

BAB II

TINJAUAN PUSTAKA

2.1. Teori Dasar

2.1.1. Jaringan Komputer

Jaringan komputer merupakan gabungan dari dua perangkat atau lebih yang terhubung satu sama lain dengan tujuan untuk berkomunikasi serta berbagi informasi dengan melalui kabel ataupun tanpa kabel (nirkabel). Pada zaman ini jaringan komputer sangat dibutuhkan, mulai dari penggunaan pribadi hingga instansi seperti perusahaan, kampus dan rumah sakit. Hampir diseluruh perusahaan menggunakan jaringan komputer untuk mempermudah pertukaran data dan berkomunikasi. Menurut (Maslan 2012) beberapa manfaat dalam menggunakan jaringan komputer yaitu dapat saling *sharing file*, menggunakan *resource* secara bersamaan, penghematan biaya, peningkatan efisiensi kerja, lebih mudah dalam pelihara file dan meningkatkan kinerja sistem.

Dalam pertukaran informasi atau data tentunya ada pihak yang mengirimkan data dan pihak yang menerima data. *Client* merupakan perangkat yang menerima layanan sedangkan *Server* merupakan perangkat yang bertugas untuk menjalankan sebuah layanan atau pemberi layanan, skema ini disebut dengan sistem *client-server*. Menurut (Sulaksono dan Suharyanto 2020) salah satu metode untuk mengamankan jaringan komputer adalah penggunaan keamanan jaringan seperti *firewall*. *Firewall* adalah sebuah sistem keamanan jaringan yang dibuat untuk melindungi komputer dari beberapa jenis ancaman yang ada.

2.1.2. Standar Jaringan Komputer

Standar jaringan komputer merupakan penetapan suatu desain dalam sebuah jaringan komputer. Standar jaringan komputer sangat dibutuhkan pada jaringan komputer untuk mendefinisikan minimum perangkat keras (*hardware*) dan perangkat lunak (*software*) untuk memastikan kompatibilitas dalam sebuah jaringan. Standarisasi jaringan komputer ini merupakan sebuah aturan yang digunakan agar sistem yang berjalan dalam jaringan komputer dapat berjalan dengan baik sehingga memungkinkan untuk dua perangkat atau lebih dapat berkomunikasi dan berbagi informasi dalam sebuah jaringan. Menurut (Ismail 2017) beberapa aspek yang harus diperhatikan dalam membangun sebuah infrastruktur jaringan komputer yaitu aspek *availability*, *flexibility*, *fault tolerance*, *scability*, *security* dan *redudancy*.

Organisasi yang bertanggung jawab atas penentuan standar dalam jaringan komputer adalah *ANSI*, *IEEE*, *IETF*, *TIA/EIA*, *FCC*, *ISO*, dan *ITU-R*. Berikut merupakan peran masing-masing dari ke tujuh organisasi tersebut:

1. *ANSI (American National Standards Institute)*

Menurut (Kalangi 2012) *ANSI* merupakan organisasi yang bertanggung jawab atas pendefinisian standar Amerika Serikat dalam industri pemrosesan informasi dan bertugas atas pendefinisian standar protokol jaringan komputer serta merepresentasikan Amerika Serikat dengan penentu standarisasi internasional lain. *ANSI* juga merupakan sebuah organisasi sukarela yang terdiri atas anggota dari pemerintah, sektor usaha, dan lainnya yang bertugas dalam pengkoordinasian aktivitas yang relevan dengan standar.

2. *IEEE (Institute of Electrical and Electronics Engineers)*

Menurut (Kalangi 2012) *IEEE* merupakan sebuah organisasi internasional yang merupakan assosiasi professional utama dalam peningkatan bidang teknologi. Kepanjangan dari *IEEE* sebelumnya adalah *Institute of Electrical and Electronics Engineers*. Tetapi dikarenakan perkembangan bidang teknologi yang diperdalam oleh organisasi *IEEE* membuat penamaan kelektron dianggap tidak sesuai lagi, sehingga *IEEE* dianggap tidak mempunyai kepanjangan lagi, tetapi *IEEE* biasa dieja sebagai *Eye-Triple-E*. *IEEE* juga memiliki badan standar atau lebih dikenal dengan *Standard Association, IEEE-SA* yang mempersatukan *substandard* industri dalam pembentukan standardisasi internasional untuk seluruh industri. Terdapat beberapa standar yang telah didefinisikan oleh *IEEE* yaitu *IEEE 802.3(Ethernet)*, *IEEE 802.11(Wifi)*, dan *IEEE 802.16(WiMAX)*.

3. *IETF (Internet Engineering Task Force)*

Menurut (Kalangi 2012) *IETF* merupakan organisasi yang berperan dalam tugas pengaturan dan penetapan protokol-protokol standar yang dipakai di *internet*. *IETF* juga merupakan organisasi yang terdiri dari banyak pihak seperti pihak yang berjalan secara organisasional maupun pihak yang berjalan secara individual yang mendalami pengembangan jaringan komputer. Organisasi *IETF* diatur oleh *IESG (Internet Engineering Steering Group)* serta mempunyai tugas untuk mencari permasalahan teknis yang terjadi pada jaringan komputer sehingga kemudian bisa memberikan solusi dari permasalahan tersebut kepada *IAB (Internet Architecture Board)*.

4. *TIA (Telecommunications Industry Association) / EIA (Electronic Industries Alliance)*

Menurut (Kalangi 2012) *TIA* merupakan sebuah organisasi terpisah yang diakui oleh *ANSI* serta bekerjasama dengan *Electronic Industries Alliance (EIA)*. *TIA* diketahui sebagai organisasi terbaik dalam pengembangan standar pemasangan kabel dengan menggunakan desain serta instalasi sistem pemasangan kabel yang cukup terkoordinasi. Sehingga dapat mendukung cakupan jaringan komputer yang cukup luas serta memenuhi kecepatan jaringan yang cukup tinggi pada sekarang dan masa yang akan datang.

5. *FCC (Federal Communications Commission)*

Menurut (Kalangi 2012) *FCC* merupakan sebuah organisasi yang bergerak pada bidang pertelekomunikasian. *FCC* bertugas untuk mengatur alur komunikasi yang keluar maupun alur komunikasi yang masuk ke dalam Amerika Serikat. *Wireless* yang berfungsi sebagai sarana telekomunikasi juga merupakan wewenang dari organisasi *FCC*. Tujuan organisasi *FCC* dalam mengatur jenis komunikasi *wireless* adalah supaya tidak terjadinya penyalahgunaan dalam penggunaan frekuensi radio atau sinyal yang digunakan pada teknologi *wireless*. *FCC* juga merupakan sebuah organisasi yang didirikan oleh pemerintah United States yang bertugas untuk bertanggung jawab atas mengatur jenis komunikasi dalam perangkat telekomunikasi, baik itu menggunakan radio, *wireless*, kabel, dan satelit. Wilayah organisasi *FCC* ini melibatkan 50 negara yang berada di United States serta beberapa distrik yang menjadi kawasan dari Negara United States.

6. *ISO (International Organization for Standardization)*

Menurut (Kalangi 2012) *ISO* merupakan sebuah organisasi yang bertugas atas penetapan standar internasional yang terdiri dari badan standar nasional dalam setiap negara. Awalnya, singkatan dari organisasi ini adalah *IOS* dan bukan *ISO*. Tetapi untuk sekarang disingkat menjadi *ISO* dikarenakan dalam bahasa Yunani kata *sos* bermakna sama (*equal*). Meskipun organisasi *ISO* adalah sebuah organisasi non-pemerintah, kemampuan organisasi ini dalam menetapkan standar yang sering dijadikan sebagai standar nasional membuat organisasi *ISO* lebih berpengaruh dibandingkan organisasi non-pemerintah lainnya. *ISO* juga mengajukan struktur serta fungsi protokol dalam komunikasi data. Model tersebut dikenal dengan *OSI (Open System Interconnection) Reference Model* yang terdiri atas tujuh lapisan (*layer*) yang memiliki fungsi yang berbeda. Setiap lapisan *OSI* terdiri atas beberapa protokol yang berbeda serta masing-masing *layer* dan protokolnya menjalankan pelayanan yang sesuai terhadap fungsi *layer* tersebut.

7. *ITU-R (International Telecommunication Union Radiocommunication Sector)*

Menurut (Kalangi 2012) *ITU-R* merupakan organisasi *global* yang bertanggung jawab atas pengaturan penggunaan frekuensi radio (*RF*) diseluruh penjuru dunia. *The United Nations (PBB)* menugaskan *ITU-R* untuk mengatur penggunaan frekuensi secara *global*. Dikarenakan wilayah yang dicakup sangat luas, *ITU-R* membaginya menjadi beberapa wilayah dan diatur oleh organisasi yang berbeda. Dari masing-masing wilayah, kemudian dibagi lagi dengan organisasi dari masing-masing negara setempat.

2.1.3. Jenis Jaringan Komputer

Pada zaman ini, banyak instansi yang telah memanfaatkan jaringan komputer sebagai media untuk pertukaran data dan informasi dikarenakan jaringan komputer berkembang dengan pesat. Pengiriman data bisa dikirim dengan baik apabila koneksi dalam jaringan perangkatnya berfungsi dengan baik dengan menggunakan kabel (*Wired*) maupun nirkabel (*Wireless*). Menurut (Sujadi dan Mutaqin 2017) koneksi dalam jaringan merupakan dasar dari sebuah jaringan yang digunakan, baik itu jenis jaringan *Local Area Network (LAN)*, *Metropolitan Area Network (MAN)* serta jenis jaringan *Wide Area Network (WAN)*. Berikut merupakan jenis-jenis jaringan komputer berdasarkan geografis secara umum:

1. *Personal Area Network (PAN)*

Menurut (Prakasa 2018) *Personal Area Network* merupakan jenis jaringan komputer yang memiliki cakupan luas area seukuran tubuh manusia atau berada disekitar tubuh manusia. Jenis jaringan komputer *PAN* biasanya digunakan dalam perangkat *wireless* seperti *wireless mouse*, *wireless keyboard*, *wireless headphone*, *wireless microphone*, *wireless printer* dan lain sebagainya. *Bluetooth* merupakan teknologi nirkabel (*wireless*) yang dikembangkan untuk *PAN*. Secara umum *bluetooth* menggunakan frekuensi yang sama dengan *Wi-Fi (2,4 Ghz)* namun *bluetooth* memiliki kekuatan pancaran sinyal yang lebih rendah sehingga hanya dapat diakses oleh perangkat yang berada disekitarnya dan didesain untuk mendukung perangkat *mobile* yang memiliki sumber daya terbatas.

2. *Local Area Network (LAN)*

Menurut (Prakasa 2018) *Local Area Network* merupakan jenis jaringan komputer yang memiliki cakupan luas area lokal yang terbatas seperti area perkantoran, perumahan atau sekolah. Sampai sekarang masih belum terdapat literatur yang menyebutkan dan memastikan batasan khusus luas area *LAN*, namun yang dapat dijadikan panduan adalah selama jaringan komputer tersebut berada pada 1 area yang sama dari sebuah institusi. Beberapa literatur juga menyebutkan bahwa luasan maksimal yang disarankan saat membangun jaringan *LAN* kurang dari 1 KM. Tujuan dari dibangunnya *LAN* adalah untuk berbagi *resource* seperti *printer*, *scanner* dan lainnya. Sehingga perusahaan tidak perlu memiliki *resource* terlalu banyak dan bisa menghemat biaya. Saat ini *LAN* dapat dihubungkan menggunakan dengan jaringan nirkabel (*WLAN*) untuk memudahkan *staff* yang menggunakan perangkat bergerak seperti *laptop*, *mobile phone* dan *smart devices* lainnya.

3. *Metropolitan Area Network (MAN)*

Menurut (Prakasa 2018) *Metropolitan Area Network* merupakan jenis jaringan komputer yang memiliki cakupan luas area sekurangnya kota. *MAN* biasanya menghubungkan antar *LAN* yang ada pada beberapa instansi atau lokasi yang berjauhan tetapi masih termasuk dalam lingkup 1 kota yang sama sehingga *staff* dapat berbagi *resource* dengan *staff* lain di instansi atau lokasi yang lain. Biasanya jenis jaringan *MAN* digunakan pada perusahaan yang memiliki cabang di beberapa lokasi dan berada dalam 1 kota yang sama. *MAN* disarankan menggunakan jenis media transmisi fiber optik yang memiliki

kecepatan yang tinggi dan memiliki *bandwith* yang cukup besar untuk menampung lalu lintas data antar instansi atau lokasi lainnya (*LAN* lainnya). Topologi jaringan yang digunakan pada *MAN* biasanya menggunakan topologi jaringan *Ring* yang menghubungkan antar instansi seperti bentuk cincin. Kelemahan dari topologi jaringan *Ring* adalah apabila *backbone* atau jalur utama ke salah satu instansi terputus, maka jaringan instansi lainnya juga akan terputus. Untuk mengatasi masalah tersebut maka dibutuhkan *backup link* yang berfungsi sebagai jalur alternatif apabila *backbone* atau utama mengalami gangguan sehingga kinerja *staff* tidak terhambat oleh permasalahan jaringan komputer.

4. *Wide Area Network (WAN)*

Menurut (Prakasa 2018) *Wide Area Network* merupakan jenis jaringan komputer yang menghubungkan banyak *MAN*. *WAN* digunakan untuk menghubungkan instansi multinasional yang terpisah di beberapa negara yang berbeda sehingga meskipun sebuah instansi berada pada lokasi yang berjauhan dapat terhubung dalam jaringan komputer yang sama. *WAN* menggunakan berbagai media transmisi data mulai dari *submarine fiber optic* (fiber optic yang di tanam bawah laut) sampai komunikasi satelit. Teknologi yang digunakan untuk menghubungkan beberapa instansi yang berada di beberapa negara yang berbeda adalah *Virtual Private Network (VPN)* atau lebih sering disebut sebagai *tunneling*. Dengan menggunakan *VPN* pengguna tidak perlu mengetahui media transmisi data yang digunakan sehingga dapat terhubung ke instansi yang berada di negara lain.

2.1.4. Model *OSI Layer*

Open System Interconnection Reference Model atau model *OSI* merupakan model kerangka jaringan yang berfungsi sebagai protokol komunikasi data melalui 7 lapisan (*layer*) yang berbeda. Lapisan-lapisan pada *OSI Layer* berfungsi agar setiap paket data dalam jaringan dapat melalui satu persatu lapisan. *OSI Layer* bekerja melalui 7 lapisan secara berurutan, sehingga model *OSI Layer* bisa digunakan untuk melacak permasalahan yang mengakibatkan kesalahan dalam koneksi jaringan, sebagai contohnya ketika pengguna (*user*) tidak bisa mengakses *internet* melalui perangkatnya, berarti ada kesalahan yang mungkin terjadi pada salah satu lapisan tersebut. Menurut (Prabowo, Darusalam, dan Ningsih 2020) cara kerja dari *OSI Layer* merupakan proses berjalannya suatu data dari sebuah perangkat ke perangkat lainnya. Seluruh data harus melewati setiap lapisan agar bisa sampai ke perangkat tujuan. Fungsi setiap lapisan *OSI* sebagai berikut:

1. *Physical Layer*

Menurut (Abdullah 2015) fungsi dari *Physical Layer* adalah mengirimkan *raw bit* kepada saluran (*channel*) komunikasi. Permasalahan *desain* pada *physical layer* yang harus diamati merupakan pemastian bahwa apabila sebuah *client* mengirimkan data sebesar 1 *bit*, maka data tersebut harus diterima oleh *client* lainnya sebesar 1 *bit* dan bukan menerima data 0 *bit*. Secara umumnya permasalahan pada *desain physical layer* yang ditemukan pada *layer* ini berhubungan dengan elektrik, mekanisme serta media fisik yang terletak di bawah dari *physical layer*.

2. *Data Link Layer*

Menurut (Abdullah 2015) fungsi dari *Data Link Layer* merupakan mentransmisi data mentah (*raw data*) serta mentransformasikan data tersebut kepada lapisan atau *layer* yang terbebas dari kesalahan transmisi. Sebelum data diteruskan kepada lapisan selanjutnya, *data link layer* juga menjalankan tugas agar data yang dikirimkan oleh pengirim terpecah menjadi sejumlah *data frame* yang sebesar ratusan atau bahkan sebesar ribuan *byte*. Kemudian *data link layer* akan mentransmisikan *frame* tersebut dengan berurutan serta memproses *acknowledgement frame* yang dikirimkan kembali dari penerima. Dikarenakan *physical layer* bertugas untuk mengirimkan serta menerima aliran *bit*, maka *data link layer* yang akan bertugas untuk mengenali serta membuat batasan-batasan *frame* tersebut. Hal tersebut dilakukan dengan memasukkan *bit* khusus ke awal *frame* serta akhir *frame*.

3. *Network Layer*

Menurut (Abdullah 2015) fungsi dari *Network Layer* merupakan mengendalikan operasi-operasi dalam *subnet*. Permasalahan *desain* dalam *network layer* adalah cara penentuan rute pengiriman (*route*) sebuah paket data. *Route* bisa didasarkan pada *static table* yang terhubung dalam jaringan. *Route* biasanya ditetapkan pada saat awal *terminal session*. *Route* sendiri juga bisa dinamik dimana terdapat perbedaan dalam setiap paketnya. Apabila sebuah *subnet* jaringan memiliki banyak paket data yang berjalan secara bersamaan, bisa terjadi kemungkinan paket-paket data tersebut sampai dalam waktu bersamaan sehingga bisa menyebabkan *bottleneck*.

4. *Transport Layer*

Menurut (Abdullah 2015) fungsi dari *Transport Layer* merupakan penerima data dari *session layer*, memecahkan data menjadi hingga menjadi bagian yang lebih kecil, meneruskan data ke *network layer* serta memastikan semua bagian data tersebut dapat sampai pada *client* lainnya dengan baik dan benar. *Transport layer* harus berhati-hati dalam pemutusan koneksi (*session*) dalam jaringan. Proses tersebut memerlukan mekanisme penamaan sehingga proses dalam sebuah perangkat memiliki cara untuk mengetahui dengan siapa perangkat tersebut berkomunikasi. *Transport layer* juga berfungsi untuk mengatur alur informasi, sehingga alur informasi dari *host* yang cepat tidak membanjiri *host* yang lambat. Pengendalian alur informasi antar *host* dengan *host* lainnya adalah pengendalian alur *routing* pada *router*.

5. *Session Layer*

Menurut (Abdullah 2015) fungsi dari *Session Layer* adalah untuk menetapkan *session* atau sesi dari sebuah perangkat dengan penggunanya. *Session* dapat berfungsi saat seseorang pengguna *login* melakukan *remote* ke *remote system* serta memungkinkan seseorang pengguna memindahkan file dari sebuah perangkat keperangkat lain. *Session layer* juga dapat disebut sebagai layanan manajemen *token* untuk sebagian protokol agar memastikan pihak yang bersangkutan tidak melakukan operasi yang sama dalam waktu bersamaan. Untuk mengatasi masalah tersebut, maka *session layer* bertugas untuk menyediakan *token* yang dapat digunakan serta pihak yang memegang *token* tersebut yang akan diizinkan untuk menjalankan operasi tertentu.

6. *Presentation Layer*

Menurut (Abdullah 2015) *Presentation Layer* bertugas untuk menjalankan fungsi-fungsi tertentu yang digunakan sebagai penjaminan penemuan sebuah penyelesaian terhadap sebuah masalah tertentu. *Presentation Layer* juga tidak memberikan izin kepada penggunanya untuk menyelesaikan sebuah masalah sendiri. Sebuah contoh layanan dari *presentation layer* adalah *encoding data*. Dikarenakan mayoritas pengguna tidak melakukan pemindahan *string bit biner* secara *random* dan pengguna bertukar data seperti nama, umur, dan jumlah tabungan serta data tersebut dinyatakan dalam bentuk karakter *string*, bilangan *interger* dan bilangan *floating*.

7. *Application Layer*

Menurut (Abdullah 2015) *Application Layer* bertugas untuk pemindahan file. Di antara sebuah sistem file dengan sistem file yang lain biasanya memiliki konvensi penamaan yang berbeda dan memiliki barisan teks yang berbeda. Perpindahan file dari sebuah aplikasi ke aplikasi lain yang berbeda biasanya membutuhkan penanganan untuk mengatasi ketidak kompatibel. Tugas tersebut juga merupakan tugas dari *application layer*, sebagai contohnya seperti *email*, *remote system*, *directory lookup* serta berbagai layanan umum dan layanan khusus lain. *Application layer* sendiri juga terdiri dari berbagai macam protokol jaringan dan berbagai macam *terminal*. Sebagai contohnya saat pengguna menggerakkan kursor *terminal* di layar, maka perangkat lunak tersebut harus menjalankan perintah yang sesuai agar kursor tersebut dapat berjalan sesuai harapan pengguna.

2.2. Teori Khusus

2.2.1. *Mail Server*

Pada zaman perkembangan teknologi ini, penggunaan *email* tidak asing lagi untuk sebagian besar orang, hampir seluruh pekerjaan dan kebutuhan pribadi perlu menggunakan *email*. *Mail server* merupakan sebuah layanan *server* yang bertugas untuk mengirim dan menerima *email*. Sederhananya *mail server* berfungsi seperti kantor pos, *mail server* menyimpan surat masuk dari pengirim surat kemudian mengirimkan surat tersebut kepada penerima seperti kantor pos pada umumnya namun surat yang dikelola oleh *mail server* berupa elektronik.

Dengan adanya *mail server* pribadi juga memiliki banyak manfaat lainnya seperti menunjang aktivitas dan komunikasi dalam sebuah perusahaan atau instansi yang cukup besar. Selain itu apabila terjadi kerusakan maka bisa langsung diatasi oleh perusahaan atau instansinya sendiri. Dikarenakan saat ini privasi dalam sebuah perusahaan atau instansi sudah menjadi elemen penting bagi setiap perusahaan atau instansi lainnya agar tidak terjadinya kebocoran data yang bisa menguntungkan kompetitor, dengan memiliki *mail server* pribadi juga bisa membuat privasi perusahaan atau instansi lebih terjaga karena memiliki jaringan sendiri yang hanya bisa digunakan oleh perusahaan atau instansinya sendiri.

Menurut (Mukhtar, Daniel Adi Putra Sitorus, dan Yulia Fatma 2020) membangun *mail server* saat ini tidak cukup dengan instalasi dan menjalankannya saja, tetapi membutuhkan beberapa proses yang dilakukan agar *mail server* tersebut dapat berjalan dengan aman dan lancar.

2.2.2. Microsoft Exchange Server

Microsoft Exchange Server merupakan *mail server* yang dikembangkan oleh *Microsoft Corporation*. Fitur utama yang disediakan oleh *Microsoft Exchange Server* adalah manajemen *email*, *calendar*, *contact* dan *tasks*. *Microsoft Exchange Server* sangat sering digunakan untuk bisnis, dikarenakan *Microsoft Exchange Server* dapat menyinkronkan *email* dari *mail server* kepada pengguna. Saat pengguna menggunakan akun *Microsoft Exchange Server*, maka data *email* pengguna tersebut dan informasi lainnya akan disinkronkan dengan perangkat pengguna tersebut, baik itu perangkat seperti komputer maupun *mobile device*.

Microsoft Exchange Server sendiri memiliki banyak fitur yang bagus seperti *Exchange ActiveSync*, *Outlook Anywhere* dan masih banyak fitur-fitur lainnya. *Exchange ActiveSync* merupakan fitur yang akan terjadi atau di *trigger* apabila ada perubahan didalam akun *email* pengguna sebagai contohnya seperti saat *email* dibalas, *email* dihapus, *email* dipindahkan dan sebagainya. Perubahan tersebut akan berubah dan berjalan secara *realtime* karena tersinkronisasi dengan fitur *Exchange ActiveSync* yang disediakan dari *Microsoft Exchange Server*. Sedangkan fitur *Outlook Anywhere* merupakan fitur yang disediakan oleh *Microsoft Exchange Server* agar pengguna *email* bisa mengakses dan mengelola *emailnya* darimana saja melalui *software* pengelola *email* (*software mail client*) seperti *Outlook Client* dan *Mozilla Thunderbird* maupun melalui *web browser* seperti *Google Chrome* dan *Mozilla Firefox* dengan memasukan *link* atau alamat dari *mail server* tersebut.

Menurut (Stanek 2017) dengan menggunakan implementasi secara lokal, *administrator* jaringan bisa mengimplementasi *Microsoft Exchange Server* didalam perangkat keras server jaringan dan mengelola semua aspek yang diperlukan dalam tahapan implementasi. Disini, *administrator* jaringan mengontrol *server* tersebut dan menentukan sendiri versi *Microsoft Exchange Server* yang akan dijalankan oleh *server* tersebut. Sedangkan dengan menggunakan implementasi secara *online*, *administrator* jaringan mengelola pengaturan tingkat layanan, konfigurasi organisasi, dan konfigurasi penerima saat menggunakan *microsoft* untuk perangkat keras *server* jaringan dan layanan lainnya. *Microsoft* sendiri akan menentukan versi *Microsoft Exchange Server* mana yang akan dijalankan server tersebut. Implementasi *online* selalu menggunakan versi terbaru dari *Microsoft Exchange Server*. *Server* yang berada pada *microsoft* diperbarui secara berkala dengan pembaruan *software* yang berubah atau meningkatkan opsi yang tersedia.

Berikut merupakan layanan-layanan atau fasilitas-fasilitas yang bisa digunakan oleh *mail server* yang dikonfigurasi dengan menggunakan *Microsoft Exchange Server* menurut (Basorudin 2018):

1. *Directory Service*

Layanan ini berfungsi mirip dengan direktori telepon atau buku telepon dimana nomor telepon seseorang dapat dicari dengan mudah. Jadi Ketika pengguna *email* ingin mengirimkan *email* maka *Microsoft Exchange Server* akan menggunakan *Directory Service* untuk mencari alamat yang dituju sehingga *email* dapat disampaikan pada tujuannya dengan baik.

2. *SMTP (Simple Mail Transfer Protocol)*

Simple Mail Transfer Protocol merupakan protokol jaringan yang berfungsi untuk mengatur alur pengiriman *email* melalui jaringan *internet* maupun alur pengiriman *email* melalui jaringan *intranet*.

3. *POP3 (Post Office Protocol)* dan *IMAP (Internet Message Access Protocol)*

Post Office Protocol dan *Internet Message Access Protocol* merupakan protokol jaringan yang berfungsi untuk pengguna *email* mengambil surat elektronik atau *email* dari *mail server* ataupun mengakses *emailnya* melalui *software mail client* seperti *Microsoft Outlook*, *Mozilla Thunderbird* dan *web browser* seperti *Google Chrome* dan *Mozilla Firefox*.

4. *Complementary Services*

Fungsi utama dari *Complementary Services* adalah untuk mendukung *mail server* agar bisa berkerjasama dengan layanan pada *IIS (Internet Information Service)* seperti layanan *NNTP (Network News Transfer Protocol)*, *POP3 (Post Office Protocol Version 3)*, *IMAP4 (Internet Message Access Protocol Version 4)*, *Outlook Web Access*, *Outlook Mobile Access*, *Outlook Anywhere*, *Exchange ActiveSync* dan layanan *IIS* lainnya.

5. *System Attendant*

System Attendant merupakan layanan dari *Microsoft Exchange Server* yang berfungsi untuk mengawasi semua fungsi komponen-komponen lainnya. Komponen tersebut berfungsi untuk menjaga kinerja sistem dalam *Microsoft Exchange Server* dan menjaga agar setiap komponen-komponen dalam *Microsoft Exchange Server* dapat menyelesaikan tugasnya dengan baik.

2.2.3. Postfix

Postfix merupakan sebuah *MTA (Mail Transfer Agent)* yang bersifat secara *opensource*. Fungsi utama dari *postfix* adalah untuk mengirimkan sebuah surat elektronik atau *email* sesuai dengan rutenya. Beberapa sistem operasi *Unix* secara *default* menggunakan *postfix* sebagai *MTA*. Diperkirakan sekitar 25% dari *mail server* di *internet* menggunakan *postfix* sebagai *MTA*nya. Alasan utama yang membuat *postfix* banyak digunakan sebagai *MTA* saat membangun sebuah *mail server* yaitu performanya yang bisa melayani sejuta *email* dalam sehari dan memiliki kompatibilitas yang tinggi. *Postfix* dengan *sendmail* kompatibel sehingga banyak *postfix* dipergunakan. Oleh karena itu maka peneliti menggunakan *postfix* sebagai *MTA* saat pengguna *email* pada *mail server* yang di rancang mengirimkan *email* ke *public(internet)* atau menerima *email* dari *public(internet)* akan melewati *postfix* sebagai *relay*.

Menurut (Manalu dan Simanihুরু 2017) salah satu kelebihan dari *postfix* adalah memiliki kemampuan dalam menahan terjadinya *Buffer Overflow* dan *postfix* juga bisa memproses surat elektronik atau *email* dalam jumlah yang banyak. Dengan begitu apabila ada satu *daemon* yang bermasalah maka yang akan terpengaruh adalah hanya *daemon* tersebut dan tidak akan terimbas ke *daeomon* lainnya didalam sistem *postfix*. Tetapi *postfix* sendiri juga memiliki beberapa kelemahan seperti *email* yang dikirimkan keluar *public(internet)* saat pertama kali bisa membutuhkan proses yang cukup lama dan apabila *server* sedang *down* dengan status tidak ada *backup* bisa terjadi kemungkinan kehilangan *email*.

2.2.4. SMTP & POP3 & IMAP

SMTP atau *Simple Mail Transfer Protocol* merupakan protokol jaringan yang berfungsi untuk mentransmisi atau pengiriman *email*. *SMTP* juga bertugas agar melakukan komunikasi dengan *mail server* untuk mengirimkan *email* dari lokal pengguna kepada *mail server* dan setelah itu dari *mail server* mengirimkan *email* kepada penerimanya. Secara sederhana *SMTP* adalah sebuah mesin yang memiliki tujuan utama untuk mengirim *email* dan menerima *email* antara para pengguna *email*. Menurut (Adiguna 2020) *SMTP* merupakan protokol sederhana yang berbasis *text*, dimana dapat menerima satu atau lebih penerima *email* yang kemudian di verifikasi.

POP3 (Post Office Protocol) merupakan protokol jaringan yang digunakan untuk mengambil data *email* yang disimpan pada *mail server* dan menghapus *email* yang berada pada *mail server* secara otomatis saat *email* tersebut telah di *download* ke perangkat pengguna sehingga pengguna tidak dapat melihat *email* yang telah terbuka sebelumnya diperangkat yang berbeda. Sedangkan *IMAP (Internet Message Access Protocol)* tetap menyimpan data *email* yang disimpan pada *mail server* walaupun telah di *download* ke perangkat pengguna sehingga pengguna bisa melihat emailnya diperangkat mana saja. Menurut (HUSEIN, SUPRIYADI, dan MULYANA 2020) perbedaan antara *POP3* dan *IMAP* adalah protokol *POP3* mewajibkan pengguna *email* untuk mendownload semua *emailnya* tanpa terkecuali sedangkan protokol *IMAP* memungkinkan pengguna untuk memilih dan membaca *email* yang diperlukan saja.

2.2.5.SPF & DKIM & DMARC

SPF Record atau *Sender Policy Framework* merupakan sebuah *record* yang disimpan pada *DNS Hosting* nama *domain* yang berfungsi untuk menentukan dari *server* mana saja yang diperbolehkan dalam mengirimkan *email* menggunakan nama *domain* tersebut. Dengan adanya *SPF* maka hanya *IP Address* yang diperbolehkan mengirimkan *email* dengan menggunakan *domain* sehingga bisa mengatasi terjadinya *email spoofing*. Biasanya saat mengirimkan *email* secara *public(internet)* bisa saja ditolak ataupun masuk sebagai *spam* pada *mail server* lainnya. Salah satu cara untuk mengurangi kemungkinan *email* yang dikirimkan secara *public(internet)* dianggap *spam* atau *spoofing* oleh *mail server* lainnya adalah membuat *SPF Record*.

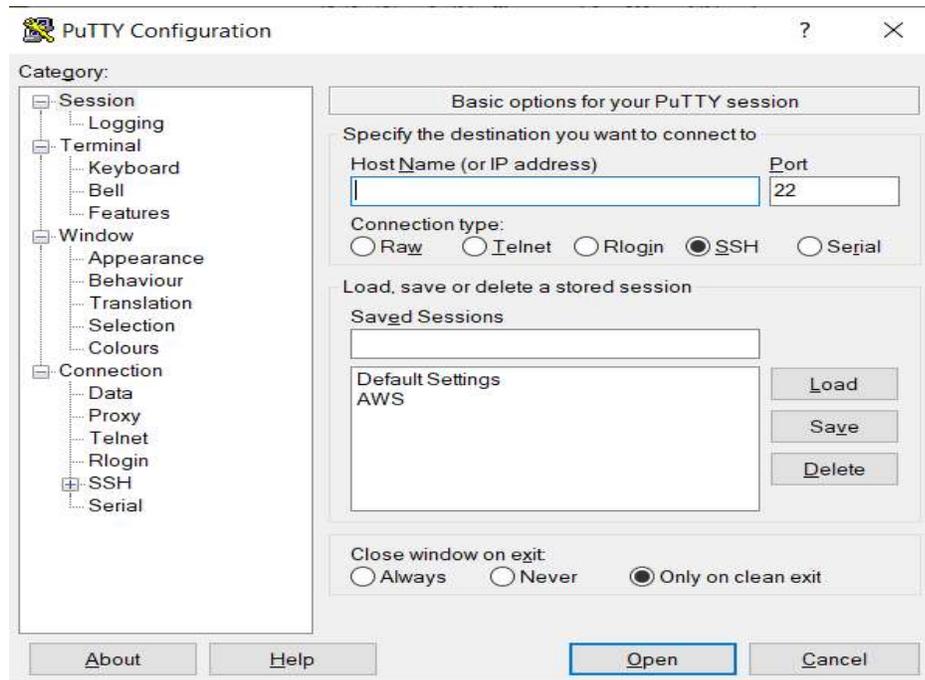
DKIM Record atau *DomainKeys Identified Mail* merupakan sebuah metode autentikasi *email* dengan cara menambahkan kriptografi pada pesan yang didalam *email*. Alasan utama menambahkan kriptografi dalam pesan *email* adalah untuk memastikan *email* yang dikirimkan berasal dari sumber yang asli dan bukan *email spoofing*. Dengan menggunakan *DKIM* maka *mail server* penerima *email* bisa memverifikasi pesan *email* tersebut dengan membandingkan kriptografi yang dipesan *email* dan kriptografi yang berada di *record DNS Hosting*. Cara kerja *DKIM* sangat mirip dengan *SPF* dimana *record* tersebut disimpan pada *DNS Hosting* dan keduanya bertugas untuk menjaga reputasi dari *domain*. *DKIM* juga merupakan salah satu cara untuk mengurangi kemungkinan *email* yang dikirimkan secara *public(internet)* dianggap *spam* atau *spoofing*.

DMARC Record atau *Domain-based Message Authentication, Reporting and Conformance* merupakan sebuah metode yang berfungsi untuk menyediakan arahan dan informasi dari sebuah *email* apabila *email* tersebut tidak terautentikasi. *DMARC* juga berguna untuk mengurangi kemungkinan *email* yang dikirimkan secara *public(internet)* dianggap sebagai *email spam* ataupun *email spoofing* sehingga bisa menaikkan reputasi *domain* serta bisa digunakan secara bersamaan dengan *SPF* dan *DKIM*. Dengan *DMARC*, *mail server* dapat memerintahkan apa yang harus dilakukan oleh *mail server* lain apabila menerima *email spoofing* atau *email* palsu dari *domainnya* seperti menolak *email* tersebut, memasukkan *email* tersebut kedalam folder *spam* ataupun memperbolehkan *email* tersebut dengan menambahkan parameter-parameter *DMARC* (*none, quarantine, reject*) kedalam *record* yang tersimpan dalam *DNS Hosting*.

Menurut (Gori Mohamed dan Visumathi 2020) *email spoofing* merupakan serangan yang sering terjadi terhadap *staff* di perusahaan yang berbeda, menurut *Anti Phishing Working Grup (APWG)*, sayangnya tidak ada mekanisme untuk mencegah *spoofing* dalam protokol transmisi *email* saat ini. Sehingga penyedia *email* bertanggung jawab untuk menerapkan autentikasi pengirim *email* menggunakan *SPF, DKIM* dan *DMARC*. Perlindungan yang terbatas pada *server* bisa menempatkan pengguna dalam posisi yang rentan terhadap serangan karena tidak semua pengirim *email* memiliki *SPF, DKIM, DMARC* pada *domainnya* sehingga sangat penting bagi penyedia *email* untuk mengautentikasi semua *email* masuk dan bagaimana penyedia *email* akan memperlakukan *email* yang tidak terautentikasi, apakah akan di *reject, accept* atau *quarantine*.

2.3. Tools/Software/Aplikasi/System

2.3.1. PuTTY



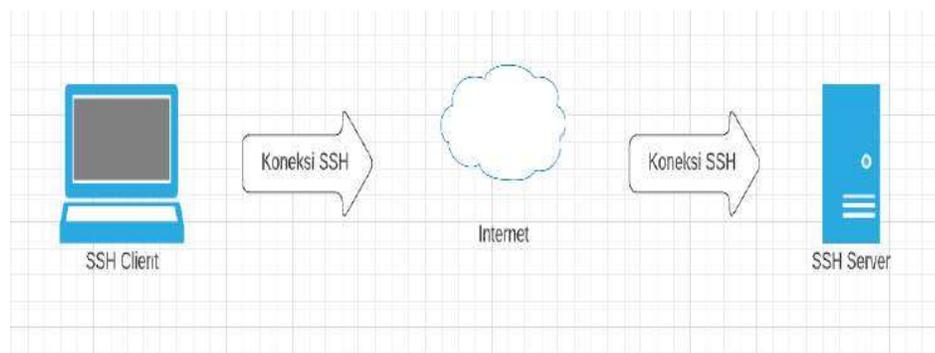
Gambar 2.1 PuTTY

Sumber : Data Olahan Peneliti (2021)

PuTTY merupakan aplikasi *opensource* yang biasanya digunakan untuk melakukan *remote access* seperti *telnet*, *RLogin* dan *SSH*. Aplikasi atau *tools* ini dapat digunakan untuk mengendalikan *server* dari jarak jauh atau ditempat yang berbeda sehingga tidak perlu datang ke lokasi *server* untuk melakukan konfigurasi-konfigurasi *server*. Ada dua cara untuk menggunakan PuTTY agar melakukan koneksi ke *server SSH*. Cara pertama adalah menggunakan *Basic*

Options, yang diperlukan oleh cara ini adalah memasukkan *IP Server SSH*, *Port Server SSH*, *Username* dan *Password Server SSH*. Cara kedua adalah dengan menggunakan *public key*, cara ini hanya membutuhkan satu kali memasukkan *username* dan *password server SSH* sehingga untuk mengakses *server* selanjutnya cukup memasukkan *IP Server SSH*, *Port Server SSH* serta *private key* dari *server SSH* tersebut. Menurut (WIDIARTA, Esabella, dan Widiantera 2020) untuk melakukan konfigurasi jaringan kedalam *cloud server* yang menggunakan layanan *SSH* maka *tools* yang dapat digunakan adalah *PuTTY*.

2.3.2.SSH Server



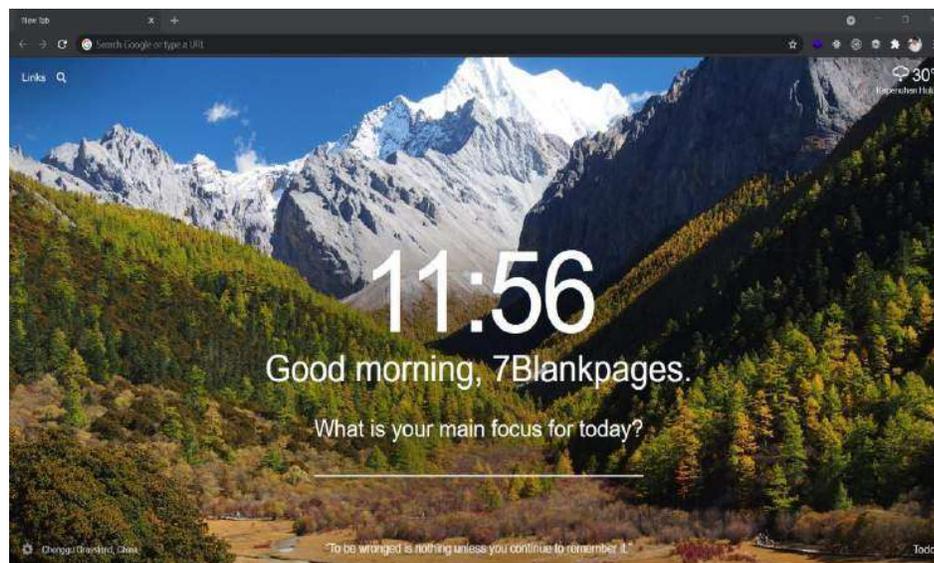
Gambar 2.2 Topologi SSH

Sumber : Data Olahan Peneliti (2021)

SSH atau *Secure Shell Protocol* merupakan sebuah protokol jaringan yang memungkinkan pengguna untuk mengakses pengaturan maupun file yang ada di dalam sebuah *server*. *SSH* atau *Secure Shell Protocol* merupakan pengembangan dari *telnet* yang dianggap tidak aman untuk digunakan karena tidak mempunyai

proses enkripsi. Fungsi utama *SSH* adalah untuk memudahkan pengguna dalam mengelola *server* tanpa harus datang ke lokasi fisik *server* sehingga mengontrol sebuah *server* dari jarak yang jauh bukanlah hal yang mustahil. Koneksi *SSH* dapat tersambung hanya dengan menggunakan kunci yang sama melalui proses verifikasi. Menurut (Ariyanto, Ismail, dan Grananta 2020) untuk mengatasi masalah efisiensi waktu dan efisiensi maka dibutuhkan *tools* untuk *system administrator* yang menggunakan protokol *SSH* karena protokol *remote* tersebut sudah aman dan masih dikembangkan serta sering digunakan sebagai *remote server* linux dan juga menggunakan metode *TELOS* (*Technical, Economic, Law, Operational, Schedule*).

2.3.3. Web Browser

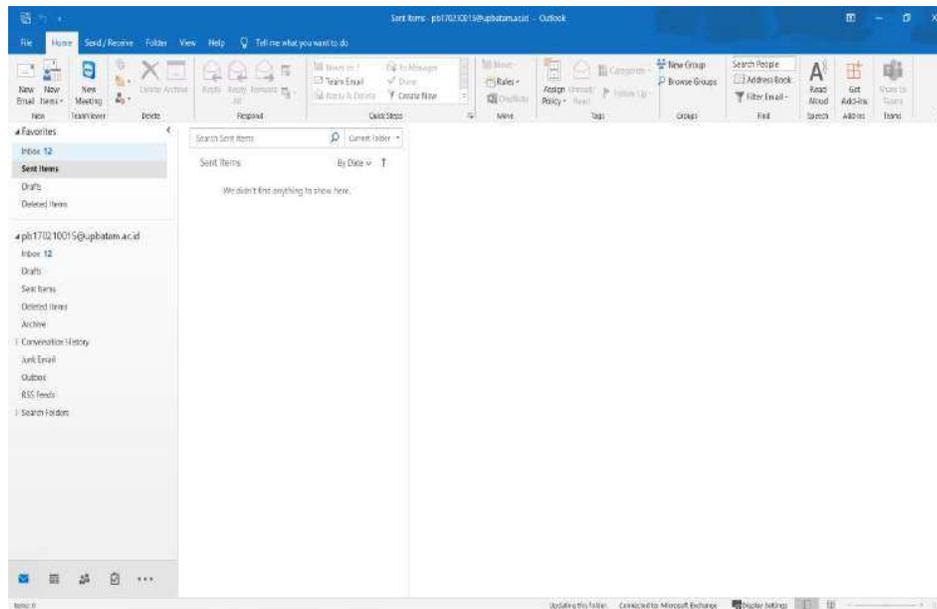


Gambar 2.3 Web Browser (Google Chrome)

Sumber : Data Olahan Peneliti (2021)

Web Browser berperan sangat penting untuk mempermudah penggunaannya untuk mendapatkan informasi. Dengan menggunakan *web browser*, pengguna bisa mencari apa saja informasi dan data yang diperlukan. Terdapat juga beberapa *Web Browser* yang sering digunakan seperti *Google Chrome*, *Mozilla Firefox*, *UC Browser*, *Microsoft Edge* dan masih banyak *web browser* lainnya. Menurut (Sidiq dan Faiz 2019) pengguna *web browser Google Chrome* paling banyak sampai 73,43% dari jumlah pengguna *web browser* di Asia. Pada posisi selanjutnya ada *Mozilla Firefox* dengan 8,87%, *Internet Explorer* 5,95%.

2.3.4. Software Mail Client

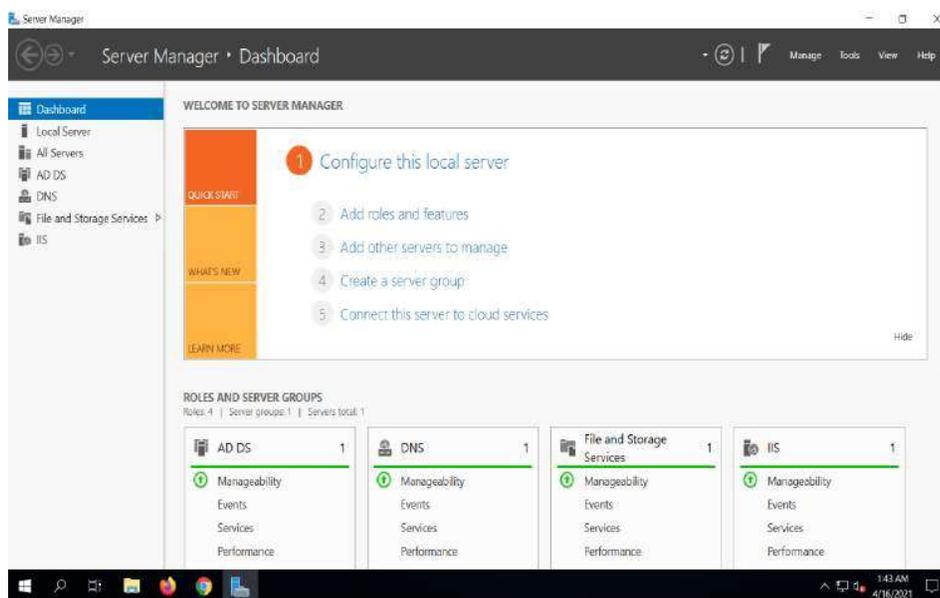


Gambar 2.4 Software Mail Client (Microsoft Outlook)

Sumber : Data Olahan Peneliti (2021)

Microsoft Outlook merupakan aplikasi yang digunakan untuk mengelola *email* atau lebih dikenal sebagai *software mail client* dari *Microsoft Corporation*. Cakupan aplikasi yang ada di *Microsoft Office* adalah *Microsoft Word*, *Microsoft Excel*, *Microsoft Outlook*, *Microsoft Power Point*, *Microsoft Access* dan lainnya (Ujiandari, Diana, dan Gata 2020). *Microsoft Outlook* juga memiliki fitur seperti pengelolaan kalender, catatan, dan buku harian apabila dikombinasikan dengan *Microsoft Exchange Server*. Terdapat juga *software mail client* lainnya yang sering digunakan selain *Microsoft Outlook* yaitu *Mozilla Thunderbird*, *Windows Mail*, *Apple Mail*, *Spark*, *Mailbird* dan lainnya.

2.3.5. Windows Server 2019



Gambar 2.5 *Windows Server 2019*

Sumber : Data Olahan Peneliti (2021)

Teknologi informasi pada saat ini telah berkembang dengan pesat dan telah terbukti menjadi sarana komunikasi dan sumber informasi yang sangat handal. Seiring dengan perkembangan teknologi yang semakin canggih dan cepat dapat dilihat implementasinya pada jaringan komputer khususnya tentang *client-server* misalnya saja penggunaan dari *Windows Server* (Maha Putra, Syafnur, dan Yesputra 2018). *Windows Server* merupakan sebuah sistem operasi dari *Microsoft Corporation* yang bisa berperan sebagai *server* atau *data center* untuk menyediakan layanan jaringan komputer seperti *Network Virtualization*, *Network Storage*, *Networking*, *Website Hosting*, *User Management* dan lainnya. *Windows Server* juga memberikan fitur untuk pengguna dalam mengakses dan manajemen *server* melalui GUI (*Graphical User Interface*) maupun mengakses dan manajemen *server* melalui CLI (*Command Line Interface*). Kekurangan pada *Windows Server* ini adalah *server* yang menggunakan *Windows Server* sebagai sistem operasinya membutuhkan spesifikasi *Hardware* yang lumayan tinggi sehingga ada bagusnya menginstall *windows server* tanpa penginstallan GUI agar menghemat *resource server*. Fungsi utama *Windows Server* adalah mengelola dan mengatur konfigurasi server dari perangkat yang terhubung dengan *server* dalam suatu jaringan komputer atau lebih di kenal sebagai jaringan *client-server* dan berperan sebagai *server* atau pusat dalam pengelolaan sebuah jaringan komputer sehingga sistem yang berada didalam suatu jaringan dapat berjalan dengan baik. Berikut merupakan spesifikasi minimum dan rekomendasi untuk *server* yang menggunakan sistem operasi *Windows Server 2019*:

Tabel 2.1 Minimum/Rekomendasi Spesifikasi *Windows Server 2019*

	Minimum Requirement	Recommend Requirement
Processor	1.4 GHz (64-bit processor)	3.1 GHz (64-bit processor)
RAM	2 GB	16 GB
Storage	160 GB	No Limit

Sumber : Data olahan peneliti (2021)

2.3.6. Ubuntu Server 18.10

```

ubuntu@ip-172-31-2-58: ~
login as: ubuntu
Authenticating with public key "imported-openssh-key"
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-1039-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

System information as of Thu Apr 15 18:48:14 UTC 2021

System load: 0.0          Processes: 113
Usage of /:  8.5% of 29.02GB   Users logged in: 0
Memory usage: 29%          IPvd address for eth0: 172.31.2.58
Swap usage:  0%             IPvd address for tun0: 10.8.0.1

 * Introducing self-healing high availability clusters in MicroK8s.
   Simple, hardened, Kubernetes for production, from RaspberryPi to DC.
   https://microk8s.io/high-availability

BI updates can be installed immediately.
0 of these updates are security updates.
To see these additional updates run: apt list --upgradable

*** System restart required ***
Last login: Sun Mar 21 20:17:47 2021 from 18.224.14.67
ubuntu@ip-172-31-2-58:~$

```

Gambar 2.6 *Ubuntu Server 18.10*

Sumber : Data Olahan Peneliti (2021)

Ubuntu merupakan sebuah sistem operasi *opensource* dan salah satu distribusi *linux* yang berbasis *debian*. Sedangkan *Ubuntu Server* merupakan *ubuntu* yang dikembangkan khusus untuk dijadikan sebagai sistem operasi *server*, sehingga tentu mempunyai perbedaan antara *Ubuntu* dan *Ubuntu Server*. *Ubuntu*

sendiri menyediakan *GUI (Graphical User Interface)* sedangkan *Ubuntu Server* tidak menyediakan *GUI* sehingga pada *ubuntu server* semua eksekusi program dijalankan melalui baris perintah yang lebih dikenal dengan *CLI (Command Line Interface)*. Saat ini sistem operasi *Ubuntu* sudah banyak digunakan, baik itu *Ubuntu Desktop* maupun *Ubuntu Server*. Alasan utama sistem operasi ini banyak digunakan adalah karena sistem operasi ini gratis dan *opensource*, sehingga tidak membutuhkan pembelian lisensi untuk *download*, *install* serta menggunakannya. Sistem operasi ini juga sangat aman untuk digunakan, karena sistem operasi *ubuntu* memiliki *built-in firewall* dan *virus protection* yang sangat kuat. *Ubuntu* juga merupakan salah satu opsi terbaik untuk menjalankan komputer yang sudah tua atau berspesifikasi rendah dikarenakan sistem operasi ini tidak menggunakan terlalu banyak *resource*. Menurut (Iqbal dan Prasetyo 2019) *Linux Ubuntu 18.10* memiliki fitur yang *Gnome 3.30* yang menggunakan sedikit *resource* sehingga pengguna dapat menjalankan lebih banyak aplikasi sekaligus tanpa menghadapi masalah kinerja. Berikut merupakan spesifikasi minimum dan spesifikasi rekomendasi untuk *Ubuntu Server 18.10*.

Tabel 2.2 Minimum/Rekomendasi Spesifikasi *Ubuntu Server 18.10*

	Minimum Requirement	Recommend Requirement
Processor	1.0 GHz Dual Core Processor	2 GHz Dual Core Processor
RAM	1 GB	4 GB
Storage	20 GB	No Limit

Sumber : Data olahan peneliti (2021)

2.4. Penelitian Terdahulu

Penelitian terdahulu merupakan penelitian yang sudah pernah dilakukan oleh peneliti lain sebelumnya dan menjadi bahan perbandingan serta menjadi bahan referensi oleh peneliti. Berikut beberapa penelitian terdahulu yang berkaitan dengan penelitian yang sedang dijalankan peneliti:

1. **Membangun *Mail Server* Berbasis *Linux* Menggunakan *Postfix* Dengan *Client Squirrel Mail*.**

Berdasarkan penelitian (Manalu dan Simanihuruk 2017) e-ISSN 2686-5319 p-ISSN 2686-6455. Kesimpulan yang dapat ditarik dari hasil penelitian tersebut adalah dengan adanya *mail server* pribadi, proses pengiriman *email* tidak lagi hanya dapat menggunakan jaringan *internet*, tapi sudah bisa dilakukan secara *local*. *Postfix* sendiri merupakan salah satu *email service* atau layanan *email* yang dapat digunakan untuk berkomunikasi dengan memanfaatkan jaringan komputer. Pengguna menjadi lebih mudah untuk berkomunikasi serta tidak memerlukan pengeluaran biaya besar untuk pengiriman *email* antara pengguna dengan pengguna lainnya. Sehingga dapat memberikan manfaat jika *mail server* ini diterapkan pada lingkungan yang memiliki keterbatasan akses *internet*. Dengan membangun *mail server*, maka *virus* yang berasal dari *flashdisk* sudah bisa diminimalisir dikarenakan pengiriman data atau komunikasi data dapat dilakukan melalui *email* antar pengguna yang terhubung pada jaringan tersebut sehingga tidak memerlukan *flashdisk* untuk melakukan pertukaran data.

2. Implementasi Pengamanan *PGP* pada *Platform Zimbra Mail Server*.

Berdasarkan penelitian (Pramana Hostiadi dan Suradarma 2017) e-ISSN 2541-5832 p-ISSN 2088-1541. Kesimpulan yang dapat ditarik dari hasil penelitian tersebut adalah pengamanan *mail server* dengan penggunaan teknik *PGP* (*Pretty Good Privacy*) dapat mengamankan komunikasi melalui *email*. Pihak yang tidak berwenang bisa saja mencuri ataupun mengakses akun *email* pengguna, namun tetap saja isi dari *email* tidak dapat terbaca dikarenakan telah dienkripsi. Hasil penelitian juga menunjukkan terdapat perbedaan dari ukuran *file attachment* penggunaan pengamanan *PGP*, ukuran *file* menjadi lebih besar dikarenakan terjadinya enkripsi *email* dengan menggunakan *private key*.

3. *Manipulating E-Mail Server Feedback For SPAM Prevention*.

Berdasarkan penelitian (Okunade 2017) e-ISSN 2545-5818 p-ISSN 1596-2490. Kesimpulan yang dapat ditarik dari hasil penelitian tersebut adalah dalam mengurangi *spam email*, penting untuk mengetahui hal yang bisa membuat *botnet spammer* bisa berkerja. Hal pertama yang harus diketahui adalah jumlah *bot* yang digunakan oleh pelaku *spam*. Terlalu banyak *bot* yang terhubung ke *server* bisa membuat *bandwidth server* menjadi buruk sehingga *mail server* akan berjalan dengan buruk juga. Lokasi fisik *bot* tidak mempengaruhi kinerja *spam*. Pengirim *spam* biasanya membeli *bot* yang berlokasi di negara berkembang karena harganya lebih murah. Feedback ini akan mengecek apakah alamat *email* tersebut ada atau tidak sehingga bisa mendeteksi pengirim yang berstatus sebagai *bot*.

4. Rancang Bangun *Mail Server* Berbasis *Squirrel Mail* Menggunakan *MTA (Mail Transfer Agent)* Pada PT. Teras Inti Media.

Berdasarkan penelitian (Desmira, Sumarto, dan Yuliani 2017) ISSN 2406-7733. Kesimpulan yang dapat ditarik dari hasil penelitian tersebut adalah dengan pengimplementasian *mail server* dengan *domain* pribadi (*majalahteras.co.id*) dapat meningkatkan komunikasi data secara *internal* dan *local* dalam PT. Teras Inti Media. *Mail server* yang berjalan merupakan *mail server* yang berjalan secara *virtual* dengan menggunakan aplikasi virtualisasi jaringan yaitu *Virtual Box*. Setelah pengimplementasian *mail server*, maka perlu diperhatikan keamanan *mail server* terlebih dibagian *spamming*, *virus* serta *junk mail* yang berkemungkinan terjadinya kerusakan data yang dikirim maupun data yang diterima.

5. Implementasi *Mail Server* Berbasis *Squirrel Mail* Dengan *Exchange Server* Menggunakan Teknologi Virtualisasi di SMK Negeri 1 Pendalian IV Koto.

Berdasarkan penelitian (Basorudin 2018) ISSN 1858-2680. Kesimpulan yang dapat ditarik dari hasil penelitian tersebut adalah dengan implementasi *mail server* di SMKN 1 Pendalian maka semua konfigurasi *email* bisa dikelola oleh *administrator* tanpa harus melakukan *remote* ke layanan *hosting*. *Mail server* tersebut dibangun dengan menggunakan sistem operasi Debian 5 dengan konfigurasi *DNS Server*, *Web Server*, *Mail Server* serta *Squirrelmail* sebagai *webmail* agar pengguna bisa mengelola *emailnya* melalui *web browser*.

6. *An Analysis Of Spam Email Detection Performance Assessment Using Machine Learning.*

Berdasarkan penelitian (Santoso 2019) e-ISSN 2527-9165 p-ISSN 2527-1682. Kesimpulan yang dapat ditarik dari hasil penelitian tersebut adalah pendeteksian *spam email* sebenarnya sudah ada diterapkan pada layanan *email* secara umum dengan menggunakan berbagai metode. Dengan penggunaan *Machine Learning* menggunakan *metode forest* mampu mendeteksi *spam email* dengan kecepatan proses hingga 0,19 detik dan tingkat akurasi sekitar 98%. (Santoso 2019) berharap agar peneliti yang selanjutnya bisa menggunakan metode yang lebih kompleks seperti *metode ensemble* dan proses *dataset* lebih banyak diterapkan sehingga bisa memberikan kinerja yang lebih baik lagi.

7. *Membangun Mail Server Berbasis Linux Menggunakan Postfix Admin Di PT. Kemuning Televisi.*

Berdasarkan penelitian (Rismayadi, Topiq, dan Nurtantho 2020) e-ISSN 2685-6964. Kesimpulan yang dapat ditarik dari hasil penelitian tersebut adalah dengan dibangunnya *mail server* pada sistem operasi *linux* menggunakan *postfix admin* bisa mempermudah *administrator mail server* tersebut dalam mengelola akun *email* yang berada di *mail server*. Penggunaan *SPF (sender policy framework)*, *DKIM (domain keys identified mail)*, *clamav* dan *spamassassin* bisa membuat *mail server* lebih aman dari serangan *virus* dan *spamming* dari pihak-pihak yang tidak bertanggung jawab.

8. Membangun *Server Mail* Menggunakan *Postfix* Pada *Kubuntu 16.04*.

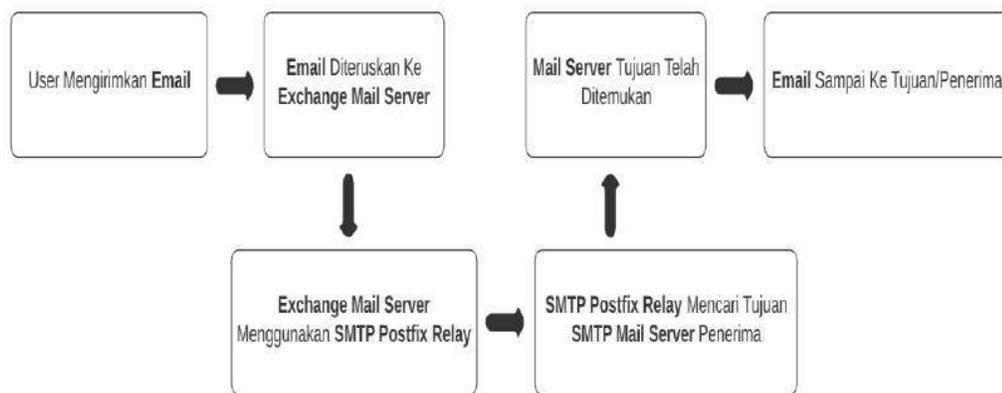
Berdasarkan penelitian (HUSEIN dkk. 2020) e-ISSN 2581-1711 p-ISSN 2541-1179. Kesimpulan yang dapat ditarik dari hasil penelitian tersebut adalah perancangan dan implementasi *mail server* pada jaringan lokal bisa dibangun dengan metode *SDLC (System Development Life Cycle) Spiral* menggunakan dua kali *plan iteration* dan dua kali *construct prototype*. *Mail server* yang bersifat *opensource* seperti *Postfix* juga bisa berjalan dengan normal dan stabil. Untuk perancangan dan implementasi *mail server* pada penelitian ini masih bersifat secara lokal, tetapi juga dapat dikembangkan menjadi *online* sehingga pengguna bisa mengelola atau mengakses *email* mereka melalui jaringan publik.

9. Analisa Dan Implementasi *Security Mail Server*.

Berdasarkan penelitian (Mukhtar dkk. 2020) ISSN 2089-3353. Kesimpulan yang dapat ditarik dari hasil penelitian tersebut adalah perancangan keamanan dalam *mail server* sangat penting dikarenakan dapat mencegah masuknya *email spam* yang dapat membuat performa *mail server* menjadi lebih lambat. Nilai *Antispam* dan *Antivirus* yang dibuat rendah ataupun dinonaktifkan bisa menjadi penyebab masuknya *Email Spam* kedalam *mail server*. Melalui peningkatan *Spam Scoring* dengan menurunkan *Kill* sebanyak 50%, *Tag* sebanyak 10% dan dengan mengaktifkan fungsionalitas *Antispam* maka *mail server* dapat mencegah masuknya *Email Spam*. Pengukuran *score hits* dapat ditentukan apakah sebuah *email* mengandung unsur *spam* atau tidak.

2.5. Kerangka Pemikiran

Kerangka pemikiran merupakan sebuah uraian dari permasalahan yang telah diidentifikasi atau dirumuskan berdasarkan fakta-fakta dan penelitian yang ada. Dari teori-teori yang telah dibahas diatas, peneliti dapat menggambarkan sebuah kerangka pemikiran untuk penelitian ini seperti berikut:



Gambar 2.7 Kerangka Pemikiran

Sumber : Data Olahan Peneliti (2021)