BAB II

LANDASAN TEORI

2.1 Jaringan Komputer

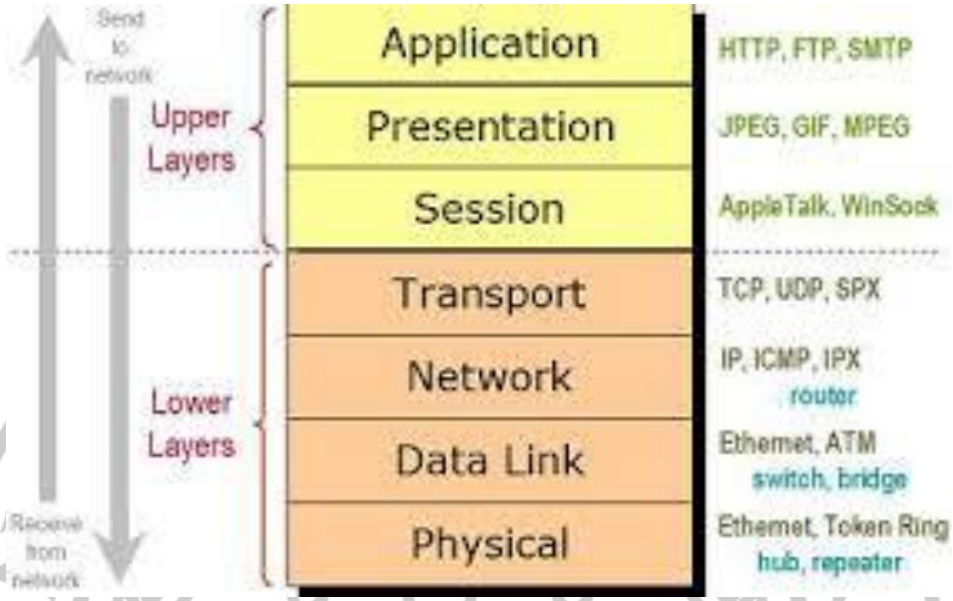
Menurut (Haryanto and Riadi 2014) sebuah jaringan komputer biasanya terdiri dari dua atau lebih komputer yang saling terhubung satu sama lain serta dapat saling berbagi sumber daya seperti *CDROM*, *printer*, pertukaran *file*, atau memungkinkan untuk saling berkomunikasi secara elektronik, komputer dapat terhubung melalui media transmisi seperti kabel, saluran telepon, gelombang radio, satelit atau infrared. jaringan komputer merupakan sekumpulan perangkat yang dapat digunakan untuk menyimpan dan memanipulasi data elektronis serta pesan-pesan, saling terkait sehingga dapat berbagi pakai berupa data, perangkat keras, dan perangkat lunak. Jaringan komputer adalah sekelompok komputer otonom yang saling berhubungan satu sama lain menggunakan protokol komunikasi sehingga dapat saling berbagi informasi, aplikasi, dan perangkat keras secara bersama-sama, tujuan membangun jaringan komputer adalah untuk membawa secara tepat tanpa adanya kesalahan dari sisi pengirim menuju ke sisi penerima melalui media komunikasi (Erfanti, Taufik, and Joko 2016).

Berdasarkan dari ketiga pengertian tersebut dapat disimpulkan bahwa jaringan komputer adalah sebuah sistem yang menghubungkan *node-node* yang terdapat pada jaringan komputer dengan menggunakan media komunikasi tertentu sehingga *node-node* pada jaringan komputer dapat saling berbagi sumber daya, berkomunikasi, dan saling bertukar informasi untuk mencapai suatu tujuan yang sama (Hanif 2018).

2.2 Model Lapisan *OSI*

Model *Open System Interconnection* (*OSI*) diciptakan oleh *International Organitation for Standardization (ISO)* yang menyediakan kerangka logika terstruktur bagaimana proses komunikasi data berinteraksi

melalui jaringan, standar ini dikembangkan untuk industri komputer agar komputer dapat berkomunikasi pada jaringan yang berbeda secara efisien (Sinsuw 2014).



Gambar 2.1 *Layer OSI*
Sumber: Sujana, 2014

Menurut Sujana (2014) terdapat tujuh *layer* pada model *OSI* dan setiap *layer* memiliki tanggung jawab khusus pada pada proses komunikasi data:

1. ***Physical***

   Pada *physical layer* tidak memiliki protokol yang spesifik, karena pada *physical layer* hanya mengirimkan *bit* data.

2. ***Data Link***

   Terdapat dua protokol pada *data link layer* yaitu:

   - *PPP (Point to Point Protocol)*

     Protokol yang digunakan untuk komunikasi *point to point* pada suatu jaringan.

   - *SLIP (Serial Line Internet Protocol)*

     Protokol yang digunakan untuk menghubungkan *serial*.

3. *Network*

Terdapat tiga protokol pada *network layer* yaitu:

- *IP (Internetworking Protocol)*

  Mekanisme transmisi yang digunakan untuk mentransportasikan data dalam paket yang disebut *datagram*.

- *ARP (Address Resolution Protocol)*

  Protokol yang digunakan untuk mengetahui alamat *IP* berdasarkan alamat fisik dari sebuah komputer.

- *RARP (Reverse Address Resolution Protocol)*

  Protokol yang digunakan untuk mengetahui alamat fisik melalui alamat *IP* komputer.

- *ICMP (Internet Control Message Protocol)*

  Mekanisme yang digunakan oleh sejumlah *host* untuk mengirim notifikasi datagram yang mengalamai masalah pada *host*nya.

- *IGMP (Internet Group Message Protocol)*

  Protokol yang digunakan untuk memberi fasilitas pesan yang simultan kepada grup penerima.

4. *Transport*

Terdapat dua protokol pada *transport layer* yaitu:

- *TCP (Transmission Control Protocol)*

  Protokol yang menyediakan layanan penuh pada lapisan *transport* untuk aplikasi.

- *UDP (User Datagram Protocol)*

  Protokol *connectionless* dan *procces-to-procces* yang hanya menambahkan alamat *port*, *checksum error control* dan panjang informasi data pada *layer* diatasnya.

5. *Session*

Terdapat empat protokol pada *session layer* yaitu:

- *NETBIOS*

  Berfungsi sebagai penyiaran pesan, maksudnya adalah memungkinkan *user* mengirim pesan tunggal secara serempak

ke komputer lain yang terkoneksi. *NETBEUI (NETBIOS Extended User Interface)* berfungsi sama dengan *NETBIOS* hanya sedikit dikembangkan lagi dengan menambah fungsi yang memungkinkan bekerja dengan perangkat keras dan perangkat lunak.

- *ADSP (AppleTalk Data Stream Protocol)*

  Fungsi dari protokol ini adalah untuk memantau aliran data dianatara dua komputer dan untuk memeriksa aliran data tersebut tidak terputus.

- *PAP (Printer Access Protocol)*

  Berfungsi sebagai *printer postscript* untuk melakukan akses pada jaringan *Apple Talk* dan untuk mengendalikan bagaimana pola komunikasi antar *node*.

- *SPDU (Session Protocol Data Unit)*

  Berfungsi sebagai penghubung antara dua *session service user*.

6. *Presentation*

Terdapat tiga protokol pada *layer presentation* yaitu:

- *TELNET*

  Protokol yang digunakan untuk melakukan *remote access* ke suatu *host*.

- *SMTP (Simple Mail Transfer Protocol)*

  Salah satu protokol yang digunakan dalam pengiriman *email* di internet atau untuk mengirim data dari komputer pengirim *email* ke *server email* penerima.

- *SNMP (Simple Network Management Protocol)*

  Protokol yang digunakan dalam suatu manajemen jaringan.

7. *Application*

Terdapat sembilan protokol pada *layer application* yaitu:

- *HTTP (Hyper Text Transfer Protocol)*

  Protokol yang digunakan untuk mentransfer dokumen dan web dalam sebuah *web browser* melalui *www*.

- *FTP (File Transfer Protocol)*

  Protokol *internet* yang berjalan dalam lapisan aplikasi yang merupakan standar untuk mentransfer *file* komputer dalam sebuah jaringan *internet*.

- *NFS (Network File System)*

  Jaringan komputer yang memungkinkan pengguna di klien komputer untuk mengakses *file* melalui jaringan dengan cara yang sama saat mengakses *file* pada sumber penyimpanan lokal.

- *DNS (Domain Name System)*

  Protokol yang digunakan untuk memberikan suatu nama *domain* pada sebuah alamat *IP* agar lebih mudah diingat.

- *POP3 (Post Office Protocol)*

  Protokol yang digunakan untuk mengambil *mail* dari suatu *mail transfer agent* yang akhirnya *mail* tersebut akan di*download* kedalam jaringan lokal.

- *MIME (Multipurpose Internet Mail Extension)*

  Protokol yang digunakan untuk mengirim *file binary* dalam bentuk teks.

- *SMB (Server Messange Block)*

  Protokol yang digunakan untuk mentransfer *server-server file* ke *DOS* dan Windows.

- *NNTP (Network News Transfer Protocol)*

  Protokol yang digunakan untuk menerima dan mengirim *newsgroup*.

- *DHCP (Dynamic Host Configuration Protocol)*

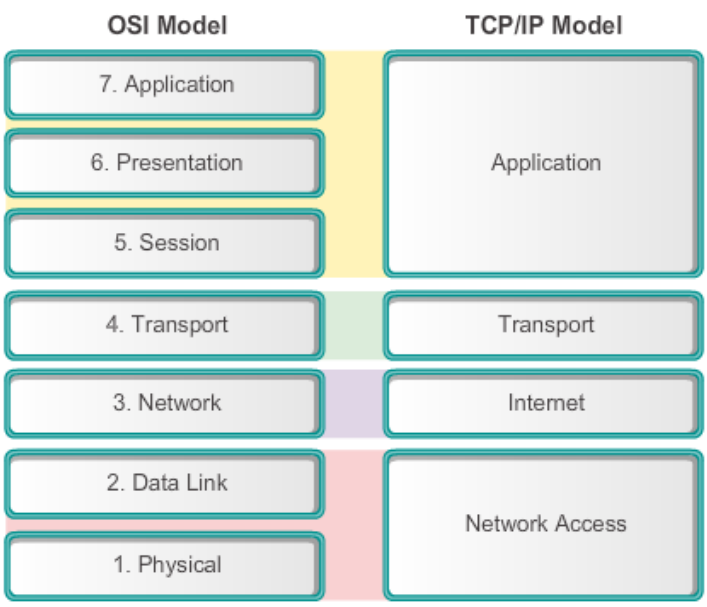
  Layanan yang memberikan alamat *IP* kepada komputer yang memintanya secara otomatis.

2.3 *Transmission Control Protocol / Internet Protocol (TCP/IP)*

TCP/IP didefinisikan sebagai protokol jaringan yang berperan dalam membangun *environment* jaringan global seperti *internet*. Protokol direferensikan pula sebagai suit *protocol DoD* (“*deeohdee*”) karena mereka

pada dasarnya dikembangkan oleh komunitas riset *Advanced Research Projects Agency* (*ARPA*) dari *US Department of Defense* (*DoD*) (Hanif 2018).

Nama *TCP/IP* diambil dari dua 'Keluarga' protokol fundamental, yaitu *TCP* dan *IP*. Meskipun demikian, suit masih memiliki protokol utama lainnya seperti *UDP* dan *ICMP*. Protokol bekerja sama dalam memberikan *framework networking* yang digunakan oleh banyak protokol aplikasi berbeda, di mana masing-masing digunakan untuk tujuan berbeda (Kader, Najoan, dan Sinsuw, 2014).



Gambar 2.2 Perbandingan *Layer TCP/IP* dan *Layer OSI*
Sumber: Wardoyo, Ryadi, dan Fahrizal, 2014

Berikut fungsi dari masing-masing *layer* pada protokol *TCP/IP* (Riadi, 2011):

1. ***Network Access Layer***

   Layer network access merupakan gabungan antara dua *layer* yaitu *network interface layer dan physical layer, network interface layer berfungsi untuk mengirim data ke layer physical melalui device jaringan kemudian dilanjutkan oleh layer physical yang*

merupakan sistem kabel yang digunakan untuk proses mengirim dan menerima data.

2. ***Internet Layer***

   Pada lapisan *internet* terjadi proses pengambilan paket dari lapisan *transport* dan menambahkan informasi alamat sebelum mengirimkannya ke lapisan *network interface*.

3. ***Transport Layer***

   Pada lapisan *transport* terdapat protokol seperti *TCP* dan *UDP* yang berfungsi menambahkan data *transport* ke paket dan melewatkannya ke lapisan *Internet*.

4. ***Application Layer***

   Pada lapisan *application* terdapat protokol seperti *FTP*, *Telnet*, *SMTP*, dan *NFS* dilaksanakan.

2.4 Keamanan Jaringan Komputer

Menurut Fitriani (2014) Keamanan jaringan komputer merupakan suatu proses untuk mencegah dan mengidentifikasi penggunaan yang tidak sah dari jaringan komputer. Langkah-langkah pencegahan membantu menghentikan pengguna yang tidak sah yang disebut "penyusup" untuk mengakses setiap bagian dari sistem jaringan komputer. Tujuan keamanan jaringan komputer adalah untuk mengantisipasi resiko jaringan komputer berupa bentuk ancaman fisik maupun logik baik langsung ataupun tidak langsung mengganggu aktivitas yang sedang berlangsung dalam jaringan komputer.

2.5 Jenis-jenis Layanan Keamanan Jaringan

Menurut Fitriani (2014) terdapat beberapa jenis layanan keamanan jaringan, diantaranya:

1. Otentikasi (*Authentication*)

   Layanan Otentikasi ada 2 macam. Pertama disebut dengan Otentikasi Entitas (*Entity Authentication*) yaitu layanan kemanan jaringan yang memberikan kepastian terhadap identitas sebuah

entitas yang terlibat dalam komunikasi data. Kedua adalah Otentikasi Keaslian Data (*Data Origin Authentication*) yaitu layanan yang memberikan kepastian terhadap sumber sebuah data.

2. Kendali Akses (*Access Control*)

   Kendali Akses adalah layanan keamanan jaringan yang menghalangi penggunaan tidak terotorisasi terhadap sumber daya. Pada aplikasi jaringan umunya kebijakan kemampuan (baca, modifikasi, tulis dan eksekusi sebuah data/layanan sistem) ditentukan oleh jenis pengguna.

3. Kerahasiaan Data (*Data Confidentility*)

   Kerahasiaan data adalah layanan keamanan jaringan yang memproteksi data tertranmisi terhadap pengungkapan oleh pihak yang tidak berwenang / berhak.

4. Keutuhan Data (*Data Integrity*)

   Keutuhan data adalah layanan keamanan jaringan yang memastikan bahwa data yang diterima oleh penerima adalah benar-benar sama dengan data yang dikirim oleh pengirim.

5. *Non-Repudiation*

   Layanan *non-repudiation* adalah layanan keaman jaringan yang menghindari penolakan atas penerima atau pengirim data yang telah dikirim.

6. Ketersediaan (*Availability*)

   Layanan *Availability* adalah layanan sistem yang membuat sumber daya sistem tetap dapat diakses dan digunankan ketika ada permintaan dari pihak yang berwenang. Serangan seperti *Denial of Service* membuat sistem tidak dapat diakses oleh pihak yang berwenang.

2.6 *Email Spoofing* dan *Phising*

(Suryana, Akbar, and Widiyasono 2016) *Email Spoofing* adalah kegiatan melakukan manipulasi data pada *header email*. Serangan yang paling populer dari *email spoofing* adalah serangan *phising*. *Email spoofing* dianggap sebagai tindakan yang berbahaya, karena melakukan manipulasi data pada *header email* untuk menyamar sebagai orang atau organisasi yang berwenang, contohnya seperti melakukan pengiriman *email* dengan nama pengirim seolah-olah *email* tersebut dikirim oleh administrator suatu organisasi. Pengirim *email spoofing* menyerang dengan berbagai macam isi pesan untuk meyakinkan korbannya.

(Suryana, Akbar, and Widiyasono 2016) *Phising* adalah bentuk pencurian identitas secara *online* yang bertujuan untuk mencuri informasi sensitif seperti sandi dan informasi kartu kredit. Serangan *phising* menggunakan kombinasi teknik *social engineering* dan teknik *spoofing* untuk membujuk pengguna agar memberikan informasi sensitif yang dapat digunakan untuk memperoleh keuntungan pribadi, salah satu contohnya adalah keuntungan finansial. *Phiser* biasanya membajak sebuah halaman web dari bank, kemudian mengirim *email* kepada korbannya supaya korbannya mengunjungi situs berbahaya dengan tujuan untuk mengumpulkan informasi rekening bank dan nomor kartu milik korbannya.

2.7 *Server*

Server adalah sebuah sistem komputer yang menyediakan jenis layanan tertentu dalam sebuah jaringan komputer. Beberapa contoh layanan *server* adalah *DHCP Server*, *DNS Server*, *FTP Server*, *Web Server*, *Mail server*, *Database Server* dan lain-lain (Saputra & Syafrizal, 2012).

2.8 Linux

Menurut Harjono (2016) Linux adalah sebuah aplikasi atau program yang menggunakan kernel sebagai sistem operasi. *Script* pertama Linux dirancang dan ditulis oleh seorang mahasiswa dari Finlandia bernama "Linus Torvalds" untuk arsitektur Intel 80386. Banyak orang memiliki

peran penting dalam mengembangkan dan memperluas Linux di berbagai belahan dunia. Peralatan sistem dan pustakanya umumnya berasal dari sistem operasi GNU yang diumumkan tahun 1983 oleh Richard Stallman. Kontribusi GNU merupakan dasar dari munculnya nama alternatif GNU/LINUX. Dia menggunakan alat proyek GNU dan dengan demikian sistem operasi dikembangkan melalui proyek GNU/LINUX.

2.9 Linux *CentOS*

CentOS merupakan singkatan dari *Community ENTerprise Operating System* yang merupakan sebuah distribusi Linux sebagai bentuk dari usaha untuk menyediakan *platform* komputasi berkelas *enterprise* yang memiliki kompatibilitas kode biner sepenuhnya dengan kode sumber yang menjadi induknya, *Red Hat Enterprise Linux (RHEL)*. *RHEL* merupakan distribusi Linux berbayar yang menyediakan akses update atas perangkat lunak dan beragam jenis dukungan teknis. Distribusi Linux ini sebenarnya merupakan gabungan dari sejumlah perangkat lunak yang didistribusikan di bawah lisensi perangkat lunak yang bebas dan kode sumber atas paket perangkat lunak ini dirilis ke publik oleh *Red Hat*. CentOS tersedia secara gratis, dukungan teknis utamanya disediakan terhadap para pengguna melalui *mailing list*, forum berbasis web, ataupun *chat*. Proyek CentOS tidak berafiliasi dengan *Red Hat*, sehingga proyek *CentOS* berjalan tanpa mendapatkan bantuan apapun dari *Red Hat*. Untuk penggalangan dana, *CentOS* berbasis donasi dari para pengguna serta sponsor dari perusahaan-perusahaan yang menggunakannya (Wicitra, Utomo, dan Wardana, 2014).

2.10 *Centos Web Panel*

CentOS Web Panel adalah panel kontrol untuk *web hosting* yang dapat digunakan secara gratis dan dirancang untuk memanajemen *VPS* maupun *Dedicated Server* dengan cepat dan mudah tanpa harus menggunakan aplikasi *SSH Client*, menawarkan sejumlah besar opsi dan fitur untuk manajemen *server* dalam paket panel kontrolnya.

Centos Web Panel system administrator dapat menggunakan satu server untuk membuat banyak server virtual untuk kebutuhan yang berbeda-beda, seperti menggunakan server untuk kebutuhan web server, DNS Server, mail server dan lain sebagainya. Hal ini membuat penggunaan server lebih efektif dan efisien dan tidak ada resource yang terbuah sia-sia karena tidak terpakai. lalu setiap server penggunaannya akan menggunakan remote untuk setiap administrator dengan pengaturan autentikasi yang berbeda-beda (Ginantra et al. n.d.).

2.11 Surat Elektronik

Surat elektronik adalah layanan yang diberikan oleh *internet* yang berkembang sejak tahun 1960, pada saat itu *internet* belum terbentuk, yang ada hanyalah kumpulan *mainframe* yang terbentuk sebagai jaringan. Mulai tahun 1980-an, surat elektronik sudah bisa dinikmati oleh khalayak umum. Surat elektronik adalah salah satu proses pengiriman surat melalui *internet* dengan menggunakan waktu yang sangat singkat. Surat elektronik *merupakan salah satu dari sekian banyak layanan internet yang ada saat ini selain Netnews, Telnet, File Transfer Protokol (FTP) dan World Wide Web (www) dan masih banyak layanan yang lainnya. Layanan internet adalah berbagai program atau fasilitas yang disediakan oleh internet, dari layanan internet tersebut yang paling banyak digunakan adalah layanan surat elektronik.* Penggunaan *electronic mail* (surat elektronik) sebagai media komunikasi yang ditunjang oleh banyaknya penyedia layanan di*internet* seperti Yahoo, Google, MSN, Wordpress, dan yang lainnya menunjukkan bahwa banyak orang melakukan komunikasi karena dengan komunikasi orang dapat beraktivitas dan meningkatkan kariernya (Mawarsih, 2014).

2.12 *Mail Server*

(Desmira, Sumarto, and Yuliani 2017) *Mail server dikenal sebagai* sebuah *mail transfer agent atau MTA, mail router atau mailer Internet adalah sebuah aplikasi yang akan menerima email masuk dari pengguna*

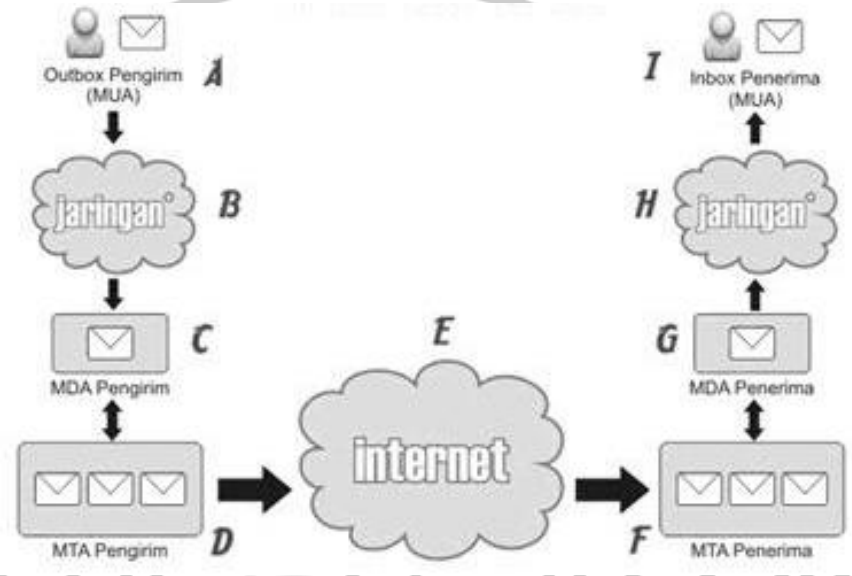
lokal (orang-orang dalam satu domain) dan jarak jauh pengirim dan meneruskan email keluar untuk pengiriman. Sebuah komputer yang didedikasikan untuk menjalankan aplikasi tersebut juga disebut sebagai mail server. Mail Server bisa diartikan sebagai induk atau rumah dari email, Setiap email yang dikirimkan dibuat untuk melewati sejumlah server mail sepanjang perjalanan ke penerima. Untuk user biasa, surat tersebut dikirim langsung tetapi proses adalah sesuatu yang dimengerti. Tanpa rangkaian Server Mail, pengguna hanya akan dapat mengirim email ke orang-orang yang memiliki alamat email dengan *domain* yang sama.

Menurut (Muarif and Irwan 2018) *Mail Server memiliki tiga komponen utama yang membentuknya, yakni Mail Transfer Agent (MTA), Mail Delivery Agent (MDA), dan Mail User Agent (MUA*):

1. Menurut Sadikin (2014) *Mail User Agent (MUA)* merupakan program yang digunakan oleh pemakai untuk membaca dan mengirim *email* pada komputer pribadinya. Contoh program atau perangkat lunak *Mail User Agent (MUA)* ini misalnya Microsoft Outlook, Microsoft Outlook Express, Lotus Notes, Pegasus Mail dan Thunderbird. *Mail User Agent (MUA)* mengambil *email* dari *email server* menggunakan protokol *Post Office Protocol (POP)* dan *Internet Message Access Protocol (IMAP).*
2. *Mail Tranfer Agent (MTA) Mail Transfer Agent merupakan salah satu komponen penting pada server internet. Mail Transfer Agent bertanggung jawab untuk mentransfer email dari mail server mengirimkan sampai ke server penerima email. Kebutuhan pengguna atas jenis MTA yang digunakan juga beragam. Berbagai kriteria biasa digunakan untuk pertimbangan. Tiap-tiap program mail server memiliki kelebihan dan kekurangan tersendiri. Beberapa MTA memiliki fasilitas yang sangat hebat sehingga mampu digunakan untuk*

menangani email dalam jumlah ratusan bahkan sampai ribuan perhari (Desmira, Sumarto, and Yuliani 2017).

3. Menurut Crocker (2009) *Mail delivery agent* atau *message delivery agent (MDA)* adalah komponen perangkat lunak komputer yang bertanggung jawab atas pengiriman pesan *email* ke kotak pesan penerima lokal.



Gambar 2.3 Proses pengiriman *email*
Sumber: Pratama, 2008

Pada gambar 2.3 dapat dijelaskan proses pengiriman *email* dimulai dari proses A yaitu pengirim *email* mengirim *email* menggunakan *MUA*, kemudian *email* diteruskan pada *MDA* yang berfungsi untuk mengatur pengiriman *email* pada *mail server* lokal (proses C), jika *email* tersebut dikirim kepada penerima yang berada pada *mail server* yang berbeda maka *email* akan dikirim melalui *MTA* untuk diteruskan ke *mail server* penerima melalui jaringan *internet* (proses E) kemudian *email* tersebut diterima oleh *MTA* pada *mail server* penerima (proses F) dan dilanjutkan ke *MDA mail server* penerima (proses G) agar *email* dapat di unduh oleh penerima *email* melalui jaringan lokal (proses H dan I).

2.13 *Mail Protocol*

Menurut (Desmira, Sumarto, and Yuliani 2017) terdapat tiga *Mail Protocol*, yaitu:

1. *POP3 (Post Office Protocol version 3)*

   POP3 merupakan protokol yang digunakan untuk pengelolaan *email*. *POP3* memudahkan seseorang dalam mendapatkan *email* mereka dari sebuah *mail server* tanpa perlu koneksi yang lama dengan internet yang tentu saja memakan biaya.

2. *IMAP (Internet Message Access Protocol)*

   IMAP (Internet Message Access Protocol) sama halnya dengan POP3, maka pesan email akan sepenuhnya disimpan dalam server email dan menggunakan komputer lokal untuk mengirim dan mengambilnya kapanpun di inginkan. Tergantung dari keinginan user. IMAP adalah protocol standar untuk mengakses atau mengambil email dari *server*.

3. *SMTP (Simple Mail Transfer Protocol)*

   SMTP merupakan salah satu jenis protocol yang bekerja dalam hal pengiriman pesan-pesan berupa surat elektronik atau email pada sebuah jaringan internet.

2.14 *Postfix*

Menurut (Wahyu noer hidayat 2010) "Postfix adalah *Mail Tranfer Agent* yang dapat diperoleh dengan gratis dan bersifat *open source*. *Postfix* merupakan *mail transfer agent default* untuk sejumlah sistem operasi yang bertipe unix. *Postfix* didistribusikan menggunakan lisensi umum *IBM* 1.0 yang merupakan lisensi perangkat lunak bebas tetapi tidak kompatibel dengan *GPL*".

Menurut (Kusmaya 2016) Postfix ditulis oleh Wietse Venema dan termasuk salah satu proyek *freeware*. Mulai digarap Wietse saat berkunjung ke *IBM* T. J. Watson *Research*. Wietse diberi kesempatan oleh IBM untuk menulis *software* ini. *Original software* tersebut diberi nama Vmailer, namun diganti menjadi *Postfix* atas saran *IBM*.

2.15 Dovecot

Menurut (Kusmaya 2016) “Dovecot adalah *open source server POP3* dan *IMAP* untuk Linux atau Unix. Program ini melengkapi *Postfix* dengan kinerja yang tinggi, kemudahan administrasi, dan keamanan yang solid. Dovecot merupakan sebuah aplikasi yang dijalankan untuk mengikuti protokol *IMAP* dan *POP3*.

2.16 *Roundcube*

Roundcube adalah solusi *webmail* gratis dan *open source* dengan antarmuka pengguna mirip *desktop* yang mudah dipasang atau dikonfigurasi dan berjalan pada *server LAMPP* standar. Tampilan menggunakan standar web terbaru untuk me*render* antar muka yang fungsional dan dapat disesuaikan. *Roundcube* menyertakan *library open-source* canggih lainnya seperti *PEAR, IMAP* yang berasal dari IlohaMail, pustaka Googiespell untuk pemeriksaan ejaan atau pembersih WasHTML oleh Frederic Motte (*Roundcube Open Source Webmail Software*, n.d.) (Hanif 2018).

2.17 *Domain Name System (DNS)*

Menurut (Saputra and Syafrizal 2012) *Domain Name System* adalah sebuah sistem yang menyimpan dan mengatur suatu informasi tentang penamaan *host* dari sebuah alamat *IP* menjadi sebuah karakter atau angka dalam sebuah jaringan internet yang di distribusikan pada *database*. *Domain name system* memiliki pengelolaan komponen inti yang terdiri dari *DNS resolver, Recursive DNS server* dan *Authoritative DNS server*. pada awal penggunaan *DNS* didalam jaringan komputer menggunakan HOSTS.TXT dari *SRI* (sekarang *SIR International*) yang berisi informasi dari nama komputer dan *IP address*.

2.18 *DNS Server*

Menurut (Kusmaya 2016) *DNS server* adalah *distribute database system* yang digunakan untuk pencarian nama komputer di jaringan yang menggunakan *TCP/IP* (*Transmission Control Protocol/Internet Protocol*). *DNS server* biasa digunakan pada aplikasi yang terhubung ke *internet*

seperti *web browser* atau *email*, dimana *DNS server* dapat membantu memetakan *hostname* sebuah komputer ke *IP Address*.

2.19 *Bind9*

BIND9 adalah aplikasi *DNS server* yang paling umum digunakan di *internet*, khususnya di sistem unix, *bind9* merupakan standar *DNS server*. *BIND9* awalnya dibuat oleh empat orang mahasiswa dengan menggunakan CSRG di Universitas California, Berkeley dan pertama kali dirilis di dalam 4.3 BSD. Paul Vixie kemudian meneruskan pemrogramannya pada tahun 1988 saat bekerja di *DEC*. Saat ini, *Bind9* dikelola oleh Konsorsium sistem *internet*. *BIND9* awalnya di tulis pada awal 1980 dan didanai oleh *DARPA* (*Defense Advanced Research Projects Agency*). Pada pertengahan 1980-an, *DEC* (*Digital Equipment Corporation*) mengambil alih pengembangan *BIND9*. Satu dari pekerja itu adalah Paul Vixie, yang terus mengerjakan *BIND9* sesudah meninggalkan *DEC* (Wahyu noer hidayat 2010).

2.20 *HTTP*

Menurut (Zabar and Novianto 2015) *HTTP* adalah sebuah protokol yang bekerja dengan cara meminta atau menjawab antara *client* dan *server*. Sebuah *client HTTP* seperti *web browser*, biasanya memulai permintaan dengan membuat hubungan *TCP/IP* ke *port* tertentu di tuan rumah yang jauh (biasanya *port* 80). Sebuah *server HTTP* yang mendengarkan di *port* tersebut menunggu *client* mengirim kode permintaan (*request*), seperti "GET / HTTP/1.1" (yang akan meminta halaman yang sudah ditentukan), diikuti dengan pesan *MIME* yang memiliki beberapa informasi kode kepala yang menjelaskan aspek dari permintaan tersebut dan diikuti dengan badan dari data tertentu. Beberapa kepala (*header*) juga dapat ditulis atau tidak, sementara yang lainnya (seperti tuan rumah) diperlukan oleh protokol HTTP/1.1. Begitu menerima kode permintaan (dan pesan bila ada), *server* mengirim kembali kode jawaban, seperti "200 OK", dan sebuah pesan yang diminta, atau sebuah pesan *error* atau pesan lainnya. Pengembangan *HTTP* dikoordinasi oleh Konsorsium *World Wide Web (W3C)* dan grup kerja

Internet Engineering Task Force (IETF), bekerja dalam publikasi satu seri *RFC*, yang paling terkenal *RFC 2616*, yang menjelaskan HTTP/1.1, versi *HTTP* yang umum digunakan sekarang.

2.21 *HTTP Server*

Menurut (Saputra and Syafrizal 2012) *HTTP Server* adalah sebuah *software* yang melayani permintaan berupa *Hypertext Transfer Protocol (HTTP)* atau *Hypertext Transfer Protocol Secure (HTTPS)* dari komputer atau *client* yang terhubung dalam jaringan *internet* atau *intranet*.

2.22 Apache HTTP Server

Menurut (Saputra and Syafrizal 2012) Apache HTTP Server adalah *web server* yang dapat dijalankan di banyak sistem operasi, seperti Unix, *BSD*, Linux, Microsoft Windows dan Novell Netware serta *platform* lainnya yang berguna untuk melayani dan memfungsikan situs web.

2.23 *Email Spam*

Menurut (Chandra, Indrawan, and Sukajaya 2016) *Spam email* dapat didefinisikan sebagai "*unsolicited bulk email*" yaitu *email* yang dikirimkan kepada ribuan penerima. *Spam email* biasanya dikirimkan oleh suatu perusahaan untuk mengiklankan produknya. Hal ini menyebabkan semakin padatnya antrian dari *mail server*. Banyak waktu yang terbuang untuk menghapus *email spam* dari kotak masuk, *spam* juga menyebabkan pemborosan biaya bagi pengguna yang menggunakan koneksi *dial-up*. Selain itu *spam* juga dapat membuang *bandwith* dan dapat menyebabkan penerima di bawah umur mengakses situs-situs yang memiliki konten negatif. Banyaknya *spam* menyebabkan kerugian dalam hal sumber daya dan memerlukan banyak waktu untuk menghapusnya.

2.24 *Spam Filter*

Spam filter merupakan *software anti spam*, *Software anti spam* bekerja dengan cara menganalisa *email* yang datang dan menggunakan sejumlah metode untuk menentukan apakah *email* yang diterima adalah

email spam atau bukan. Keberhasilan *spam filter* dalam mencegah masuknya *email spam* tergantung dari *software anti spam* yang digunakan serta metode-metode yang diterapkan oleh *software anti spam* untuk mendeteksi dan mencegah *email spam* (Fachrurrazi 2014).

2.25 *SpamAssassin, ClamAV, dan Amavisd-New*

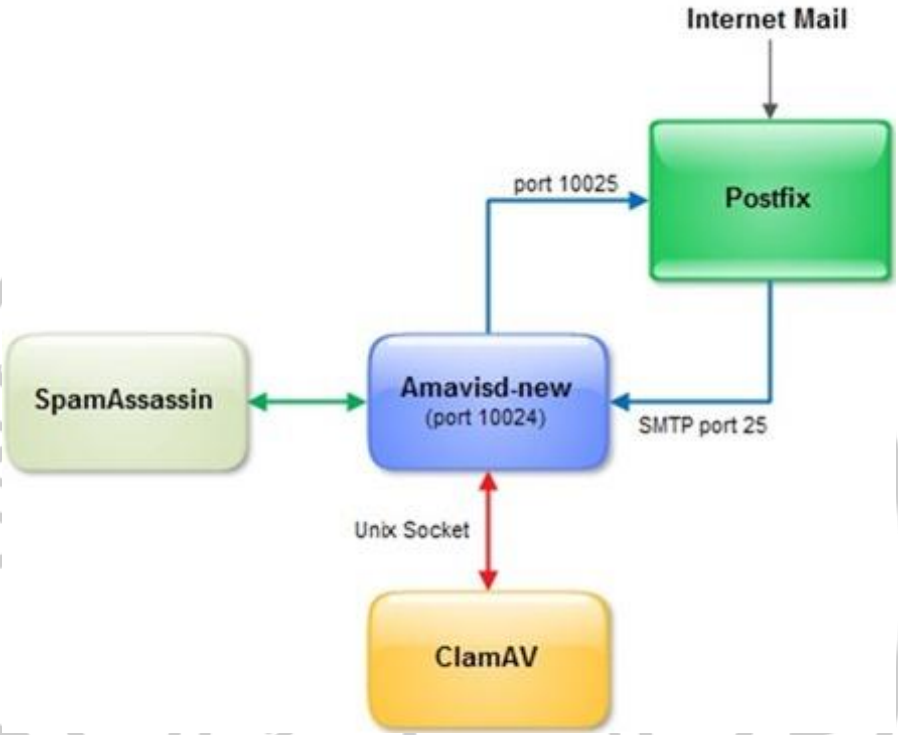
Menurut (Nurlina and Irmayana 2015) *SpamAssassin* adalah aplikasi yang sudah teruji secara luas menggunakan proyek *open source* yang berfungsi sebagai *mail filter* untuk mendeteksi *spam*. *SpamAssassin* berjalan pada *server* dan sebagai *filter spam* sebelum sampai pada pada kotak masuk pengguna. *SpamAssassin* diintegrasikan dengan *mail server* agar secara otomatis menyaring semua *email spam* dan aturan penggunaan atau tes untuk menentukan *email spam* atau *ham*. *SpamAssassin* dapat memberikan tanda dengan mengubah *subject email* atau langsung menghapus *email spam* yang masuk.

SpamAssassin menggunakan berbagai mekanisme untuk menangani *email spam*, berikut mekanisme yang diterapkan SpamAssassin:

1. Pengecekan *header email*.
2. Pengecekan isi *email*.
3. Pengelompokan *email address* secara manual kedalam *whitelist* atau *blacklist*.
4. *Bayesian filtering*.
5. Penyaringan *database spam* kolaboratif (*DCC*, *Pyzor*, dan *Razor2*).
6. Berbasis jaringan seperti *blacklist URL*, *blacklist DNS*, *checksum* berbasis *filter*, dan algoritma *Hash*.

Menurut (Kusmaya 2016) *ClamAV* adalah *anti virus open source (GPL)* yang dirancang untuk mendeteksi *trojan*, *virus*, *malware*, dan ancaman berbahaya lainnya. Secara *de facto ClamAV* adalah standar untuk pemindaian *mail gateway*.

Amavisd-new adalah antarmuka yang memiliki kinerja yang tinggi dan dapat diandalkan. *Amavisd-new* memiliki beberapa fitur seperti pemindai *virus* dan modul *SpamAssassin*. *Amavisd-new* berkomunikasi ke *MTA* melalui protokol *SMTP* atau *LMTP*, atau dengan menggunakan program pembantu .



Gambar 2.4 Cara Kerja *SpamAssassin*, *ClamAV*, dan *Amavisd-New*
Sumber: Valsecchi, 2013

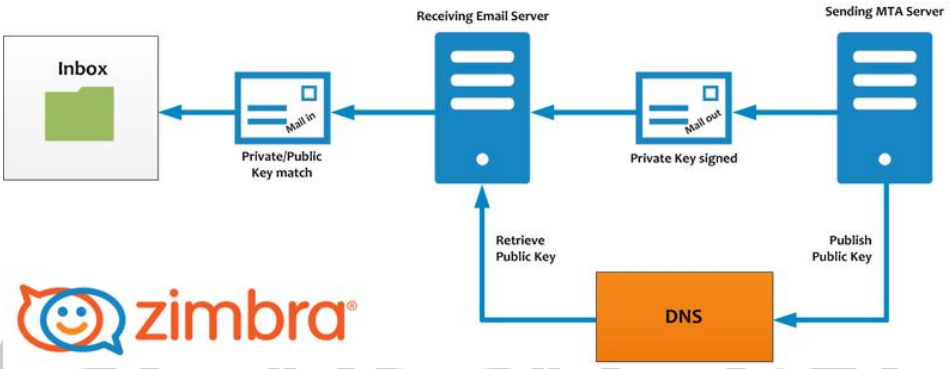
Cara kerja *SpamAssassin*, *ClamAV*, dan *Amavisd-New* dapat dilihat seperti gambar 2.4 yaitu Amavisd-New menerima email dari Postfix (MTA), kemudian menyebarkannya ke ClamAV dan SpamAssassin untuk memeriksa spam dan virus lalu mengembalikan email ke Postfix (MTA) untuk diteruskan ke penerima email.

2.26 *DomainKeys Identified Mail (DKIM)* dan *OpenDKIM*

Domain Keys Identified Mail (DKIM) adalah metode otentikasi *email* yang dirancang untuk mendeteksi *spoofing email*. Ini memungkinkan penerima untuk memeriksa bahwa *email* yang diklaim berasal dari *domain* tertentu memang diotorisasi oleh pemilik domain tersebut. Hal ini dimaksudkan untuk mencegah alamat pengirim palsu dalam *email* yang

sering digunakan untuk melakukan *phishing* dan *spam email*. (Hansen, Crocker, Baker, 2009).

Menurut Barovih (2011) *OpenDKIM* adalah pengiriman *email* yang menggunakan mekanisme otentikasi *framework* menggunakan kunci publik yang dimasukan ke dalam *DNS* maupun *email*.

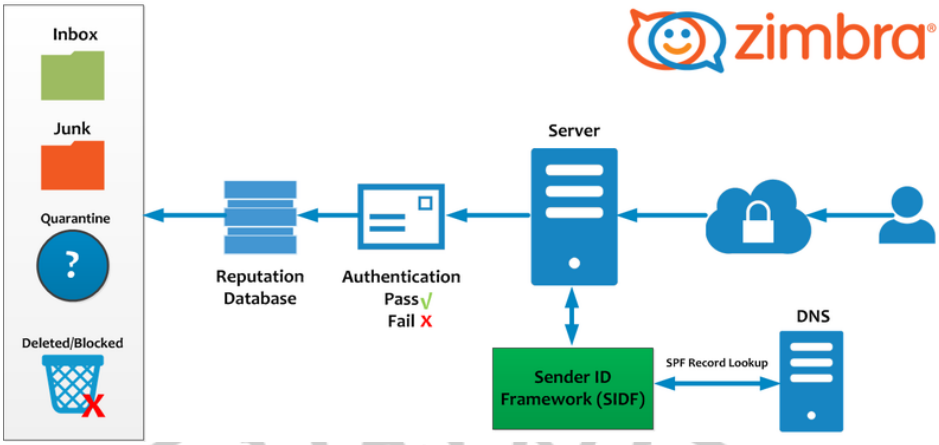


Gambar 2.5 Cara Kerja *DKIM*
Sumber: Zimbra Incorporation, 2005

Cara kerja *DKIM* dapat dilihat seperti pada gambar 2.5 yaitu mail server pengirim mempublish public key pada pada DNS server pengirim, setiap email yang dikirim melalui *mail server* pengirim akan diberikan private key, setelah email sampai pada mail server penerima maka mail server penerima akan mencocokan *private key* yang terdapat pada email dengan public key yang terdapat pada *DNS* server penerima, jika public dan private key cocok maka email tersebut dapat dipastikan berasal dari pengirim yang asli, namun jika public dan private key tidak cocok maka email tersebut dapat dipastikan sebagai email spoofing.

2.27 *Sender Policy Framework (SPF)*

Sender Policy Framework (SPF) adalah sistem validasi email, yang dirancang untuk mencegah email yang tidak diinginkan menggunakan sistem spoofing. Untuk memeriksa masalah keamanan umum ini, SPF akan memverifikasi IP sumber email dan membandingkannya dengan data TXT *DNS* dengan konten *SPF* (*Zimbra Incorporation, Best Practices on Email Protection: SPF, DKIM and DMARC, 2005*).



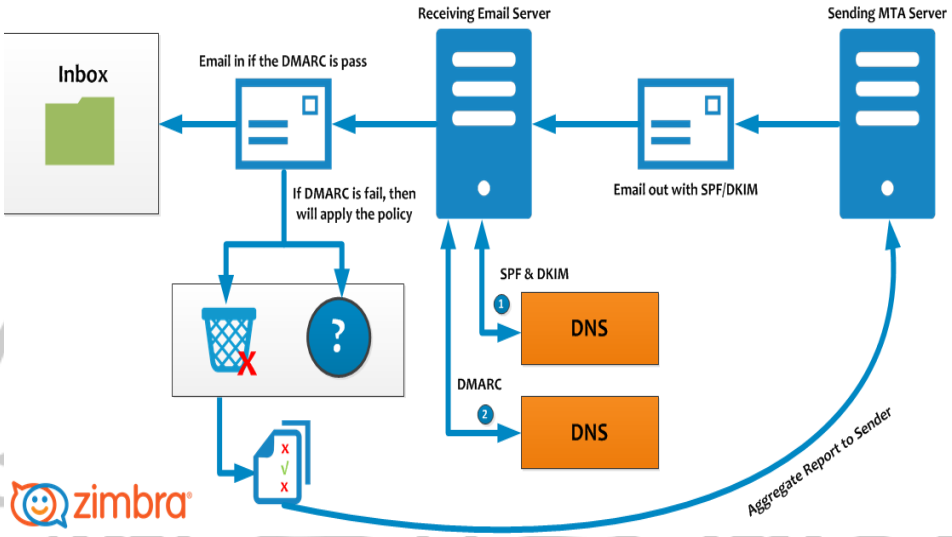
Gambar 2.6 Cara Kerja *SPF*
Sumber: Zimbra Incorporation, 2005

Cara kerja SPF dapat dilihat seperti pada gambar 2.6 yaitu email yang dikirim oleh pengirim akan diteruskan pada mail server penerima, selanjutnya mail server penerima akan mengecek Sender ID Framework yang berada pada DNS server pengirim, jika alamat IP server pengirim email sesuai dengan alamat IP yang telah diotorisasi oleh SPF record pada DNS server pengirim email maka email tersebut akan diberi nilai PASS, namun jika alamat IP server pengirim email tidak sesuai dengan alamat IP yang telah diotorisasi oleh SPF record pada DNS server pengirim email maka email tersebut akan diberi nilai FAIL atau SOFTFAIL dan selanjutnya database reputasi akan memberi nilai pada email tersebut berdasarkan pada laporan SPF masing-masing email untuk dijadikan pertimbangan tindakan apa yang akan dilakukan pada email tersebut.

2.28 Domain-Based Message Authentication, Reporting & Conformance (DMARC)

Domain-based Message Authentication, Reporting, and Conformance (DMARC) adalah metode autentikasi email standar. DMARC membantu administrator organisasi mencegah peretas dan penyerang lain melakukan spoofing terhadap organisasi dan domain. Spoofing adalah jenis serangan yang memalsukan alamat Dari dalam pesan email. Pesan palsu seolah tampak berasal dari organisasi atau domain yang ditiru identitasnya.

DMARC juga memungkinkan Anda meminta laporan dari server email yang menerima pesan dari organisasi atau domain Anda. Laporan ini berisi informasi untuk membantu Anda mengidentifikasi kemungkinan masalah autentikasi dan aktivitas berbahaya untuk pesan yang dikirim dari domain Anda (Nightingale 1945).



Gambar 2. 7 Cara Kerja *DMARC*
Sumber: Zimbra Incorporation, 2005

DMARC melalukan pengecekan melalui mekanisme yang sama dengan SPF Record dan DKIM Record. Saat pengguna mengirim email (melalui server indoglobal.com), maka mail server akan membubuhkan tandatangan yang dapat dicek oleh mail server penerima untuk memastikan keabsahan email tersebut (Nightingale 1945).

Mail server penerima akan melakukan pengecekan melalui dua cara:

a. Dengan mekanisme SPF, yaitu dengan cara melihat IP address mail server yang mengirimkan email. Jika IP address tersebut tertera pada record SPF, maka email tersebut dianggap sah (Nightingale 1945) .
b. Dengan mekanisme DKIM, yaitu dengan cara melihat tanda tangan yang ada di email. Jika tanda tangan di email sesuai dengan yang dipublikasikan pada record DKIM, maka email dianggal sah (Nightingale 1945).

Pengecekan DMARC dianggap sah jika paling tidak salah satu dari kondisi di atas terpenuhi.

2.29 *Gmail*

Gmail adalah layanan email yang intuitif dan efisien. Gmail menyediakan penyimpanan sebesar 15 GB, dengan lebih sedikit spam, dan dapat diakses melalui perangkat seluler (Gmail .n.d).

2.30 *Emkei's Mailer*

Emkei's Mailer adalah *Mailer* palsu *online* gratis dengan berbagai fitur seperti lampiran, enkripsi, *Editor HTML*, dan pengaturan lanjutan. (Emkei's Mailer, 2009).

Emkei's Mailer dapat digunakan untuk mengirim *email spoofing* dengan memalsukan alamat *email* pengirim pesan. *Emkei's Mailer* dapat diakses menggunakan *browser* dengan alamat *domain* www.emkei.cz. *Emkei's Mailer* dapat diakses secara gratis sehingga memberikan kemudahan dalam mengirim *email spoofing*.

2.31 *Yahoo! Mail*

Yahoo! Mail merupakan sebuah penyedia surat elektronik (webmail) dari Yahoo!. Yahoo! Mail merupakan penyedia surat elektronik terbesar di internet dengan jutaan pengguna. Saingan utama Yahoo! Mail ialah Windows Live Hotmail, Gmail dan AOL Mail (Arrington, 2006).