MODEL PENANGANAN *E-MAIL SPAM* DENGAN PENDEKATAN TEKNIK SMTPI

Nandang Iriadi

AMIK Bina Sarana Informatika
Jl.Oto Iskandar Dinata No. 25 Tangerang, Banten, Indonesia
nandangiriadi@yahoo.com

Abstract
The ability to use e-mail as essential to the ability to use the phone. E-mail system is very important that many people would complain if the e-mail system can not waste bekerja.E-mail (SPAM) is a problem almost all Internet users and the various efforts to control has been done. Without knowing the factors that cause the occurrence of SPAM, then this problem will still continue. This paper set forth an analysis of SPAM with SMTP Method I, to find fault in the system and the significant factors that cause other Spam.Analisis ontology of the system architecture of e-mail describing the parts and systems so that such connectedness can identify system weaknesses. Then all the significant factors associated with each other by relations of causality and proven method SMTPI messages sent by SMTP will be sent in the queue. SMTP will avoid replying to the message from the queue if connected to a remote machine .. is the use of filtering solutions that are considered quite effective from the technical point of view. filtering is essentially aimed at helping e-mail recipients to filter (select) which automatically e-mail right from spam e-mail, saving time and tenaga.Hasil analysis showed that not only technical factors such as the architecture of e-mail system and authentication process that factors in SPAM, but also other factors such as less sweeping application of security policy (security policy), and economic factors such as cost of sending an e-mail is low.

Keyword: E-mail, Spam, E-mail filter,SMTPI Methodics

I. PENDAHULUAN

Perkembangan *Internet* tumbuh dengan pesat sejak ditemukannya. Berjalan dengan itu muncullah layanan-layanan yang mendukung kegiatan manusia melalui media *internet.* Salah satu layanan yang populer sejak ditemukannya *internet* adalah *Electronic Mail (E-mail).E-Mail* yang awalnya didefinisikan sebagai surat yang berbentuk *file text* yang dikirimkan melalui *internet.* spam *(unsolicited "junk" e-mail*) atau *e-mail* sampah, merupakan problem yang mengganggu pengguna aplikasi *Internet mail. E-mail* yang berisi propaganda seringkali membuat pengguna *Internet email* merasa dirugikan, karena banyak waktu dan sumber daya yang dikerahkan untuk memilah *Spam* dan menanggu-langi kejadian ini.Produk-produk seperti *Spam Filter, blacklist provider,* dan aplikasi *e-mail khusus* yang dapat mendeteksi kehadiran *Spam* telah banyak diimplementasikan. Tetapi permasalaan *Spam* tetap belum secara tuntas dihilangkan. Untuk itu perlu dilakukan kajian yang lebih mendalam tentang Spam untuk memper-oleh faktor-faktor yang cukup signifikan sebagai penyebab *Spam.E-Mail* sekarang ini sudah berkembang lebih atraktif dengan adanya teknologi *HTML E-Mail,* sehingga *E-Mail* tidak hanya berupa tulisan saja, namun dapat disisipkan dengan gambar ataupun *file-file* lainnya. Hal ini membuat perkembangan *E-mail* awalnya dengan tujuan untuk saling berkomunikasi menjadi lebih luas lagi karena kemampuannya dapat digunakan sebagai sarana informasi dan untuk media transaksi di *internet (E-Commerce).*

Oleh karena perkembangannya serta tingkat kemudahan dalam penggunaannya *(ease of use),* beberapa orang mulai berpikir untuk menggunakan fasilitas *E-mail* untuk kegiatan *Spamming.* Pelaku *Spamming* biasanya disebut dengan *Spammer. Spammer* ini melakukan *Spamming* sehingga menghasilkan *Spam Mail. E-mail spam* sendiri didefinisikan sebagai *E-mail* yang berisi hal-hal yang tidak kita inginkan dan kadang dikirimkan oleh orang yang tidak dikenal sebelumnya. *(unsolicited commercial e-mail).* Biasanya juga disebut dengan *Bulk/Junk E-mail.*Masalah *spam* ini berdasarkan pada kenyataan bahwa biaya (*cost*) untuk mengirimkan *e-mail* ke satu orang dan 1.000

orang tidak jauh berbeda. *Barrier* untuk melakukan *mass mailing* sangat rendah. Hal ini berbeda dengan melakukan pemasaran konvensional dimana untuk mengirimkan sebuah kartu pos atau surat akan jauh berbeda untuk satu orang dan 1.000/orang. *Spam* ini tidak dikenali oleh anti-*virus* karena memang dia bukan *virus*. penyaringan terhadap *spam* harus dilakukan secara khusus. Namun mekanisme untuk melakukan penyaringan *spam* ini masih sukar karena kesulitan dalam membedakan antara *e-mail* biasa dan *e-mail* yang *spam*. Pada mulanya proses penyaringan *spam* dilakukan dengan mencari kata-kata tertentu di *e-mail* yang diterima. Kata-kata yang populer digunakan sebagai subyek dari *e-mail* antara lain *"Make money fast", "viagra",* dan seterusnya. Namun ternyata hal ini tidak efektif karena para *spammer* mengubah kata-kata tersebut menjadi kata-kata plesetan. Misalnya huruf "i" dari kata"*viagra*" diganti dengan angka "1" menjadi "*v1agra*". Hebatnya manusia adalah kita masih dapat mengerti bahwa yang dimaksudkan adalah *viagra*.Namun program komputer masih kesulitan dalam membedakan atau menyamakan kedua hal tersebut. Akibatnya jika memasukkan kata "*viagra*" ke dalam penyaringan, maka kata "*v1gra*" akan lolos dari penyaringan dan *e-mail spam* tersebut masih tetap masuk ke *mailbox* . Pendekatan berikutnya dalam melawan *spam* adalah dengan menggunakan statistik (*Bayesian*) yang menghitung kata-kata di dalam *e-mail*. Jika ada banyak kata yang merupakan kata kunci dari *spammer*, maka statistik akan menunjukan probabilitas bahwa *e-mail* tersebut merupakan *spam*. Namun lagi-lagi *spammer* lebih pintar, yaitu dengan menambahkan kata-kata yang tidak bermakna di dalam *e-mail* yang dikirimkan sehingga mengacaukan hasil statistik. (Semakin banyak kata-kata yang tidak beraturan semakin tinggi nilai *entropi* dari sinyal. semakin jauh dari label *spam*.) Jumlah e-mail *spam* ini sudah sangat banyak sehingga dapat melumpuhkan *server e-mail*. Banyak tempat yang tidak menjalankan penyaringan terhadap spam karena tidak mampu. Masalah *spam* masih menjadi masalah utama dalam sistem *e-mail* saat ini. Ada organisasi yang bernama CAUCE (*Coalition Against Unsolicited Commercial E-mail*) yang menggalang upaya-upaya untuk membendung *spam*.

II. PEMBAHASAN

Menurut Budi raharjo(2005:91)*E-mail* merupakan aplikasi yang paling utama di jaringan *Internet*. Hampir setiap orang yang menggunakan Internet memiliki alamat *e-mail*. Saat iniakan aneh jika anda tidak memiliki alamat *e-mail*. Kemampuan kemampuan menggunakan *e-mail* sama esensialnya dengan kemampuan menggunakan telepon .Sistem *e-mail* sudah sangat pentingnya sehingga banyak orang akan mengeluh jika sistem *e-mail* tidak dapat bekerja. Bahkan banyak bisnis yang dilakukan dengan menggunakan *e-mail*. Dapat dibayangkan jika sistem e-mail tidak dapat bekerja dalam waktu yang lama.Sebelum mendiskusikan permasalahan *e-mail*, ada baiknya kita kenali dulu sistem *e-mail*. *E-mail* merupakan salah satu media komunikasi utama dalam lingkungan internet. *Electronic mail* adalah salah satu sarana komunikasi yang cukup handal, perbandingan-nya dengan mail adalah waktu pengirimannya yang sangat cepat. *Electronic mail* atau dising-kat *e-mail* bukanlah pelayanan "*end to end*", karena mesin pengirim dan penerima tidak perlu berkomunikasi secara langsung. Proses penyampaian *electronic mail* dapat dianalogikan dengan penyampaian surat oleh Kantor Pos dan Giro. Kegagalan pengiriman *e-mail* pada umumnya disebabkan karena kesalahan menulis alamat dapat juga disebabkan oleh mesin penerima atau sebagian jaringan mengalami ganguan, tetapi biasanya jaringan mencoba beberapa kali sebelum gagal..Proses ini disebut *"store and forward"*. Alamat yang dituju harus ditentukan dan kemudian surat tadi diletakkan di kotak pos, kemudian mobil pos akan mengambil surat tersebut untuk dibawa ke kantor pos terdekat, dari kantor pos asal kemudian surat tadi dikirim ke kantor pos terdekat dengan alamat tujuan dan akhirnya dari kantor pos tadi surat tersebut dikirim ke kotak pos tujuan.Seiring dengan perkembangan tersebut, muncul juga penyalahgunaan dari fungsi *Email* yang ada. Beberapa pihak mulai menggunakan media ini untuk mengirimkan *Spam Email* yang merugikan dan tidak dikehendaki oleh penerima. Hal tersebut menimbulkan banyak kerugiandi kalangan komunitas internet. Menurut Budi raharjo(2005:92) Sistem *e-mail* terdiri dari dua komponen utama, yaitu

1. *Mail User Agent* (MUA)

MUA merupakan komponen yang digunakan oleh pengguna *e-mail*.Biasanya disebut program mail. Contoh MUA adalah *Eudora*.

2. *Mail Tranfer Agent* (MTA).

Netscape, Outlook, Pegasus, Thunderbird, pine,

mutt, elm, mail, dan masih banyak lainnya lagi. MUA digunakan untuk menuliskan *e-mail* seperti halnya mesin ketik digunakan untuk menulis surat jaman dahulu.MTA merupakan program yang sesungguhnya mengantar *e-mail*. Biasanya dikenal dengan istilah *mailer*. MTA ini biasanya bukan urusan pengguna, akan tetapi merupakan urusan dari *administrator*. Contoh MTA antara lain *postfix, qmail, sendmail, exchange, MDaemon, Mercury,* dan seterusnya.

A. E-mail Spam

Menurut Budi Raharjo(2005:99) *Spam* adalah didefinisikan sebagai "*unsolicited e-mail*", yaitu *e-mail* yang tidak kita harapkan. *Spam* ini berupa *e-mail* yang dikirimkan ke banyak orang. Biasanya isi dari *e-mail* ini adalah promosi.*Spam* adalah pengiriman sejumlah *message* yang sama yang memaksa orang lain yang tidak menginginkan adanya *message* itu mau tidak mau harus menerimanya. *e-mail* merupakan salah satu teknologi yang sangat membantu manusia untuk berkorespondensi satu sama lain. Hal ini disebabkan e-mail tidak mengenal batasan waktu, tempat dan biaya yang amat murah ketika seseorang ingin melakukan korespondensi dengan kenalannya di seluruh dunia selama dapat mengakses jaringan internet. *E-mail juga* telah mengubah cara perusahaan menjalankan bisnis mereka khususnya berinteraksi (surat menyurat) dengan pelanggan mereka. Namun ada beberapa hal yang perlu di perhatikan mengenai keamanan *e-mail.* Selama *e-mail* masih menggunakan jaringan internet sebagai media penghantarnya, maka *e-mail* juga sangat rentan terhadap celah keamanan seperti yang terjadi pada jaringan *internet. Spam* merupakan salah satu celah keamanan dalam *e-mail* sehingga di perlukan suatu mekanisme pengamanan *e-mail* yang efektif untuk mengurangi celah keamanan tersebut. *Spam* selalu menuliskan bahwa mereka akan menghapus nama-nama orang yang tidak ingin berada didalam daftar pengiriman spam tersebut, tapi hamper tidak dilakukan *Spammer* juga tau bahwa para pengguna *internet* tidak ingin menerima pesan dari mereka, sehingga mereka menggunakan alamat palsu di message yang mereka sehingga mereka tidak perlu menanggung biaya penerimaan balasan dari orang-orang yang mereka kirimkan pesan tersebut, dapat juga mereka memanfaatkan masa "trial" dari suatu ISP. Bahkan walau kita mengabaikan mengapa kita harus melakukan sesuatu untuk keluar dari list yang kita tidak pernah ikut, hal ini menjadi sangat tidak mungkin bila volume dari spam itu menjadi lebih besar. Sekarang ini, kebanyakan dari kita hanya mendapat beberapa spam per-harinya. Tetapi jika 1/10 dari 1% user internet memutuskan untuk membuang spam tersebut dengan rate menengah yaitu 100.000 per-hari, rate tersebut dapat dengan mudah dicapai dengan dial-up account dan sebuah PC. Maka tiap orang akan menerima 100 spam perharinya. Jika 1 % user melakukan spamming dengan rate tersebut, maka kita semua akan memperoleh 1000 spam perharinya. Apakah realistis jika kita realistis jika kita meminta orang untuk men-delete 100 message di inbox-nya perharinya? Tentu sulit. Dapat dibayangkan jika spam semakin berkembang.Kebanyakan *spam* yang ada di *internet* adalah berupa iklan, promosi dari suatu produk. Peningkatan jumlah spammers, seperti *Quantum Communciations*, mengirimkan sebagian atau bahkan seluruh mail miliknya melalui intermediate system, untuk menghindari pem-block-an dari suatu system untuk spammers. Hal ini akan memenuhi network dan disk dari intermediate system dengan message spam yang tidak diinginkan, akan menghabiskan waktu dari pengelola system.Kebanyakan spammers menggunakan teknik "*hit and run*" spamming dimana mereka menggunakan account dari sebuah *provider* selama beberapa hari (untuk *trial*) untuk mengirimakan ribuan dan kemudian meninggalkan *account* tersebut, sehingga akan meninggalkan masalah baru bagi para provider. Kebanyakan spammer telah melakukan hal ini puluhan kali, memasa para provider untuk meluangkan waktu ekstar untuk membereskan masalah ini.*Spam* ini sangat menguntungkan bagi pengirim, karena hanya membutuhkan biaya yang kecil, sementara tidak sebaliknya jika kita memandang dari sisi penerima. Menurut Anjik dan Rianto(2008:173) *Spam* adalah suatu *e-mail* yang membawa pesan-pesan yang sifatnya komersial.*spam* pertama terjadi pada bulan Mei 1978 dijaringan *ARPANET* sebelum *internet* terbatas dalam lingkup militer dan akadenis di prakasai oleh seorang pekerja *Digital Equipment Corporation*(DEC).*Spam* dikirimkan oleh pembuat iklan dengan biaya operasi yang sangat rendah, karena *spam* ini tidak memerlukan senarai (*mailing list*) untuk mencapai para pelanggan-pelanggan yang diinginkan. Sebagai akibatnya banyak pihak yang dirugikan. Selain pengguna *Internet* itu sendiri, ISP (Penyelenggara Jasa *Internet* atau *Internet Service Provider*), dan masyarakat umum juga merasa tidak nyaman. Karena biasanya sangat

mengganggu dan kadang-kadang membohongi, berita *spam* termasuk dalam kegiatan melanggar hukum dan merupakan perbuatan pidana yang bisa ditindak melalui undang-undang *Internet.*

B. Tipe Spam

Menurut Iron Port(2004).Ada dua tipe spam dengan akibatnya masing-masing pada pengguna internet, yaitu :

1. Cancellable Usenet spam

Merupakan sebuah pesan yang dikirmkan kepada 20 atau bahkan lebih pengguna *Usenet newsgroup,* pesan ini kebanyakan tidak berguna bagi anggota *Usenet newsgroups. Usenet spam* ini biasanya ditujukan pada orang-orang yang disebu *"lurkers"* yaitu orang-orang yang membaca newsgroup tetapi jarang mem-posting atau memberikan alamat *e-mail* nya. *Usenet spam* ini membebani user dengan mengirimkan posting-posting yang tidak perlu. Selain itu *Usenet spam* ini juga akan membatasi *system administrator* ataupun pemilik untuk mengatur hal-hal yang penting yang seharusnya dimasukkan dalam sistem miliknya

2. Target *E-mail spam*

Target dari *e-mail spam* ada *user* individu dengan *e-mail message* secara langsung. *List* dari *e-mail spam* ini biasanya didapat dari Usenet posting, mencuri *mailing list* tertentu dari internet, atau mencari alamat-alamat dari *web*. *E-mail spam* ini biasanya membebani user untuk mengeluarkan uang lebih banyak karena menerimanya.Bentuk lain dari *e-mail spam* adalah mengirimkan spam tersebut kedalam suatu *mailing list* (baik publik maupun *private*), karena kebanyakan *mailing list* membatasi aktivitas dari para penggunanya, *spammers* akan menggunakan alat otomatis untuk memasukkan *spam* kesebanyak-banyaknya ke *mailing list*, sehingga mereka bisa mendapatkan alamat sebanyak-banyaknya ataupun dengan menggunakan *mailing list* sebagai target langsung pengiriman *spam*

C. **Penyaringan *Spam***

penyaringan merupakan penyelesaian utama yang dianggap cukup efektif dari segi teknis. penyaringan pada intinya bertujuan membantu penerima *e-mail* untuk menyaring (memilih) secara otomatis mana *e-mail* yang benar dan mana spam, sehingga menghemat waktu dan tenaga. Sejak maraknya *spam,* telah berkembang banyak solusi penyaringan. Dari yang sederhana hingga menggunakan algoritma kompleks. Dari yang bersifat personal hingga bersama-sama. Dari yang gratis sampai jasa komersial oleh pihak ketiga. Jika kita memperoleh *e-mail* pertama kalinya dari seseorang, maka *challenge-response filter* akan mengirim *e-mail* kembali ke alamat pengirim tersebut dan memerintahkannya untuk meng-akses alamat *web* tertentu dan mengisi suatu *form* sebelum *e-mail* yang ia kirim dapat kita terima. Dengan cara seperti ini, kita dapat menyaring *spam* dengan akurat. Karena hanya pengirim yang benar-benar berkepentingan dengan kita yang akan melaksanakan prosedur tersebut. Tetapi metode ini dapat dikatakan kasa, karena membuat orang lain melakukan pekerjaan ekstra untuk mengirim *e-mail* kepada kita. Selain itu kekurangan metode ini adalah *legitimate e-mail* dapat hilang atau terlambat sampai, karena pengirimnya tidak mengetahui bahwa ia harus melakukan suatu prosedur dari *challenge-response filter* agar *e-mail* nya dapat diterima. Kekurangan yang lain adalah karena penyaringan ini hanya menyeleksi *e-mail* berdasarkan alamat pengirimnya, maka spammers yang melakukan *spoofing* akan mampu menaklukkan penyaringan ini. Sehingga penyaringan ini tidak terlalu efektif untuk memblok *e-mail spam*. Cara yang dapat dilakukan adalah dengan mengkombinasikan filter ini dengan penyaringan secara statistik, yaitu *e-mail* yang dikategorikan sebagai spam oleh penyaringan secara statisitk, merubah kembali oleh dengan adanya perubahan penyaringan ini. Dengan cara seperti ini, keakuratan Bayesian penyaringan akan bertambah, dan merespon penyaringan juga dapat digunakan dengan efektif *spam*,penyaringan hanya akan membant meringankan masalah yang ada. Di lain hal filtering juga dapat mendatangkan *spam-spam* baru. Hal ini bisa terjadi karena pihak penjual penyaringan *spam* komersial dengan sengaja memasukkan nama clien nya sebagai daftar daftar *spam*. Maka pihak pengelola *server* (*client*) yang tidak ingin terganggu oleh *spam* terpaksa membeli penyaringan dari pihak komersial. penyaringan dapat memilah *e-mail* yang benar dengan *spam* tapi penyaringan tidak mampu mencegah masuknya *spam* ke dalam jaringan. Untuk itu dibutuhkan suatu cara untuk menahan *spam* yang biasa disebut *realtime black hole*. Cara ini untuk mementahkan *spam* yang akan masuk kedalam jaringan,*spam-spam* tersebut datang dari pihak (mesin) lain. Daftar mesin-mesin yang mengirimkan *spam* ini akan terus di perbaharui oleh suatu organisasi,daftar ini dapat dimanfaatkan untuk menolak *e-mail* atau apapun bentuknya yang datang dari mesin yang terdaftar sebagai pengirim *spam*. Menurut Neal Krawetz(2004)Penyaring berbasis anti

spam mempunyai pendekatan yang signifikan. keterbatasannya adalah sebagai berikut:

a. **Mengkombinasikan penyaringan**

Pengirim spam dan bulk-mailing aplikasi tidak statis , mereka cepat beradaptasi sekitar filter. Misalnya, untuk counter daftar kata, pengirim *spam* mengacak ejaan kata (*"viagra", "V1agra", "\ / iaagra").* karakter yang berbeda di setiap e-mail diciptakan untuk *bypassing hash filter*. Dan yang sedang populer penyaringan secara statistik dengan masuknya kata-kata dan kalimat acak. Penyaringan *spam* yang paling efektif hanya untuk beberapa bulan . Dalam rangka untuk menjaga kelangsungan anti *spam,* sistem penyaring menetapkan aturan harus terus diperbarui - biasanya pada harian atau mingguan. Penyaringan adalah penyelesaian terutama dari segi teknis. penyaringan pada intinya bertujuan membantu penerima *e-mail* untuk memilah-milah secara otomatis mana *e-mail* yang benar dan mana *spam*, sehingga menghemat waktu dan tenaga. Sejak maraknya *spam*, telah berkembang banyak solusi penyaringan. Dari yang sederhana hingga menggunakan algoritma kompleks. Dari yang bersifat personal hingga secara bersama-sama. Dari yang gratis sampai jasa komersial oleh pihak ketiga.Saat ini teknologi penyaringan sudah cukup memuaskan. Solusi seperti *Spam Assassin* misalnya yang menjadi favorit banyak *sysadmin/user* menggunakan berbagai cara untuk mengidentifikasi *spam*. Mulai dari deteksi *header*, pencarian kata-kata yang umum ada di *spam,* hingga integrasi dengan sistem penyaringan lain. murni mengandalkan analisis konten sebab, Inti dari spam adalah pesannya. Jadi yang harus kita usahakan adalah mengenali *spam* dari pesan.Kualitas penyaringan ditentukan dari *rendahnya* pesan biasa salah terdeteksi sebagai *spam* dan tingginya kebenaran. Dengan penyaringan yang ada sekarang, telah dimungkinkan mencapai akurasi di atas 95% kebenaran dan kesalahan mendekati 0%. Bahkan banyak penyaringan telah memiliki kemampuan untuk melakukan *autoreporting:* manakala *spam* ditemukan, langsung dilaporkan atau ditambahkan ke dalam basisdata untuk membantu proses penanganan *spam* lainnya. penyaringan hanyalah satu sisi dari solusi berbasiskan teknis. penyaringan tidak menyelesaikan akar permasalahan, hanya membantu meringankan beban penerima dalam menyortir *e-mail*. Meskipun disaring namun jumlah total *spam* yang sebetulnya masuk setiap hari terus bertambah. Ada sisi lain juga masalah penyaringan ini, yaitu adanya pihak-pihak yang bermain di air keruh. Ada beberapa penjual solusi penyaringan komersial yang dengan sengaja memasuk-masukkan calon klien ke dalam berbagai daftar spam. Dengan tujuan membuat klien terpaksa membutuhkan penyaringan. Jadi di sisi ini maraknya penyaringan justru akan mendorong meningkatkan jumlah *spam*.

b. Berpikiran Positif

Yang lebih efektif penyaringan *spam*, semakin tinggi kemungkinan *e-mail* sebagai *spam*. Sebagai contoh, *e-mail* yang berisi kata "*viagra*" Hampir pasti akan ditandai sebagai spam tanpa isi. Sebaliknya, penyaringan *spam* yang hampir tidak menghasilkan pikiran positif yang mungkin untuk menghasilkan sejumlah pikiran negative mengenai *spam*.

c. Meninjau Kembali Penyaringan Spam

Karena kemungkinan pesan palsu, yang ditandai sebagai s*pam* biasanya tidak segera dingenai hapus. Sebaliknya, pesan akan disimpan dalam kotak masuk untuk diperiksa. ini berarti bahwa pengguna masih harus melihat *spam*, meskipun hanya oleh subjek, karena mereka mencari *e-mai*l. Pada dasarnya, penyaring hanya membantu penyortiran *e-mai* masuk.

Menurut Brian Bagnall(2000:43) Penyaringan teks pada *e-mai l* terdiri dari tiga bagian:

1. **Menambahkan alamat *e-mail* ke daftar pengirim.**

Ketika kamu mendapat satu *e-mail* yang kamu pengaruhi seperti *junk e-mail* yang dapat menambahkan alamat *e-mail* ke Konten atau daftar pengirim melalui Aksi *junk e-mail* Tambahkan ke daftar Pengirim *junk e-mail* Menambahkan ke Dewasa Daftar Pengirim konten. Waktu berikutnya kamu mendapat satu *e-mail dari* ini pengirim, aksi ditetapkan berlaku bagi ini.

2. **Tambahkan alamat *e-mail* untuk daftar eksepsi.**

Satu *e-mail* mungkin diidentifikasi sebagai jong, tapi kamu tidak mempengaruhi alamat pengirim ini seperti
demikian. menempatkan pengirim ini alamat *e-mail* pada daftar eksepsi. Aktifkan Alat Pemandu Ketentuan dan lihat aturan memanggil Eksepsi. bagian dari Ketentuan dapat mengedit nilai daftar eksepsi dengan memilih . Satu mengedit tulisan yang memperbolehkan kamu untuk memelihara daftar alamat *e-mail* yang mencegah *e-mail* berasal dari pengirim ini untuk disampaikan ke penyaringan *e-mail*.

3. **Perbaharui penyaringan konten**

Sesuatu akan mengasumsikan bahwa penyaringan *e-mail* mampu untuk perubahan, tapi dapat menciptakan penyaringan *e-mail* sendiri berlandaskan berkas tulisan satu praktek lebih baik untuk mencek Situs untuk pembaharuan, atau cari cara di *internet* untuk penyaringan dari pihak ketiga.

D. Metode Penyaringan

Menurut Jonathan A dziarski (2005:40)terdapat beberapa metode penyaringan yang dapat digunakan untuk mencegah spam diantaranya :

a. Keyword filtering

Metode ini merupakan *Application Layer Filtering* (ALF). Dengan metode ini, *spam* di-blok berdasarkan kata-kata tertentu yang sering dituliskan pada *spam-mail*

b. Signature –Based Filtering

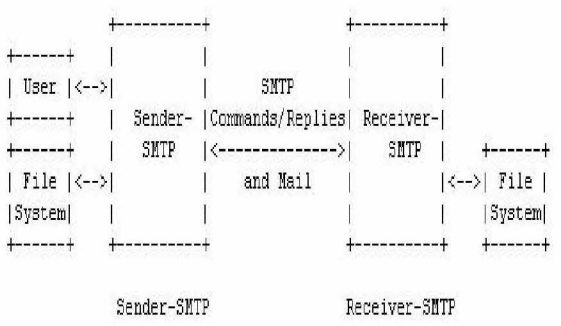
Metode ini akan membandingkan *e-mail* yang datang dengan *spam-mail* yang telah diketahui. Hal ini dilakukan dengan membuat beberapa alamat *e-mail* palsu. *Spam-mail* yang biasanya dikirim ke beratus-ratus alamat *e-mail* juga akan dikirim ke alamat-alamat palsu ini. Sehingga dengan membuat daftar alamat-alamat mana saja yang mengirim *e-mail* ke alamat palsu ini, *e-mail spam* dapat diblok. Salah satu cara untuk menunjukkan bahwa dua buah e-mail sama dilakukan dengan memberikan "*signature*" pada setiap *e-mail*. Metode untuk memberikan *signature* antara lain dengan memberikan angka untuk setiap huruf, lalu semua angka tersebut dijumlahkan. Sehingga setiap *e-mail* akan memiliki "*signature*" yang berbeda. Dalam hal ini, dua e-mail yang memiliki signature yang sama, dan dikirim ke beberapa alamat dapat dikategorikan sebagai *e-mail spam*. Cara inilah yang diterapkan pada *signature-based filtering*. Tetapi metode penyaringan ini sangat mudah dikalahkan oleh *spammers*. Cukup dengan menambahkan sembarang karakter yang berbeda pada setiap *copy spam-mail*, akan membuat memperbanyak *e-mail spaml* itu memiliki signature yang berbeda. Sehingga metode ini tidak terlalu efektif untuk menyaring *spam*. *Spammer* selalu mencari cara untuk mengelabui *Spam Filter* dengan melihat cara yang dilakukan oleh *Spam Filter* yang digunakan. Selain itu juga digunakan teknik yang bersifat *rule* untuk mengurangi tingkat kesalahan *False Positive* dari metode *statistic*.

c. Bayesian (Statistical) Filtering

Metode Penyaringan secara statistik merupakan metode anti penyaringan *spam* yang terbaru. Metode ini mengenali *spam* berdasarkan kata-kata (token) yang terkandung pada sebuah e-mail. Metode penyaringan ini pertama kali perlu pelatihan dengan menggunakan dua koleksi *e-mail*, satu koleksi merupakan *e-mail spam*, dan koleksi yang lain merupakan *e-mail* yang secara sah. Dengan cara seperti ini, pada setiap *e-mail* baru yang diterima, penyaringan secara statistik dapat memperkirakan probabilitas *spam* berdasarkan kata-kata yang sering muncul di koleksi *e-mail spam* atau di koleksi *e-mail* Panyaraingan secara statistik efektif untuk memblok *spam* karena penyaringan ini dapat secara otomatis mengkategorikan *e-mail spam* atau *legitimate e- mail*. Kelemahan dari *Bayesian chain rule* ini adalah tiap kata diasumsikan terpisah dan tidak tergantung satu sama lain. Padahal dalam menganalisis suatu teks, setiap kata saling berhubungan satu dengan yang lain.

***E. Simple Mail Transfer Protocol* (SMTP)**

Menurut Jonathan B..Postel(1982) tujuan *Simple Mail Transfer Protocol* (SMTP) adalah untuk mentransfer *mail* yang dapat dipercaya secara efisien, SMTP ini bebas terhadap subsistem transmisi dan hanya membutuhkan stream kanal data yang dapat dipercaya.*Fitur* yang penting dari SMTP ini adalah kemampuannya untuk merelay e-mail melalui berbagai macam *transport* servis, karena Mail adalah aplikasi atau penggunaan dari komunikasi interproses



Gambar 1 Model SMTP(Jonathan 1982)

Cara kerja dari model SMTP ini adalah sebagai berikut : Jika ada permintaan e-mail dari pengguna, maka pengiriman SMTP akan menyediakan kanal transmisi 2 arah kepada pengiriman SMTP. Pengiriman SMTP dapat menentukan tujuan atau meneruskannya lagi. *Command* SMTP dikeluarkan oleh sender SMTP dan dikirmkan kepada pengiriman SMTP, dan SMTP replies pada arah sebaliknya.Apablika

kanal transmisi sudah diberikan, sender SMTP akan mengirimkan *e-mail* command yang menandakan pengiriman *e-mail*. Bila penerima SMTP dapat menerima *e-mail* maka ia akan mengirim dengan ok kirim, kemudian SMTP akan mengirimkan RCPT *command* yang memberitahukan penerima dari e-mail tersebut, jika tidak maka pengiriman SMTP akan menolaknya.SMTP menggunakan beberapa *spoo*l dan *queue*. Pesan yang dikirim oleh SMTP akan dikirimkan dalam *queue*. SMTP akan menghindari membalas pesan dari *queue* jika dihubung-kan ke *remote machine. Jika* pesan tidak dapat dibalas dengan waktu yang telah ditentukan maka pesan akan dikembalikan ke pengirim atau dipindahkan. Interaksi antara *Message User Agent* dan ke *Message Transfer Agent* hingga diterima oleh Penerima Jika lebih dari satu penerima pada lokasi penerima dikenali, beberapa RCPT akan dikirim tetapi pesan itu sendiri yang hanya dikirim sekali. Setelah masing-masing RCPT akan terdapat beberapa pengenalan. Perintah data diikuti oleh jalur -jalur pesan sampai dengan periode tunggal pada line itu sendiri yang mengenali akhir dari pesan. Keter-hubungan akan ditutup dengan perintah *quit*.Alamat pengirim dan penerima menggunakan standar internet termasuk nama dan domain user. Domain akan diganti dengan informasi yang lain sebagai keterhubungan langs-ung yang telah dibentuk atau terdapat mesin pembalas dalam path. SMTP menggunakan *domain name server* untuk semua alamat.Sekalipun *e-mail* digambarkan akan dapat sampai ke tempat tujuan seketika itu juga, kenyatannya tidak sesederhana itu. *E-mail Internet* tergantung juga pada teknologi "*store and forward*", yang berarti pesan-pesan akan ditahan dan disimpan dalam satu komputer atau lebih sepanjang perjalanan surat tersebut dan diteruskan lagi pada selang waktu yang tetap atau pada saat lalu lintas jaringan memungkinkan. Transmisi data SMTP menggunakan format yang sederhana. Semua teks pesan ditransfer ke dalam karakter ASCII 7 bit. Pada akhir suatu pesan akan dikenali menggunakan periode tunggal pada jalur tersebut. Jika dalam beberapa hal jalur pesan dimulsi dengan periode tertentu, beberapa saat kemudian ditambahkan oleh protokol untuk menghindari terjadinya hal yang membinggungkan dengan indikator akhir pesan.

F. Prosedur-prosedur pada SMTP

a) Mail

Ada 3 tahap pada transaksi mail SMTP :

1. MAIL command

Pada MAIL command ini akan diberikan identifikasi dari pengirim

MAIL <SP> FROM :<reverse-path> <CRLF>

Perintah ini memberitahukan kepada receiver SMTP bahwa ada transaksi email baru dan untuk mereset semua tabel state dan buffer, termasuk semua penerima atau mail data. Command ini akan memberikan *reverse-path* yang digunakan untuk melaporkan jika terjadi error. Jika diterima, maka receiver SMTP akan mengirimkan kode 250 OK *reply*

2. RCPT command

Disini akan diberikan informasi dari penerima

RCPT <SP> TO:<forward-path> <CRLF>Perintah ini akan memeberikan *forward path* yang akan mendefinisikan penerima. Jika diterima maka receiver SMTP akan mengirmkan kode 250 OK *reply* dan menyimpan *forward path* tersebut. Bila penerima tidak diketahui maka *receiver* SMTP akan mengirimkan kode 550 *Failure reply*. Prosedur kedua ini dapat diulangi sampai beberapa kali

3. Data *command*

Berisi data dari MAIL dan indikasi akhir dari transaksi

DATA <CRLF>

Jika diterima, maka *receiver* SMTP akan mengirimkan kode 354 Intermediate reply dan menganggap semua baris dari data adalah message text. Jika akhir dari teks diterima dan diterima dan disimpan. SMTP *receiver* akan mengirimkan 250 OK *reply* Akhir dari *e-mail* data ini juga berisi konfirmasi dari transaksi mail dan memberitahukan kepada receiver SMTP untuk memproses mail data dan mengirimkannya kepada pengirim.

Contoh:Mail from:<Smith@Alpha.ARPA>
R: 250 OK
S: RCPT TO:<Jones@Beta.ARPA>
R: 250 OK
S: RCPT TO:<Green@Beta.ARPA>
R: 550 No such user here
S: RCPT TO:<Brown@Beta.ARPA>
R: 250 O
S: DATA
R: 354 Start mail input; end with
<CRLF>.<CRLF>
S: Blah blah blah...
S: ...etc. etc. etc.

S: <CRLF>.<CRLF>
R: 250 OK

b) Forwarding

Ada 2 kasus *reply receiver* SMTP dari Forwarding ini, yaitu dimana informasi tujuan (*forward path*) salah, tetapi *receiver* SMTP mengetahui tujuan yang benar .ada 2 kategori perintah diantaranya:

a. 251 *User not local; will forward to <forward path> Reply* ini memberitahukan bahwa receiver SMTP mengetahui mailbox dari user ada pada host yang lain dan memperbaiki *forward path* yang sebelumnya untuk digunakan selanjutnya. Pada kasus ini receiver bertanggung jawab untuk mengirimkan pesan

b. 551 User not local; please try <*forward-path*>Perbedaan pada kasus pertama ialah bahwa receiver SMTP menolak menerima email untuk user ini dan pengirim harus me-*redirec*t email berdasarkan informasi yang disediakan oleh receiver SMTP atau mengirimkan pesan error pada user yang dituju.

Contoh :
S: RCPT TO:<Postel@USC-ISI.ARPA>
R: 251 User not local; will forward to <Postel@USC-ISIF.ARPA>
S: RCPT TO:<Paul@USC-ISIB.ARPA>
R: 551 User not local; please try <Mockapetris@USC-ISIF.ARPA>

c) Verifying and Expanding

Merupakan fitur tambahan dari SMTP, command ini digunakan untuk memverifikasi nama user atau untuk meng-*expand mailing list.* Digunakan dengan perintan VRFY dan EXPN, dengan argument karakter *string*. Untuk VRFY, argumennya adalah nama user dengan responnya adalah Nama lengkap dari user serta mailboxnya. Sedangkan untuk EXPN argumennya adalah *mailing list.*

Contoh :
VRFY
S : VRFY Smith
R : 250 Fred Smith <Smith@USC-ISIF.ARPA>
S : VRFY Smith
R : 251 User not local; will forward to <Smith@USC-ISIQ.Arpa>
S : VRFY Jones
R : 550 String does not match anything
S : VRFY Jones
R : 551 User not local; please try <Jones@USC-ISIQ.ARPA>
S : VRFY Gourzenkyinplatz
R : 553 User ambiguous
EXPN
S : EXPN Example-People
R : 250-Jon Postel <Postel@USC-ISIF.ARPA>
R : 250-Fred Fonebone <Fonebone@USC-ISIQ.ARPA>
R : 250-Sam Q. Smith <SQSmith@USC-ISIQ.ARPA>
R : 250-Quincy Smith <@USC-ISIF.ARPA: Q-Smith@ISI-VAXA.ARPA>
R : 250-<joe@foo-unix.ARPA>
R : 250 <xyz@bar-unix.ARPA>
S : EXPN Executive-Washroom-List
R : 550 Access Denied to You

d) Sending and Mailing

Sending adalah pengiriman keterminal dari suatu user, sementara mailing adalah pengiriman ke mailbox dari suatu user, karena fungsi keduanya hampir identik, maka fungsi keduanya digabungkan kedalam SMTP

Ada 3 perintah utama pada command sending, yaitu :

1. SEND <SP> FROM: <reverse-path> <CLRF>

Perintah ini berguna untuk mengirimkan mail data ke terminal dari user. Jika user sedang tidak aktif atau tidak mail tersebut tidak sampai, maka pada host akan muncul 450 Reply

2. SOML <SP> FROM: <reverse-path> <CRLF>

SOML ini merupakan sarana pengiriman email dimana tidak mengharuskan user tersebut aktif atau tidak, jika tidak aktif maka mail tersebut akan dimasukkan kedalam kotak masuk dari pengguna

3. SAML <SP> FROM: <reverse path> <CRLF>

Pada kasus SAML ini mail data yang datang pada suatu user dari suatu host akan langsung dimasukkan kedalam kotak masuk.

e) Opening and Closing

Saat kanal transmisi terbuka, maka ada sebuah pertukaran informasi yang menjamin bahwa host tersebut adalah host yang dimaksud *command* yang digunakan dalam membuat suatu koneksi pada kanal transmisi dan saat memutuskan koneksi adalah :

***HELO* <SP> <domain> <CRLF>** ***QUIT* <CRLF>**

Pada command HELO, host akan mengirimkan command yang mendefinisikan informasi

dirinya.

Contoh :
Memulai suatu koneksi
R: 220 BBN-UNIX.ARPA Simple Mail Transfer Service Ready
S: HELO USC-ISIF.ARPA
R: 250 BBN-UNIX.ARPA
Mengakhiri suatu koneksi
S: QUIT
R: 221 BBN-UNIX.ARPA Service closing transmission channel

f) Relaying

Forward-path biasanya adalah rute yang berupa bentuk "@x atau @y" dimana x dan y adalah nama host, bentuk ini akan membedakan alamat dan rute, dimana rute adalah cara bagaimana untuk mencapai alamat tersebut. Elemen dari forward-path akan dipindahkan menjadi *reverse-path* pada saat message dikirimkan dari satu *server* SMTP ke *server* SMTP yang lain.

Contoh
Pesan pemberitahuan bahwa e-*mail* yang dikirimkan tidak sampai
S: MAIL FROM:<>
R: 250 ok
S:RCPT TO:<@HOSTX.ARPA:JOE@HOSTW.ARPA>
R: 250 ok
S: DATA
R: 354 send the mail data, end with .
S: Date: 23 Oct 81 11:22:33
S: From: SMTP@HOSTY.ARPA
S: To: JOE@HOSTW.ARPA
S: Subject: Mail System Problem
S:
S:Sorry JOE, your message to SAM@HOSTZ.ARPA lost.
S: HOSTZ.ARPA said this:
S: "550 No Such User"
S: .
R: 250 ok

g) Domains

Penggunaan nama domain menggantikan alamat dari nama host menjadi alamat global. Nama host digantikan dengan bentuk nama domain yang diikuti dengan nama host dan dipisahkan oleh tanda titik "."
Contoh
"USC-ISIF.ARPA", "Fred.Cambridge.UK" "PC7.LCS.MIT.ARPA"
adalah identifikasi nama host-dan-domain

h) Changing Roles

Command TURN digunakan untuk membalik peran dari 2 program yang berkomunikasi pada kanal transmisi.Jika program A adalah sender SMTP dan ia mengirimkan command TURN dan menerima ok reply (250) maka program A akan menjadi *receiver* dari SMTP. Jika kita menolak perubahan tersebut makan receiver akan mengirimkan 502 *reply*

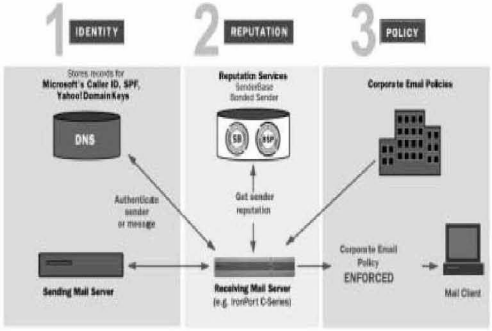
G. Penanganan SPAM dengan Metode SMTPi

Menurut Chris Brenton dan Cameron Hunt(2005:123) *Simple Mail Transfer Protocol* (SMTP) adalah digunakan untuk melakukan transfer *pesan e-mail* diantara sistem.SMTP menggunakan sebuah jenis koneksi yang bersifat *message-switched* atau aktif jika ada pesan yang masuk. Setiap pesan *e-mail* diproses sampai selesai sebelum session antara dua system diakhiri. Jika ada lebih dari satu pesan *e-mail* dikirimkan,maka sebuah sesi terpisah akan dibuat untuk setiap pesan *e-mail*. Konsep ini mengatakan bahwa SMTP menggunakan informasi yang ditulis pada amplop surat (*message header*) dan tidak melihat isi surat (*message body*). Daftar tujuan-tujuan e-mail diperoleh *user agent* dari *message header*. Dalam beberapa kasus, alamat tujuan biasanya sudah tercantum dalam *message header*. Dalam kasus lain, *user agent* mungkin perlu memperluas nama-nama dalam *mailing list*, membuang duplikat, dan mengganti nama-nama *mnemonic* dengan nama-nama yang aktual. Jika terdapat *blind carbon copies* (BCC), *user agent* perlu menyiapkan pesan sesuai dengan kebutuhan ini. Ide dasarnya adalah format-format dan gaya-gaya ganda yang dibuat manusia dalam antar muka (*interface*) pengguna yang digantikan oleh daftar standar untuk SMTP *send program*. SMTP *sender* mengambil pesan dari antrian dan mentransmisikan ke *host* tujuan lewat transaksi SMTP dengan membuat sebuah atau lebih koneksi TCP *port* 25 dari *host target*. Sebuah *host* mungkin saja mempunyai banyak SMTP *sender* yang aktif secara simultan jika ia mempunyai banyak *mail* yang harus dikirimkan dan ia juga mempunyai kapabilitas untuk menciptakan SMTP *receivers* jika ada permintaan.Ketika SMTP *sender* telah selesai megirimkan suatu pesan, maka ia akan menghapus alamat tujuan yang dimaksud dari daftar tujuan. Ketika semua alamat tujuan untuk pesan telah selesai diproses, pesan tersebut

dihapus dari antrian. Dalam pemrosesan antrian, SMTP *sender* dapat melakukan bermacam-macam optimasi. Jika sebuah pesan dikirimkan untuk beberapa pengguna pada satu buah *host*, pesan informasi tersebut hanya perlu dikirimkan satu kali. Jika pesan-pesan tersebut sudah siap untuk dikirimkan ke sebuah *host,* maka SMTP *sender* dapat membuka sebuah koneksi TCP, mentransfer semua pesan tersebut, kemudian menutup koneksi, daripada membuka dan menutup sebuah koneksi berulang-ulang untuk tiap-tiap pesan.SMTP *sender* harus berurusan dengan bermacam-macam kesalahan. *Host* tujuan bisa saja tidak dapat dijangkau, tidak beroperasi, atau koneksi TCP bisa gagal ketika surat sedang dalam proses transfer. Pengirim bisa memasukkan kembali surat tersebut ke dalam antrian untuk dikirimkan beberapa waktu kemudian, tetapi bila setelah periode waktu tertentu surat masih tidak dapat dikirimkan, maka surat tersebut tidak jadi dikirimkan agar tidak memenuhi antrian untuk jangka waktu yang tidak terbatas. Kesalahan yang paling umum adalah kesalahan menuliskan alamat tujuan yang dapat terjadi pada saat memasukkan *input* atau karena alamat tujuan memiliki alamat baru di *host* yang berbeda. SMTP *sender* harus mengalihkan (*redirect*) pesan jika memungkinkan atau mengirimkan pesan kesalahan pada pengirim.Menurut Anjik Sukmaji dan Rianto(2008:143) SMTP adalah *protocol* standar yang dapat dipergunakan untuk mengirim *e-mail* ke suatu tujuan yang sudah ditentukan..SMTP berjalan di *text based protocol.*Sehingga semua yang dikirimkan dalam bentuk ASCII.Tujuan utama dari penggunaan SMTP adalah untuk *transfer mail reliably and efficiently.*proses SMTP akan dimulai
dengan insial jabat tangan(*handshaking*) selesai saluran transmisi akan terbentuk dan
SMTP akan diberikan respon yang menandakan respond yang menandakan *command* tersebut telah diterima dan terjadi *error condition.* SMTP client juga disebut sebagai *Mail User Agent* (MUA).Sedangkan SMTP *server* lebih dikenal dengan dengan *Mail Transfer Agent* (MTA). Untuk *attachment* yang berbentuk biner akan dilakukan proses *encode* dalam bentuk 8 bit MIME(*Multipurpose Internet Mail Extension*).SMTP menggunakan *port* TCP 25.SMTP bersifat *"push"protocol* dimana hanya bersifat mengirimkan untuk "*pull*" protocol dari remote server(*mail server)* digunakan*l Post Office Protocol*(POP3). atau *internet mail Acces Protocol*(IMAP). Memastikan akuntabilitas dari pengirim dalam pengiriman *e-mail* yang aman dan dapat dipercaya sangat diperlukan. SMPTPi adalah next-generation dari infrastruktur e-mail. SMTPi ini memiliki 3 f*ramework* dengan komponen penting yaitu identitas, reputasi dan policy tertentu dari suatu *system messaging* yang baru dan aman yang dibuat diatas SMTP. "i" dibelakang SMTP itu adalah untuk *identity*. Perpindahan dari identitas dan reputasi dari *mail* sistem akan membuat pengirim menjadi mudah dipantau dan mengurangi masalah-masalah yang ada dengan *e-mail*. SMPTi ini berpedoman pada skema autentifikasi, reputasi pengiriman data dan kemampuan untuk membuat sebuah kebijakan *e-mail* berdasarkan atas kedua aspek diatas.SMTP dapat digunakan oleh pengguna sebagai protokol untuk saling menukar *e-mail* antar pengguna dalam komputer yang sama atau komputer yang lain.layanan SMTP yaitu:

1. Untuk mengirimkan satu pesan kesatu atau banyak penerima
2. untuk mengirim pesan termasuk teks,suara,video dan grafik.
3. untuk mengirim pesan ke user dalam satu jaringan ataupun diluar jaringan

H. Implementasi SMPTi



Gambar II.1 Implementasi SMTPi(Iron Port 2004)

Menurut Iron Por(2004) Implementasi SMTP

terbagi menjadi

1. Identity

Secara akurat akan menunjukkan identitas dari pengirim sehingga membuat penerima *e-mail* yakin bagaimana ia harus memperlakukan message yang masuk, terkait dengan reputasi dari pengirim. Dengan melakukan ini, makan akan lebih mudah untuk menghapus *spam* dari *inbox* penerima Membuat suatu mekanisme

identitas yang menyeluruh untuk *e-mail* adalah masalah yang tidak mudah dan perlu dilakukan secara bertahap.

Mengetahui identitas pada pengiriman *e-mail* memiliki 2 keuntungan :Memungkinkan user untuk mengetahui reputasi dari pengirim dan dapat membuat keputusan yang baik bagaimana harus memperlakukan *e-mail* dari pengirim tersebut berdasarkan reputasinya (diterima atau ditolak) Memberikan informasi bagi pengirim untuk memperbaiki perilaku mereka untuk meningkatkan reputasi mereka dalam pengiriman *e-mai.*

a. Server Level Identity *berdasarkan IP address*

Identitas dari mekanisme level server adalah alamat IP dari pengirim. Sebuah alamat IP dapat diverifikasi dan dimanage, dan hampir tidak mungkin untuk dipalsukan, karena dikirimkan dengan menggunakan koneksi TCP/IP. Apabila alamat IP salah dalam pengartian *make two-way* SMTP *conversation* tidak mungkin terjadi karena pengembalian paket untuk melakukan komunikasi SMTP tidak bisa dirutekan kembali ke alamat IP asal.IP address sendiri memiliki keterbatasan sebagai identitas, dan keterbasan ini akan memungkinkan untuk dikembangkannya autentifikasi level Domain

b. Domain Level Identity

Sistem Autentifikasi tingkat domain akan memungkinkan perusahaan untuk menentukan mail server mana yang diperbolehkan untuk mengirimkan *e-mail* dengan menggunakan nama doamin. Hal ini dapat mencegah bentuk-bentuk pemalsuan alamat *e-mail* seperti "pishing" dan "*joe-jobs*". "*Pishing*" terjadi jika pengirim menggunakan nama doamin yang sudah banyak dikenal seperti *e-bay.com* atau *yahoo.com* pada "*FROM*: " *address.* "Joe-*jobs"* merupakan bentuk lain pemalsuan yang berbahaya, dimana pengirim membuang e-mail yang tidak diinginkan dan memalsukan "*envelope*" addrss dari orang yang tidak terkait sama sekali. Maka hal ini akan membuat pengirim terhindar dari pengiriman kembali message yang tidak diinginkan dan mendiskriditkan orang yang alamatnya telah dipalsukan tersebut.Untuk beberapa tahun kedepan, identitas dari level-domain dapat dilakukan dengan menggunakan standar seperti *Sender Policy Framework* (SPF), *Calle*r-ID dan Domainkeys, tetapi untuk tiap jenisnya ada keuntungan dan kerugiannya.SPF dan *Caller-ID* berusaha untuk mengatasi keterbatasan pembuatan list "*authorized source IP's*" pada "*envelope sender"* atau *header* dari domain pada DNS. Sedangkan *Domain Keys*, menggunakan *private key* untuk enkripsi pada setiap pengiriman message.Solusi yang paling baik, belum dapat ditentukan, penggunaaan dari *header cryptography* yang akan memungkinkan user mengidentifikasikan diri mereka sendiri dalam berbagai tingkatan (individu, organisasi dan perusahaan).SPF merupakan solusi dengan biaya rendah untuk masalah "*unwanted bounce"* tetapi tidak mengatasi spam untuk masalah imitasi alamat *e-mail* dan membatasi beberapa aplikasi *e-mail* seperti pengiriman. Sementara *Caller ID* mengatasi masalah imitasi alamat *e-mail* tetapi biaya lebih tinggi untuk implementasi pengiriman *e-mail.* Lalu *Domain Keys* merupakan solusi yang paling baik untuk pemalsuan, tetapi sangat rumit, membutuhkan perubahan dari infrastruktur e-mail yang sudah ada sekarang

c. Universal Identity

Masalah utama dari autentifikasi tingkat Domain adalah bahwa ia tidak dapat mengidentifikasikan user individual. "*Universal Identity*" akan menyediakan bentuk identitas yang lebih fleksibel dan aman dengan menggunakan digital certificates. Model ini memungkinkan pengirim untuk mengidentifikasikan diri mereka sendiri pada berbagai tingkatan seperti individual, organisasi atau suatu perusahaan.

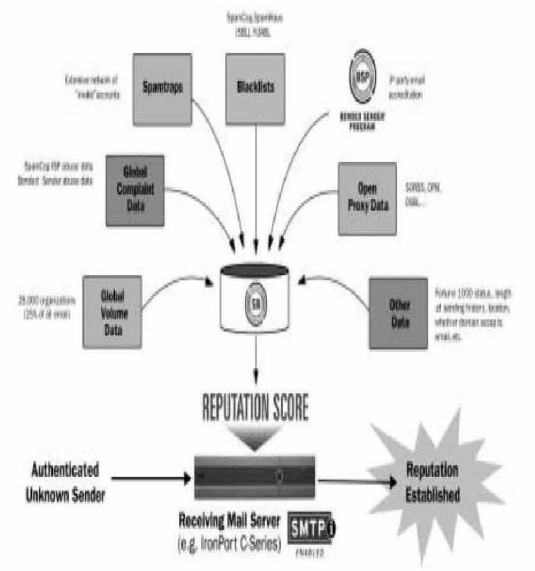
2. Reputation

Reputasi dari pengirim dapat ditelusuri dengan memonitor *history mail*-nya. *Track service* dari reputasi pengirim merupakan range dari parametere terukur, seperti volume dari *e- mail* yang dikirimkan, bertentangan, Negara asal, kehadiran dari *relay open proxy*, konfigurasi DNS yang terkait, serta data-data terkait lainnya. Paramater ini dapat menentukan reputasi dari pengirim.Tidak seperti *blocklist*, yang merupakan pengaruh dari generasi pertama dari servis untuk menentukan reputasi pengirim, servis reputasi generasi kedua seperti "*Sender Base*" akan menyediakan data secara detil (nilai reputasi dari -10 hingga +10) yang akan memungkinakn penerima menentukan kebijakannya sendiri dan thresholds. *SenderBase* adalah *Open Service,* dimana *system administrator* dan *open source spam filter* dapat mengakses tanpa mengeluarkan biaya. Untuk dapat berguna, reputasi dari *e-mail* dan pelayanan akreditasi harus terbuka, memiliki data-data yang otentik dan Seiring dengan berkembangnya SMTPi, penerima dari *e-mail* akan menerpakan batasan yang lebih dari *e-mail* yang berasal dari sumber yang tidak memiliki

identitas dan reputasi. Perpindahan SMTP menuju sistem SMTPi (*identity and reputation)* akan membuat *e-mail l*ebih aman dan terjamin

3. Sender Base

Merupakan bentuk *database* pertama dari pengirim *e-mail.* Memiliki *host* pada *www.senderbase.org*, *SenderBase* merupakan semacam badan pelaporan servis dari *e-mail*, menyediakan data-data dari ISP atau perusahaan yang nantinya akan digunakan untuk menentukukan keputusan terhadap suatu sumber *e-mail.*Diguanakan oleh lebih dari 30.000 *administrator mail, SenderBase* memonitor jumlah (volume) pengiriman *e-mail*, tingkat keluham, *account* dari "*spamtraps*", daerah asal dari *mai*l, informasi yang dibatasi, status dari *open proxy* serta parameter-parameter lain yang digunakan untuk menentu kualitas dari pengirim. Semuanya ini akan sangat berguna bagi *administrator*



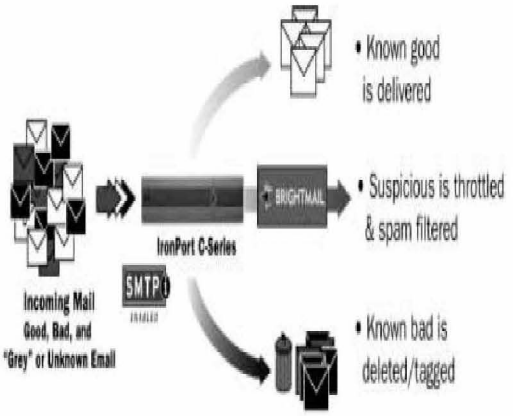
Gambar II.2 Filterisasi SPAM dengan Metode SMTP i(Iron Port 2004)

4. Bonded Sender Program

Merupakan servis akrediatai *e-mail. Bonded Sender* menggunakan mekanisme pasar yang unik untuk memastikan bahwa *e-mail* komersial yang terpercaya tidak dikatergorikan kedalam *spam* dan tidak terkena *filter spam*. Pengiri dari *e-mail* komersial yang tidak termasuk dalam spam, harus mendaftarkan *e-mail* nya dengan membayar sujumah uang. Jika end user memberikan keluhan bawah pesan yang masuk adalah bukan yang diinginkan, maka dapat dilakukan *claim*. Mekanisme ini menjamain bahwa hanya perngirim yang terpercaya yang dapat menggunakan program ini.

5. Policy

Setelah mengautentifikasi *e-mail* dari pengirim dan mengetahui reputasinya, penerima *e-mail* perlu untuk membuat suatu cara yang sesuai untuk membuat suatu kebijakan *e-mail* berdasarkan informasi yang sudah diperoleh sebelumnya Sekarang ini kebanyakan *e-mail gateway* memproses semua *e-mail* yang masuk melalui suatu penyaringan *spam*. Metode ini akan meningkatkan biaya dari infrastruktur dan mengurangi tingkat efektifitas dari pendeteksian *spam.*Sebuah solusi kebijakan *e-mail,* respon yang mendukung variabel yang berdasarkan atas kualiatas dan tingkat kepercayaan atas sumber dari *e-mail* yang masuk. *E-mail* yang berasal dari pengirim yang diketahui dapat dilalukan dari Penyaringan spam , sedangkan *e-mail* yang berasal dari sumber yang tidak dipercaya dapat dihapus dan *e-mail* yang berasal dari sumber yang mencurigakan dapan diblok dan dilewatkan melalaui penyaringan *spam* yang sangat sensitive



Gambar II.3 Penyortiran e-mail masuk(Iron Port 2004)

\

III. PENUTUP

3.1. Kesimpulan

Spam adalah pengiriman sejumlah *message* yang sama yang memaksa orang lain yang tidak menginginkan adanya *message* yang mau tidak mau harus menerimanya. Tidak semua mail yang berisi propaganda dapat di-kategorikan sebagai *Spam*. Jika isi *e-mail* tersebut relevan dengan minat penerima *e-mail,* maka *e-mail* tersebut bukan *Spam* bagi pengguna *e-mail* tersebut. Hal

ini yang menyebabkan usaha untuk mengirimkan Spam terus dilancarkan, karena penerima yang tepat akan benar-benar membalas atau berminat terhadap isi yang ditawarkan.SMTPi merupakan salah satu solusi untuk penanganan *spam* yang berbasiskan SMTP. Kelebihan dari SMPTi ini adalah karena adanya 3 aspek utama yaitu Identitas,Reputasi dan Kebijakan. Walaupun demikian,bisa dikatakan tidak mudah menghindari *spam* karena teknik yang digunakan hampir menyerupai pengiriman *e-mail* normal. Kebanyakan *spam* yang ada di *internet* adalah berupa iklan, promosi dari suatu produk. *Spam* ini sangat menguntungkan bagi pengirim, karena hanya membutuhkan biaya yang kecil, sementara tidak sebaliknya jika kita memandang dari sisi penerima. *Spam* adalah tindakan yang tak bertanggung jawab. *Spam* jelas-jelas merugikan banyak pihak, sementara hanya menguntungkan satu dua pihak. *Spam* pun tak diinginkan praktis oleh semua orang. Jadi, demi masa depan yang baik, adalah seharusnya spam berkurang atau ditiadakan sama sekali. Jikalau nanti Indonesia sudah menyusul dan mulai membuat peraturan seputar *cyberspace* termasuk untuk mengatur *spamming*,

marilah kita semua bersama-sama mendukungnya. Atau kalau belum, marilah mulai mendorong pihak-pihak yang di atas sana untuk segera merealisasikan hal ini.

3.2. Saran

Spam dengan menggunakan SMTPi Sangat perlu, karena Memastikan akuntabilitas dari pengirim dalam pengiriman e-mail yang aman dan dapat dipercaya sangat diperlukan. SMPTPi adalah generasi terbaru dari infrastruktur *e-mail*. SMTPi ini memiliki 3 *framework* dengan komponen penting – identitas, reputasi dan policy tertentu dari suatu system messaging yang baru dan aman yang dibuat diatas SMTP. Perpindahan dari identitas dan reputasi dari mail system akan membuat pengirim menjadi mudah dipantau dan mengurangi masalah-masalah yang ada dengan *e-mail*. SMPTi ini berpedoman pada skema *autentifikasi*, reputasi pengiriman data dan kemampuan untuk membuat sebuah keamanan *e-mail* berdasarkan atas kedua aspek diatas.

DAFTAR PUSTAKA

Bagnall Brian.2000.*E-mail Virus Protection* Syngress Publishing, Inc.800 Hingham StreetRockland, MA 02370

Brenton, Chris dan Cameron Hunt.2005.,*Network Security*.Jakarta: Elexmedia Komputindo.

Costales Bryan , Marcia Flynt.2005. sendmail Milters A Guide for Fighting Spam Addison Wesley Professional Pearson Education, Inc. rights and Contracts Department. Lake Street Upper Saddle River, NJ 07458

Raharjo, Budi.2005.Keamanan Sistem Informasi Berbasis Internet. Jakarta :PT Indocisc dan Bandung:PT Insan Infonesia

Sukmaji Anjik dan Rianto.2008.Jaringan Komputer.Yogyakarta:Andi

Zdziarski Jonathan A..2005. Ending spam : Bayesian content filtering and the art of statistical language classification. No Starch Press, Inc. 555 De Haro Street, Suite 250, San Francisco

Referensi Web

Iron Port. 2004.*An e-mail security architecture* IronPort Systems, Inc.1100 Grundy Lane, Suite 100 San Bruno, California 94066 (http://www.ironport.com/pdf/ironport_e-mail_authentication_wp.pdf) (diakses 20 Agustus 2009)

Krawetz Neal.2004.*Anti-Spam Solutions and Security*. (http://www.securityfocus.com/infocus/1763) (Diakses 20 Agustus 2009)

B.Postel Jonathan .1982.Simple mail transfer protocol Information Sciences Institute University of Southern California 4676 Admiralty Way Marina del Rey, California90291(http://www.freesoft.org/CIE/RFC/821/2.htm) (Diakses 20 Agustus 2009)