuk mencari batas *threshold* frekuensi SMS *originating* yang diperbolehkan oleh aplikasi *anti spamming* SMS mengikuti filter threshold sebelumnya yaitu diatas 150 kali pengiriman per setengah jamnya.

Input	*Table query* yang berisikan 3 (dua) *field Message Identifier*, *Calling Mobile Identification Number*, dan Frekuensi.
Proses	Ambil data *Calling Mobile Identification Number* yang frekuensi *Keyword* memenuhi kriteria dan melebihi batas *threshold* yang diizinkan kedalam *Table query* baru.
Output	*Table query* yang berisikan 1 (satu) *field Calling Mobile Identification Number.*

3.3.11. LANGKAH KE-11

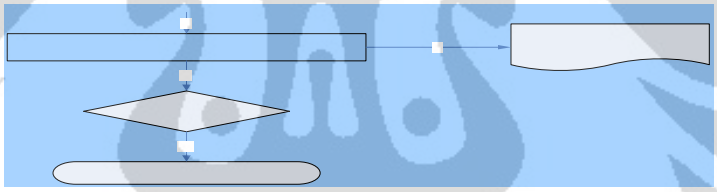


Gambar 3.13. Model Anti Spamming SMS Langkah ke-11 [18]

Proses didalam Oracle yang melakukan proses terakhir berupa *capturing* nomor-nomor *suspect spaming* dari hasil proses aplikasi seperti yang telah dijelaskan diatas sehingga siap untuk dikirimkan ke HLR untuk proses *blokir service* SMS *originating*.

Input	*Table query* yang berisikan 3 (dua) *field Message Identifier*, *Calling Mobile Identification Number*, dan Frekuensi.
Proses	Ambil data *Calling Mobile Identification Number* yang frekuensinya diatas batas *threshold* yang diizinkan kedalam *table query* baru.
Output	*Table query* yang berisikan 1 (satu) *field Calling Mobile Identification Number*.

3.3.12. LANGKAH KE-12



Gambar 3.14. Model Anti Spamming SMS Langkah ke-12 [18]

Adalah proses terakhir untuk melakukan *bloking* MIN hasil proses *anti spamming* diatas kedalam *command* HLR untuk dilakukan proses blokir dan *blacklist* nomor-nomor *spamming* untuk dokumentasi.

Input	*Table query* yang berisikan 1 (satu) *field Calling Mobile Identification Number*.
Proses	Ambil data *Calling Mobile Identification Number* dan digabungkan dengan *command* HLR untuk proses *blokir* SMS.
Output	1. Dokumentasi *Calling Mobile Identification Number* yang tertangkap oleh aplikasi *anti spamming*. 2. Proses *iterasi* ke langkah ke-1 dengan mengikuti *setting*

	timer yang telah ditentukan.

Dengan adanya proses *iterasi* pada langkah ke-12 menunjukan bahwa desain aplikasi ini dirancang untuk terus beroperasi mengikuti *schedule* yang telah ditentukan secara kontinyu dan *real time* 24 jam *non stop*.

3.4. DESAIN TIME TABLE APLIKASI

Berikut adalah desain *time table* aplikasi yang dirancang dan diperlukan dalam setiap tahapan proses yang harus dilewati oleh aplikasi *anti spamming* SMS sebagai berikut :

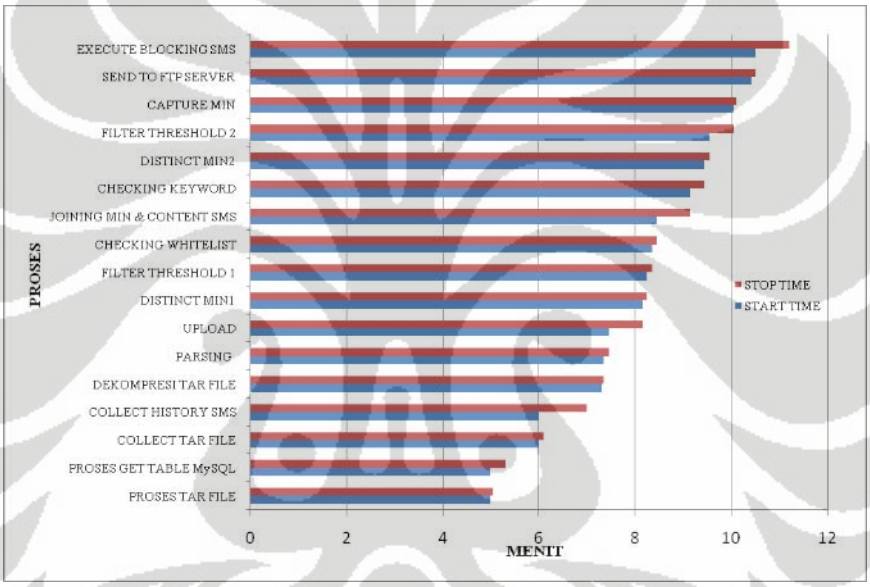
Tabel 3.11. Time Table Aplikasi Anti Spamming SMS [18]

NO	PROSEDUR	SMSC	FTP SERVER	APPLICATION SERVER	HLR	TIME	
						START	STOP
1	START						
	SHELL SCRIPT RUNNING	minute 05				00.05.00	
	PROSES TAR FILE	max 5 sec				00.05.00	00.05.05
	PROSES GET MySQL	max 30 sec				00.05.00	00.05.30
2	COLLECTING					SLEEP	
	COLLECT TAR FILE		max 10 sec			00.06.00	00.06.10
	COLLECT HISTORY SMS		max 60 sec			00.06.00	00.07.00
3	PARSING & UPLOAD					SLEEP	
	DEKOMPRESI TAR FILE			max 5 sec		00.07.30	00.07.35
	PARSING			max 10 sec		00.07.35	00.07.45
	UPLOAD			max 30 sec		00.07.45	00.08.15
4	DISTINCT MIN1			max 10 sec		00.08.15	00.08.25
5	FILTER THRESHOLD 1			max 10 sec		00.08.25	00.08.35
6	CHECKING WHITELIST			max 10 sec		00.08.35	00.08.45
7	JOINING MIN & CONTENT			max 30 sec		00.08.45	00.09.15
8	CHECKING KEYWORD			max 30 sec		00.09.15	00.09.45
9	DISTINCT MIN2			max 10 sec		00.09.45	00.09.55
10	FILTER THRESHOLD 2			max 10 sec		00.09.55	00.10.05
11	CAPTURE MIN			max 5 sec		00.10.05	00.10.10
12	BLOCKING MIN					SLEEP	
	SEND TO FTP SERVER		max 10 sec			00.10.40	00.10.50
	EXECUTE DI HLR				max 30 sec	00.10.50	00.11.20
	STOP						

Time table diatas adalah desain tahapan proses perjalanan aplikasi *anti spamming* SMS memerlukan waktu tempuh maksimal 6 menit dan 20 detik dari mulai *start* sampai dengan *stop*. Nilai maksimal adalah batas aman program berjalan yang diperoleh berdasarkan kecepatan proses program pada setiap tahapnya dan dikalikan dengan 2 (dua) untuk memastikan tidak ada proses yang terlewatkan. Proses-proses yang memerlukan pergantian perangkat dan terjadi *hop*

pada prosesnya missal dari SMSC ke FTP *Server* maka dilakukan penambahan proses *sleep*/*pause* selama 30 (tiga puluh) detik untuk memastikan tidak ada proses sebelumnya yang terlewatkan. Proses *sleep* ini dilakukan 3 (tiga) kali setiap tahapan proses yang dilakukan oleh perangkat yang berbeda yaitu antara SMSC ke FTP *server*, FTP *server* ke *Anti Spamming Server*, dan *Anti Spamming Server* ke HLR dalam satu kali periode aplikasi berjalan.

Untuk lebih memudahkan melihat tahapan dan waktu kerja aplikasi, berikut grafik *time table* aplikasi *anti spamming* SMS :



Grafik 3.1. Time Table Application Anti Spamming SMS [18]

3.5. DESAIN PENGGUNAAN BAHASA PEMROGRAMAN

Desain aplikasi yang dibuat didesain harus dapat berjalan dalam *platform operating system* yang berbeda dan menggunakan bahasa pemrograman yang berbeda. Hal ini diperlukan karena proses ini membutuhkan alur waktu cepat, agar proses dapat berjalan cepat maka pemrograman harus didesain dengan seminimal mungkin konversi, menggunakan fitur-fitur *operating system* yang ada, dan harus *compatible* dengan perangkat terkait sehingga dapat meminimalkan *interoperability*.

Beberapa bahasa pemrograman dan *database* yang digunakan dalam merangkai aplikasi *anti spamming* SMS adalah sebagai berikut yaitu HP-UX di sisi SMSC, MySQL *database* disisi SMSC, Red-Hat dan Oracle di sisi *Anti Spamming Server* serta Sun Solaris dan PostGre-SQL di sisi HLR, untuk lebih jelasnya dapat dilihat pada tabel 3.12 tentang penggunaan bahasa pemrograman pada aplikasi *anti spamming* SMS berikut ini :

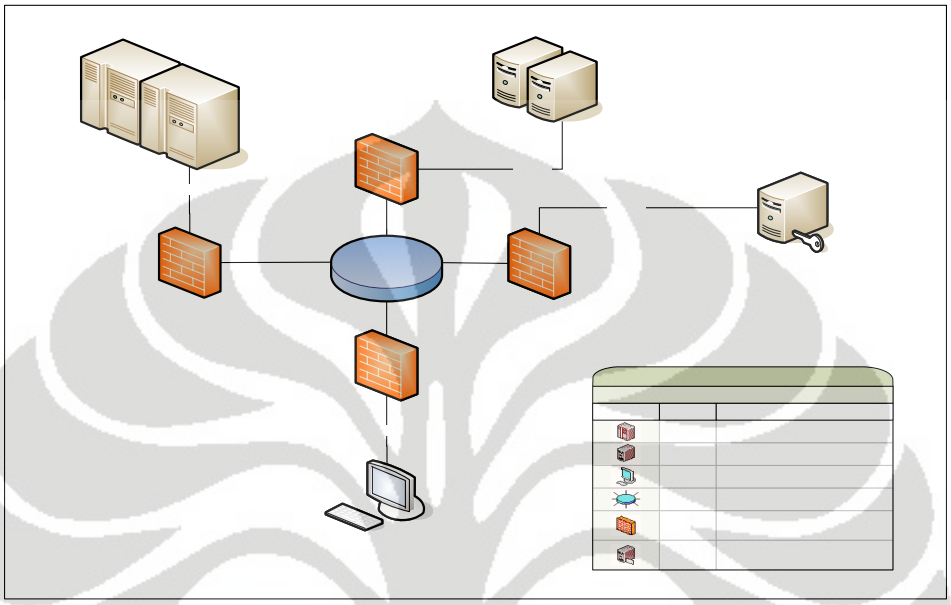
Tabel 3.12. Bahasa Pemrograman Pada Aplikasi Anti Spamming SMS [18]

NO	PROSEDUR	SMSC	FTP SERVER	APPLICATION SERVER	HLR
1	START				
	SHELL SCRIPT RUNNING	HP-UNIX			
	PROSES TAR FILE	HP-UNIX			
	PROSES GET TABLE MySQL	MYSQL			
2	COLLECTING				
	COLLECT TAR FILE		HP-UNIX		
	COLLECT HISTORY SMS		MYSQL		
3	PARSING & UPLOAD				
	DEKOMPRESI TAR FILE			ORACLE	
	PARSING			ORACLE	
	UPLOAD			ORACLE	
4	DISTINCT MIN1			ORACLE	
5	FILTER THRESHOLD 1			ORACLE	
6	CHECKING WHITELIST			ORACLE	
7	JOINING MIN & CONTENT SMS			ORACLE	
8	CHECKING KEYWORD			ORACLE	
9	DISTINCT MIN2			ORACLE	
10	FILTER THRESHOLD 2			ORACLE	
11	CAPTURE MIN			ORACLE	
12	BLOCKING MIN				
	SEND TO FTP SERVER		HP-UNIX		
	EXECUTE DI HLR				POSTGRE-SQL
	STOP				

Dengan menggunakan bahasa pemrograman yang disesusaikan dengan kondisi bahasa pemrograman yang ada dimasing-masing perangkat, maka performansi program dalam menjalankan aplikasi akan berjalan lebih cepat karena *compatible*, memimimalkan faktor *interoperability software*, dan yang terpenting adalah menjamin faktor *reability* dalam rangka proses *iterasi* yang akan dijalankan secara terus menerus selama 24 jam *non stop*.

3.6. KONFIGURASI PERANGKAT ANTI SPAMMING

Berikut adalah konfigurasi perangkat *anti spamming* SMS :



Gambar 3.15. Konfigurasi Perangkat Anti Spamming SMS Flexi [18]

Gambar 3.15 adalah gambar konfigurasi perangkat yang mendukung aplikasi *anti spamming* SMS di jaringan SMS Telkom Flexi yang meliputi 16 *node* HLR, 4 *node* SMSC, 1 *node* FTP *Server*, IP Network eksisting, 4 *node* IPS sekuriti jaringan TCP/IP eksisting serta 1 *node Server* aplikasi *anti spamming* SMS.

Dari gambar tersebut terlihat bahwa semua proses aplikasi ini berjalan dalam jaringan TCP/IP yang memiliki mekanisme sekuriti jaringan IPS sehingga *node-node* yang dipergunakan dan sudah didefinisikan dalam melakukan proses *anti spamming* sudah aman dari berbagai *intrution* dan *prevention* dari luar konfigurasi yang sudah didefinisikan.

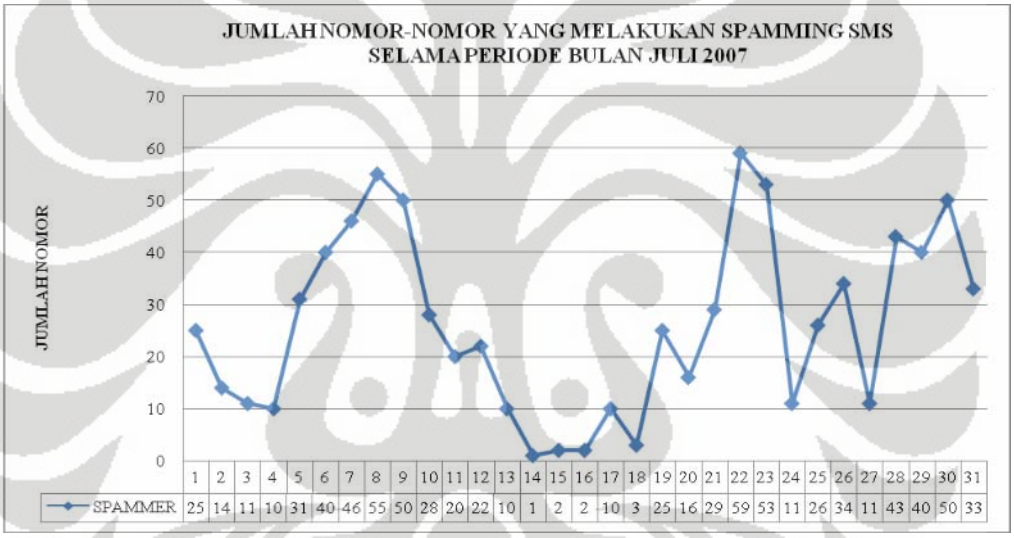
Kick off implementasi aplikasi *anti spamming* SMS dimulai pada tanggal 01 Juli 2007 pada seluruh perangkat terkait dengan aplikasi ini sesuai dengan gambar 3.15 konfigurasi umum *anti spamming* SMS diatas.

HLR

BAB IV
HASIL IMPLEMENTASI DAN ANALISA

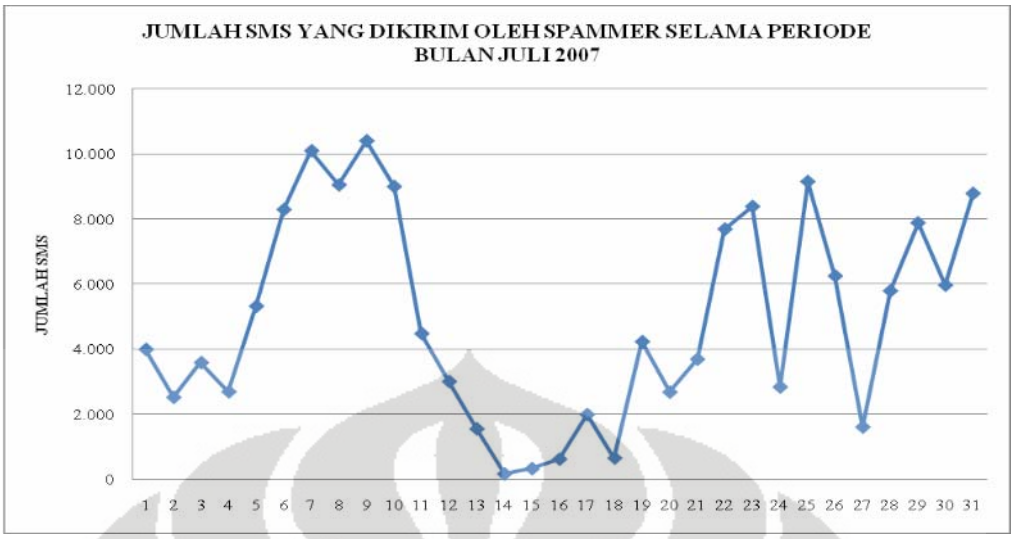
4.1. ANALISIS TERHADAP HASIL KELUARAN APLIKASI

Berikut ini adalah hasil *capture* aplikasi *anti spamming* SMS dalam bentuk grafik selama periode 1 (satu) bulan pertama diimplementasikannya aplikasi *anti spamming* SMS di network Telkom Flexi selama periode Juli 2007 sebagai berikut :



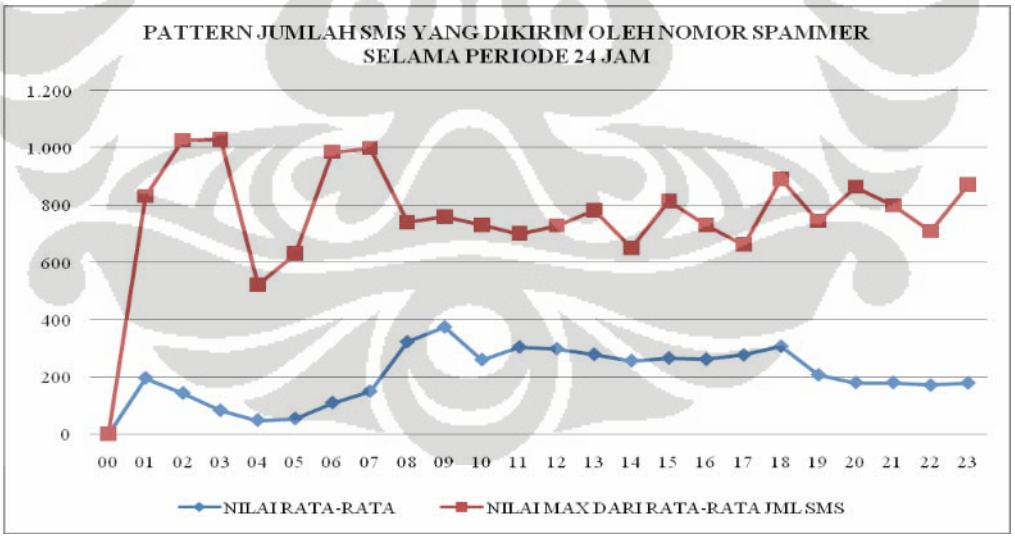
Gambar 4.1. Grafik Jumlah Nomor-Nomor Yang Melakukan Spamming SMS Selama Periode Bulan Juli 2007 [18]

Gambar 4.1 diatas menunjukan grafik jumlah nomor-nomor yang melakukan *spamming* SMS dan terjaring oleh aplikasi *anti spamming* SMS selama periode bulan Juli 2007, dimana data jumlah *spammer* yang melakukan *spamming* SMS sebanyak 810 *spammer* dengan rata-rata harian sebanyak 26,12 *spammer*.



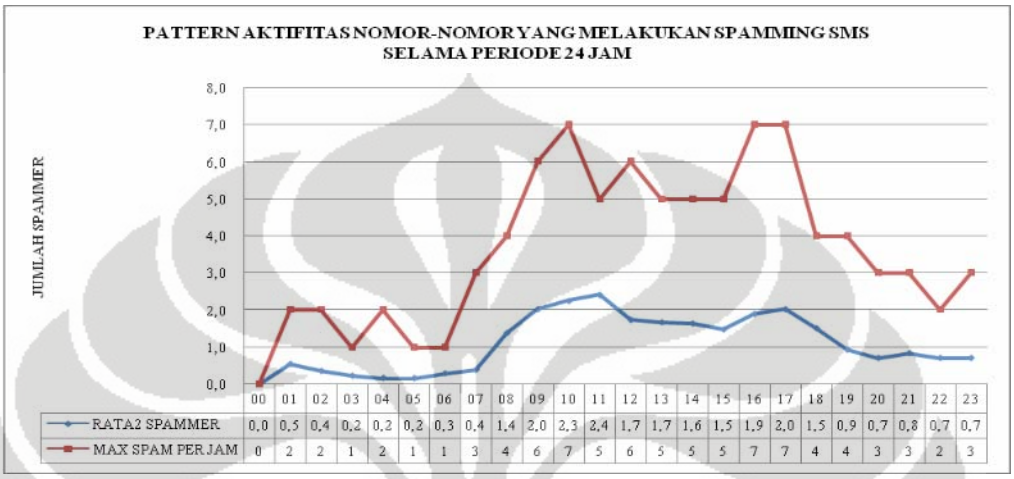
Gambar 4.2. Grafik Jumlah SMS Yang Dikirim Spammer Selama Periode Bulan Juli 2007 [18]

Gambar 4.2 diatas menunjukan grafik akumulasi jumlah SMS *spamming* harian yang berhasil masuk SMSC adalah sebanyak 152.662 SMS, atau rata-rata *spammer* mengirimkan sebanyak 189 SMS sebelum terkena proses *blokir* aplikasi *anti spamming* SMS.



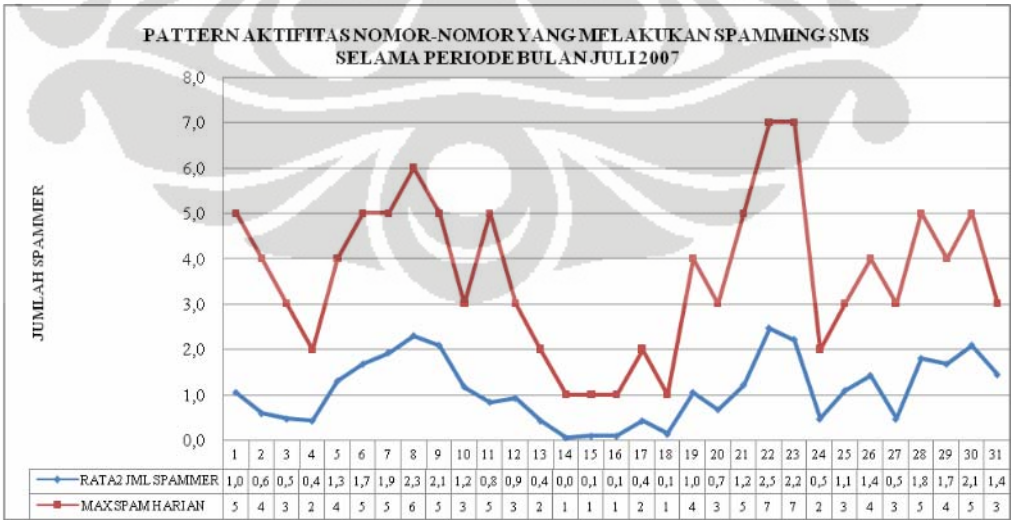
Gambar 4.3. Grafik Rata-Rata Jumlah SMS Yang Dikirimkan Oleh Nomor-Nomor Spamming Selama Bulan Juli 2007 [18]

Gambar 4.3 diatas menunjukan grafik *pattern* rata-rata jumlah SMS yang dikirimkan selama periode 24 jam adalah sebesar 4.925,58 SMS, dengan jumlah pengiriman SMS tertinggi ada pada antara pukul 01.00 sampai dengan 03.00 dini hari, dan antara pukul 05.00 sampai dengan 07.00 pagi hari.



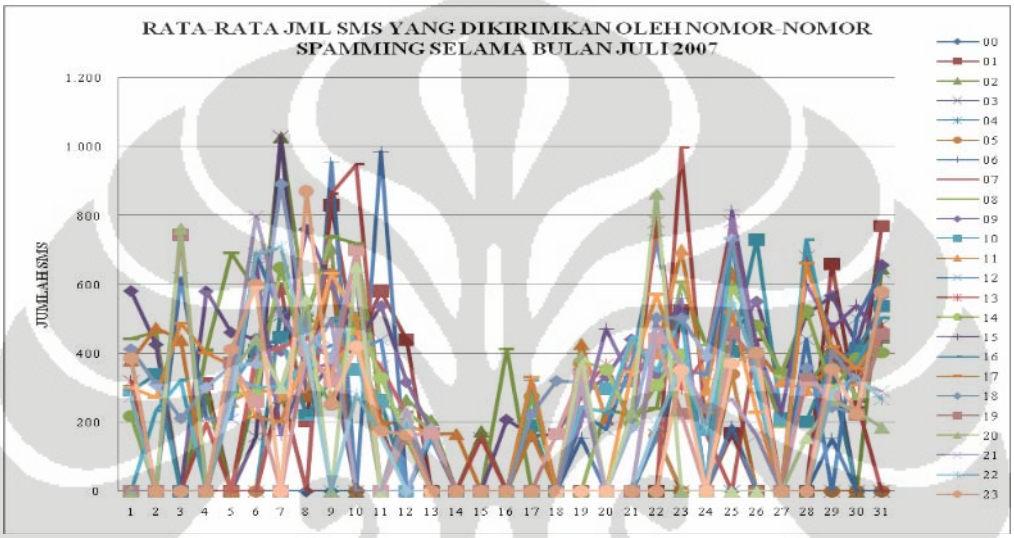
Gambar 4.4. Grafik Pattern Aktifitas Spammer SMS Selama Periode 24 Jam [18]

Gambar 4.4 diatas menunjukan grafik *pattern* aktifitas *spamming* SMS yang dilakukan oleh para *spammer* selama periode 24 jam dimana antara pukul 09.00 sampai 17.00 merupakan waktu favorit para *spammer* untuk menjalankan aksi *spamming* SMS.



Gambar 4.5. Grafik Pattern Aktifitas Nomor-Nomor Spammer Selama Periode Bulan Juli 2007 [18]

Gambar 4.5 diatas menunjukan grafik *pattern* jumlah *spammer* SMS yang melakukan aktifitas *spam* SMS selama periode bulan Juli 2007 rata-rata sebesar 1,09 *spammer* per jam, dengan jumlah rata-rata SMS yang dikirimkan adalah sebanyak 205,19 SMS per jam. Terlihat lonjakan pengiriman SMS tertinggi pada bulan Juli terjadi pada akhir minggu pertama dan minggu ketiga atau pada tanggal 7-9 Juli 2007 dan 21-23 Juli 2007.



Gambar 4.6. Grafik Rata-Rata Jumlah SMS Yang Dikirimkan Oleh Nomor-Nomor Spamming Selama Bulan Juli 2007 [18]

Gambar 4.6 diatas menunjukan grafik *pattern* rata-rata setiap jam jumlah SMS yang dikirim oleh para *spammer* SMS periode bulan Juli 2007, terlihat dari grafik diatas jumlah frekuensi *spamm* SMS yang dikirimkan setiap jamnya oleh para *spammer* jauh melebihi batas *threshold* maksimum SMS setiap setengah jam yang diseting sebesar 150 SMS.

4.2. ANALISIS PERFORMANSI SMSC JAKARTA DAN SURABAYA

Script program *anti spamming* SMS yang dijalankan pada perangkat SMSC di jaringan Telkom Flexi ditempatkan pada 4 *node* SMSC yang terdapat di lokasi Jakarta dan Surabaya masing-masing sebanyak 2 *node*.

Berikut adalah batas *boundary* area layanan SMS Telkom Flexi yang dicatu oleh ke-4 SMSC yang meliputi :

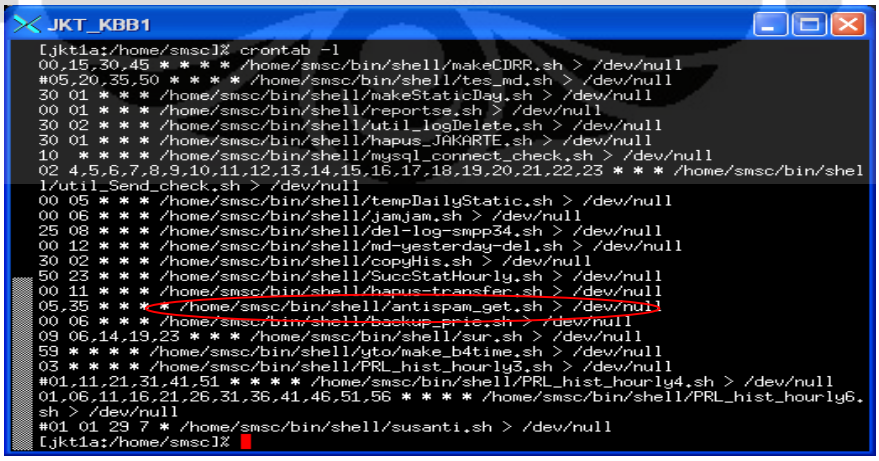
- SMSC Jakarta-1 melayani Divisi Regional II dan III.
- SMSC Jakarta-2 melayani Divisi Regional I.
- SMSC Surabaya-1 melayani Divisi Regional V dan IV.
- SMSC Surabaya-2 melayani Divisi Regional VI dan VII.

Semua SMSC tersebut memiliki spesifikasi yang sama dari sisi *hardware*, *software*, dan kapasitas transmisi. Hal yang membedakan antara SMSC satu dan lainnya adalah okupansi trafik SMS yang berbeda karena wilayah layanannya yang berbeda-beda. Kaitannya dengan *script* program yang akan dijalankan pada perangkat SMSC maka hal yang harus diamati disini adalah performansi SMSC dengan melihat seberapa besar pengaruh kenaikan / lonjakan *load processor* atau CPU dan *load memory* di *server* SMSC pad saat *script running*.

Untuk melihat performansi CPU dan *memory server* di SMSC pada saat *script* tersebut berjalan akan digunakan perintah "*top -s 1 -d 60 -f filename.txt*" dimana "-s" adalah *time periode*, "-d" adalah *how many times to capture*, "-f" adalah *output file name* sehingga dapat di*capture* berapa perubahan dan pergerakan *load* CPU dan *memory* setiap detiknya.

4.2.1. PERFORMANSI CPU DAN MEMORY LOAD SMSC JAKARTA

Berikut adalah *capture crontab file* pada perangkat SMSC dilokasi Jakarta-1 Kebayoran Baru dimana *script* program aplikasi *anti spamming* SMS yang dipasang akan diproses secara periodik oleh *operating system* SMSC seperti terlihat pada gambar 4.7 dibawah ini :



Gambar 4.7. Capture file crontab pada SMSC Jakarta1 [19]

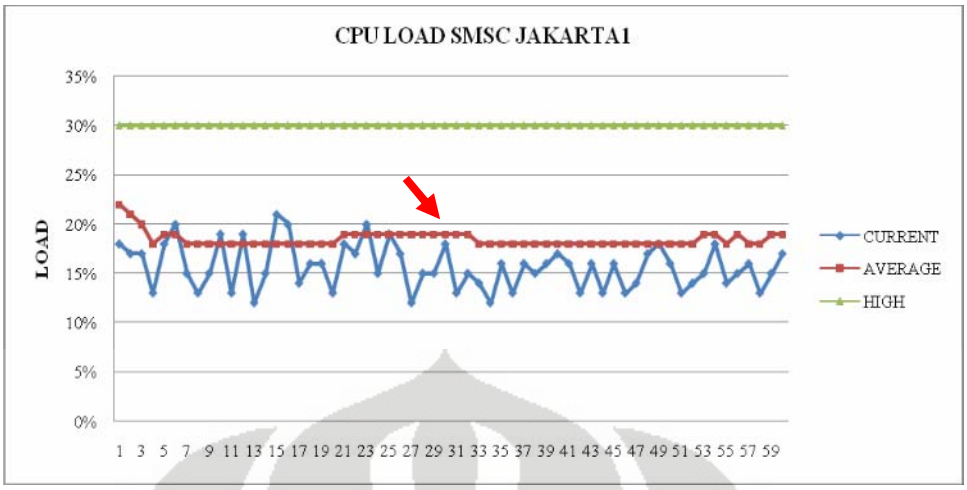
Gambar 4.7. diatas menggambarkan bahwa *file script* berada pada *direktory /home/smsc/bin/shell/antispam_get.sh* dan *crontab file* di*setting* agar dapat diproses secara otomatis pada menit ke-5 dan menit ke-35 setiap jamnya selama 24 jam *nonstop* dan hasil *capture* performansi CPU *load* tersebut dapat dilihat pada tabel 4.1 dibawah ini :

Tabel 4.1. Capture CPU Load SMSC Jakarta1 [19]

CPU LOAD			
SECOND	CURRENT	AVERAGE	HIGH
25	19%	19%	30%
26	17%	19%	30%
27	12%	19%	30%
28	15%	19%	30%
29	15%	19%	30%
30	18%	19%	30%
31	13%	19%	30%
32	15%	19%	30%
33	14%	18%	30%
34	12%	18%	30%
35	16%	18%	30%

Tabel 4.1 diatas menunjukan *highlight capture* performansi CPU *load* pada perangkat SMSC Jakarta-1 yang dilakukan pada saat 30 detik sebelum dan 30 detik setelah *script running*, terlihat pada detik ke-30 yang merupakan detik pertama *script* mulai *running*, terlihat ada lonjakan *current* CPU *load* sebesar 3% dari 15% ke 18% dan berfluktuasi sampai detik ke-35 sebesar 16%.

Dengan mengacu kepada tabel 3.4 *time table* aplikasi bahwa *running script* ditahap ini akan berlangsung maksimal selama 5 detik, maka dalam periode 5 detik setelah *script running* berdasarkan hasil *capture* performansi CPU *load* lonjakan tersebut masih berada dibawah rata-rata CPU *load* hari berjalan sebesar 19% dan dibawah CPU *load* tertinggi selama *server* hidup sebesar 30% seperti ditunjukan pada gambar 4.7 berikut ini :



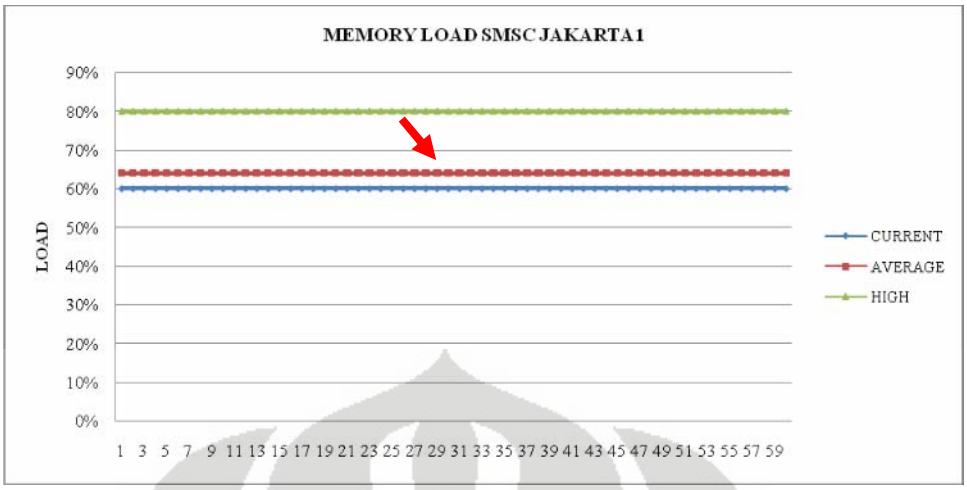
Gambar 4.8. Grafik Capture CPU Load SMSC Jakarta-1 [19]

Dari gambar 4.8 diatas dapat disimpulkan bahwa kenaikan CPU *load* masih berada dalam batas aman seperti disyaratkan pada proposal tesis, dimana jika lonjakan *current load* yang ditimbulkan oleh *script* angkanya berada dibawah atau sama dengan 5% maka dapat dinyatakan *script* yang dibuat dan dipasang pada perangkat SMSC layak untuk dijalankan. Selanjutnya adalah *capture* performansi *memory load* SMSC Jakarta-1 seperti ditunjukan pada tabel 4.2. berikut ini :

Tabel 4.2. Capture Memory Load SMSC Jakarta-1 [19]

MEMORY LOAD			
SECOND	CURRENT	AVERAGE	HIGH
25	60%	64%	80%
26	60%	64%	80%
27	60%	64%	80%
28	60%	64%	80%
29	60%	64%	80%
30	60%	64%	80%
31	60%	64%	80%
32	60%	64%	80%
33	60%	64%	80%
34	60%	64%	80%
35	60%	64%	80%

Tabel 4.2. diatas menunjukan *highlight capture* performansi *memory load* pada perangkat SMSC selama 30 detik sebelum dan 30 detik sesudah *script running*, terlihat disini tidak ada lonjakan apapun pada *current memory load* dan angka stabil pada nilai 60 % seperti yang ditunjukan pada grafik 4.8 berikut ini :

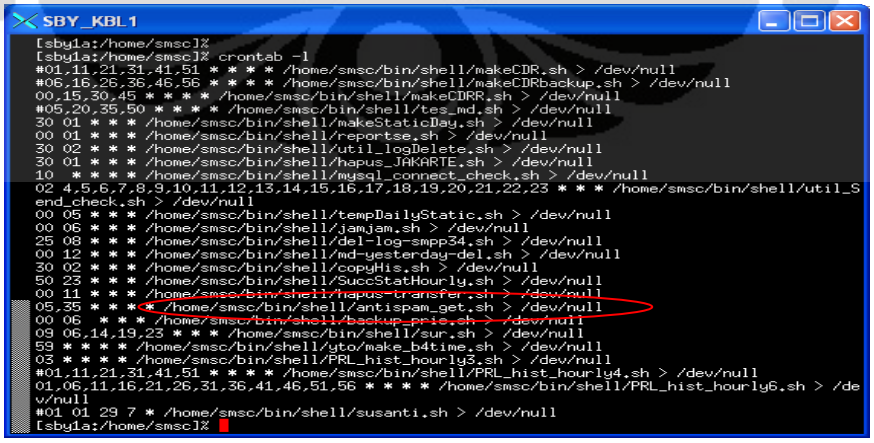


Gambar 4.9. Grafik Capture Memory Load SMSC Jakarta-1 [19]

Dari gambar 4.9 diatas dapat disimpulkan bahwa besar *current memory load* pada saat *script* berjalan adalah tetap, dengan demikian *script* tersebut berada dalam batas aman seperti disyaratkan pada proposal tesis selama kenaikan *load* berada dibawah atau sama dengan 5% maka dapat dinyatakan *script* yang dibuat dan dipasang di perangkat SMSC layak untuk dijalankan.

4.2.2. PERFORMANSI CPU DAN MEMORY LOAD SMSC SURABAYA

Berikut adalah *capture crontab file* pada perangkat SMSC dilokasi Surabaya-1 Kebalen dimana *script* program aplikasi *anti spamming* SMS yang dipasang akan diproses secara periodik oleh *operating system* SMSC seperti terlihat pada gambar 4.10 dibawah ini :



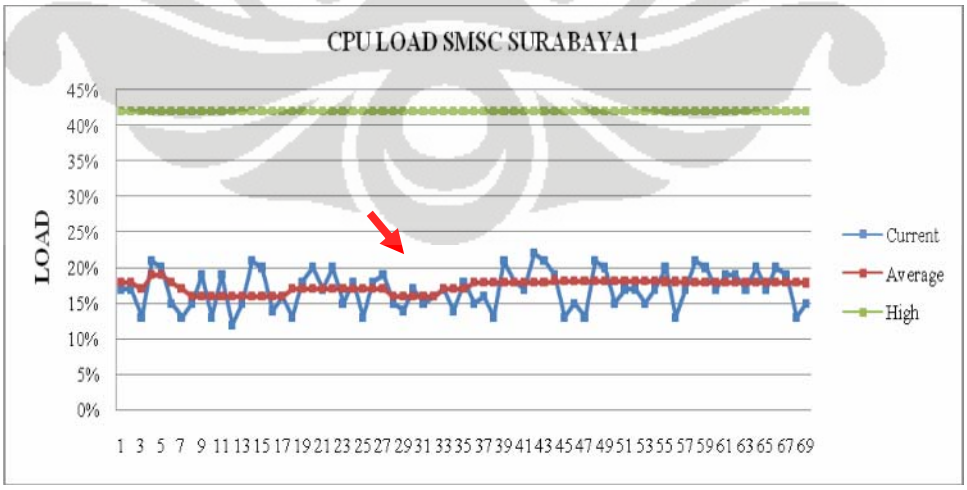
Gambar 4.10. Capture file crontab pada SMSC Surabaya [19]

Gambar 4.10 diatas menggambarkan bahwa *file script* berada pada *direktory /home/smsc/bin/shell/antispam_get.sh* dan *crontab file* di*setting* agar dapat diproses secara otomatis pada menit ke-5 dan menit ke-35 setiap jamnya selama 24 jam *nonstop* dan hasil *capture* dapat dilihat pada tabel 4.2 dibawah ini :

Tabel 4.3. Capture CPU Load SMSC Surabaya-1 [19]

CPU LOAD			
SECOND	CURRENT	AVERAGE	HIGH
27	19%	17%	42%
28	15%	16%	42%
29	14%	16%	42%
30	17%	16%	42%
31	15%	16%	42%
32	16%	16%	42%
33	17%	17%	42%
34	14%	17%	42%
35	18%	17%	42%

Tabel 4.3 diatas menunjukan *highlight capture* performansi CPU *load* pada perangkat SMSC Surabaya-1 dimana pada detik ke-30 adalah detik pertama *script* mulai *running*, terlihat ada lonjakan *current* CPU load sebesar 3% dari 14% ke 17% pada detik ke-30 dan berfluktuasi sampai detik ke-35 sebesar 18%, selama periode 5 detik setelah *script running* terlihat pencapaian tertinggi *load* sebesar 4% dan angka ini berada 1% diatas *load* rata-rata CPU pada satu hari berjalan sebesar 17%, dan dibawah *load* CPU tertinggi selama server hidup sebesar 42% seperti ditunjukan pada gambar 4.11 berikut ini :



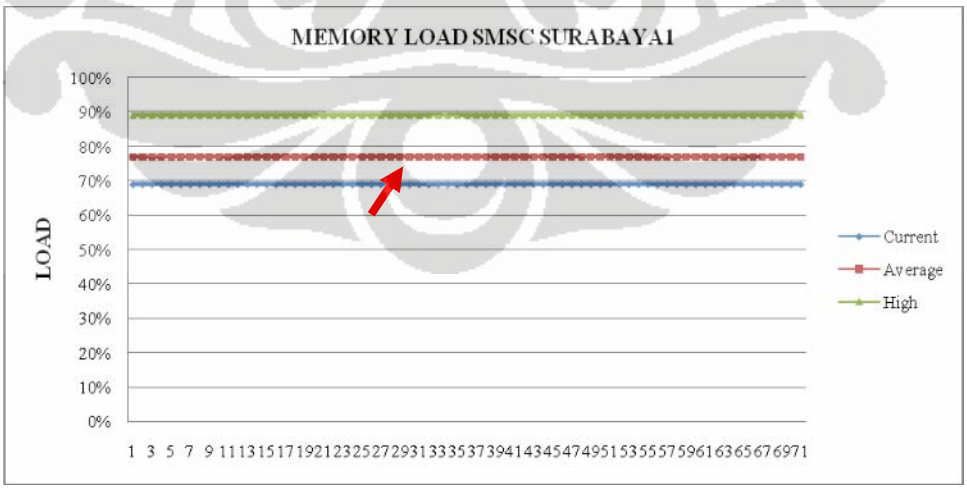
Gambar 4.11. Grafik Capture CPU Load SMSC Surabaya-1 [19]

Dari gambar 4.11 diatas dapat disimpulkan bahwa kenaikan CPU *load* tersebut masuk dalam batas aman seperti yang disyaratkan pada proposal tesis yaitu jika lonjakan yang timbul dibawah atau sama dengan 5% maka dapat dinyatakan *script* yang dibuat dan dipasang di perangkat SMSC layak untuk dijalankan. Selanjutnya adalah *capture* performansi *memory load* pada perangkat SMSC Surabaya-1 seperti ditunjukan pada tabel 4.4 berikut ini :

Tabel 4.4. Capture Memory Load SMSC Surabaya-1 [19]

MEMORY LOAD			
SECOND	CURRENT	AVERAGE	HIGH
25	69%	77%	89%
26	69%	77%	89%
27	69%	77%	89%
28	69%	77%	89%
29	69%	77%	89%
30	69%	77%	89%
31	69%	77%	89%
32	69%	77%	89%
33	69%	77%	89%
34	69%	77%	89%
35	69%	77%	89%

Tabel 4.4 diatas menunjukan *highlight* performansi *memory load* pada perangkat SMSC yang dilakukan selama 30 detik sebelum dan setelah *script running* dimana tidak ada lonjakan pada *current memory load* dan angka stabil pada nilai 69% seperti yang ditunjukan pada gambar 4.12 berikut ini :



Gambar 4.12. Grafik Capture Memory Load SMSC Surabaya-1 [19]

Dari gambar 4.12 diatas dapat disimpulkan bahwa *current memory load* pada saat *script* berjalan adalah tetap, dengan demikian *script* tersebut berada dalam batas aman seperti disyaratkan pada proposal tesis selama kenaikan *load* berada dibawah atau sama dengan 5% maka dapat dinyatakan *script* yang dibuat dan dipasang di perangkat SMSC layak untuk dijalankan.

4.3. ANALISIS PERFORMANSI FTP SERVER

Berikut adalah *capture crontab file* pada perangkat FTP *Server* yang menjadi *gateway* antara SMSC, HLR dan aplikasi *anti spamming* SMS dimana *script* program yang dipasang dan akan diproses secara periodik oleh *operating system* FTP *Server* seperti ditunjukan pada gambar 4.13 dibawah ini :

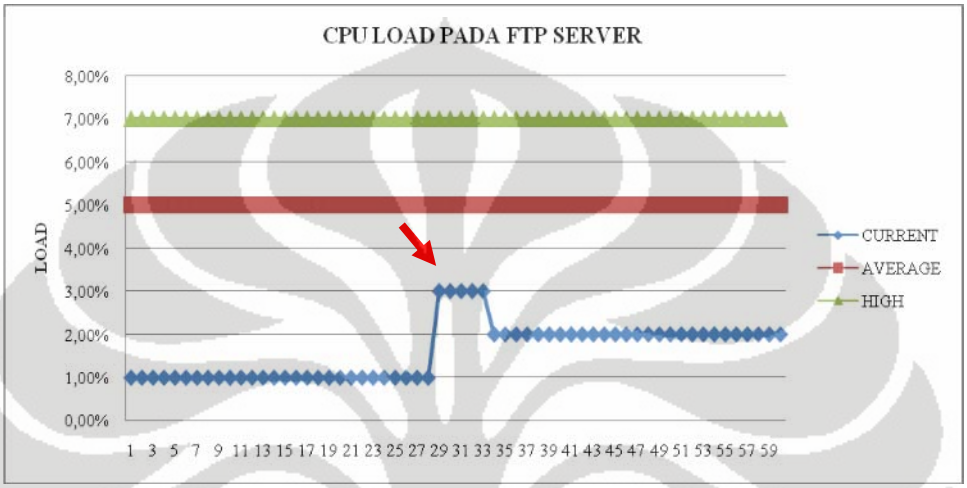
Gambar 4.13. Capture File Crontab Pada FTP Server [19]

Gambar 4.3 diatas terlihat *script file* aplikasi yang berada pada *direktory /home/smsc/spamming/antispam_get.sh* dan */home/smsc/spamming/send_MIN.sh* telah di*setting* dalam *crontab file* agar dapat diproses otomatis pada menit ke-6 dan ke-36 serta menit ke-11 dan ke-41 setiap jamnya selama 24 jam *nonstop* dan berikut hasil *capture* pada tabel 4.5 dibawah ini :

Tabel 4.5. Capture CPU Load FTP Server [19]

CPU LOAD			
SECOND	CURRENT	AVERAGE	HIGH
25	1,00	5,00	7,00
26	1,00	5,00	7,00
27	1,00	5,00	7,00
28	1,00	5,00	7,00
29	1,00	5,00	7,00
30	3,00	5,00	7,00
31	3,00	5,00	7,00
32	3,00	5,00	7,00
33	3,00	5,00	7,00
34	2,00	5,00	7,00
35	2,00	5,00	7,00

Tabel 4.5 diatas menunjukan *highlight capture* performansi CPU *load* perdetik pada perangkat FTP *server* yang dilakukan selama 30 detik sebelum dan 30 detik setelah *script running*, terlihat ada lonjakan *current load* CPU sebesar 2% pada detik ke-30 dari 1% ke 3% dan setelah detik ke-34 *load* cenderung stabil pada angka 2% seperti yang ditunjukan pada gambar 4.14 berikut ini :



Gambar 4.14. Grafik Capture CPU Load FTP Server [19]

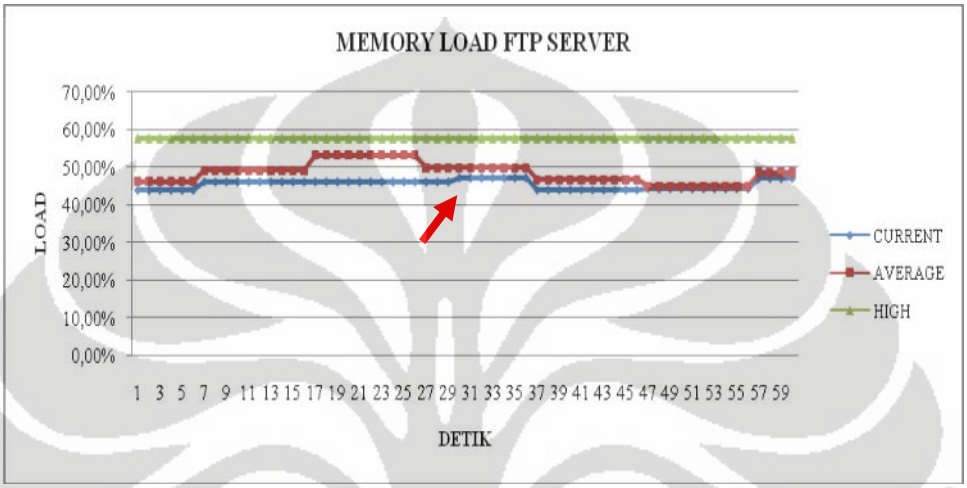
Dari gambar 4.11 diatas dapat disimpulkan bahwa *current* CPU *load* pada saat *script* berjalan naik sebesar 2%, dengan demikian *script* tersebut berada dalam batas aman seperti disyaratkan pada proposal tesis selama kenaikan *load* berada dibawah atau sama dengan 5% maka dapat dinyatakan *script* yang dibuat dan dipasang di perangkat FTP *server* layak untuk dijalankan.

Selanjutnya adalah *capture* performansi *memory load* pada perangkat FTP *Server* seperti ditunjukan pada tabel 4.6 berikut ini :

Tabel 4.6. Capture Memory Load FTP Server [19]

MEMORY LOAD			
SECOND	CURRENT	AVERAGE	HIGH
25	46,03%	53,20%	57,65%
26	46,03%	53,20%	57,65%
27	46,03%	49,86%	57,65%
28	46,03%	49,86%	57,65%
29	46,03%	49,86%	57,65%
30	47,07%	49,86%	57,65%
31	47,07%	49,86%	57,65%
32	47,07%	49,86%	57,65%
33	47,07%	49,86%	57,65%
34	47,07%	49,86%	57,65%
35	47,07%	49,86%	57,65%

Tabel 4.6 diatas menunjukan *highlight capture* performansi *memory load* perdetik pada perangkat FTP *Server* yang dilakukan selama 30 detik sebelum dan 30 detik setelah *script running,* terlihat ada lonjakan sebesar 1,04% pada *current memory load* pada detik ke-30 dari 46,03% ke 47,07% seperti ditunjukan pada gambar 4.15 berikut ini :



Gambar 4.15. Grafik Capture Memory Load FTP Server [19]

Dari gambar 4.15 diatas dapat disimpulkan bahwa *current memory load* pada saat *script* berjalan berada dalam batas aman seperti disyaratkan pada proposal tesis selama kenaikan *load* berada dibawah atau sama dengan 5% maka dapat dinyatakan *script* yang dibuat dan dipasang di perangkat FTP *Server* layak untuk dijalankan.

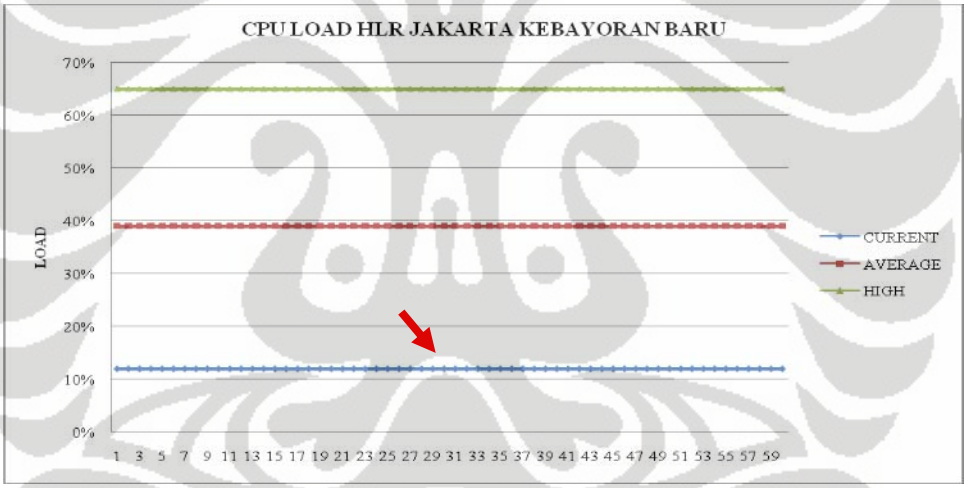
4.4. ANALISIS PERFORMANSI HLR

Berikut *capture* performansi HLR dilokasi Jakarta Kebayoran Baru selama *script* program berlangsung, dimana data diambil selama 30 detik sebelum dan 30 detik sesudah *script* berjalan seperti ditumjukan pada tabel 4.7 berikut ini :

Tabel 4.7. Capture CPU Load HLR Jakarta Kebayoran Baru [19]

CPU LOAD			
SECOND	CURRENT	AVERAGE	HIGH
26	12%	39%	65%
27	12%	39%	65%
28	12%	39%	65%
29	12%	39%	65%
30	12%	39%	65%
31	12%	39%	65%
32	12%	39%	65%
33	12%	39%	65%
34	12%	39%	65%
35	12%	39%	65%

Tabel 4.7 diatas menunjukan *highlight capture* performansi CPU *load* perdetik pada perangkat HLR yang dilakukan selama 30 detik sebelum dan 30 detik setelah *script running*, terlihat tidak ada lonjakan *current* CPU *load* seperti ditunjukan pada gambar 4.16 berikut ini :



Gambar 4.16. Grafik Capture CPU Load HLR Jakarta Kebayoran [19]

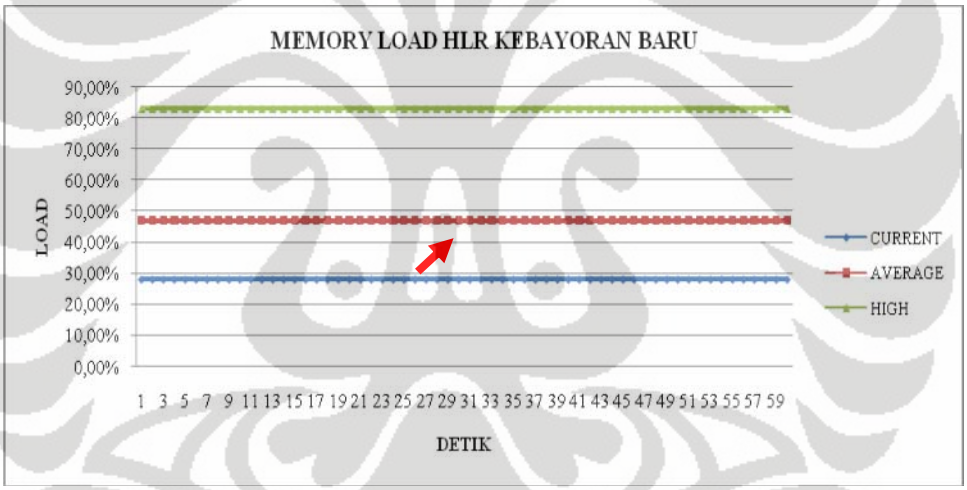
Dari gambar 4.13 diatas dapat disimpulkan bahwa *current* CPU *load* pada saat *script* berjalan berada dalam batas aman seperti disyaratkan pada proposal tesis selama kenaikan *load* berada dibawah 5% maka dapat dinyatakan *script* yang dibuat dan dipasang di perangkat HLR layak untuk dijalankan.

Selanjutnya adalah *capture* performansi *memory load* pada perangkat FTP *server* seperti ditunjukan pada tabel 4.8 berikut ini :

Tabel 4.8. Capture Memory Load HLR Jakarta Kebayoran Baru [19]

MEMORY LOAD			
SECOND	CURRENT	AVERAGE	HIGH
25	28,00%	47,00%	83,00%
26	28,00%	47,00%	83,00%
27	28,00%	47,00%	83,00%
28	28,00%	47,00%	83,00%
29	28,00%	47,00%	83,00%
30	28,00%	47,00%	83,00%
31	28,00%	47,00%	83,00%
32	28,00%	47,00%	83,00%
33	28,00%	47,00%	83,00%
34	28,00%	47,00%	83,00%
35	28,00%	47,00%	83,00%

Tabel 4.8 diatas menunjukan *capture* performansi *memory load* perdetik pada perangkat HLR yang dilakukan selama 30 detik sebelum dan 30 detik setelah *script running*, ternyata tidak ada lonjakan *current memory load* seperti ditunjukan pada gambar 4.17 berikut ini :



Gambar 4.17. Grafik Capture Memory Load HLR Jakarta Kebayoran [19]

Dari gambar 4.17 diatas dapat disimpulkan bahwa *current memory load* pada saat *script* berjalan berada dalam batas aman seperti disyaratkan pada proposal tesis selama kenaikan *load* berada dibawah atau sama dengan 5% maka *script* yang dibuat dan dipasang di perangkat HLR layak untuk dijalankan.

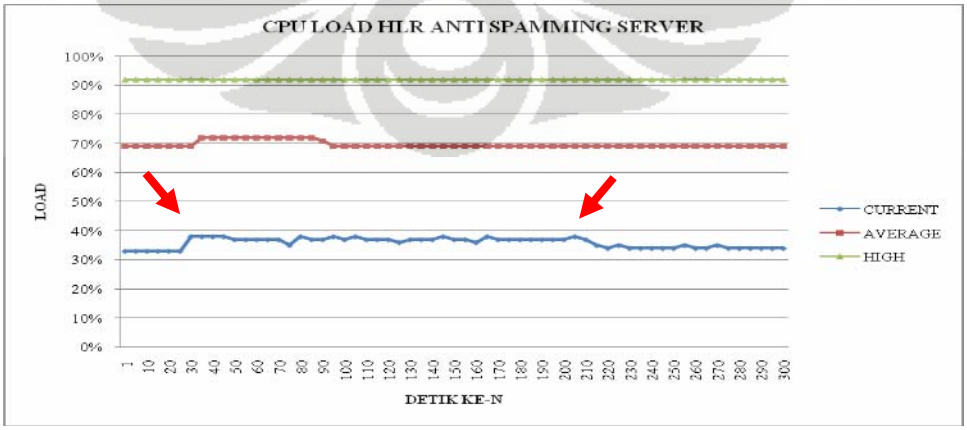
4.5. ANALISIS PERFORMANSI ANTI SPAMMING SERVER

Berikut *capture* performansi *anti spamming server* dimana data diambil selama 30 detik sebelum dan 300 detik sesudah *running* dengan interval waktu pengambilan di*setting* setiap 5 detik seperti ditunjukan pada tabel 4.9 berikut ini :

Tabel 4.9. Capture CPU Load Anti Spamming Server [19]

CPU LOAD			
SECOND	CURRENT	AVERAGE	HIGH
15	33%	69%	92%
20	33%	69%	92%
25	33%	69%	92%
30	38%	69%	92%
35	38%	72%	92%
40	38%	72%	92%
200	37%	69%	92%
205	38%	69%	92%
210	37%	69%	92%
215	35%	69%	92%
220	34%	69%	92%
225	35%	69%	92%

Tabel 4.9 diatas menunjukan *highlight capture* performansi CPU *load* dengan interval 5 detik pada perangkat *anti spamming server* yang dilakukan selama 300 detik, dimana terjadi lonjakan trafik sebesar 5% dari 33% ke 38% pada detik ke-30 dan setelah memasuki detik ke-356 sampai dengan selesai, *current load* berfluktuasi dikisaran angka 37%-38%,hal ini terjadi karena kondisi pertama kali *running script*, proses yang dilakukan adalah dekompresi *tar f*ile dan proses *upload* data kedalam *database* yang memerlukan energi cukup besar, seperti dilihat pada gambar 4.18 berikut ini :



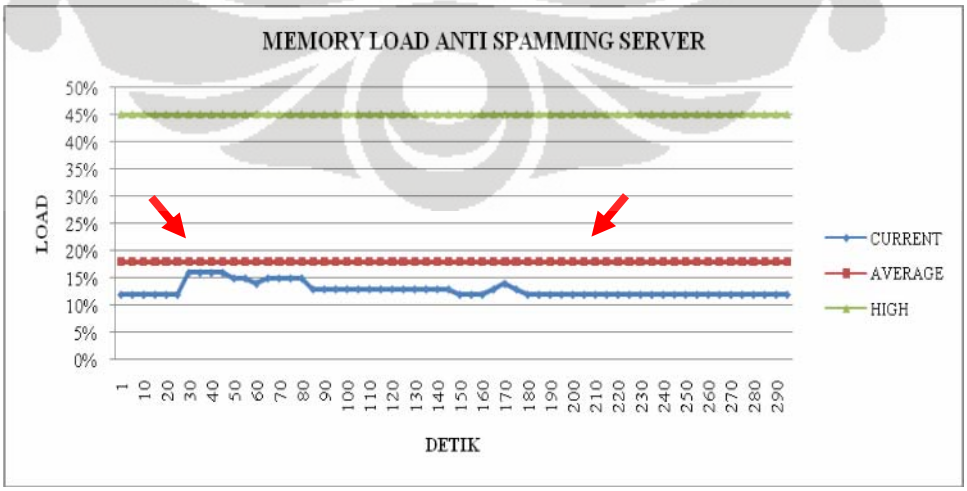
Gambar 4.18. Grafik Capture CPU Load Anti Spamming Server [18]

Dari gambar 4.15 diatas dapat disimpulkan bahwa *current* CPU *load* pada saat *script* berjalan berada dalam batas aman seperti disyaratkan pada proposal tesis selama kenaikan *load* berada dibawah atau sama dengan 5% maka dapat dinyatakan *script* yang dibuat dan dipasang di perangkat *anti spamming server* layak untuk dijalankan. Selanjutnya adalah hasil *capture memory load* pada perangkat *anti spamming server* seperti ditunjukan pada tabel 4.10 berikut ini :

Tabel 4.10. Capture Memory Load Anti Spamming Server [18]

MEMORY LOAD			
SECOND	CURRENT	AVERAGE	HIGH
15	12%	18%	45%
20	12%	18%	45%
25	12%	18%	45%
30	16%	18%	45%
35	16%	18%	45%
40	16%	18%	45%
45	16%	18%	45%
195	12%	18%	45%
200	12%	18%	45%
205	12%	18%	45%
210	12%	18%	45%
215	12%	18%	45%
220	12%	18%	45%
225	12%	18%	45%

Tabel 4.10 diatas menunjukan *highlight capture* performansi *memory load* dalam interval 5 detik pada perangkat *anti spamming server* yang dilakukan selama 300 detik, dimana ada lonjakan *current load* sebesar 4% pada detik ke-15 dari 12% ke 16% dan berfluktuasi pada kisaran 12% - 14% sampai *running* selesai seperti ditunjukan pada gambar 4.19 berikut ini :



Gambar 4.19. Grafik Capture Memory Load Anti Spamming Server [19]

Dari gambar 4.19 diatas dapat disimpulkan bahwa *current memory load* pada saat *script* berjalan berada dalam batas aman seperti disyaratkan pada proposal tesis selama kenaikan *load* berada dibawah atau sama dengan 5% maka dapat dinyatakan *script* yang dibuat dan dipasang di perangkat *anti spamming server* layak untuk dijalankan.

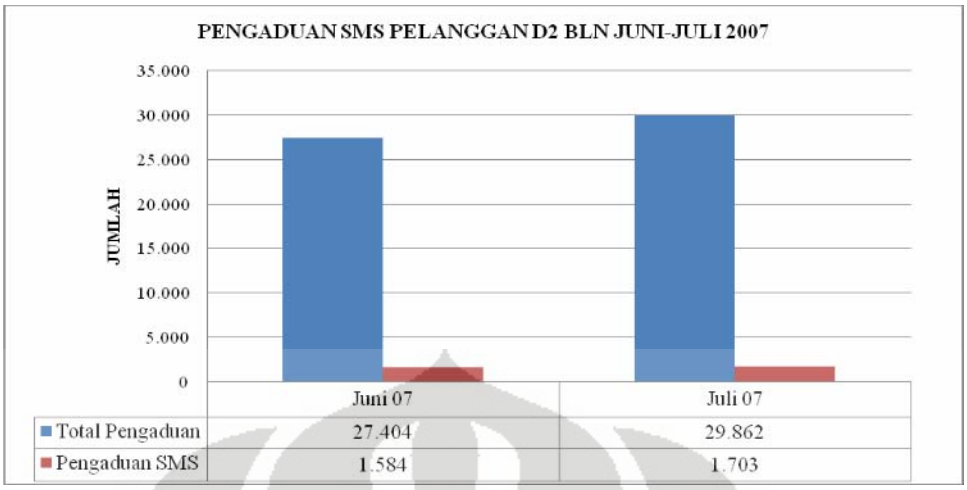
4.6. ANALISIS DATA COMPLAIN HANDLING

Berikut ini adalah data *complain handling* yang masuk di *helpdesk Customer Care* Telkom Flexi Area Divisi Jakarta yang menerima keluhan dari para pelanggan flexi yang berada dalam wilayah Divisi Regional II Jakarta, Bogor, Depok, Tangerang, Bekasi dan sekitarnya serta eskalasi *complain* yang berasal dari *Call Center* 147 selama periode bulan Juli 2007 berikut ini :

Tabel 4.11. Rekap Complain Handling Divre II Juli 2007 [22]

NO	URAIAN	DIVRE-II
1	Pengaduan Proses Aktivasi	6.124
2	Pengaduan RUIM	5.932
3	Pengaduan Gangguan Network	6.952
4	Pengaduan Buka Tutup Isoliran	75
5	Pengaduan Tagihan/Billing	65
6	Pengaduan Fitur TELKOMFlexi	325
7	Pengaduan Akses TELKOMFlexi (Dial)	1.869
8	Pengaduan SMS	1.703
9	Pengaduan pulsa / voucher	1.035
10	Pengaduan product Flexi	5.680
11	Lain-lain	102
	JUMLAH	**29.862**

Dari total 29.862 pengaduan yang berasal dari pelanggan Divre II, jumlah pengaduan SMS mencapai 1.703 pengaduan atau 5,70% dari total pengaduan bulan Juli 2007. Pengaduan SMS naik sebesar 8,96% dari bulan sebelumnya sebesar 1.584 pengaduan seperti ditunjukan pada gambar 4.20 berikut ini :



Gambar 4.20. Grafik Perbandingan Pengaduan SMS Divre II Juni-Juli 2007 [22]

Dari gambar 4.20 diatas dapat disimpulkan bahwa jumlah pengaduan SMS meningkat sebesar 8,96% dari 1.584 pengaduan, naik menjadi 1.703 pengaduan, namun dari total pengaduan yang masuk, kontribusi pengaduan SMS menurun 0,08% dari 5,78% menjadi 5,70%.

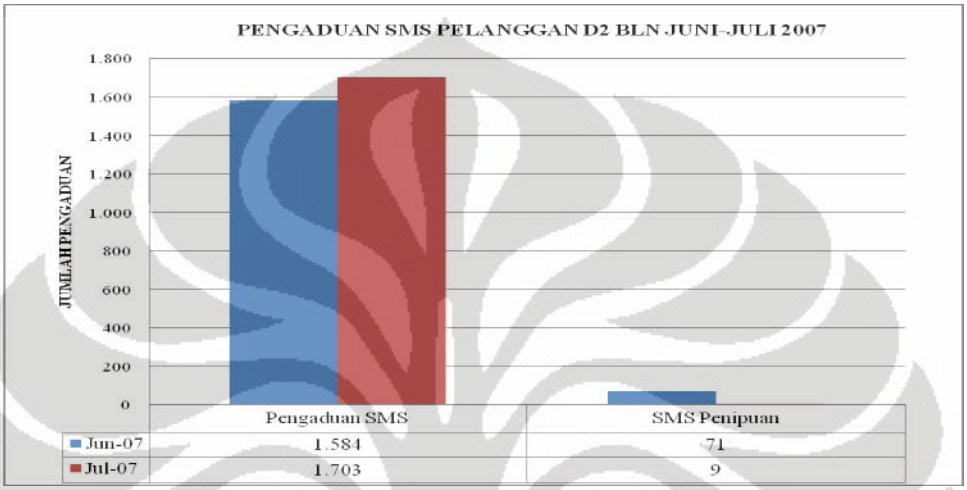
4.6.1. ANALISIS DATA PENGADUAN SMS

Berikut adalah rincian detil data pengaduan SMS yang berasal dari para pelanggan divre II pada bulan Juli 2007 sebagai berikut :

Tabel 4.12. Rekap Pengaduan SMS Divre II Juni 2007 [22]

NO	PENGADUAN SMS	DIVRE II
1	SMS berulang	953
2	SMS rusak/cacat	58
3	SMS Penipuan	9
4	SMS tidak sampai	23
5	SMS lambat	89
6	SMS content	421
7	SMS Provisioning Combo	150
	JUMLAH	1.703

Dari tabel 4.12. diatas dapat disimpulkan bahwa dari 1.703 pengaduan SMS sebesar 9 pengaduan atau 0,53 % mengadukan tentang SMS penipuan, jika dibandingkan secara *head to head* maka pengaduan tentang SMS penipuan turun sebesar 87,32% dibandingkan dengan bulan sebelumnya seperti ditunjukan pada gambar 4.21 berikut ini :



Gambar 4.21. Grafik Perbandingan Pengaduan SMS dan SMS Penipuan Divre II bulan Juni-Juli 2007 [22]

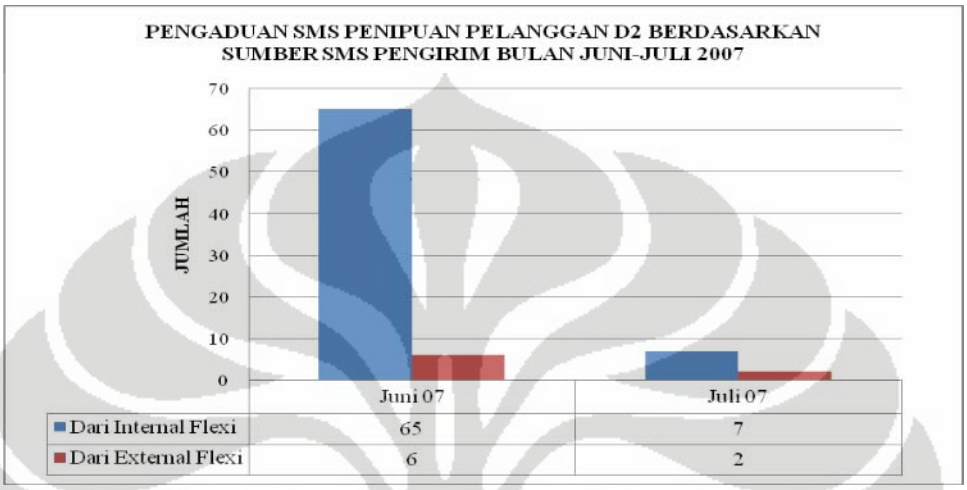
Dari gambar 4.21 diatas dapat disimpulkan bahwa terjadi indikasi penurunan keluhan SMS penipuan sebesar 88,17% dari sebelumnya 4,48% menjadi 0,53% dari total keseluruhan pengaduan tentang SMS.

Kemudian dari informasi pelanggan yang melaporkan tentang SMS penipuan *helpdesk* dapat meng*collect* informasi nomor-nomor yang dilaporkan telah mengirimkan SMS penipuan, secara umum pengirimnya berasal dari nomor Flexi dan nomor operator lain seperti ditunjukan pada tabel 4.13 berikut ini :

Tabel 4.13. Rekap Data Penipuan SMS Divre II Juli 2007 [22]

NO	PENGIRIM SMS PENIPUAN	DIVRE II
1	Dari Internal Flexi	7
2	Dari External Flexi	2
	JUMLAH	9

Dari tabel 4.13 diatas dapat disimpulkan bahwa dari 9 pengaduan SMS penipuan tersebut sebanyak 7 nomor atau 77,77% diantaranya dikirimkan dari nomor-nomor Flexi, dan 22,23% sisanya berasal dari operator lain seperti ditunjukan pada gambar 4.22 berikut ini :



Gambar 4.22. Grafik Pengaduan SMS Penipuan Divre II Berdasarkan Sumber SMS Pengirim Bulan Juni-Juli 2007 [22]

Dari gambar 4.22 diatas dapat disimpulkan bahwa telah terjadi penurunan terhadap keluhan SMS penipuan yang berasal dari nomor Flexi sebesar 89,23%.

4.6.2. ANALISIS DATA CONTENT SMS

Dilanjutkan dengan proses *cross check* dengan data SMSC maka diperoleh *content* SMS yang dikeluhkan dan diadukan oleh pelanggan. Berikut adalah data hasil pengecekan *content* SMS dari nomor-nomor yang dilaporkan oleh pelanggan seperti ditunjukan pada Tabel 4.14 berikut ini :

Tabel 4.14. Nomor-Nomor Pengirim SMS Penipuan dan Content SMS [22]

No	FLEXI	CONTENT SMS
1	02170296804	Plgn Yth,No.SIM CARD,anda meraih Gebyar "POIN HADIAH",dr TELKOMSEL.Hrp, Hub Call Center: (021) 68525853 (021) 68525854 Pengirim:222
2	02170867718	SELAMAT! Andamen-dpt"PANENPOIN" simPATIJITU"Rp.35jt drPT.TELKOMSELHub Call Center;021-68651855021-68651877Pengirim:+777
3	02168823181	Pelanggan YthNo,Flexi anda!!menang undianMelalui programRegistrasi flexi.U/Ket harap hub:021-93738587021-93738287Pengirim:4444
4	02170298918	Selamat,No.Sim Card Anda telah Meraih UNDIAN TELKOMSELpoin u/info sgr HUB:TELKOMSEL021-9351 3497021-9351 3498pengirim:777
5	02168706654	Selamat! No.Sim Card Anda meme-nangkan UndianMelalui Programregistrasi Flexiinfo harap hub:021-68593757021-68651839Pengirim:4444

6	02170298932	Selamat,No.SimCard Anda telahMeraih UNDIANTELKOMSELpoin u/info sgr HUB: TELKOMSEL 021-9308 3997 021-9288 3447 Pengirim:777
7	02168593757	Selamat! No.Sim Card Anda meme-nangkan UndianMelalui Programregistrasi Flexiinfo harap hub:021-68593757021-68651839Pengirim:4444
No	**OLO**	**CONTENT SMS**
1	02193363819	SELAMAT! Andamen-dpt GRANDPRIZE "FLexi"Rp.45jt dari,PT.TELKOM PUSAT.Hub:Call Center:021 68661741021 68652837Pengirim:Telkom
2	081382522711	Selamat anda m_dpt HadiahGrand Prize"dr.Telkom FLEXI.Rp.45 jt.Thp 06Hub:Call Center:021 6867 7414021 6864 6927Pengirim:Telkom

Dari tabel 4.14 diatas dapat disimpulkan bahwa *content* SMS yang berasal dari 7 nomer flexi tersebut terbukti merupakan bentuk SMS penipuan, sesuai dengan yang dikeluhkan oleh pelanggan. Kemudian dilanjutkan dengan pengecekan tunggakan SMS ke-7 nomor tersebut, maka diperoleh hasil seperti ditunjukan pada tabel 4.15 berikut ini :

Tabel 4.15. Jumlah Tunggakan dan Jumlah SMS Spam Penipuan [21]

NO	FLEXI	TUNGGAKAN (Rp)	JUMLAH SPAM (SMS)
1	02170296804	33.565	685
2	02170867718	23.961	489
3	02168823181	12.446	254
4	02170298918	46.942	958
5	02168706654	85.848	1.752
6	02170298932	48.314	986
7	02168593757	5.880	120
	JUMLAH	**256.956**	**5.244**

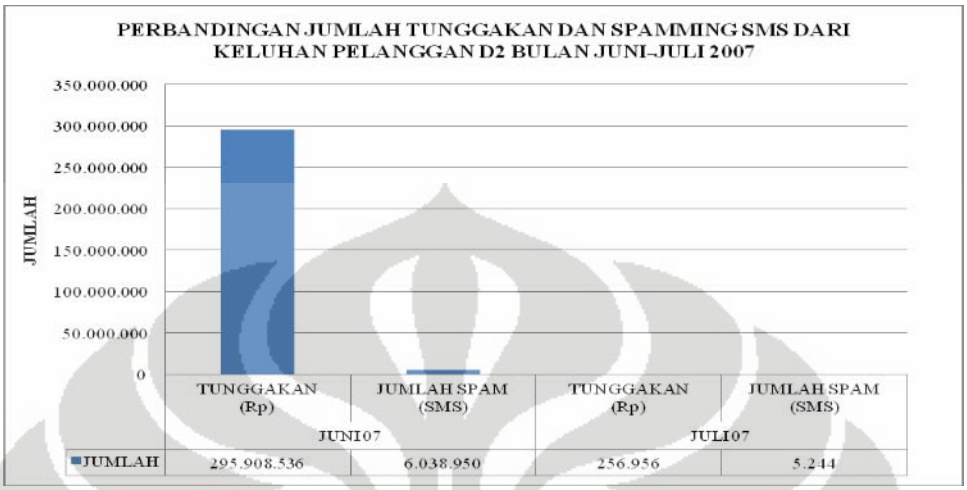
Dari tabel 4.15 diatas terlihat bahwa jumlah tunggakan yang berasal dari nomor-nomor yang melakukan *spamming* adalah sebesar Rp. 256.956 (dua ratus lima puluh enam ribu Sembilan ratus lima puluh enam rupiah), dan jumlah SMS *spam* yang dikirimkan oleh ke-7 nomor tersebut adalah sebanyak 5.244 SMS.

Tabel 4.16. Perbandingan Tunggakan dan Jumlah SMS Spam Penipuan [21]

	JUNI 07		JULI 07	
	TUNGGAKAN (Rp)	JML SPAM (SMS)	TUNGGAKAN (Rp)	JML SPAM (SMS)
JUMLAH	295.908.536	6.038.950	256.956	5.244
AVERAGE	4.552.439	92.907	36.708	749
MAXIMUM	24.774.865	505.609	85.848	1.752
MINIMUM	1.082.266	22.087	5.880	120

Tabel 4.16 diatas adalah perbandingan jumlah tunggakan dan *spamming* SMS yang berasal dari pengaduan pelanggan tentang SMS penipuan dari

pelanggan divre II selama periode bulan Juni-Juli 2007 seperti ditunjukan pada gambar 4.23 berikut ini :



Gambar 4.23. Grafik Perbandingan Jumlah Tunggakan dan Spamming SMS dari Keluhan Pelanggan Divre II bulan Juni-Juli 2007 [21]

Dari gambar 4.23 diatas dapat disimpulkan bahwa telah terjadi indikasi penurunan *fraud billing* sebesar 99,91% dengan jumlah tunggakan awal sebesar Rp. 295.908.536 menjadi Rp. 256.956, serta penurunan jumlah SMS *spam* sebesar 99,91% dari 6.038.950 SMS menjadi 5.244 SMS.

4.7. ANALISIS DATA FRAUD BILLING SMS

4.7.1. ANALISIS DATA BULAN JUNI 2007

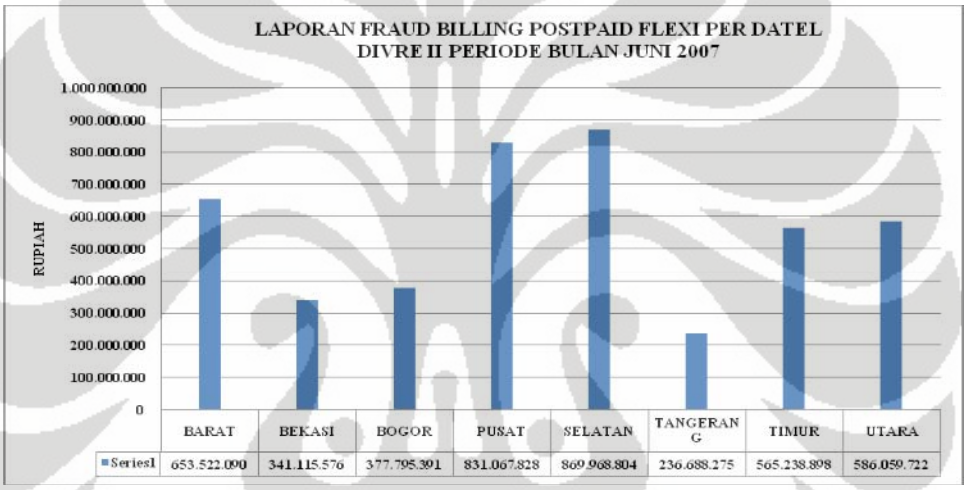
Berikut adalah data *fraud billing* periode bulan Juni 2007 yaitu data ditemukannya pertama kali sumber *fraud billing* berasal seperti ditunjukan dalam tabel 4.17 dibawah ini :

Tabel 4.17. Data Fraud Billing Divre II Bulan Juni 2007 [21]

DATEL	DATA FRAUD BILLING JUNI	
	TAGIHAN	SSF
BARAT	653.522.090	1.065
BEKASI	341.115.576	503
BOGOR	377.795.391	551
PUSAT	831.067.828	1.388
SELATAN	869.968.804	1.231

TANGERANG	236.688.275	408
TIMUR	565.238.898	930
UTARA	586.059.722	979
TOTAL	**4.461.456.584**	**7.055**

Tabel 4.17 diatas menunjukan dalam periode bulan Juni 2007 diindikasikan terdapat potensi kerugian pencairan piutang sebanyak 7.055 pelanggan Flexi *Postpaid* sebesar Rp. 4.461.456.584,- yang berada dalam layanan divisi regional II Jakarta, Bogor, Depok, Tangerang, Bekasi dan sekitarnya. Berikut adalah komposisi jumlah *fraud billing* per Datel seperti ditunjukan pada gambar 4.24 berikut ini :



Gambar 4.24. Laporan Fraud Billing Postpaid Periode Bulan Juni 2007 [21]

Dari gambar 4.24 diatas terlihat bahwa jumlah *fraud billing* tertinggi ada di Datel Jakarta Selatan sebesar Rp. 869.968.804,- diikuti oleh Datel Jakarta Pusat sebesar Rp. 831.067.828,- dan Datel Jakarta Barat sebesar Rp. 653.522.090,-.

Data *fraud billing* dapat didefinisikan sebagai kumpulan data yang terdiri atas nomor-nomor yang pemakaian *usage call* diatas satu juta rupiah, dan nomor-nomor tersebut bukan kategori pelanggan *Platinum* atau *Gold.*

Data awal *usage* diperoleh dari ISC (*Information System Center*) Telkom dan data *usage* tersebut diterima oleh manajeman Divre II untuk dibandingkan dengan *database* pelanggan Divre II sebelum dilakukan proses blokir. Berikut adalah komposisi pelanggan *postpaid* dan *prepaid* Divre II aktif pada bulan Juni 2007 seperti ditunjukan pada tabel 4.18 berikut ini :

Tabel 4.18. Komposisi Postpaid dan Prepaid Divre II Bulan Juni 2007 [22]

PELANGGAN	CLASSY	TRENDY						GRAND TOTAL (CLASSY+ACTIVE)
		VALID	ACTIVE	GRACE	EXPIRED	BLOCK	TOTAL	
JULI 07	319.404	598.489	899.914	136.021	10.322	8.054	1.652.800	1.219.318

Tabel 4.18. diatas adalah komposisi jumlah pelanggan *postpaid* dengan *brand* produk Flexi Classy dan pelanggan prepaid dengan *brand* produk Flexi Trendy. Jumlah pelanggan *postpaid* mencapai 319.404 pelanggan atau 26,19% dari total komunitas pelanggan Telkom Flexi Divre II. Jika data pelanggan *postpaid* tersebut dibandingkan dengan jumlah data *fraud billing postpaid* pada bulan Juni 2007 yang berjumlah 7.055 nomor, maka pelanggan *postpaid* yang masuk dalam katagori *fraud billing* adalah sebesar 2,21%. Berikut ini adalah rincian detil data *fraud billing* bulan Juni 2007 yang dirinci dalam Datel, jumlah tagihan, dan SSF (Satuan Sambungan Flexi) seperti ditunjukan pada tabel 4.19 berikut ini :

Tabel 4.19. Fraud Billing Pelanggan Postpaid Divre II bulan Juni 2007 [21]

TGL ISOLIR	DATEL																	
	BARAT		BEKASI		BOGOR		PUSAT		SELATAN		TANGERANG		TIMUR		UTARA		TOTAL	TOTAL
	TAGIHAN	SSF	TAGIHAN	SSF	TAGIHAN	SSF	TAGIHAN	SSF	TAGIHAN	SSF	TAGIHAN	SSF	TAGIHAN	SSF	TAGIHAN	SSF	TAGIHAN	SSF
03/06/2007									5.319.727	1							5.319.727	1
04/06/2008	602.084	1	1.985.725	2	4.542.956	6	577.361	1	5.219.254	7			1.868.963	3	1.187.395	1	15.983.738	21
05/06/2008			4.106.561	3	3.839.811	4			1.198.852	1			1.091.585	2			10.236.809	10
06/06/2009													1.127.570	1			1.127.570	1
07/06/2009			1.157.848	2	1.098.938	2			1.028.218	1							3.285.004	5
08/06/2010	14.561.633	22	12.380.968	16	18.355.440	24	19.198.130	29	51.557.995	42	3.156.483	5	9.092.353	14	9.060.283	14	137.363.285	166
09/06/2010	9.255.280	14	4.371.646	6	6.876.212	11	6.309.732	11	13.136.485	16	1.026.899	2	8.309.892	13	4.329.324	6	53.615.470	79
10/06/2011	14.093.038	23	8.357.275	16	15.307.375	22	11.996.120	21	19.469.736	30	3.129.606	6	11.318.765	19	12.590.398	23	96.262.313	160
11/06/2011	14.124.156	23	10.348.779	16	9.876.627	16	19.873.435	33	23.001.877	36	4.747.559	9	16.918.843	30	10.946.325	19	109.837.701	182
12/06/2012	4.621.349	9	1.570.029	3	4.161.809	6	3.607.803	6	7.785.839	13	1.052.886	2	2.538.218	4	8.133.558	14	33.471.491	57
13/06/2012	13.827.410	26	9.309.581	17	9.705.547	16	14.204.245	26	21.785.513	37	5.142.997	10	9.698.558	17	16.981.518	28	100.655.369	177
14/06/2013	5.603.865	10	3.011.088	5	3.031.351	6	6.634.540	12	18.079.184	25	1.510.718	3	5.659.289	9	7.236.402	13	50.766.437	83
15/06/2013	7.396.960	12	7.196.013	12	5.643.303	9	9.767.991	17	16.394.226	26	1.515.509	2	9.284.744	17	9.752.329	15	66.951.075	110
16/06/2014	17.684.741	29	11.231.769	18	10.340.077	18	19.956.933	35	22.054.433	34	3.058.267	6	13.551.094	23	18.560.264	33	116.437.578	196
17/06/2014	20.598.258	31	10.197.998	19	13.469.429	20	24.074.292	40	26.121.109	43	6.306.838	11	12.241.302	21	18.023.704	33	131.032.930	218
18/06/2015	28.092.359	48	13.723.186	24	12.871.962	22	36.997.725	66	40.657.570	72	7.797.015	14	22.522.837	38	29.615.782	51	192.278.437	335
19/06/2015	39.261.007	66	13.036.794	21	17.870.747	28	38.660.321	68	30.366.936	54	14.426.096	26	27.932.993	47	30.253.192	48	211.808.086	358
20/06/2016	89.448.281	109	73.294.546	72	73.532.612	73	110.904.605	134	174.535.119	154	26.794.115	42	70.457.232	89	32.582.069	59	651.548.579	732
21/06/2007	39.963.781	72	22.928.216	37	17.874.363	27	60.528.504	107	47.971.100	74	22.751.763	40	37.741.424	62	46.470.366	77	296.229.517	496
22/06/2007	55.459.119	93	19.049.600	33	28.612.553	47	70.300.082	125	53.394.478	92	21.103.698	39	44.691.639	77	68.060.790	111	360.671.959	617
23/06/2007	29.063.682	48	8.622.631	15	14.345.801	23	39.561.663	70	32.196.982	54	15.390.102	27	29.806.567	49	34.537.728	56	203.525.156	342
24/06/2007	34.821.271	63	17.295.164	29	17.304.275	31	42.787.560	79	32.428.139	56	14.271.814	26	33.284.827	62	24.427.917	42	216.620.967	388
25/06/2007	34.049.330	57	8.088.546	13	15.848.374	24	39.822.340	68	32.843.043	51	8.105.024	14	21.987.939	39	28.038.361	46	188.782.957	312
26/06/2007	32.688.163	54	8.581.574	14	13.698.085	22	31.508.325	56	25.991.592	43	10.711.228	18	24.289.517	42	25.923.749	43	173.392.233	292
27/06/2007	42.752.053	77	23.358.768	36	8.185.743	15	63.018.769	100	39.673.419	63	17.926.446	33	41.042.500	70	45.848.816	76	281.806.514	470
28/06/2007	50.444.868	84	26.472.396	42	21.331.279	34	87.275.004	152	72.096.343	115	26.822.136	39	55.748.918	90	48.889.632	84	389.080.576	640
29/06/2020	55.109.402	94	21.438.875	32	30.070.722	45	73.502.348	132	55.661.635	91	19.940.975	34	53.031.329	92	54.609.820	87	363.365.106	607
TOTAL	653.522.090	1.065	341.115.576	503	377.795.391	551	831.067.828	1.388	869.968.804	1.231	236.688.275	408	565.238.898	930	586.059.722	979	4.461.456.584	7.055

Dari total *fraud billing* sebesar Rp. 4.461.456.584,- dan setelah dilakukan proses *cross check* detil terhadap rincian *billing* SMS per nomor maka didapat jumlah *fraud billing* SMS sebesar Rp. 473.453.657,- atau 10,61% dari jumlah total *fraud billing* bulan Juni 2007 dengan pemakaian SMS rata-rata adalah sebesar Rp. 67.108,- per SSF, dan pemakaian SMS tertinggi sebesar Rp. 24.774.865,-.

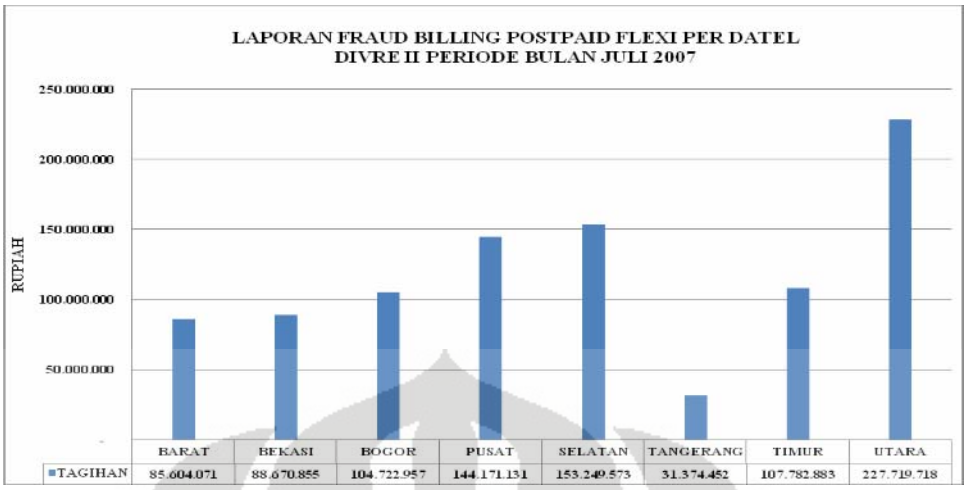
4.7.2. ANALISIS DATA BULAN JULI 2007

Berikut adalah data *fraud billing* periode bulan Juli 2007 seperti ditunjukan pada tabel 4.20 berikut ini :

Tabel 4.20. Data Fraud Billing Divre II Bulan Juli 2007 [21]

DATEL	DATA FRAUD BILLING JULI	
	TAGIHAN	SSF
BARAT	85.604.071	84
BEKASI	88.670.855	87
BOGOR	104.722.957	100
PUSAT	144.171.131	135
SELATAN	153.249.573	148
TANGERANG	31.374.452	31
TIMUR	107.782.883	105
UTARA	227.719.718	218
TOTAL	**943.295.640**	**908**

Data tabel 4.20 diatas menunjukan potensi kerugian pencairan piutang sebanyak 908 pelanggan Flexi *Postpaid* sebesar Rp. 943.295.640 yang berasal dari 8 Datel yang berada dalam layanan Telkom Flexi Divre II dengan komposisi jumlah *fraud billing* per Datel seperti ditunjukan pada gambar 4.25 berikut ini :



Gambar 4.25. Laporan Fraud Billing Postpaid Periode Bulan Juli 2007 [21]

Dari gambar 4.25 diatas terlihat bahwa jumlah fraud billing tertinggi ada di Datel Jakarta Utara sebesar Rp. 227.719.718,- diikuti oleh Datel Jakarta Selatan sebesar Rp. 153.249.573,-. Berikut adalah komposisi pelanggan postpaid *dan* prepaid *Divre II aktif pada bulan Juli 2007 seperti ditunjukan dalam tabel 4.21 berikut ini :*

Tabel 4.21. Pelanggan Postpaid dan Prepaid Divre II Bulan Juli 2007 [22]

PELANGGAN	CLASSY	TRENDY						GRAND TOTAL (CLASSY+ACTIVE)
		VALID	ACTIVE	GRACE	EXPIRED	BLOCK	TOTAL	
JULI 07	325.365	658.880	908.714	106.684	12.775	11.054	1.698.107	1.234.079

Tabel 4.21 diatas adalah komposisi jumlah pelanggan *postpaid* dengan *brand* produk Flexi Classy dan pelanggan prepaid dengan *brand* produk Flexi Trendy. Jumlah pelanggan *postpaid* mencapai 325.365 pelanggan atau 26,37% dari total komunitas pelanggan Telkom Flexi Divre II. Jika data pelanggan *postpaid* tersebut dibandingkan dengan jumlah data *fraud billing postpaid* pada bulan Juli 2007 yang berjumlah 908 nomor, maka besaran pelanggan yang masuk dalam katagori *fraud billing* adalah sebesar 0,28%.

Berikut ini adalah rincian detil data *fraud billing* periode bulan Juli 2007 yang dirinci dalam datel, jumlah tagihan, dan SSF (satuan sambungan flexi) seperti ditunjukan pada tabel 4.22 berikut ini :

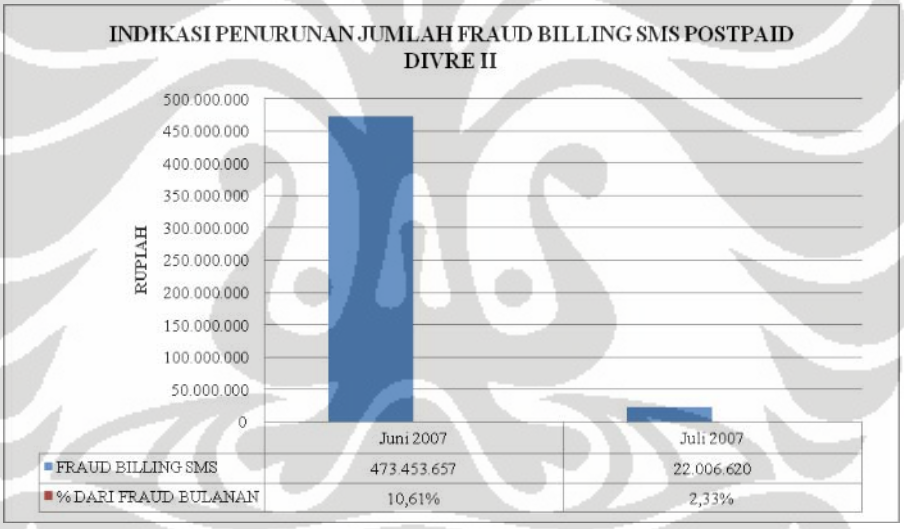
Tabel 4.22. Fraud Billing Pelanggan Postpaid Divre II bulan Juli 2007 [21]

TGL ISOLIR	DATEL																	
	BARAT		BEKASI		BOGOR		PUSAT		SELATAN		TANGERANG		TIMUR		UTARA		TOTAL	TOTAL
	TAGIHAN	SSF	TAGIHAN	SSF	TAGIHAN	SSF	TAGIHAN	SSF	TAGIHAN	SSF	TAGIHAN	SSF	TAGIHAN	SSF	TAGIHAN	SSF	TAGIHAN	SSF
05/07/2007					1.329.455	1			3.663.393	3	1.008.085	1					6.000.933	5
06/07/2007	1.025.267	1	2.178.711	2	5.593.721	4			1.080.190	1					1.027.899	1	10.905.788	9
07/07/2007			1.006.960	1	2.059.274	2			2.060.315	2							5.126.549	5
08/07/2007					4.157.005	4	2.228.917	2	11.622.948	11	1.000.649	1			7.599.939	7	26.609.458	25
09/07/2007					2.172.479	2	4.221.887	4	2.241.588	2	1.000.295	1	1.180.875	1	5.322.922	5	16.140.046	15
10/07/2007			2.025.801	2	1.102.059	1			10.432.068	10			3.132.412	3	5.146.009	5	21.838.349	21
11/07/2007	1.008.927	1	1.014.575	1	4.114.781	4	4.279.421	4	5.071.239	5	1.023.399	1	3.101.689	3	8.389.642	8	28.003.673	27
12/07/2007	1.052.329	1	1.012.494	1	5.151.892	5	4.234.497	4	5.140.468	5			2.054.806	2	12.403.314	12	31.049.800	30
13/07/2007	2.053.951	2	3.102.046	3	7.272.407	7	1.066.566	1	3.126.550	3			1.036.380	1	6.206.867	6	23.864.767	23
14/07/2007	1.043.347	1			1.026.049	1	4.085.774	4	1.014.234	1	1.030.900	1	2.059.883	2	8.276.436	8	18.536.623	18
15/07/2007	1.023.390	1	1.001.950	1	3.059.741	3	4.151.662	4	1.059.134	1	1.010.151	1	3.022.930	3	12.519.700	12	26.848.658	26
16/07/2007			1.044.439	1	2.055.440	2	3.069.000	3					3.039.166	3	8.117.638	8	17.325.683	17
17/07/2007	2.057.446	2			3.050.166	3	10.363.724	10	4.265.813	4	1.030.300	1	5.092.826	5	10.424.906	10	36.295.181	35
18/07/2007	2.043.605	2	2.010.103	2	2.029.230	2	9.181.908	9	7.128.114	7	2.013.097	2	5.039.466	5	8.205.274	8	37.650.797	37
19/07/2007	4.123.178	4	6.072.856	6	3.099.277	3	6.166.131	6	5.068.937	5			3.052.073	3	10.172.989	10	37.755.441	37
20/07/2007	1.002.486	1	1.003.774	1	2.037.890	2	6.111.537	6	3.224.080	3	1.006.263	1	4.095.793	4	5.084.564	5	23.566.387	23
21/07/2007	7.053.046	7	2.013.903	2	8.216.783	8	4.046.375	4	1.024.628	1	1.002.514	1	4.071.729	4	9.109.365	9	36.538.343	36
22/07/2007			1.015.526	1	1.051.344	1	1.004.469	1	2.014.875	2			1.030.404	1	5.240.461	5	11.357.079	11
23/07/2007	1.049.221	1	1.000.523	1	1.007.296	1	5.044.231	5	1.016.975	1	2.022.192	2	2.010.463	2	1.016.718	1	14.167.619	14
24/07/2007	3.076.762	3	8.142.383	8	4.137.711	4	8.316.645	8	8.201.579	8	1.005.926	1	4.015.698	4	11.506.379	11	48.403.083	47
25/07/2007	4.103.562	4	6.040.579	6	6.040.752	6	5.126.271	5	7.158.885	7	2.007.948	2	5.160.297	5	9.221.858	9	44.860.152	44
26/07/2007	3.016.322	3	4.074.104	4	1.034.235	1	3.092.772	3	7.108.684	7	1.009.251	1	3.265.633	3	7.166.411	7	29.767.412	29
27/07/2007	3.045.536	3			2.016.133	2	1.003.987	1	4.131.913	4	1.024.095	1	5.047.433	5	5.013.318	5	21.282.415	21
28/07/2007	9.120.401	9	12.203.749	12	8.184.855	8	29.495.249	26	21.644.487	21			14.405.766	14	19.479.001	19	114.533.508	109
29/07/2007	14.448.684	14	15.363.988	15	9.280.534	9	12.252.196	10	11.124.130	11	4.060.850	4	16.509.762	16	19.397.089	19	102.437.233	98
30/07/2007	17.178.054	17	14.281.858	14	10.329.445	10	15.627.912	15	12.489.939	12	4.010.130	4	9.281.990	9	20.427.638	17	103.626.966	98
31/07/2007	7.068.557	7	3.060.533	3	4.113.003	4			11.134.407	11	5.108.407	5	7.075.409	7	11.243.381	11	48.803.697	48
TOTAL	85.604.071	84	88.670.855	87	104.722.957	100	144.171.131	135	153.249.573	148	31.374.452	31	107.782.883	105	227.719.718	218	943.295.640	908

Dari total *fraud billing* sebesar Rp. 943.295.640,- tersebut kemudian dilanjutkan dengan proses *cross check* rincian *billing* SMS per nomor maka didapat jumlah *fraud b*illing SMS sebesar Rp. 22.006.620,- atau 2,33% dari

jumlah total *fraud billing* bulan Juli 2007 dengan pemakaian SMS rata-rata sebesar Rp. 24.452,- per SSF dan pemakaian SMS tertinggi sebesar Rp. 346.352,-.

Dari laporan diatas maka secara umum telah terjadi indikasi penurunan *fraud billing* SMS yang signifikan seperti ditunjukan pada gambar 4.26 berikut ini :



Gambar 4.26. Indikasi Penurunan Fraud Billing SMS Postpaid Divre II [21] [22]

Dari gambar 4.26 diatas dapat disimpulkan bahwa terjadi indikasi penurunan *fraud billing* SMS antara periode bulan Juni dan Juli 2007 yaitu sebesar 95,35% dari sebelumnya sebesar Rp. 473.453.657,- turun ke angka Rp. 22.006.620,- serta turunnya angka kontribusi *fraud billing* SMS sebesar 10,61% di bulan Juni menjadi 2,33% di bulan Juli 2007.

BAB V
KESIMPULAN

Implementasi aplikasi *anti spamming* SMS terbukti menjadi *tools* yang efektif di jaringan SMS Telkom Flexi dalam menekan angka keluhan pelanggan terhadap SMS penipuan sebesar 87,32% dan menekan angka *fraud billing* SMS sebesar 95,35%.

DAFTAR REFERENSI

[1] _____,Forum Komunikasi SMS Lintas Operator, Medan, 10 Agustus 2006.

[2] _____”,”PT. Telkom, 2007”, http://www.telkom.co.id/pojok-media/siaran-pers/, Mei 2007.

[3] Gwenael Le Bodic, ”*Mobile Messaging Technologies And Service, SMS, EMS and MMS*”, Wiley, 2005.

[4] _____,PT. Telkom, Konfigurasi Jaringan SMS, 2007.

[5] _____,PT. Telkom, Laporan Bulanan Usage SMS Flexi diatas Rp. 1 juta, 2007.

[6] _____”,” The Other Side, www.master.web.id/mwmag/issue/08/content/fokus-the_other_side/fokus-the_other_side.html, November 2002.

[7] Tedjo Tripomo, S.T, M.T, Udan S.T, M.T ”*Manajemen Strategi*”, Rekayasa Sain, 2005.

[8] Moh. Nazir, Ph. D, ”Metode Penelitian”, Ghalia Indonesia, 2003.

[9] Drs. Suarga, M.Sc, M.Math, Ph.D, “Algoritma Pemrograman”, Penerbit Andi Yogyakarta, 2006.

[10] Fredy Rangkuti, ”*Analisis SWOT Teknik Membedah Kasus Bisnis*”, Gramedia Pustaka, 1998.

[11] _____,PT. Telkom, Trafik VAS Messaging Area Divisi Jakarta, 2007.

[12] Evara Samsyiar, S.Kom, “Oracle 9i Optimasi Database”, Elex Media Komputindo, Gramedia, 204.

[13] Imam Heryanto, Budi Raharjo, “Oracle SQL dan PL/SQL Metode praktis mempelajari pemrograman Oracle”, Informatika, 2006.

[14] Bernaridho I. Hutabarat, M.Sc, OCP, “Oracle 8i untuk Administrator Database”, Elex Media Komputindo, Gramedia, 2003.

[15] Hewlet Packard Company, “HP-UX Reference – Release 11.i Section 1M, System Administrator Command, Vol 4 of 9, Part 2 of 2 (N-Z), Hewlet Packard, 2000.

[16] Hewlet Packard Company, “HP-UX Reference – Release 11.i Section 3(A-M), Library Function, Vol 6 of 9, Part 1 of 2 (N-Z), Hewlet Packard, 2000.

[17] Betha Sidik, Ir., “ MySQL Untuk Pengguna, Administrator, dan Pengembang Aplikasi”, Informatika, 2003.

[18] _____,PT. Telkom, Data Aplikasi Anti Spamming SMS, 2007.

[19] _____,PT. Telkom, Data Performansi VAS, 2007.

[20] _____,PT. Telkom, Data Performansi HLR, 2007.

[21] _____,PT. Telkom, Data Fraud Billing Bulan Juli, 2007.

[22] _____,PT. Telkom, Data Customer Care Area Jakarta, 2007.

[23] _____, PT. Telkom, Resume hasil questioner SWOT, 2007.