

Laporan Proyek Akhir
Keamanan Sistem Informasi
EC-5010

Analisis Fraud pada Jaringan IP dan Next-Generation

Judge Septopanduviyatmo
13200006

1. Pendahuluan

Fraud merupakan suatu bentuk penipuan ataupun kecurangan yang dilakukan oleh orang yang tidak bertanggung jawab. Pada makalah ini, fraud yang dimaksud adalah fraud pada bidang telekomunikasi, khususnya yang menggunakan jaringan IP (*Internet Protocol*) dan Next-Generation. Pada bagian berikutnya dari makalah ini akan dijelaskan definisi fraud secara lebih mendalam.

Karena fraud merupakan tindakan yang ilegal, maka fraud harus dapat dideteksi dengan tepat dan cepat. Untuk itu perlu didesain suatu Sistem Manajemen Fraud (SMF) yang dapat mendeteksi fraud secara tepat dan cepat sehingga dapat membantu proses investigasi kejadian-kejadian fraud tersebut. Sistem Manajemen Fraud ini juga akan dibahas secara lebih mendalam pada bagian berikutnya dari makalah ini.

Makalah ini sendiri mendiskusikan peranan penting dari Sistem Manajemen Fraud (SMF) dalam mengatasi masalah fraud pada jaringan IP dan Next-Generation, kelemahan teknologi berbasis IP (*Internet Protocol*) yang mudah diserang, algoritma dan analisis data yang efektif. Jaringan Next-Generation yang bersifat terbuka dan terdistribusi memungkinkan akses yang mudah ke layanan, informasi, dan sumber daya jaringan. Hal ini memancing para *hacker*, pelaku fraud, dan unit-unit kejahatan yang terorganisasi untuk mengakses layanan, informasi, dan sumber daya jaringan secara ilegal. Para pelaku fraud memperkenalkan berbagai teknik fraud yang baru dan kompleks setiap harinya. Kegiatan mereka ini sangat sulit untuk dideteksi sehingga dapat menimbulkan kerugian di sisi operator dan juga penyedia layanan. Oleh karena itu, diperlukan pendekatan yang baru dalam bidang manajemen fraud untuk mengantisipasi berbagai fraud yang akan mungkin terjadi.

2. Fraud Telekomunikasi

Fraud merupakan kata yang berasal dari bahasa Inggris. Berdasarkan kamus ringkas Oxford, fraud didefinisikan sebagai tindakan kriminal berupa penipuan atau kecurangan; penggunaan sesuatu berbentuk apa pun secara salah untuk mendapatkan keuntungan yang tidak seharusnya didapat. Definisi fraud telekomunikasi sendiri cukup banyak, mungkin sebanyak manajer fraud yang bekerja di industri yang mengungkapkan definisi fraudnya masing-masing. Berikut ini akan diberikan beberapa definisi fraud telekomunikasi yang diperoleh dari beberapa referensi.

Di [1] disebutkan bahwa fraud telekomunikasi merupakan pencurian layanan telekomunikasi atau penggunaan layanan telekomunikasi untuk melakukan fraud dalam bentuk yang lain. Korbannya meliputi pelanggan, penyedia layanan bisnis dan penyedia layanan telekomunikasi. Para pelaku fraud melakukan fraud untuk berbagai macam alasan, di antaranya adalah untuk memperoleh keuntungan, untuk menyembunyikan kegiatan ilegal (seperti perdagangan obat-obatan terlarang, prostitusi, dan sebagainya), dan untuk hiburan (beberapa pelaku memperoleh kepuasan ketika berhasil melakukan fraud).

Di [2], fraud telekomunikasi didefinisikan sebagai pencurian layanan atau penyalahgunaan jaringan suara dan data yang dilakukan secara sengaja. Masih menurut [2], tujuan para pelaku fraud telekomunikasi ini adalah untuk menghindari atau paling tidak mengurangi biaya yang seharusnya mereka bayar untuk penggunaan suatu layanan telekomunikasi.

Dari definisi fraud telekomunikasi yang telah disebutkan sebelumnya, definisi fraud telekomunikasi dapat dirangkum menjadi sebagai berikut. Fraud telekomunikasi adalah penggunaan perangkat dalam bentuk apapun, baik itu perangkat keras (*hardware*) maupun lunak (*software*), untuk melakukan pencurian layanan telekomunikasi sehingga pelakunya dapat terhindar dari kewajiban membayar biaya yang seharusnya dibayar untuk penggunaan layanan telekomunikasi tersebut, atau untuk menggunakan layanan telekomunikasi untuk melakukan fraud telekomunikasi dalam bentuk lainnya.

Fraud telekomunikasi sebenarnya merupakan bisnis bernilai jutaan dolar. Kerugian yang disebabkan oleh fraud diperkirakan berkisar antara 30 juta dolar sampai lebih dari 40 juta dolar pada tahun 2000, atau dengan kata lain, penyedia

layanan telekomunikasi kehilangan sekitar 3% sampai 8% dari rata-rata keuntungan tahunannya [3]. Secara domestik (di Amerika Serikat), perkiraan kerugian akibat fraud pada industri telekomunikasi Amerika Serikat berkisar antara 4% sampai 6% dari pendapatan. Secara internasional, keadaannya lebih buruk, kerugian yang dilaporkan oleh penyedia layanan mencapai 20% dari pendapatan [4]. Statistik saat ini menunjukkan bahwa kerugian global akibat fraud telah mencapai 55 juta dolar per tahun. Hal ini menjadikan fraud telekomunikasi sebagai bisnis yang lebih besar daripada bisnis perdagangan obat-obatan terlarang internasional [2].

Jaringan Next-Generation telah terbukti sebagai lahan yang subur untuk pertumbuhan fraud teknologi dan aktivitas kejahatan. Saat ini telah banyak penipuan-penipuan dengan teknologi tinggi yang canggih yang dapat dilakukan oleh unit-unit kejahatan yang terorganisasi dan *hacker* yang memiliki pengetahuan akan teknik-teknik fraud. Ketersediaan informasi mengenai *hacking* dan kemudahan untuk melakukan kegiatan-kegiatan yang ilegal memungkinkan bahkan orang yang amatir untuk menyerang dan menyalahgunakan jaringan, sumber dayanya, dan *account* pelanggannya. Hal-hal seperti ini akan sering terjadi dan dapat menyebabkan penyedia layanan kehilangan keuntungannya, jaringannya menjadi *down*, dan kegagalan layanan yang disediakannya. Akibatnya jaringan menjadi tidak aman dan tidak efisien.

Pada jaringan Next-Generation, kerugian yang dialami oleh penyedia layanan dapat menjadi semakin besar seiring dengan bertambahnya layanan-layanan baru dan meningkatnya jumlah transaksi bisnis yang dilakukan melalui jaringan yang terbuka dan terdistribusi. *Landscape* dari jaringan Next-Generation yang dinamis, akan terus berubah-ubah untuk mengakomodasi masuknya pemain-pemain baru, *merger* dan akuisisi perusahaan penyedia jasa layanan. Jaringan Next-Generation harus mampu menangani munculnya teknologi baru yang terus berkembang, berbagai metode akses yang baru, dan skema *billing* yang juga baru. Teknik fraud generasi baru akan lebih kompleks dan bervariasi dibandingkan teknik fraud yang ada sekarang, sehingga solusi efektif untuk mengatasi masalah fraud ini memerlukan perlengkapan dan metodologi yang benar-benar baru dan inovatif. *Hacker* dan para pelaku kejahatan dunia maya seringkali memiliki teknologi yang lebih canggih dibandingkan teknologi yang dimiliki oleh para personil pengelola jaringan. Mereka juga lebih cepat memiliki pengetahuan yang dibutuhkan untuk menghindari mekanisme keamanan jaringan jauh

sebelum para personil pengelola jaringan mendapatkan pelatihan mengenai hal tersebut. *Internet Relay Chat* (IRC) memungkinkan para *hacker* untuk saling bertukar ide, tips, dan lokasi situs web yang menyediakan perlengkapan *hacking* melalui koneksi jaringan yang terbuka, menyediakan segudang informasi berbahaya mengenai *hacking*. Metode *hacking* yang sebelumnya berbasis *command-line* telah digantikan oleh *Graphical User Interface* (GUI) yang lebih memudahkan orang untuk belajar. Hal ini memungkinkan orang awam sekalipun untuk belajar dan memahami berbagai teknik fraud untuk kemudian melakukannya.

3. Keamanan Jaringan Penyedia Layanan

Secara tradisional, intrusi jaringan yang bersifat ilegal sebenarnya berhubungan dengan devais-devais yang mengendalikan akses ke jaringan seperti firewall, N-IDS, H-IDS, dan server autentikasi, seperti server RADIUS (*Remote Authentication Dial-In User Service*). Akan tetapi devais-devais ini tidak lagi berguna dalam menghadapi tipe-tipe fraud baru yang dilakukan pada jaringan Next-Generation berbasis IP. Devais-devais tadi awalnya dibuat untuk tujuan yang spesifik dan tidak mencakup berbagai kemungkinan fraud IP. Setiap devais tersebut didesain untuk mendukung hanya satu protokol (biasanya IP), terbatas hanya pada satu lokasi, dan hanya aman untuk satu bagian dari jaringan saja.

Firewall melakukan *filtering* awal terhadap trafik yang akan menuju bagian atau sumber daya tertentu dari jaringan. Firewall biasanya mengklasifikasikan trafik berdasarkan alamat IP-nya. Ini sebenarnya menjadikan firewall tidak handal. Mekanisme autentikasi dan otorisasi dengan menggunakan server AAA (*Authorization, Authentication, and Accounting*) atau RADIUS membatasi akses ke jaringan dan sumber dayanya, memungkinkan penggunaan sumber daya jaringan bila pelanggan atau pengguna melewati tahap identifikasi dengan memasukkan passwordnya masing-masing. Akan tetapi, password untuk tahap identifikasi pengguna dapat dengan mudah didapatkan atau ditebak, sehingga seorang pengguna yang sedang terkoneksi ke jaringan belum tentu pengguna sah atau legal yang sebenarnya.

Network Intrusion Detection System (N-IDS) dapat membatasi serangan pada protokol tertentu dengan menangkap paket-paket dan *streams* yang mencurigakan ke

host tertentu. Sementara *Host Intrusion Detection System* (H-IDS) dapat membatasi serangan terhadap aplikasi tertentu dengan menangkal aktivitas mencurigakan yang dilakukan pada tingkat aplikasi di sistem operasi.

Devais-devais yang telah disebutkan di atas belum dapat mengenali teknik dan pola fraud yang baru dan canggih yang dapat mempengaruhi pendapatan operator jaringan dan penyedia layanan.

Fraud IP dapat dilakukan dari beberapa titik di jaringan secara bersamaan, atau dari beberapa titik yang berbeda secara bergantian. Oleh karena itu, kesuksesan deteksi aktivitas fraud membutuhkan pertukaran informasi antara semua elemen jaringan, devais, dan antar muka, diikuti dengan perbandingan dan analisis semua trafik data yang melewati jaringan. Elemen jaringan dan mekanisme keamanan yang ada sekarang ini sangat kurang kemampuannya dalam mengkomunikasikan dan mempertukarkan informasi berharga di antara mereka. Untuk mengkomunikasikan informasi berharga tadi dibutuhkan intervensi penghubung yang pintar untuk memonitor semua titik interkoneksi dan mengumpulkan, memproses, serta mendistribusikan data yang relevan serta meyakinkan bahwa semua kemungkinan intrusi telah tercakupi.

4. Kelemahan Jaringan IP dan Next-Generation

Infrastruktur jaringan Next-Generation dan IP berbasis paket dan *multilayer*, dengan arsitektur terbuka dan terdistribusi. Tidak ada mekanisme keamanan yang melekat pada infrastruktur jaringan Next-Generation dan IP. Aplikasi *mission-critical*, yang digunakan untuk transmisi layanan dengan keuntungan tinggi seperti layanan suara, *e-commerce*, dan transaksi keuangan, dijalankan pada jaringan yang sedemikian terbuka dan tidak terlindungi ini. Berikut ini berbagai kelemahan jaringan IP dan Next-Generation yang dapat dimanfaatkan untuk melakukan fraud:

- ✍ Identifikasi pengguna dilakukan pada *layer* IP, sementara *layer* IP sendiri dapat dengan mudah ditembus, sehingga paket-paket yang melalui jaringan akan dapat dengan mudah ditandai atau dicirikan sebagai alamat IP yang 'dipinjam' (*borrowed IP address*). Ini memungkinkan pengguna ilegal untuk menyamar atau berkedok sebagai pengguna yang sah. Penyusup ini menyalahgunakan layanan dan mengambil keuntungan dari pengguna yang

sah. Yang sangat dirugikan tentu pengguna yang sah itu, dimana seringkali ia tidak sadar bahwa *account*-nya digunakan oleh orang lain sampai datangnya tagihan yang tiba-tiba membengkak sedemikian mahalannya. Dan hal ini biasanya baru disadari setelah si penyusup sudah pergi jauh. Tipe fraud seperti ini biasa disebut *IP spoofing*. Kemungkinan bahwa sebuah alamat IP telah diubah atau dipalsukan menyebabkan data yang dikeluarkan oleh *layer* IP menjadi tidak handal.

- ✎ Seperti telah disebutkan sebelumnya bahwa firewall juga menggunakan alamat IP untuk mengklasifikasikan trafik, dan oleh karenanya ia bukan merupakan perlengkapan yang cukup ampuh dalam keamanan jaringan karena alamat IP mudah dipalsukan dan disalahgunakan.
- ✎ Sistem operasi populer yang kelemahannya telah diketahui banyak orang, seperti Linux, Windows, dan Unix, berjalan di atas server yang penting dan kritis (termasuk firewall, RADIUS, dan server autentikasi), sehingga memungkinkan serangan dilakukan dengan mudah, bahkan oleh anak-anak sekalipun dengan skrip *kiddies*-nya.
- ✎ Protokol-protokol pada jaringan IP dan Next-Generation seperti *routing protocol*, *Voice-over-IP (VoIP) signalling*, resolusi *Domain Name Service (DNS)*, dan email (POP, SMTP) merupakan pengetahuan yang sudah umum diketahui oleh banyak orang sehingga memungkinkan orang untuk melakukan manipulasi pada transmisi data melalui protokol-protokol tersebut.
- ✎ Medium komunikasi berbagi pakai seperti modem kabel, transmisi nirkabel, dan *Local Multipoint Distribution System (LMDS)* membutuhkan penggunaan devais koneksi yang sederhana dan murah yang memungkinkan penggunaan panggilan dan layanan jaringan secara bebas, koneksi ilegal ke internet dengan menggunakan *account* atau ID pengguna yang sah, dan pemalsuan atau peniruan pengguna yang telah sah terdaftar untuk mengakses layanan yang berhak ia terima. Selain medium komunikasi berbagi seperti di atas, berbagai perbuatan tidak bertanggung jawab seperti pelanggaran privasi yang disebabkan oleh akses ilegal ke layanan user lainnya, *password sniffing* (mendapatkan password orang lain secara ilegal tanpa sepengetahuan orang tersebut), dan fraud clip-on juga membutuhkan devais akses yang sederhana dan murah pula.

- ✍ Kurangnya mekanisme kontrol yang melekat pada infrastruktur jaringan dan aplikasi berbasis IP atau web turut menyebabkan rendahnya kemampuan bertahan hidup suatu jaringan. Kurangnya mekanisme kontrol manajemen trafik memungkinkan terjadinya pencurian bandwidth, yaitu adanya pengguna yang mentransmisikan trafik yang ukurannya lebih besar daripada ukuran yang dialokasikan untuknya sehingga menyebabkan pengguna lainnya memperoleh bandwidth yang lebih kecil dari yang seharusnya diperoleh. Kurangnya kontrol kemacetan dan *overload* trafik memungkinkan terjadinya sabotase dalam bentuk serangan *Denial-of-Service* (DoS) pada berbagai layanan jaringan (kebanyakan serangan terjadi pada situs-situs web populer). Salah satu cara untuk melakukan serangan ini adalah dengan membanjiri server dengan permintaan layanan yang sah secara berulang-ulang, sehingga kinerja server menjadi menurun atau sama sekali tidak bisa melayani permintaan pengguna lain yang merupakan pengguna sah yang membayar biaya layanan jaringan.
- ✍ Skema *billing* baru yang berdasarkan pada *content* dan kualitas layanan menciptakan kelemahan sistem lainnya yang dapat disalahgunakan oleh orang-orang yang tidak bertanggung jawab. Makin baik kualitas layanan, makin tinggi keuntungan yang diperoleh penyedia layanan. Ini merupakan satu potensi yang besar bagi para pelaku fraud untuk terus meningkatkan metode fraudnya.

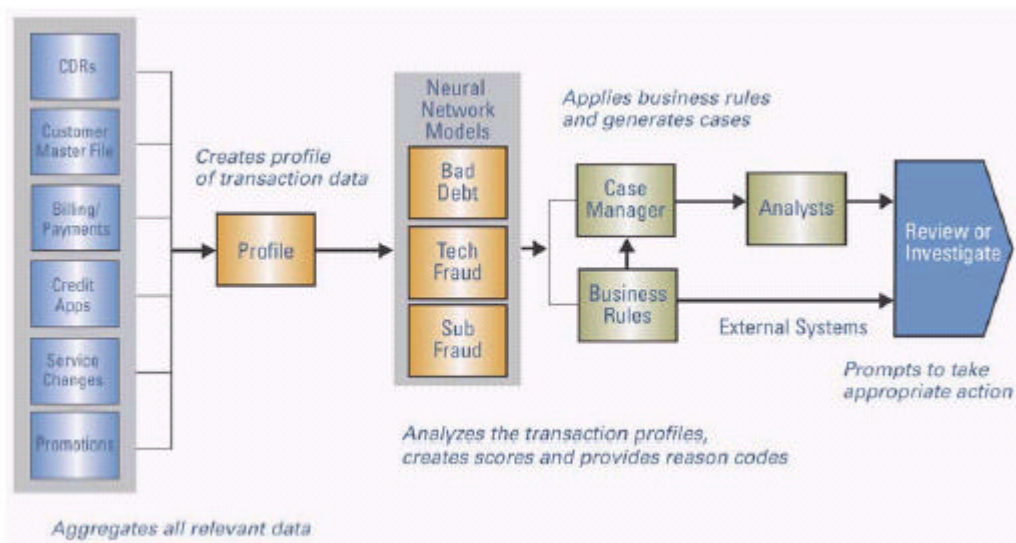
5. Sistem Manajemen Fraud (SMF)

Sistem manajemen fraud (SMF) adalah suatu sistem aplikasi yang dapat mendeteksi dan menangani kasus-kasus fraud dengan cepat dan efektif. Suatu SMF harus memiliki kemampuan sebagai berikut [5]:

- ✍ Mengumpulkan dan menyimpan data transaksi pelanggan, menganalisis transaksi dengan algoritma atau metode tertentu, seperti model jaringan syaraf tiruan (*neural network*), dan meng-*update* profil transaksi pelanggan.
- ✍ Menganalisis interaksi antara ribuan variabel data transaksi pelanggan secara simultan dan secara otomatis mengidentifikasi pola fraud yang mungkin terjadi.

- ✍ Memiliki Manajer Kasus yang mudah untuk digunakan dan menyediakan antar muka yang *user-friendly*.
- ✍ Melaporkan daftar lengkap kemungkinan fraud yang terjadi berdasarkan profil transaksi, analisis performa sistem, dan investigasi kasus.
- ✍ Mampu mendukung sistem dengan jutaan pelanggan dan transaksi harian.

SMF memiliki tiga komponen utama, yaitu pengumpul dan penyimpan data, penganalisis data, serta Manajer Kasus sebagai antar muka ke pengguna akhir. Pengumpul dan penyimpan data merupakan suatu sistem basis data yang dapat mengambil dan menyimpan data, baik itu data pelanggan, data transaksi, data *billing*, dan sebagainya. Sementara komponen penganalisis data harus mampu menganalisis data yang tersimpan di basis data dan mendeteksi adanya fraud dari data-data tersebut. Data-data mengenai detail fraud, seperti pelanggan yang dicurigai melakukan fraud, waktu terjadinya fraud, profil transaksi, profil pelanggan, dan seterusnya, ditampilkan oleh Manajer Kasus ke pengguna akhir (investigator) sebagai antar muka yang harus bersifat *user-friendly*. Berikut ini contoh arsitektur SMF [5]:



Gambar 1 Arsitektur Sistem Manajemen Fraud (SMF) [5]

5.1 Pengumpulan dan Penyimpanan Data

Pengumpulan data merupakan langkah awal dari kerja SMF. Mendapatkan informasi yang lengkap dan beragam dari berbagai *layer* jaringan merupakan faktor kunci untuk kesuksesan sebuah SMF di lingkungan jaringan IP dan Next-Generation [3]. *Probing* untuk mendapatkan informasi tentang jaringan dan penggunaannya

dilakukan pada berbagai *layer* dan tingkatan jaringan. Berikut ini akan dibahas cara memperoleh informasi-informasi tersebut.

5.1.1 Rekaman Penggunaan Tingkat Aplikasi

Rekaman penggunaan tingkat aplikasi memberikan gambaran mengenai layanan yang disediakan untuk pelanggan. Pada umumnya, rekaman ini juga digunakan untuk *billing*, karena rekaman ini menyediakan semua detail yang dibutuhkan mengenai layanan yang digunakan. Rekaman untuk *billing* ini diambil dari server-server yang menyediakan layanan tertentu seperti layanan telpon, layanan video, dan sebagainya. Rekaman tingkat aplikasi dapat diperoleh dari devais-devais seperti:

- ✍ *Media gateway controllers* (protokol MGCP, H.248) dan *gatekeepers* (protokol H.323) pada sistem VoIP.
- ✍ Server *broadcast* untuk *music on demand* dan server video.
- ✍ Switch suara (*voice switches*).
- ✍ Server email dan server Web atau WAP (*Wireless Access Protocol*) untuk komunikasi nirkabel.

5.1.2 Tingkat Login dan Autentikasi

Jaringan IP dan NGN pada umumnya memiliki berbagai mekanisme login, autentikasi, otorisasi, dan keamanannya masing-masing. Mekanisme-mekanisme ini biasa disebut '*layer* login dan autentikasi' dan dapat menyediakan informasi yang sangat penting bagi sebuah sistem penganalisis fraud. Informasi yang disediakan oleh mekanisme login dan autentikasi dapat diperoleh dari devais-devais:

- ✍ Server RADIUS (*Remote Authentication Dial-In User Service*) dan LDAP
- ✍ *Remote access server* (RAS)
- ✍ Server DHCP
- ✍ Server DNS (*Domain Name Service*)
- ✍ Firewalls
- ✍ Gateway VPN (*Virtual Private Network*)

5.1.3 Informasi Tingkat Jaringan

Informasi tingkat jaringan menjelaskan trafik dan alirannya pada *layer* IP. *Layer* ini biasanya mengkarakterisasi konsumsi *bandwidth* dan sumber daya jaringan. Elemen jaringan yang menyediakan informasi ini antara lain:

- ✍ Router dan switch
- ✍ Cisco Netflow
- ✍ SNMP/RMON I + II
- ✍ NAT (*Network Address Translation*)

5.1.4 Tingkat Akses

Jaringan akses digunakan sebagai teknologi yang menghubungkan pelanggan dengan sumber daya jaringan yang disediakan oleh operator. Teknologi akses diimplementasikan misalnya dengan menggunakan kabel, *wireless*, DSL (Digital Subscriber Line), dan *dialup*. *Layer* ini menyediakan informasi mengenai lokasi pengguna, perangkat keras, dan alamat terminal pengguna seperti IMSI, nomor serial, alamat MAC, dan sebagainya. Statistik yang diperoleh dari tingkat jaringan akses biasanya tidak terpengaruh dengan apa yang ada pada *layer* IP, sehingga informasi dari tingkat ini sangat berguna untuk mendeteksi kejadian-kejadian yang mencurigakan. Informasi tingkat akses dapat diperoleh dari elemen-elemen sebagai berikut:

- ✍ RAS
- ✍ CMTS
- ✍ DSLM
- ✍ *Integrated Multiservice Access Platform* (IMAP)
- ✍ LMDS/WLL base stations

5.1.5 Triggered Content Events

Triggered content events dihasilkan oleh *probes* yang memeriksa setiap paket yang dibawa sepanjang jaringan. *Probes* ini dapat mencari teks di dalam paket yang dianggap sebagai sebagai skrip “eksploit” (digunakan untuk hacking). *Triggered content events* saat ini digunakan oleh sistem deteksi intrusi (*Intrusion Detection System*), tetapi sebenarnya juga berguna untuk mendeteksi perilaku-perilaku fraud.

Setelah diambil dan dikumpulkan, data-data tadi harus disimpan oleh suatu sistem basis data. Sistem basis data yang paling sederhana berupa file teks sederhana yang menyimpan detail dari data dalam bentuk kolom dan baris. Tetapi sistem basis data dengan file teks sederhana ini tidak akan dapat mengolah data dengan jutaan baris dan puluhan kolom, karena akan menjadi sangat rumit dan kompleks. Untuk menangani data dengan jutaan baris, kita harus memiliki sistem manajemen basis data relasional (*Relational Data Base Management System*) yang dapat menyimpan dan mengolah data dengan efisien dan efektif. Saat ini terdapat banyak RDBMS yang tersedia, baik yang gratisan maupun yang harus membayar. Bila kita menginginkan RDBMS gratisan yang cukup baik, kita dapat memilih RDBMS MySQL atau PostgreSQL. Untuk segmen korporat, RDBMS yang biasa dipilih adalah Oracle dan MS SQL Server. Harga RDBMS untuk segmen korporat seperti Oracle dan MS SQL Server biasanya sangat mahal karena memiliki berbagai fitur yang sangat berguna untuk pengolahan dan pemrosesan data.

5.2 Algoritma Analisis Data

Banyak algoritma yang telah dikembangkan untuk mendeteksi fraud di jaringan telpon dan seluler, seperti yang digunakan oleh N-IDS dan H-IDS. Institusi-institusi penelitian saat ini sedang melakukan penelitian mengenai algoritma IDS yang baru, dimana metode deteksi yang digunakan telah mencakup kemampuan yang dimiliki oleh sistem pakar (*expert system*), *data mining*, intelegensia buatan (*artificial intelligence*), dan pembelajaran mesin (*machine learning*). Algoritma-algoritma ini dapat diimplementasikan dengan berbagai bahasa pemrograman yang ada, seperti dengan bahasa C, Java, Oracle PL/SQL, dan sebagainya.

SMF untuk jaringan IP dan Next-Generation harus mampu mengembangkan metode deteksinya saat ini melalui pengenalan algoritma-algoritma yang baru agar tidak hanya mampu mendeteksi teknik-teknik fraud yang ada saat ini, tapi juga teknik-teknik fraud yang baru dan canggih. Selain itu, SMF juga harus mampu mengurangi jumlah kesalahan pengklasifikasian biner dalam menentukan fraud. Di [6] disebutkan bahwa ada dua tipe kesalahan pengklasifikasian biner, yaitu alarm yang salah (*false-positive*) dan kasus fraud yang tidak tertangkap (*false-negative*) seperti yang terlihat pada Tabel 1 di bawah ini.

Tabel 1 Tipe kesalahan pengklasifikasian biner [6]

	Fraud	Bukan Fraud
Alarm menyala	Tepat	<i>False-positive</i>
Alarm tidak menyala	<i>False-negative</i>	Tepat

Berikut ini diberikan beberapa metode analisis data untuk mendeteksi fraud dari data yang telah kita peroleh dari berbagai lapisan jaringan sebelumnya.

5.2.1 Analisis Berdasarkan Batas (*Threshold-based analysis*)

Identifikasi fraud dengan membandingkan pola trafik dengan batas yang telah didefinisikan sebelumnya merupakan metode yang sederhana dan sangat efektif. Sistem ini berdasarkan pada konsep dimana kebanyakan kerugian yang dialami oleh penyedia jaringan disebabkan oleh fraud yang dilakukan pada skala yang besar. Metode seperti ini dapat menghasilkan peringatan ketika, sebagai contoh, jumlah panggilan dari suatu lokasi tertentu melebihi batas jumlah panggilan yang ditetapkan untuk lokasi itu. Metode ini dapat digunakan untuk mengenali pencurian panggilan dengan durasi panjang, pendek, dan panggilan dengan biaya yang mahal.

Kelebihan algoritma ini adalah ia dapat diimplementasikan dengan sederhana dan efisien, sehingga dapat mendukung jumlah trafik yang besar yang dibawa sepanjang jaringan. Akan tetapi, metode ini membutuhkan *fine-tuning* untuk menyesuaikan *setting* batas (*threshold*) agar sesuai dengan kebutuhan operator jaringan. Kelemahan algoritma ini adalah ia tidak dapat mendeteksi beberapa tipe fraud, terutama fraud-fraud tipe baru.

5.2.2 Analisis *Inference-Rules*

Analisis *inference-rules* merupakan metode pendeteksi fraud yang berdasarkan pada sistem pakar (*expert system*) dan mesin penghasil aturan (*rules*). Teknik ini memungkinkan konfigurasi awal *inference-rules* yang spesifik dan canggih untuk menentukan tipe fraud yang mungkin muncul. Sebagai contoh, administrator sistem dapat mengatur sistem dengan *inference-rules* sebagai berikut yang berguna untuk mendeteksi fraud tipe panggilan balik (*callback*):

- ☞ Jika panggilan dilakukan oleh nomor domestik C
- ☞ **dan** tujuan panggilan merupakan nomor luar negeri X

- ✍ **dan** durasi panggilan kurang dari 10 detik
- ✍ **dan** nomor luar negeri X memanggil nomor domestik C selama 30 detik
- ✍ **maka** peringatan adanya fraud tipe panggilan balik (*callback*) menyala; panggilan ini perlu diproses lebih lanjut untuk investigasi.

Analisis *inference-rules* sangat sulit untuk di-*manage* karena konfigurasi aturan-aturannya membutuhkan pemrograman yang presisi, melelahkan, dan menghabiskan waktu untuk setiap kemungkinan tipe fraud. Dinamika kemunculan berbagai tipe fraud yang baru membutuhkan aturan-aturan yang harus disesuaikan dengan tipe-tipe fraud yang sudah ada dan tipe-tipe fraud baru yang canggih.

Kelemahan dari metode ini adalah skalabilitas. Semakin banyak data sistem yang harus diproses, performanya akan semakin menurun drastis. Kelebihannya, sistem ini sangat baik untuk mendeksi berbagai pola trafik dan tipe fraud.

5.2.3 Analisis Berbasis Profil

Analisis berbasis profil dapat juga digunakan untuk mendeteksi aktivitas fraud. Profil pelanggan menggambarkan kebiasaan dan pola penggunaan layanan jaringan setiap penggunanya. Deviasi atau penyimpangan dari profil pelanggan ini dapat secara cepat diketahui oleh operator jaringan. Sebagai contoh, pelanggan “Jones” yang berdomisili di Amerika Serikat diketahui biasa melakukan panggilan dengan pola mingguan sebagai berikut: 5 – 15 panggilan lokal, 2 – 10 panggilan interlokal, dan 0 – 4 panggilan internasional. Sistem ini akan melakukan perbandingan dan analisis rekaman penggunaan mingguan pelanggan “Jones” dengan profil kebiasaannya dan menampilkan hasilnya.

Untuk mengilustrasikan tipe analisis ini, di bawah diberikan daftar panggilan VoIP yang dilakukan oleh pelanggan “Jones” selama seminggu:

Tabel 2 Daftar panggilan VoIP pelanggan Jones [3]

Nama:	Mr. Jones	
ID Pelanggan:	#0667-33	
Layanan	VoIP	
Nomor	Lokasi	Durasi (menit)
552-4625	NY	1,23
237-2671	TX	5,02
346-2899	NY	2,35
211-2328	CO	4,12
921-5032	MI	2,53
517-8321	NY	9,44
573-1129	NY	1,23
321-4002	NY	7,08
627-5384	GA	4,20
44-20-3441-2755	London UK	10,00
312-4002	NY	3,27
237-2671	TX	6,36
44-20-3441-2633	London UK	11,45
573-1129	NY	4,31
544-2829	NY	2,33
552-4625	NY	6,17

Log panggilan tidak normal berikut ini mengindikasikan fraud pada penglihatan pertama kita, yaitu banyaknya panggilan internasional yang lebih dari biasanya (0 – 4 panggilan):

Tabel 3 Log panggilan tidak normal [3]

Nama:	Mr. Jones				
ID Pelanggan:	#0667-33				
Layanan	VoIP				
Nomor	Lokasi	Durasi (mnt)	Nomor	Lokasi	Durasi (mnt)
234-1-442-3611	Nigeria	125,03	234-1-442-3611	Nigeria	125,03
234-1-442-3611	Nigeria	51,34	234-1-442-3611	Nigeria	94,22
234-1-442-3611	Nigeria	45,22	234-1-442-3611	Nigeria	132,45
234-1-442-3611	Nigeria	143,54	234-1-442-3611	Nigeria	174,12
234-1-442-3611	Nigeria	156,26	258-1-702-4391	Mozambik	64,53
517-8321	NY	6,03	258-1-702-4391	Mozambik	132,44
509-237-1062	Haiti	81,43	517-8321	NY	1,23
509-237-1062	Haiti	128,27	258-1-702-4391	Mozambik	156,06
234-1-442-3611	Nigeria	110,41	258-1-702-4391	Mozambik	123,20
509-237-1062	Haiti	73,46	258-1-702-4391	Mozambik	130,00
509-237-1062	Haiti	147,04	509-237-1062	Haiti	53,27
237-2671	TX	4,35	509-237-1062	Haiti	121,36
44-20-3441-2633	London	10,52	509-237-1062	Haiti	104,45
258-1-702-4391	Mozambik	172,55	517-8321	NY	4,31
258-1-702-4391	Mozambik	180,43	517-8321	NY	2,33
258-1-702-4391	Mozambik	97,38	627-5384	GA	5,21

Analisis berbasis profil memiliki banyak keuntungan. Kita dapat dengan cepat melihat adanya fraud dari daftar panggilan seperti yang diberikan di atas. Kita juga tidak membutuhkan aturan fraud yang dikonfigurasi sebelumnya seperti pada algoritma analisis *inference-rules*. Akan tetapi algoritma ini juga memiliki kelemahan, yaitu kemungkinan bahwa pelanggan “Jones” benar-benar melakukan koneksi ke Nigeria, Haiti, dan Mozambik memungkinkan adanya alarm *false-positive* dalam jumlah yang cukup besar. Pemeriksaan alarm *x-positive* untuk menentukan apakah termasuk *false-positive* atau *true-positive* memerlukan investigasi melelahkan dengan durasi yang panjang yang harus dilakukan oleh banyak pegawai.

5.2.4 Jaringan Syaraf Tiruan (*Neural Networks*)

Jaringan syaraf tiruan (*neural networks*) merupakan pendekatan inovatif yang didesain untuk berfungsi seperti otak manusia. Penciptaan teknologi ini bermula dari ide bahwa sistem yang mensimulasikan tanggapan syaraf, seperti asimilasi independen data *real-time* dan pemicu rantai perintah yang berurutan untuk merespon data ini, lebih pintar dibandingkan dengan sistem konvensional. Jaringan syaraf tiruan (*neural networks*) dapat mengkalkulasi dan menganalisis profil pengguna secara independen, sehingga ia dapat beradaptasi dengan kelakuan pengguna-pengguna lainnya. Jaringan syaraf tiruan diklaim dapat mengurangi biaya operasi karena kemampuan belajar mandiri. Akan tetapi jaringan syaraf tiruan juga memiliki kelemahan, yaitu ketika mengidentifikasi deviasi atau penyimpangan profil pengguna, jaringan syaraf tiruan tidak dapat menjelaskan dengan logis hasil kalkulasinya tadi (alasan mengapa profil pengguna yang diperiksanya diduga mengandung fraud). Algoritma analisis berbasis profil dapat diimplementasikan dengan menggunakan jaringan syaraf tiruan ini untuk meningkatkan kemampuan deteksinya dan mengurangi jumlah kesalahan *false-positive* maupun *false-negative*.

5.3 Manajer Kasus

Manajer Kasus berfungsi sebagai antar muka antara Sistem Manajemen Fraud (SMF) dengan pengguna akhir. Pengguna akhir akan menganalisis dan menginvestigasi lebih lanjut kasus-kasus fraud yang ditampilkan oleh Manajer Kasus. Data-data yang ditampilkan dapat disesuaikan dengan kebutuhan operator jaringan, misalnya saja nomor kasus fraud, pelanggan yang dicurigai melakukan fraud, status kasus fraud, tipe fraud, tanggal terjadinya kasus fraud, dan sebagainya.

Manajer Kasus biasanya diimplementasikan sebagai aplikasi berbasis web, atau paling tidak memiliki tampilan seperti sebuah *browser* web. Di bawah ini diberikan contoh tampilan Manajer Kasus sistem manajemen fraud (SMF) dari FairIsaac.

Fraud Manager for Telecommunications FairIsaac

Home | **View Case** | Create Case | View Transaction | Get Report | Manage | Log Off | Help

Queue Search

Queue: all authorized queues

Search Filter: 2 Page Size: 10

-- search fields --

-- search fields --

Search **Display**

Search Result Total: 26

No	Case Number	Account Number	Status	Fraud Type	Creation Time	Highest Sub Score	Highest Tech Score
1	201	0000000000000456209768	Closed	Not Fraud	05-12-2002 15:17:28	747	0
2	202	0000000000000371038880	Closed	Fraud: Hacking	05-12-2002 15:17:58	724	0
3	203	0000000000000021104271	Unresolved	Unresolved	05-12-2002 15:18:23	629	0
4	204	0000000000000371042948	Pending	Unable to Confirm	05-12-2002 15:18:35	825	0
5	205	0000000000000440084884	Unresolved	Unresolved	05-12-2002 15:18:28	801	0
6	206	0000000000000426422286	Unresolved	Unresolved	05-12-2002 15:18:20	805	0
7	207	0000000000000371054056	Unresolved	Unresolved	05-12-2002 15:18:34	827	0
8	208	0000000000000456209576	Unresolved	Unresolved	05-12-2002 15:18:34	805	0
9	209	0000000000000422880010	Closed	Not Fraud	05-12-2002 15:10:54	700	0
10	210	0000000000000106855879	Unresolved	Unresolved	05-12-2002 15:20:10	537	0

<< Previous Page
go to page 1 . 2 . 3
Next Page >>

Gambar 2 Tampilan Manajer Kasus Sistem Manajemen Fraud (SMF) [5]

6. Kesimpulan

☞ Kelemahan jaringan IP dan Next-Generation:

- Identifikasi pengguna dilakukan pada *layer* IP, sementara *layer* IP sendiri dapat dengan mudah ditembus, sehingga memungkinkan terjadinya *IP spoofing*.
- Firewall menggunakan alamat IP untuk mengklasifikasikan trafik, sehingga bukan merupakan perlengkapan yang cukup ampuh dalam keamanan jaringan karena alamat IP mudah dipalsukan dan disalahgunakan.
- Sistem operasi populer yang kelemahannya telah diketahui banyak orang, seperti Linux, Windows, dan Unix, berjalan di atas server yang penting dan kritis (termasuk firewall, RADIUS, dan server autentikasi), sehingga memungkinkan serangan dilakukan dengan mudah.
- Protokol-protokol pada jaringan IP dan Next-Generation seperti *routing protocol*, *Voice-over-IP (VoIP) signalling*, resolusi *Domain Name Service (DNS)*, dan email (POP, SMTP) merupakan pengetahuan yang sudah umum diketahui oleh banyak orang sehingga memungkinkan orang untuk

melakukan manipulasi pada transmisi data melalui protokol-protokol tersebut.

- Medium komunikasi berbagi pakai seperti modem kabel, transmisi nirkabel, dan *Local Multipoint Distribution System* (LMDS) membutuhkan penggunaan devais koneksi yang sederhana dan murah,
 - Kurangnya mekanisme kontrol yang melekat pada infrastruktur jaringan dan aplikasi berbasis IP atau web turut menyebabkan rendahnya kemampuan bertahan hidup suatu jaringan.
 - Skema *billing* baru yang berdasarkan pada *content* dan kualitas layanan menciptakan kelemahan sistem lainnya yang dapat disalahgunakan oleh orang-orang yang tidak bertanggung jawab.
- ✍ Sistem Manajemen Fraud (SMF) adalah suatu sistem aplikasi yang dapat mendeteksi dan menangani kasus-kasus fraud dengan cepat dan efektif.
- ✍ SMF memiliki tiga komponen utama, yaitu pengumpul dan penyimpan data, penganalisis data, serta Manajer Kasus sebagai antar muka ke pengguna akhir.
- ✍ Data dapat dikumpulkan dari berbagai *layer* dan tingkat jaringan, di antaranya adalah:
- Rekaman penggunaan tingkat aplikasi
 - Tingkat login dan autentikasi
 - Informasi tingkat jaringan
 - Tingkat akses
 - *Triggered Content Events*
- ✍ Algoritma analisis data diperlukan untuk mendeteksi kemungkinan fraud. Algoritma tersebut di antaranya adalah:
- Analisis berdasarkan batas (*Threshold-based analysis*)
 - Analisis *inference-rules*
 - Analisis berbasis profil
 - Jaringan syaraf tiruan (*Neural Networks*)
- ✍ Manajer Kasus berfungsi sebagai antar muka antara sistem manajemen fraud (SMF) dengan pengguna akhir.

7. Referensi

- [1] *Telecommunication Fraud Prevention*. Canadian Irregular Network Access Association (CINAA). 2000. <http://www.travel-net.com>.
- [2] Riaan Jacobs. *Telecommunications Fraud, The Single Biggest Cause of Revenue Loss for Telecommunications Providers*. Dimension Data Service Provider Solution (SPS).
- [3] *Fraud Analysis in IP and Next-Generation Networks*. The International Engineering Consortium. <http://www.iec.org>
- [4] Michael H. Cahill, Diane Lambert, Jose C. Pinheiro, Don X. Sun. *Detecting Fraud in the Real World*.
- [5] *Risk and Fraud Management for Telecommunications, Improve Profitability and Network Efficiencies for Telecommunications Operators*. A Fair Isaac White Paper. October 2003. <http://www.fairisaac.com>.
- [6] *The Theoretical Background of Fraud Detection*. <http://www.dinkla.net>.