BAB II
KERANGKA TEORITIS

A. TINJAUAN PUSTAKA

Penelitian ini dilakukan berdasarkan adanya penelitian rujukan yaitu penelitian sebelumnya yang memanfaatkan teknologi *Virtual Private Network (VPN)* pada teknologi pengembangan jaringan komputer. Pada beberapa penelitian sebelumnya telah dilakukan pemanfaatan teknologi *VPN* didalam lingkungan sekitar, baik itu lingkungan kantor, kampus dan organisasi lainnya. Penelitian sebelumnya menunjukan bahwa teknologi *VPN* ini memiliki banyak manfaat maupun fungsi, dengan adanya komunikasi jarak jauh dan kecepatan yang baik, maka pekerjaan manusia dapat dilakukan dengan cepat dan produktif.

1. ANALISA *VIRTUAL PRIVATE NETWORK* MENGGUNAKAN *OPENVPN* DAN *POINT TO POINT TUNNELING PROTOCOL* (Prihatin Oktivasari & Andri Budhi Utomo, November 2016)

Pesatnya perkembangan teknologi memberikan fasilitas terhadap kita dalam segala hal, termasuk hal yang berkaitan dengan pekerjaan yang biasa dilakukan manusia. Perkembangan teknologi dalam bidang komputer membuat manusia menyadari akan pentingnya kebutuhan fasilitas yang disediakan oleh teknologi tersebut, khususnya dalam bidang pekerjaan. Dengan kemajuan zaman tersebut, membuat suatu instansi, baik pemerintah maupun swasta harus dapat melakukan proses pengolahan sistem informasi yang cepat, tepat dan akurat. Sebuah instansi harus dapat memanfaatkan kemajuan teknologi dalam bidang komputer dan jaringan untuk dapat menghemat tenaga, waktu, biaya dan lain-lain.

Untuk dapat mewujudkan hal tersebut, maka dukungan dari sisi infrastruktur jaringan pada sistem informasi dari instansi yang terkait, sangat diperlukan. Dengan memanfaatkan penggunaan jaringan *internet*, dapat membantu dalam mengatasi batasan jarak dan waktu. Kini seseorang dapat dengan mudah mengambil data atau mengolah data yang tersimpan di dalam jaringan lain, contohnya jaringan di dalam sebuah instansi seperti perusahaan baik negeri atau swasta juga dalam sebuah instansi yang bergerak dalam dunia pendidikan seperti sekolah dan perguruan tinggi, dari mana saja dan kapan saja. Hal tersebut dapat dilakukan jika jaringan tersebut terkoneksi dengan *internet*.

Cara atau sistem yang dapat digunakan untuk melakukan hal tersebut adalah menggunakan *Virtual Private Network (VPN)*. Dengan *VPN* sebuah

instansi dapat memperluas akses secara aman terhadap jaringan internalnya melalui jaringan internet dengan biaya yang relatif murah. Seluruh aplikasi dan data yang penting pada jaringan tersebut, dapat diakses oleh pihak tertentu saja yang diberikan wewenang tanpa memperhatikan jarak dan tempat dimana diaksesnya. Oleh karena itu dalam penelitian ini akan diimplementasikan dan dianalisis sistem *Virtual Private Network* antara *OpenVPN* dan *PPTP*, dengan pengujian performa yaitu *packetloss, roundtrip* dan *winSCP transfer*, sedangkan untuk keamanan adalah pengujian *denial of service dan sniffing.*

Teknologi *tunneling* merupakan teknologi yang bertugas untuk manangani dan menyediakan koneksi *point-to-point* dari sumber ke tujuannya. Disebut *tunnel* (terowongan) karena koneksi *point-to-point* tersebut sebenarnya terbentuk dengan melintasi jaringan umum, namun koneksi tersebut tidak mempedulikan paket-paket data milik orang lain yang sama-sama melintasi jaringan umum tersebut, tetapi koneksi tersebut hanya melayani transportasi data dari pembuatnya. Hal ini sama dengan penggunaan jalur *busway* yang pada dasarnya menggunakan jalan raya, tetapi jalur sendiri untuk dapat dilalui bus khusus. Koneksi *point-to-point* ini sesungguhnya tidak benar-benar ada, namun data yang dihantarkannya terlihat seperti benar-benar melewati koneksi pribadi yang bersifat *point-to-point*.

Pada jurnal ini menganalisa teknologi *VPN PPTP* dan *OpenVPN*, kedua teknologi tersebut dapat berjalan dengan baik untuk memenuhi kebutuhan menghubungkan jaringan komputer. Dari segi kemudahan konfigurasi *PPTP* lebih mudah dalam pengerjaannya namun, dalam segi keamaan *OpenVPN* lebih baik dibanding dengan *PPTP*.

2. IMPLEMENTASI JARINGAN *VIRTUAL PRIVATE NETWORK (VPN)* MENGGUNAKAN PROTOKOL *EOIP* (Herman Kuswanto, Januari 2017)

Makin meningkatnya penggunaan *internet* di kalangan perusahaan sebagai pendukung segala kinerja dan aktifitas dari perusahaan, menjadikan jaringan *internet* sebagai alat komunikasi yang tak lagi terbataskan oleh ruang dan waktu, perusahan banyak memanfatkan *internet* sebagai media penghubung di antara kantor cabang perusahanya dengan memanfatkan fasilitas aplikasi berbasis *web*, dengan aplikasi tersebut akan lebih memudahkan perusahan dalam menyampaikan informasi.

Internet sebagai suatu mediasi komunikasi selain sangat bermanfaat namun tetap memiliki kelemahan dalam keamananya tidak semua aplikasi dapat di lewatkan melalui jalur *internet*, terlebih untuk *transmisi* data yang penting. Maka dalam pemanfaatnya sebagai media *transmisi* perlu di lakukan peningkatan keamananya. Untuk mengatasi masalah tersebut salah satunya dengan membangun sebuah jaringan *Virtual Private Network (VPN)* pada jaringan publik atau *internet*. *VPN* memberikan suatu jalur komunikasi melalui jaringan publik dengan melakukan proses *tunneling* dimana jaringan yang terbentuk hanya bisa diakses oleh jaringan yang mempunyai *tunnel* yang sama, sehingga semua data yang di*transmisi* lebih terjaga kerahasianya.

Ethernet Over Internet Protocol (EoIP) merupakan protokol *proprietary Mikrotik (Mikrotik)*, salah satu fitur yang ada pada *Mikrotik RouterOs* untuk membentuk suatu model *VPN*, dengan memanfaatkan fitur *EoIP* dapat dibentuk suatu jalur *VPN* yang disebut dengan *tunnel* yang dapat di lewatkan pada jaringan publik atau *internet*, dengan memanfatkan *EoiP* biaya yang dikeluarkan lebih murah dibanding dengan sewa *VPN-IP* yang relatife lebih mahal.

Ethernet over internet protokol tunnel (EoIP) merupakan protokol pada *Mikrotik RouterOs* yang berfungsi membangun sebuah *Network Tunnel* antar *mikrotik Router* di atas sebuah koneksi *TCP/IP* (Riyadi dan Chris). Hal yang perlu diketahui mengenai *EoIP*

a. *Eoip* bisa berjalan di berbagai macam jenis koneksi yang mendukung *IP*
b. Maksimal jumlah *tunnel* yang bisa di buat oleh *Eoip* adalah 65535 *tunnel.*
c. *Interface EoIP* dapat melakukan *Bridging* dengan *interface EoIP* yang lain.
d. Fungsi utama dari *EoIP* adalah secara transparan dapat melakukan *Bridge* ke *network remote*.
e. Kelemahan dari *EoIP* adalah tidak adanya *enkripsi* data.

Pada jurnal penelitian ini menjelaskan cara implementasi membangun jaringan *Virtual Private Network (VPN)* menggunakan metode *Eoip* untuk menghubungkan 2 jaringan komputer atau lebih. Metode ini berjalan dengan baik untuk menerapkan *VPN* namun tidak ada tambahan *security* pada proses *pairing* jaringan komputer.

3. **IMPLEMENTASI *VIRTUAL PRIVATE NETWORK (VPN)* DENGAN *OTENTIKASI RADIUS SERVER* PADA PT. ANUGERAH TUNGGAL MANDIRI JAKARTA** (Rosmana & Fitri Latifah, Maret 2015)

Seiring dengan maraknya penggunaan *internet*, banyak perusahaan yang kemudian beralih menggunakan *internet* sebagai bagian dari jaringan mereka untuk menghemat biaya. Akan tetapi permasalahan keamanan masih menjadi faktor utama dalam *reliabilitas* suatu jaringan. *Virtual Private Network* (*VPN*) merupakan salah satu cara yang dapat digunakan untuk membuat jaringan yang bersifat *private* dan koneksi jarak jauh (*remote access*) dengan tingkat keamanan yang tinggi diatas jaringan publik atau *internet*.

Teknologi *VPN* sendiri sebenarnya dapat didukung oleh beberapa protokol keamanan, salah satunya adalah *Remote Authentication Dial-In User Service (RADIUS). RADIUS server* digunakan dalam implementasi *remote access VPN* karena pada *RADIUS* terdapat fungsi *authentication, authorization*, dan *accounting (AAA)*. Pada proses *authentication* menawarkan proses otentikasi *user*, *authorization* menawarkan *access-control* untuk *user* dan *accounting* digunakan untuk melacak konsumsi *network-resource* yang dilakukan oleh *user*. Dengan adanya proses mekanisme tersebut dapat meningkatkan sistem keamanan jaringan.

Dalam merancang dan mengimplementasikan *VPN* pada sebuah jaringan nirkabel Universitas Putra Indonesia menunjukan bahwa dengan gagasan awal seluruh dosen, karyawan dan mahasiswa dapat dengan mudah memperoleh data ataupun informasi dari internet dengan tetap memastikan bahwa kerahasiaan dari data yang sensitif dapat terjaga pada saat terkoneksi. Sehingga dibangun sebuah sistem baru dengan mempertimbahkan beberapa aspek keamanan dan hak akses. Sistem tersebut yaitu *Virtual Private Network (VPN)* yang memberikan fungsi dalam menjaga kerahasian data (*Confidentiality*), keutuhan data (*Data Integrity*) serta otentikasi sumber (*Origin Authentication*).

Pada jurnal penelitian ini membahas teknologi dengan otentikasi *radius*. Seperti yang sudah dibahas oleh jurnal diatas bahwa, radius memiliki fungsi *authentication, authorization*, dan *accounting (AAA)* sehingga dari segi keamanan sudah ada namun teknologi yang digunakan masih terbilang lemah. Otentikasi dari perangkat keras yang digunakan oleh pengguna itu dibutuhkan untuk kemanan yang lebih baik.

4. **ANALISIS PERFORMANSI *REMOTE ACCESS VPN* BERBASIS *IPSEC* DAN BERBASIS *SSL* PADA JARINGAN *IPv6*** (Alex Yuasta, Fazmah Arif Yulianto, S.T., M.T., Gandeva Bayu Satrya, S.T., M.T., Desember 2014)

Virtual Private Network (VPN) merupakan suatu teknologi membangun jaringan *private* dalam jaringan publik. Teknologi tersebut mampu meningkatkan keamanan komunikasi pada jaringan publik, karena komunikasi tersebut seolah-olah berada pada sebuah jaringan *private*. Karena keunggulan tersebut, *VPN* telah banyak diimplementasikan pada jaringan *internet. Internet* saat ini masih menggunakan standar pengalamatan *Internet Protocol version 4 (IPv4)*. Standar pengalamatan *IPv4* akan digantikan dengan standar pengalamatan *Internet Protocol version 6 (IPv6).* Hal ini mengharuskan *VPN* yang merupakan suatu solusi keamanan pada jaringan *IPv4* agar tetap bisa mengerjakan fungsinya pada jaringan *IPv6*.

Proses penggantian sistem pengalamatan ini tidak berlangsung serentak. Beberapa jaringan sudah mulai menggunakan standar pengalamatan *IPv6*, biasanya jaringan berstatus *Local Area Network (LAN)* . Salah satu penyebab beberapa jaringan masih menggunakan standar pengalamatan *IPv4* seperti *internet* dikarenakan keterbatasan perangkat keras. Dimana perangkat keras yang digunakan sekarang masih banyak yang belum mendukung jaringan yang menggunakan sistem pengalamatan *IPv6*.

Standar pengalamatan *IPv6* memiliki beberapa perbedaan dengan standar *IPv4*, misalnya pada panjangnya *header* dan *payload*. Perbedaan-perbedaan tersebut diperkirakan akan memberikan perbedaan kinerja antara *VPN* pada jaringan *IPv4* dengan *VPN* pada jaringan *IPv6*.

Saat ini banyak kantor yang menerapkan metode *work-at-home* yaitu mengerjakan pekerjaan kantoran di rumah. Pegawai kantor yang bekerja di rumah tetap harus terhubung dengan jaringan internal kantor. Sehingga dibutuhkan sebuah *VPN* berjenis *remote access* agar pegawai tersebut bisa terhubung ke jaringan internal kantor melalui *Internet*.

Ada beberapa jenis protokol yang biasa digunakan pada *VPN* seperti *Internet Protocol Security (IPSec), Secure Socket Layer (SSL), Point to Point Tunnelling (PPTP)*, dan *Layer 2 Tunneling Protocol (L2TP)*. Namun dilihat dari segi dukungan keamanan protokol *IPSec* dan *SSL* merupakan protokol yang paling banyak digunakan.

Karena telah mampu memenuhi kriteria dukungan keamanan, maka akan digunakan kriteria *Quality of service (QoS)* dalam menentukan mana

protokol keamanan yang lebih baik. Dimana dalam menganalisa *QoS*, akan digunakan parameter *throughput* dan *delay*.

Pada Jurnal penelitian ini menjelaskan tentang teknologi *VPN Ipsec* dengan metode keamanan *ssl*. Teknologi dan metode ini memiliki keamanan yang sangat baik dalam keamanan jaringan maupun keamanan transfer data didalam jaringan *VPN*. Namun pada teknologi *Ipsec* tidak semua perangkat *router* dapat menjalankan *IPSec server*, mungkin karena itulah keamanan dalam *VPN IPSec* terlihat istimewa.

5. **Implementasi *Kriptografi* Kunci Publik Dengan *Algoritma RSA-CRT* Pada Aplikasi Instant Messaging** (Ashari Arief & Ragil Saputra, Mei 2016)

   Instant messaging merupakan salah satu bentuk kemajuan teknologi komunikasi yang mempermudah penyampaian informasi. Saat ini, dengan semakin banyaknya pengguna aplikasi *instant messaging* berakibat pada dampak negatif berupa penyadapan data khususnya saat terjadi komunikasi yang bersifat rahasia. *Algoritma RSA* merupakan salah satu *algoritma* dalam *kriptografi* kunci publik. Pada proses *enkripsi* dan *dekripsi* digunakan kunci yang berbeda. Proses *dekripsi algoritma RSA* sering terjadi kendala karena ukuran kunci *dekripsi* yang relatif besar dapat memperlambat proses. Untuk mempercepat proses dekripsi, *algoritma RSA* dapat dimodifikasi dengan *algoritma CRT (Chinese Remainder Theorem)*, sering disebut dengan *algoritma RSA-CRT*. Implementasi *algoritma kriptografi RSA-CRT* pada aplikasi *instant messaging* pada panjang bit n mulai dari 56 bit sampai 88 bit, proses dekripsi *RSA-CRT* dua kali lebih cepat dibandingkan proses dekripsi *RSA*.

   CRT (Chinese Remainder Theorem) merupakan suatu *algoritma* untuk mengurangi perhitungan *aritmatika modular* dengan *modulus* besar untuk perhitungan yang sama untuk masing-masing faktor dari *modulus*. *CRT* dapat memperpendek ukuran bit eksponen *dekripsi* (merupakan kunci publik *RSA* atau *RSA-CRT*) dengan cara menyembunyikan d pada sistem *kongruen* sehingga mempercepat waktu *dekripsi* serta dapat digunakan bersama *algoritma RSA* yang disebut *RSA-CRT.*

   Untuk meningkatkan keamanan dari segi pengiriman pesan yang dibuat dalam saluran yang tidak aman serta modifikasi *algoritma RSA* dengan menggunakan *teorema CRT* agar dapat dibandingkan dengan *algoritma RSA*, perlu dibangun sebuah aplikasi *instant messaging* dengan mengimplementasikan *algoritma kriptografi RSA-CRT.*

Pada jurnal penelitian ini Implementasi *algoritma kriptografi* kunci publik dengan *algoritma RSA-CRT* pada aplikasi *instant messaging*, proses *dekripsi* menggunakan *algoritma RSA-CRT* untuk 1.800 karakter dengan bit n dari 56 bit sampai 88 bit memiliki kecapatan rata-rata dua kali lebih cepat dibandingkan menggunakan algoritma *RSA*. Semakin besar panjang *string*, nilai n kemungkinan besar semakin cepat waktu *dekripsi* menggunakan *RSA CRT*.

6. **Penerapan *Algoritma Asimetris RSA* Untuk Keamanan Data Pada Aplikasi Penjualan CV.Sinergi Computer Lubuklinggau Berbasis Web** (Susanto & Andri Anto Tri Susilo, November 2018)

   Masalah keamanan data merupakan masalah yang sangat serius dalam kegiatan bisnis di era digital. kegiatan bisnis di era digital merupakan kegiatan bisnis yang sebagian besar menggunakan teknologi aplikasi komputer serta menjadikan komputer server sebagai tempat menyimpan data-data dalam kegiatan bisnis sehingga dapat disimpulkan media komputer menjadi faktor utama di dalam kegiatan bisnis yang dilakukan. Keamanan data yang menjadi masalah utama bukan hanya data yang tersimpan di komputernya saja, namun juga keamanan data yang dikirimkan lewat jaringan komputer dan aplikasi komputer tetapi keamanan data yang disimpan di dalam *database*.

   Database merupakan sekumpulan informasi yang disimpan di dalam komputer secara sistematik yang dapat digunakan melalui sebuah program komputer tertentu untuk menjalankannya. Keamanan *database* menjadi solusi terakhir pada saat aplikasi komputer mengalami gangguan yang disebabkan oleh pihak luar setelah berhasil melewati keamanan jaringan komputer dan keamanan aplikasi komputer. Dalam sebagian kegiatan bisnis, keamanan *database* menjadi masalah utama setelah menjamin keamanan pada jaringan komputer dan aplikasi komputernya. Contohnya pada kegiatan bisnis penjualan peralatan elektronik yaitu *database* akan menyimpan data-data penjualan, seperti data produk dan data pelanggan serta hak akses pelanggan, dan jika kegiatan bisnis tersebut terintegrasi dengan identitas data lainya antara lain kartu kredit maka harus menjamin kerahasiaan identitas data karena menyangkut privasi pelanggan. Semua yang menyangkut data pribadi pelanggan harus dijamin kerahasiaannya bahkan dari karyawan sekalipun tidak mempunyai hak untuk mengakses atau melihat data identitas pelanggan tersebut. *Database* yang aman akan menjadi tolak ukur sebuah perusahaan dalam keberlangsungan kegiatan bisnis yang dilakukan perusahaan tersebut.

Keamanan *database* dapat dilakukan dengan beberapa cara contohnya pembatasan hak akses pada *database* tersebut, pengunaan nama *field* data yang hanya pahami oleh pemilik aplikasi dan tidak terdapat pegawai yang dapat mengakses *database* dan memahami alur *database* yang ada sehingga terhindar dari manipulasi data dan lainnya, serta menerapkan metode *kriptografi* pada aplikasi terhadap *field* data di dalam *database*nya dengan tujuan *field* data yang disimpan menjadi lebih terjamin privasinya dan tidak dapat dimengerti oleh pihak luar mapun pihak dalam.

Kriptografi sendiri merupakan ilmu dan sekaligus seni untuk mengamankan data yang didalamnya terdapat *algoritma* tertentu yang bertujuan sebagai *confusion* atau pembingungan, dengan cara mengubah teks polos *(plaintext)* menjadi teks yang tidak bisa dibaca artinya secara langsung oleh manusia atau teks rahasia *(ciphertext)*. *Kriptografi* mempunyai proses *enkripsi* dimana dapat mengubah teks atau data *(plaintext)* menjadi teks rahasia *(ciphertext)*, kemudian sebaliknya proses *deskripsi* yang dapat mengembalikan teks rahasia *(ciphertext)* menjadi teks atau data *(plaintext)*. Dalam proses ini digunakan kunci rahasia, semakin banyak kunci rahasia yang digunakan maka semakin bagus. *Algoritma kriptografi* diklasifikasikan menjadi dua yaitu *algoritma simetris* dan *algoritma asimetris*. Contoh *algoritma kriptografi Asimetris* yaitu *algoritma RSA (Rivest, Shamir, Adleman)*.

Pada jurnal penelitian ini menjelaskan penerapan *algoritma asimetris RSA* untuk keamanan data yang telah dilakukan oleh peneliti, setiap data yang diinputkan ke dalam aplikasi penjualan, data atau karakter yang dimasukkan tersebut disimpan di *database* berbentuk *enkripsi* penjumlahan angka jika data yang dimasukan lebih dari satu karakter tetapi jika data yang dimasukan hanya satu karakter maka data atau karakter yang dimasukkan tersebut disimpan di *database* berbentuk enkripsi angka, dengan data yang tersimpan di dalam *database* ini dalam bentuk penjumlahan angka maka data konsumen, data produk dan data pendukung lainnya aman tersimpan di dalam *database* tersebut karena sulit dimengerti oleh pihak lain. Semakin besar nilai bilangan prima yang dimasukan pada nilai p dan q dari *algoritma asimetris RSA* ini maka semakin terjamin keamanan datanya.

7. **Perbandingan *Protokol L2TP* dan *PPTP* Untuk Membangun Jaringan *Intranet* Di Atas *VPN*** (Akbar Rachmawan & Agus Prihanto, S.T.,M,Kom 2018)

Perkembangan jaringan komputer sangat pesat. Jaringan komputer sudah menjadi hal mendasar dalam semua bidang. Hal ini dapat dilihat dari mayoritas orang-orang di dunia sudah pernah mengakses *internet*. Ide pembuatan jaringan pribadi atau *Virtual Private Network*, adalah sebagai suatu keuntungan dari suatu infrastruktur dalam jaringan komunikasi terbuka (*internet*). *Tunneling VPN* pada layer 2 ada metode *tunneling PPTP* dengan *L2TP*.

Dari latar belakang diatas, penulis memunculkan gagasan membuat perbandingan antara protokol *tunneling PPTP* dan *L2TP* untuk mengetahui bagaimana perbandingan mekanisme kerja kedua tunneling dilihat dari keamanan apa saja yang digunakan sebagai *algoritma autentikasi* dan *enkripsi* pada saat komunikasi data. Dari penelitian yang dilakukan menunjukkan bahwa pada saat *autentikasi, L2TP* memerlukan waktu sedikit lebih lama dibandingkan dengan *PPTP.* Hal itu dikarenakan *L2TP* dapat dipadukan dengan *IPSec* sehingga memungkinkan keamanan yang lebih tinggi dari pada *tunneling PPTP*. Namun, untuk performa kedua *tunneling*, *PPTP* sedikit lebih unggul dalam hal kecepatan *transfer* data dari pada *L2TP*. Nilai *delay PPTP* lebih kecil dibandingkan *L2TP*, serta nilai *throughput* lebih besar dari pada *L2TP*.

Untuk membangun sebuah *tunnel*, diperlukan sebuah protokol pengaturnya sehingga *tunnel* secara logika ini dapat berjalan dengan baik bagaikan koneksi *point-to-point* sungguhan. Saat ini, tersedia banyak sekali protokol pembuat *tunnel* yang bisa digunakan seperti *PPTP*, dan *L2TP*.

Pada jurnal penelitian ini dapat disimpulkan bahwa fitur keamanan yang digunakan oleh *tunneling L2TP* sedikit lebih unggul dari pada kemanan yang digunakan pada *PPTP. L2TP* dapat dipadukan dengan *IPSec* sedangkan *PPTP* tidak dapat dipadukan dengan keamanan tambahan yaitu *IPSec*. Nilai *throughput PPTP* lebih besar dibandingkan dengan *L2TP/IPSec* karena *autentikasi* dan *enkripsi* yang digunakan tidak sebanyak dan serumit *L2TP/IPSec*. *L2TP/IPSec* memiliki *delay* sedikit lebih lama dan memiliki *throughput* yang lebih kecil daripada *PPTP*.

8. **DATA *SECURITY IN CLOUD COMPUTING USING RSA ALGORITHM*** (Parsi Kalpana & Sudha Singaraju, September 2012)

Cloud Computing is the key driving force in many small, medium and large sized companies and as many cloud users seek the services of cloud computing, the major concern is the security of their data in the cloud. Securing data is always of vital importance and because of the critical nature of cloud computing and the large amounts of complex data it carries, the need is even more important. Hence forth, concerns regarding data privacy and security are proving to be a barrier to the broader uptake of cloud computing services.

Every cloud service(s) seeker either an individual or a company should ask the right questions to the cloud provider before hosting their data or applications on the cloud. Prospective cloud providers should let you know; Are they financially sound? Do they have good security policies and procedures in place? Is the infrastructure meant to host your data shared with lots of other users, or will it be segregated by virtualization?

As many companies move their data to the cloud the data undergoes many changes and there are many challenges to overcome. To be effective, cloud data security depends on more than simply applying appropriate data security procedures and countermeasures. Computer based security measures mostly capitalizes on user authorization and authentication.

Cloud Computing is an emerging paradigm which has become today's hottest research area due to its ability to reduce the costs associated with computing. In today's era, it is most interesting and enticing technology which is offering the services to its users on demand over the internet. Since Cloud Computing stores the data and disseminated resources in the open environment, security has become the main obstacle which is hampering the deployment of Cloud environments. Even though the Cloud Computing is promising and efficient, there are many challenges for data security as there is no vicinity of the data for the Cloud user. To ensure the security of data, we proposed a method by implementing *RSA algorithm*.

Pada jurnal penelitian ini meningkatkan keamanan data pada *Cloud Computing* dengan cara implementasi *Algoritma RSA* di dalam *Cloud Computing* sehingga keamanan data pada *Cloud Computing* lebih baik dari sebelumnya.

9. ***VIRTUAL PRIVATE NETWORK*** (Ritika kajal, Deepshikha saini, Kusum Grewal, October 2012)

A *VPN* is a private network that uses a public infrastructure (usually the Internet) to connect remote sites or users. The VPN as the name suggest uses “virtual “connections routed through the Internet from the business's private network to the remote site or remote employee. It is a new technology which can be applied to LAN as well as to WLAN.

A VPN maintains privacy of data through security procedures and tunneling protocols. In effect, data is encrypted at sender‟s side and forwarded via "tunnel” which is then decrypted at receiver„s side. An additional layer of security can be added by encrypting not only the data, but also the originating and receiving network addresses. Two VPN technologies that are being used are:

a. Site-to-site VPN - A site-to-site VPN allows multiple offices in fixed locations to establish secure connections with each other over a public network such as the Internet. It also provides extensibility to resources by making them available to employees at other locations.
b. Remote Access VPN - A remote-access VPN allows individual users to establish secure connections with a remote computer network. These users can access the secure resources on that network as if they were directly plugged in to the network's servers.

Virtual Private Network (VPN) is rapidly growing technology which plays a great role in Wireless LAN (WLAN) by providing secure data transmission. The purpose of VPN is to provide safe and secure communication by creating virtual tunnels between pair of hosts, once tunnel is created data transfer can take place. This paper presents a comprehensive study of VPN-IPSec and SSL VPN, architecture and protocols used. The salient of this paper to present comparison analysis of both technologies IPSec and SSL VPN together with their advantages and disadvantages.

Pada jurnal penelitian ini membahas pembangunan infrastruktur *VPN* menggunakan teknologi *IPSec* dan *SSL.*

10. **PERFORMANCE EVALUATION OF REMOTE ACCESS VPN PROTOCOLS ON WIRELESS NETWORK** (Ahmed A.Jaha, Maret 2015)

VPN solutions can be deployed on a wireless network infrastructure to secure transmission between wireless clients and their wired enterprise network. There are many software platforms that can be used to implement software-based VPN solution such as windows, Linux, Solaris, Mac, and

BSD. In this paper, the performance evaluation of some remote access VPN solutions, namely Point to Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol over Internet Protocol Security (L2TP/IPSec), and Secure Socket Layer (SSL) will be empirically investigated on wireless networks. Some of QoS performance metrics like throughput, latency, jitter, and packet loss are measured to explore the impact of these VPNs on the ultimate performance perceived by end user applications. All experiments were conducted using wireless VPN client connected to domain controller server through VPN server.

Over the past several years, wireless technology has enhanced the computer networking. The Wireless Local Area Network (WLAN) technology represented a convenient alternative to conventional wired LANs due to everywhere network access without wires, growing data rates, improving quality of service, and decreasing the prices. Vulnerability of the wireless medium to some security threats increasing the priority of security issues. A Virtual Private Network (VPN) is a simple solution to achieve secure communications over the use of a public network infrastructure such as the Internet, maintaining privacy through the use of a tunneling protocol and security procedures. It is also possible to similarly deploy VPNs on a wireless network infrastructure to secure transmission between wireless clients and their wired enterprise network. This method has been warmly accepted by the academia and industry as an alternative to securing WLANs. It involves in the creation of a VPN tunnel through the use of a tunneling protocol that encrypts traffic over the WLAN. Although VPN servers are usually hardware-based devices, there are many software platforms that can be used to implement software-based VPN servers such as windows, Linux, BSD, and Solaris but the main two are Windows and Linux platforms.

From the results that were collected from the testbeds and the user applications requirements, the following conclusion remarks are gained:

a. In order to have strong security, *L2TP/IPSec* combines *L2TP*'s tunnel with *IPSec*'s secure channel which increases the overhead packets. So, *L2TP/IPSec* on both *windows server 2003* and *fedora core 6* has produced a good performance values.
b. The performance values of both *PPTP and L2TP/IPSec* on *windows server 2003* are better than the performance values of both *PPTP* and *L2TP/IPSec* on *fedora core 6*

Pada jurnal penelitian ini membandingkan kualitas *VPN* dan keamanan pada protokol *PPTP* dan *L2TP.*

Dari beberapa jurnal yang telah diuraikan bagaimana teknologi *VPN* dapat menghubungkan sebuah jaringan yang terpisah jauh secara geografis untuk dapat mengakses jaringan lainnya secara *private* melalui jaringan public. Pada jurnal ini akan menggunakan teknologi *VPN* dan metode *RSA Public Key* sebagai sistem keamanan dalam menghubungkan antar *router* dan membuat *tunneling* jaringan.

B. LANDASAN TEORI

Dalam landasan teori ini dikemukakan teori-teori yang dapat membantu dalam penelitian.

1. Jaringan Komputer

Jaringan komputer adalah sebuah sistem yang terdiri dari dua atau lebih sistem komputer yang melaksanakan tugasnya dan saling berhubungan satu sama lainnya. Hubungan yang dibentuk dapat berupa bentuk hubungan komunikasi seperti pesan instan, berbagi sumber daya (*resource*) seperti data, CPU dan *hardware* (CD-Rom, printer), dan akses terhadap informasi seperti *web*. Misalnya koneksi antara dua komputer, sehingga keduanya dapat bertukar informasi satu sama lain. Bentuk koneksi tersebut dapat melalui serat optik, kawat tembaga, gelombang mikro, dan satelit komunikasi (radio, satelit).

Gambar 2.1 Topologi Jaringan Komputer
(Sumber : ilmuonline.net)

Tujuan dari jaringan komputer ini adalah setiap komputer yang termasuk kedalam sistem dapat menerima dan memberikan layanan (*service*). Pihak yang menerima layanan disebut dengan klien (*client*), dan yang memberikan layanan disebut dengan peladen (*server*). Sehingga sistem yang terbentuk

dari layanan ini disebut dengan sistem *client-server*, bahkan sistem ini digunakan pada hampir seluruh aplikasi pada jaringan komputer.

Fungsi jaringan komputer adalah sebagai berikut :

a. Keamanan

   Jaringan komputer yang termasuk kedalam sistem memberikan sebuah layanan hak akses terhadap file atau sumber daya yang lain, sehingga terlindungi dari pengambilan hak cipta..

b. Kecepatan

   Jaringan komputer akan membuat kerjaan menjadi lebih cepat melalui fasilitas *sharing* nya yang memungkinkan dan memudahkan perpindahan (*transfer*) data antara dua komputer atau lebih.

c. Media Komunikasi

   Jaringan komputer memungkinkan kerjasama antara orang-orang yang terpisah dengan jarak. Baik untuk berkomunikasi, bahkan bertukar data.

d. Akses Informasi

   Informasi yang dapat diakses lebih luas, bahkan informasi bisa diakses dan didapatkan dari jarak yang jauh sekalipun

e. Berbagai Sumber.

   Berbagi sumber disebut juga dengan *resource sharing*, yaitu seluruh program, peralatan dan data yang digunakan oleh setiap orang yang termasuk kedalam sistem tanpa dipengaruhi oleh lokasi *client* dan *server*nya.

Dari penjelasan diatas dapat ditarik kesimpulan bahwa jaringan komputer memang dibutuhkan untuk memaksimalkan kinerja komputer. Dengan adanya jaringan komputer berbagai macam informasi, ilmu serta tukar data dapat dilakukan..

Dina Amalia, IDwebhost. 2018. *Pengertian Jaringan Komputer dan Manfaatnya* [online]. Ada di: https://idwebhost.com/blog/pengertian-jaringan-komputer-dan-manfaatnya/ [Diakses tanggal 20 Juni 2019].

2. VPN

Virtual Private Network (*VPN*) adalah sebuah teknologi komunikasi yang memungkinkan dapat terkoneksi ke jaringan publik dan menggunakannya untuk dapat bergabung dengan jaringan lokal. *VPN* merupakan koneksi *virtual* yang bersifat *private*, dikarenakan jaringan yang dibuat tidak nampak secara fisik hanya berupa jaringan *virtual*, dan jaringan tersebut tidak semua orang dapat mengaksesnya sehingga sifatnya *private*. Dengan cara tersebut maka akan didapatkan hak dan pengaturan yang sama seperti halnya

berada di dalam kantor atau *LAN* itu sendiri, walaupun sebenarnya menggunakan jaringan milik publik.

Menurut Ardiyansyah (2008) teknologi *VPN* menyediakan beberapa fungsi utama untuk penggunaannya. Fungsi-fungsi utama tersebut antara lain sebagai berikut:

a. *Confidentially* (Kerahasiaan)

Dengan digunakannnya jaringan publik yang rawan pencurian data, maka teknologi *VPN* menggunakan sistem kerja dengan cara meng*enkripsi* semua data yang lewat melalui. Dengan adanya teknologi *enkripsi* tersebut, maka kerahasiaan data dapat lebih terjaga. Walaupun ada pihak yang dapat menyadap data yang melewati *internet* bahkan jalur *VPN* itu sendiri, namun belum tentu dapat membaca data tersebut, karena data tersebut telah teracak. Dengan menerapkan sistem *enkripsi* ini, tidak ada satupun orang yang dapat mengakses dan membaca isi jaringan data dengan mudah.

b. *Data Integrity* (Keutuhan Data)

Ketika melewati jaringan internet, sebenarnya data telah berjalan sangat jauh melintasi berbagai negara. Pada saat perjalanan tersebut, berbagai gangguan dapat terjadi terhadap isinya, baik hilang, rusak, ataupun dimanipulasi oleh orang yang tidak seharusnya. Pada *VPN* terdapat teknologi yang dapat menjaga keutuhan data mulai dari data dikirim hingga data sampai di tempat tujuan.

Gambar 2.2 Koneksi Jaringan VPN

(Sumber : mybrandamb.blogspot.com)

c. *Origin Authentication* (Autentikasi sumber)

Teknologi *VPN* memiliki kemampuan untuk melakukan autentikasi terhadap sumber-sumber pengirim data yang akan diterimanya. *VPN* akan

melakukan pemeriksaan terhadap semua data yang masuk dan mengambil informasi dari sumber datanya. Kemudian, alamat sumber data tersebut akan disetujui apabila proses autentikasinya berhasil. Dengan demikian, *VPN* menjamin semua data yang dikirim dan diterima berasal dari sumber yang seharusnya. Tidak ada data yang dipalsukan atau dikirim oleh pihak-pihak lain.

d. *Non-repudiation*

Yaitu mencegah dua pihak dari menyangkal bahwa mereka telah mengirim atau menerima sebuah *file* mengakomodasi perubahan.

e. Kendali akses

Menentukan siapa yang diberikan akses ke sebuah sistem atau jaringan, sebagaimana informasi apa dan seberapa banyak seseorang dapat menerima.

IDCloudHost. 2016. *Pengertian VPN, Manfaat, dan Cara Kerja VPN* [online]. Ada di: https://idcloudhost.com/panduan/pengertian-vpn-manfaat-dan-cara-cerja-vpn/ [Diakses tanggal 20 Juni 2019].

3. Internet

Internet adalah suatu gabungan sebuah jaringan dua atau lebih perangkat komputer yang ada di seluruh dunia dan bisa dibilang merupakan suatu rangkaian perangkat komputer yang terbesar di dunia, serta ukurannya akan terus mengalami suatu perkembangan hingga tanpa batas waktu yang ditentukan selama teknologi terus berkembang dan maju di dunia ini. Akan tetapi sebuah perangkat komputer tersebut hanya sebagian dari beberapa definisi tentang sebuah jaringan *internet*, karena ketika kita membahas sebuah jaringan internet maka yang ditujukan ialah semua yang bergantung tentang predikat yang sudah melekat terhadapnya seperti contoh yaitu sebuah informasi dan para penggunanya serta sebuah *software* dan *hardware* yang dimanfaatkan.

Pengertian dari jaringan *internet* atau koneksi *internet* di atas merupakan gambaran secara umum, Suatu sistem sebuah jaringan yang berkaitan di dalam suatu lingkup umum atau global bertujuan memfasilitasi sebuah komunikasi layanan *file* atau data seperti contoh yakni *transfer file*, surat elektronik, *remote login, newsgroup* dan *World Wide Web* ialah definisi jaringan sebuah internet yang digunakan sebagai suatu sistem . Dalam era saat ini penggunaan jaringan internet telah dinikmati jutaan orang yang ada diseluruh dunia dengan berbagai macam kepentingan yang berbeda-beda. Padahal pada saat dulu penggunaan jaringan *internet* hanya terbatas

kepada sebuah lembaga akademis dan militer saja akan tetapi saat ini sudah digunakan secara umum.

Jaringan *internet* yang saat ini kita gunakan pada awalnya memang hanya bertujuan untuk mengetahui strategi musuh antar negara atau sebagai penyebar informasi secara khusus namun semakin berkembangnya teknologi jaringan *internet* sudah mengalami berbagai haluan cara dan tujuan contohnya dalam pembuatan robot pengendalian sistem atau jalur pesawat dan berbagai macam lainnya. *Pengertian jaringan internet* saat ini bisa di simpulkan bahwa sesuatu sistem yang bermanfaat bagi kehidupan masyarakat dengan melalui perangkat-perangkat tertentu serta bertujuan untuk meningkatkan perkembangan teknologi dunia tanpa batasan.

Sedangkan menurut Onno W.Purbo menjelaskan bahwa *Internet* pada dasarnya merupakan sebuah media yang digunakan untuk mengefesiensikan sebuah proses komunikasi yang disambungkan dengan berbagai aplikasi, seperti *Web, VoIP, E-mail*.

Adzikra Ibrahim ,Pengertiandefinisi. 2017. *Pengertian Jaringan internet dan tujuannya* [online]. Ada di: https://pengertiandefinisi.com/pengertian-jaringan-internet-dan-tujuannya/ [Diakses tanggal 20 Juni 2019].

4. IP Address Public

IP Address public adalah sebuah *IP address* atau alamat jaringan yang bersifat unik (pada bagian *network identifier*) untuk tiap-tiap komputer dan digunakan pada jaringan *internet*. *IP Address public* hanya dimiliki oleh masing-masing komputer diseluruh dunia termasuk juga perangkat-perangkat lain yang terhubung untuk memudahkan dalam pengenalan satu sama lain. Apabila masih menggunakan *IPv4*, maka daya tampungnya sangat terbatas untuk *IP Address public*, sehingga salah satu cara umum yang paling sering digunakan adalah dengan *NAT (Network Address Translator).* Umumnya user internet memperoleh *IP Address public* dari *provider* (penyedia layanan akses *internet*).

Host yang menggunakan *IP public* dapat diakses oleh seluruh *user* yang tergabung di *internet* baik secara langsung maupun tidak langsung (melalui *proxy/NAT*). *IP Address* juga dikelompokkan berdasarkan negara, Indonesia umumnya dimulai dengan kepala 202 & 203. IP publik inilah yang biasanya saat ini menggunakan *IPV4* dan ditakutkan akan habis dalam waktu dekat. Lembaga yang mengatur atau menyediakan *IP Public* adalah *IANA*, singkatan dari *Internet Authorized Numbering Association.*

Sebuah alamat IP publik dapat berupa statis atau dinamis. Sebuah alamat *IP public static* tidak dapat berubah dan digunakan terutama untuk *hosting* halaman *Web* atau layanan di *Internet*. Di sisi lain sebuah alamat IP publik yang dinamis dipilih dari sebuah *pool* yang tersedia pada alamat dan perubahan masing-masing terjadi satu kali untuk menghubungkan ke *Internet*. Sebagian besar pengguna internet hanya akan memiliki IP dinamis yang bertugas untuk setiap komputer. Ketika terjadi disconnetted atau jaringan terputus/padam apabila menghubungkannya kembali maka otomatis akan mendapat IP baru.

Secara singkatnya, *IP Address Public* adalah alamat jaringan yang bersifat unik (pada bagian *network identifier*) untuk tiap komputer dan digunakan pada jaringan *internet*. Satu *IP Address* hanya bisa digunakan untuk satu perangkat jaringan saja, jadi tidak mungkin dua buah komputer menggunakan *IP Address* yang sama akan bisa mengakses jaringan.

TeoriKomputer. 2014. *Pengertian dan fungsi IP Public pada Jaringan IP address public* [online]. Ada di: http://www.teorikomputer.com/2014/12/pengertian-dan-fungsi-ip-address-public.html [Diakses tanggal 20 Junii 2019].

5. IP Address Private

IP Private adalah IP yang dapat dikatakan sebagai IP pribadi dan biasa digunakan dalam jaringan lokal, *IP Private* ini biasa digunakan dalam jaringan lokal yang biasanya terdapat di sekolah, kantor, PT dll sehingga dengan menggunakan *IP Private* ini user dapat melakukan *transfer* data tanpa harus terhubung ke *internet* secara langsung, akan tetapi setiap *user* harus berada dalam satu *Local Area Network (LAN)* yang sama agar dapat melakukan pertukaran data. *Administrator* jaringan juga bebas menentukan alamat IP pilihannya sendiri, tidak seperti *IP Public* yang sudah ditetapkan dan didaftarkan oleh lembaga internasional.

Disebut *IP address private* karena IP ini hanya dikenali dan bisa diakses dari jaringan local saja dan tidak bisa diakses melalui jaringan *internet* secara langsung tanpa bantuan *router* yang mempunyai fitur *NAT*. *IP private* digunakan untuk jaringan lokal agar sesama komputer dapat saling berkomunikasi, misalnya digunakan di jaringan sekolah, kantor, toko, warnet dan sebagainya. Perangkat yang terhubung ke jaringan lokal seperti printer, komputer, laptop, *smart device* biasanya akan mendapatkan *IP address private*. Agar *IP private* dapat terhubung ke *internet* maka diperlukan *router* yang mempunyai kemampuan untuk melakukan *NAT* (*Network Address Translation*) agar semua *device* dengan *IP private* dapat terkoneksi ke

internet dengan menggunakan *IP public* yang terkoneksi langsung ke *Internet*. Meskipun sudah terkoneksi ke *internet*, *IP private* tetap tidak bisa diakses langsung dari jaringan *internet*.

Tabel 2.1 *Clustering IP Address Versi 4*

Class	Network Bits	Host Bits	Desimal Address Range	Subnet Mask
Class A	8 bits	24 bits	1-126	255.0.0.0
Class B	16 bits	16 bits	128-191	255.255.0.0
Class C	24 bits	8 bits	192-223	255.255.255.0
Class D	Reserved for Multicasting		224-239	N/A
Class E	Reserved for R & D		240-255	N/A

Dalam penggunaannya *IP private* tidak perlu didaftarkan ke pihak otoritas sebelum digunakan karena penggunaan *IP private* telah diatur, dialokasian dan distandarkan oleh *IANA* (Lembaga yang mengatur penggunaan dan pengalokasian IP address di seluruh dunia) dalam dokumen *RFC 1918.* Alokasi *IPv4 private* sesuai standar internasional ketika *Internet Engineering Task Force* (*IETF*) telah menunjuk *Internet Assigned Numbers Authority* (*IANA*) untuk mengalokasikan *IPv4* untuk jaringan *private*.

Ananda Rizky, Warung Informasi. 2017. *Ip Private* [online]. Ada di: https://darsammania.blogspot.com/2017/01/ip-private.html [Diakses tanggal 20 Juni 2019].

6. Intranet

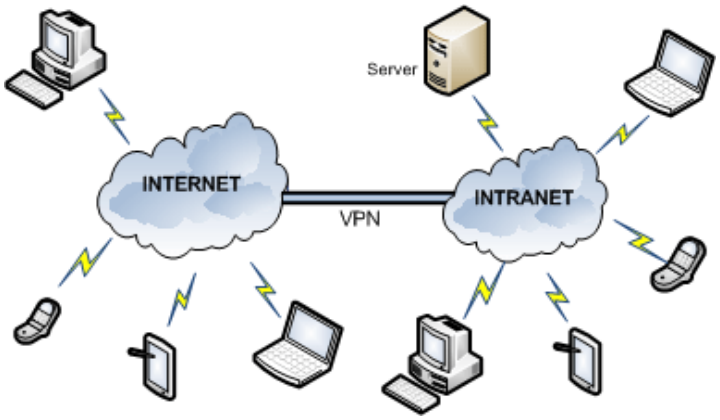
Intranet adalah sekumpulan jaringan komputer yang cukup besar dan bersifat *private* yang dihubungkan dengan menggunakan saluran telepon, satelit atau mode komunikasi yang lainnya. Biasanya jaringan *intranet* digunakan oleh sebuah instansi atau lembaga untuk membagikan informasi rahasia dalam bentuk web base kepada para pegawai atau karyawan, jadi tidak semua orang dapat mengakses intranet hanya orang-orang tertentu yang dapat mengakses *intranet* sebuah perusahaan atau instansi.

Sesuai dengan definisi dari *intranet* itu sendiri fungsi dari *intranet* adalah untuk menghubungkan komputer satu dengan komputer lain juga perangkat jaringan yang lain seperti: *switch, server,* printer dan *access point*, akan tetapi layanannya terbatas hanya satu lokasi saja.

Intranet dapat disebut jaringan pribadi *(Private Network)* yang mengunakan *internet* untuk saling berbagi dan bertukar informasi di dalam jaringan lokal contohnya adalah: Perusahaan, Kantor, Sekolah, Universitas dll. *Intranet* juga termasuk ke dalam salah satu jaringan *LAN (Local Area Network)* yang hanya bisa mencakup wilayah kecil.

Dapat disimpulkan Fungsi *Intranet* adalah berfungsi mengkomunikasikan komputer satu dengan yang lain, persis seperti *internet* tatapi memiliki layanan yang terbatas, tak seluas dan seberagam jaringan *internet*.

Menurut M. Miftakul Amin (2012:181), pengertian *intranet* adalah *local area network (LAN)* yang menggunakan standar komunikasi dan segala fasilitas Internet, diibaratkan berinternet dalam lingkungan lokal.



Gambar 2.3 Koneksi *VPN* Sebagai Perantara Jaringan *Intranet*
(Sumber : denisamanda.wordpress.com)

Admin, UTopiccomputers. 2017. *Apa Itu Intranet ? Berikut Adalah Pengertian dan Fungsinya* [online]. Ada di: https://www.utopicomputers.com/apa-itu-intranet-berikut-adalah-pengertian-dan-fungsinya/ [Diakses tanggal 20 Juni 2019].

7. Router

Router adalah suatu perangkat luar komputer atau alat yang mengirimkan paket data melalui jaringan *internet* menuju perangkat lain atau tujuannya menggunakan proses yang dinamakan *routing*.

Routing adalah proses yang terjadi saat pengiriman paket data dari jaringan satu ke jaringan yang lainnya yang terjadi melalui 3 lapisan (jaringan *internet protocol*) dari *stack* protokol 7 lapis *OSI*. Fungsi *router* itu sendiri adalah menghubungkan 2 jaringan atau lebih untuk menyalurkan data informasi dari jaringan satu ke jaringan lainnya. Dalam proses penyaluran

sinyal data informasi, perangkat baik yang menerima atau yang mengirim harus terkoneksi dengan *internet*.

Fungsi utama dari *router* sendiri yakni sebagai pembagi atau penyalur *IP address* secara stastis atau memakai *DHCP* kepada seluruh perangkat komputer atau laptop yang terhubung pada perangkat *router*. Setelah fungsi dari *router* berjalan, maka setiap komputer yang terhubung memiliki *IP address* yang unik sehingga dapat digunakan untuk melakukan *browsing*, setting *LAN* dan *internet*.

Cara kerja *router*, *router* bekerja dengan cara merutekan paket atau data informasi yang disebut dengan *routing*. Dengan teknik *routing* tersebut, *router* dapat mengetahui arah rute perjalanan informasi tersebut akan dituju, apakah berada pada satu jaringan yang sama atau berbeda. Jika informasi yang dituju mengarah kepada jaringan yang berbeda, maka *router* akan meneruskannya kepada jaringan tersebut, sebaliknya apabila paket yang dituju adalah jaringan yang sama, maka *router* akan menghalangi paket keluar serta meneruskan paket tersebut dengan *routing* pada jaringan yang sama sampai terkirim ke tujuan.

Penggunaan *router* sendiri paling sering kita temui pada warnet, perkantoran, administrasi sekolah, perhotelan dan berbagai usaha atau tempat yang menggunakan fasilitas layanan *internet*. Teknologi *router* sudah lebih modern dan canggih dengan adanya fungsi *wireless*. Dengan kelebihan ini, setiap perangkat atau gadget yang mampu menangkap sinyal gelombang radio, dapat menerima gelombang radio yang dipancarkan *router* sehingga dapat langsung terhubung dengan *internet*.

CatatanTeknisi. 2013. *Pengertian dan Cara Kerja Router* [online]. Ada di: https://catatanteknisi.com/pengertian-cara-kerja-router/ [20 Juni 2019].

8. Algoritma RSA

Algoritma RSA adalah *algoritma* yang sangat maju dalam bidang *kriptografi* kunci public (kriptografi *public key*) yang sangat popular dan masih digunakan sampai saat ini. *RSA* merupakan *algoritma* yang paling cocok untuk *digital signature* seperti halnya *enkripsi*. Algoritma *RSA* masih digunakan secara luas dalam *protocol electronic commerce* dan dipercaya dalam pengamanan dengan kunci yang sangat panjang. *Algoritma RSA* disebut sebagai kunci publik karena kunci *enkripsi* dapat dibuat *public* yang berarti semua orang dapat mengetahuinya. Walaupun dibuat *public key*, keamanan *algoritma RSA* sangat terjaga. Hal itu dikarenakan kunci yang digunakan untuk *enkripsi* pada algoritma *RSA* berbeda dengan kunci yang digunakan untuk *dekripsi*nya. Keamanan *enkripsi* dan *dekripsi* algoritma *RSA*

terletak pada kesulitan untuk memfaktorkan *modulus n* yang sangat besar. Penamaan *algoritma RSA* diambil dari nama penemunya, yaitu *Rivest, Shamir* dan *Adleman* yang diplubikasikan pada tahun 1977 di *MIT* yang bertujuan untuk menjawab tantangan dari *Algoritma* Pertukaran Kunci *Diffie Helman.*

Algoritma RSA mengikuti skema *Block Cipher*, yaitu sebelum dilakukan *enkripsi, plainteks* yang ada dibagi ke dalam blok-blok yang sama panjang dimana *plainteks* dan *cipherteks*nya berupa *integer* antara 1 sampai *n* dengan *n* biasanya berukuran 1024 bit dan panjang bloknya berukuran tidak lebih dari log (*n*) + 1 dengan basis 2.

Penyajian *algoritma* secara garis besar dapat dibagi dalam dua bentuk penyajian yaitu tulisan dan gambar. *Algoritma* yang disajikan dengan tulisan yaitu dengan struktur bahasa tertentu (misalnya bahasa Indonesia atau bahasa Inggris) dan *pseudocode. Pseudocode* adalah kode yang mirip dengan kode pemrograman yang sebenarnya seperti *Pascal*, atau C, sehingga tepat digunakan dalam menggambarkan *algoritma* yang akan dikomunikasikan kepada programmer.

Sedangkan untuk *algoritma* yang disajikan dengan gambar adalah dengan *flowchart. Flowcart* adalah bagan *(chart)* yang menunjukkan alir *(flow)* di dalam program atau merupakan prosedur sistem secara logika. *Flowcart* digunakan untuk alat bantu komunikasi dan untuk dokumentasi.

Misbahul Makruf, AllMakruf. 2014. *Penjelasan Tentang Algoritma RSA* [online]. Ada di: https://allmakruf.blogspot.com/2014/12/algoritma-rsa.html [Diakses tanggal 20 Juni 2019].

9. Enkripsi

Enkripsi adalah suatu metode yang digunakan untuk mengkodekan data sedemikian rupa sehingga keamanan informasinya terjaga dan tidak dapat dibaca tanpa di *dekripsi* (kebalikan dari proses *enkripsi*) dahulu. *Encryption* berasal dari bahasa *yunani kryptos* yang artinya tersembunyi atau rahasia.

Dikarenakan *enkripsi* telah digunakan untuk mengamankan komunikasi di berbagai negara, hanya organisasi-organisasi tertentu dan individu yang memiliki kepentingan yang sangat mendesak akan kerahasiaan yang menggunakan enkripsi. Di pertengahan tahun 1970-an, *enkripsi* kuat dimanfaatkan untuk pengamanan oleh sekretariat agen pemerintah Amerika Serikat pada domain publik, dan saat ini *enkripsi* telah digunakan pada sistem secara luas, seperti I*nternet e-commerce*, jaringan telepon bergerak dan ATM pada bank.

Enkripsi mengacak data menjadi bentuk yang tidak masuk akal, sehingga tidak ada yang bisa mengerti apa itu kecuali mereka memiliki kunci untuk menguraikannya. Sepasang kunci (kunci yang sama atau unik yang digunakan untuk *enkripsi* dan *dekripsi*) biasanya dibagikan antara pengguna di bagian awal dan akhir. Definisi standar *enkripsi* adalah "proses mengubah informasi atau data menjadi kode, terutama untuk mencegah akses tidak sah". Cara termudah untuk menggambarkannya adalah dengan menggunakan analogi gembok satu-satunya orang yang dapat membukanya adalah yang memegang kunci gembok tersebut.

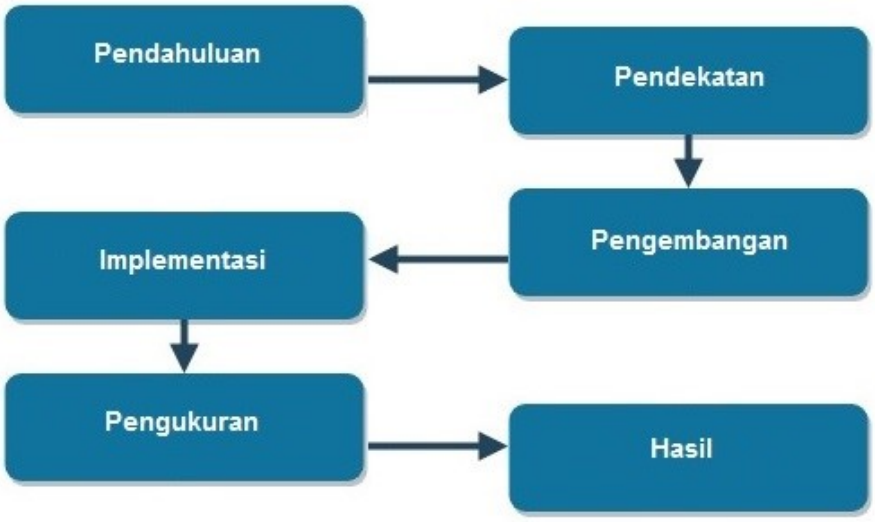
Hal ini bisa ditunjukkan dengan menggunakan contoh berikut. Anda mungkin ingin mengirim pesan yang ditujukan untuk sedikit orang, seperti "gonggongan anjing di tengah malam", yang akan dienkripsi menjadi *"148$%AsdjW34398J3Q(*(#q$wjkIsaefQ(#$*02342kjsadf"*. Informasi ini akan dikirim dalam bentuk terenkripsi antara satu komputer ke komputer lain dan hanya dapat disusun ulang (di*dekripsi*) oleh target yang dituju menggunakan kunci.

Enkripsi dapat digunakan untuk tujuan keamanan, tetapi teknik lain masih diperlukan untuk membuat komunikasi yang aman, terutama untuk memastikan integritas dan autentikasi dari sebuah pesan. Contohnya, Message Authentication Code (MAC) atau digital signature. Penggunaan yang lain yaitu untuk melindungi dari analisis jaringan komputer.

Julia, SJ. 2019. *Panduan lengkap untuk enkripsi VPN* [online]. Ada di: https://id.wizcase.com/blog/panduan-lengkap-untuk-enkripsi-vpn/#2 [Diakses tanggal 28 Desember 2019].

C. KERANGKA PEMIKIRAN

Permasalahan yang terjadi pada jaringan komputer saat ini adalah lemahnya keamanan jaringan *intranet* yang dibangun dari teknologi *VPN*. Pendekatan atau metode yang digunakan dalam penelitian ini adalah metode *Algoritma RSA* dengan cara pengumpulan data berupa teknologi *VPN* yang dapat bekerja dengan baik menggunakan metode *RSA Key* dan juga mencari perangkat keras yang bisa menggunakan teknologi *VPN*. Model pengembangan dari teknologi ini akan membuat sebuah kemanan yang bekerja bersama dengan metode *RSA Key*. Dengan adanya teknologi tersebut maka dapat dijadikan sebagai bahan evaluasi dari penelitian ini yaitu untuk dapat meningkatkan keamanan jaringan intranet menggunakan teknologi teknologi *VPN*.



Gambar 2.4 Kerangka Pemikiran

D. HIPOTESIS

Hipotesis yang dapat ditetapkan dalam penelitian ini adalah Penerapan *Algoritma RSA* pada *VPN* diduga dapat meningkatkan keamanan jaringan *intranet*.