# ABSTRACT

*Computer networks are one of the most widely used technologies. The function of a computer network is to connect one device to another. Public network (public network / internet) can be traversed by all internet users. Therefore, each user can use the opportunity to interfere with other users' private communications, so that public networks are at risk of security threats. The data transfer process must have a working network whose channels have guaranteed security. This is because data passing through a channel may contain important information. Using a VPN can be a solution to this problem. VPN technology creates a tunnel through the internet network. In this study, VPN access is used, using the OpenVPN method which uses the TLS encryption protocol in the client and server connections. OpenVPN server will be installed on azure so it can be accessed from anywhere. The results of this study will test the speed of download, upload, latency and jitter using speedtest, and on security will test packet sniffing using the Wireshark application.*

*Keywords: Network, OpenVPN, cloud*

# BAB I

# Pendahuluan

## 1.1 Latar Belakang

Pesatnya perkembangan teknologi terutama pada dunia internet memudahkan pertukaran informasi dari dan ke berbagai tempat. Meski telah memiliki bermacam- berbagai jenis protokol keamanan, namun masih terdapat celah yang menembus keamanannya, yang berakibat pencurian data informasi berarti. Salah satu contohnya adalah kala seseorang sedang menggunakan sosial media di jaringan publik semacam wifi gratis. Pada jaringan wifi gratis tersebut bisa jadi sudah ada pihak tidak bertanggung jawab yang dengan berencana mengambil informasi individu dan data berarti dari orang tersebut[1]. Saat berselancar di internet ada risiko kerugian dengan adanya data dapat diambil orang yang tidak bertanggung jawab.

VPN merupakan suatu bentuk *private* internet melalui *public network* (internet), dengan menekankan pada keamanan data dan akses global. Dalam pengaplikasian VPN untuk mendapatkan koneksi yang bersifat *private*, data harus di-enskripsi dahulu untuk menjaga kerahasiaannya sehingga paket yang tertangkap ketika melewati jaringan publik tidak terbaca karena harus melewati proses deskripsi. Ada banyak *platform* perangkat lunak yang dapat digunakan untuk mengimplementasikan VPN berbasis *software* solusi, seperti Windows, Linux, Solaris, Mac, dan BSD. *Private network* dianggap lebih efisien karena kecepatan transfer data yang lebih besar dari pada kecepatan transfer data pada jaringan internet, selain itu keamanan dianggap lebih bagus karena hanya bergerak dalam lingkup terbatas saja [2]. OpenVPN merupakan salah satu opensource gratis untuk teknologi VPN yang dapat bekerja dibanyak *platform*. OpenVPN menggunakan protokol enkripsi TLS dengan menerapkan sertifikat digital dalam koneksi client dan server[3].

Penggunaan azure *cloud computing* berkaitan dengan pembelajaran yang saya lakukan pada kegiatan studi independent di PT MariBelajar yang membahas berbagai layanan Microsoft. Azure merupakan sebuah *cloud computing* yang dibuat oleh Microsoft. Azure sudah memiliki *service*

OpenVPN pada system market sehingga pembuatan OpenVpn acces server akan lebih cepat dan mudah.

## 1.2 Rumusan Masalah

1. Bagaimana merancang dan menerapkan OpenVPN acces server pada lingkungan Azure?
2. Bagaimana pengaruh penggunaan VPN terhadap performa pada jaringan?
3. Bagaimana pengaruh penggunaan VPN pada kemanan jaringan?

## 1.3 Tujuan Kegiatan

1. Merancang dan menerapkan OpenVPN access server pada lingkungan azure dengan menggunakan virtuak machine
2. Mengukur pengaruh penggunaan VPN terhadap parameter kecepetan *download*, *upload*, *latensi* dan *jitter*
3. Membuktikan pengaruh keamanan pada penggunaan VPN untuk mencegah *sniffing* paket.

## 1.4 Manfaat Kegiatan

1. Dapat merancang dan menerapkan OpenVPN access server pada lingkungan azure dengan menggunakan virtuak machine
2. Dapat mengetahui pengaruh penggunaan VPN terhadap kecepetan *download*, *upload*, *latensi* dan *jitter*
3. Dapat mengetahui pengaruh penggunaan VPN pada kemanan jaringan

# BAB II

# Deskripsi Kerja

## 2.1 Deskripsi Penugasan Kerja

Untuk deskripsi kegiatan yang ada di *Cloud fundamental track* disajikandalam bentuk tabel.

Tebel 2. 1 tabel kegiatan

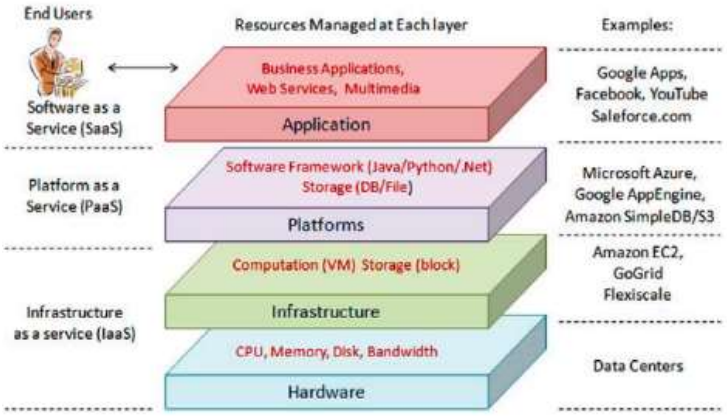
| Bulan ke- | Minggu ke- | Modul |
|---|---|---|
| 1 | 1 | Microsoft Azure Fundamentals |
| | 2 | Microsoft Azure Fundamentals |
| | 3 | Microsoft Azure Fundamentals |
| | 4 | Microsoft Azure Fundamentals<br>Microsoft Azure Data Fundamentals |
| 2 | 1 | Microsoft Azure Data Fundamentals |
| | 2 | Microsoft Azure Data Fundamentals |
| | 3 | Microsoft Azure Data Fundamentals |
| | 4 | Microsoft Azure AI Fundamentals |
| 3 | 1 | Microsoft Azure AI Fundamentals |
| | 2 | Microsoft Azure AI Fundamentals<br>Microsoft Power *Platform* Fundamentals |
| | 3 | Microsoft Power *Platform* Fundamentals |
| | 4 | Microsoft Power *Platform* Fundamentals |
| 4 | 1 | Microsoft Power *Platform* Fundamentals<br>Microsoft Dynamics 365 Fundamentals ERP |
| | 2 | Microsoft Dynamics 365 Fundamentals ERP |
| | 3 | Microsoft Dynamics 365 Fundamentals ERP<br>Microsoft Dynamics 365 Fundamentals CRM |
| | 4 | Microsoft Dynamics 365 Fundamentals CRM |

## 2.2 Teori Dasar pendukung

### 2.2.1 Cloud Computing

*Cloud* adalah awan, sebagai gambaran Internet, yang bagi user, tidak perlu tahu ada di mana. Yang penting bagi user adalah dapat terhubung ke Internet. Entah melalui jaringan telpon, jaringan kabel, jaringan hotspot, jaringan seluler, atau melalui warnet, yang penting terhubung ke Internet dengan koneksi yang (kalau bisa) cepat dan gratis. *Cloud*

*computing* atau komputasi awan merupakan tren baru di bidang komputasi terdistribusi dimana berbagai pihak dapat mengembangkan aplikasi dan layanan berbasis SOA (*Service Oriented Architecture*) di jaringan internet[4].




Gambar 2. 1 Arsitekture cloud computing[5]

Arsitektur *cloud computing* dapat dibedakan kedalam 4 (empat) lapisan, yaitu: lapisan perangkat keras. Layanan *cloud computing* yang umum ditawarkan terdapat tiga jenis, yaitu SaaS (*Software as a Service*), PaaS (*Platform as a Service*), IaaS (*Infrastructure as a Service*)[5].

a. SaaS (*Software as a Service*)

   *Software as a Service* (SaaS) merupakan lapisan teratas dari arsitektur *cloud computing*, dimana jenis *service* ini berupa sejumlah aplikasi-aplikasi yang ditawarkan ke pihak para penggunanya. Sa*as a*dalah aplikasi lapisan atas yang disampaikan berbasis pada permintaan (on-demand) layanan aplikasi untuk mengirimkan perangkat lunak secara khusus ke tujuannya. SaaS dapat diakses dari jarak jauh (remote) oleh pengguna melalui internet berdasarkan model harga. Kemampuan dari layanan ini akan dikirimkan kepada penggunanya dengan menggunakan aplikasi penyedia yang berjalan pada infrastruktur *cloud*. Aplikasi dapat diakses dari berbagai perangkat klien melalui sistem antarmuka, seperti web browser (misalnya: email berbasis web).

b. PaaS (*Platform as a Service*)

*Platform as a Service* (PaaS) adalah *middleware service* atau layanan perangkat lunak perantara yang menfasilitasi berjalannya program aplikasi-aplikasi lainnya di lingkungan *cloud*. PaaS menyediakan layanan aplikasi lapisan arsitektur *cloud* untuk membangun, menguji dan menyebarkan aplikasi yang sedang pada tahapan pengembangan. Kemampuan dari jenis delivery *service* ini yaitu untuk mendukung pengguna dalam menyebarkan aplikasi yang sedang dikerjakan dengan menggunakan bahasa pemrograman dan alat-alat tertentu yang didukung oleh penyedia jasa ke pengguna lainnya melalui fasilitas *cloud*. Para pengguna tidak mengelola atau mengendalikan infrastruktur secara fisik, termasuk jaringan, server, sistem operasi, ataupun media penyimpanan, namun mereka memiliki hak pengendalian secara penuh terhadap aplikasi yang sedang digunakan dan memungkinkan dilakukannya hosting konfigurasi aplikasi di lingkungannya.

c. IaaS (*Infrastructure as a Service*)

*Infrastructure as a Service* (IaaS) merupakan domain dari perangkat keras (hardware), perangkat lunak (*software*) dan perangkat-perangkat jaringan lainnya. IaaS secara umum dikenal sebagai tingkatan lapisan terbawah dari *cloud* delivery *service*. Kemampuan dari jenis delivery *service* ini diberikan kepada pengguna untuk meningkatkan kapasitas dalam hal pengelolaan sistem komputasi, seperti server dan unit-unit pengolahan lainnya, peningkatan media penyimpanan, peningkatan trafik jaringan, dan sumber daya lain yang mendasari sistem komputasi dimana penggunanya dapat menyebarkan dan menjalankan perangkat lunak secara bebas, yang dapat mencakup sistem operasi dan aplikasi. Secara mendasar, para pengguna tidak mengetahui lokasi fisik perangkat yang mereka kelola, pengelolaan dan pengendalian sepenuhnya melalui infrastruktur *cloud* yang disediakan oleh penyedia jasa layanan ini. Akan tetapi, pengguna diberikan pengendalian penuh terhadap sistem komputasi, sistem operasi,

media penyimpanan dan aplikasi yang mereka gunakan. Namun demikian, pengguna dibatasi pengontrolannya yaitu hanya pada komponen jaringan yang dipilih.

### 2.2.2 Microsoft Azure

Microsoft Azure adalah *platform* komputasi awan Microsoft, menyediakan berbagai macam layanan yang dapat digunakan tanpa membeli dan menyediakan perangkat keras sendiri. Azure memungkinkan pengembangan solusi yang cepat dan menyediakan sumber daya untuk menyelesaikan tugas yang mungkin tidak dapat dilakukan di lingkungan lokal. Layanan komputasi, penyimpanan, jaringan, dan aplikasi Azure memungkinkan organisasi untuk fokus membangun solusi hebat tanpa perlu khawatir tentang bagaimana infrastruktur fisik dirakit. Azure menyediakan banyak layanan *platform* komputasi[6].

a. *Compute service*s

   Layanan komputasi Ini termasuk Azure Mesin *Virtual* (Linux dan Windows), App *Service*s (Web Apps, Mobile Apps, Logic Apps, API Apps, and Function Apps), Batch (for large-scale parallel and batch *compute* jobs), RemoteApp, *Service* Fabric, and the Azure Container *Service*.

b. Data *service*s

   Layanan data Ini termasuk Azure Storage (comprised of the Blob, Queue, Table, and Azure Files *service*s).

c. *Application service*s

   Layanan aplikasi ini termasuk layanan yang dapat Anda gunakan untuk membantu membangun dan mengoperasikan aplikasi Anda, seperti Azure Active Directory (Azure AD), *Service Bus for connecting distributed systems*, HDInsight for processing big data, Azure Scheduler, and Azure Media *Service*s.

d. *Network service*s

Layanan jaringan seperti *Virtual Network*s, ExpressRoute, Azure DNS, Azure Traffic Manager, and the Azure Content Delivery *Network*.

### 2.2.3 Virtual *Private* Network

*Virtual Private Network* (VPN) adalah sebuah teknologi komunikasi yang memungkinkan untuk dapat terkoneksi ke jaringan publik dan menggunakannya untuk dapat bergabung dengan jaringan local. 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[7]. Fungsi-fungsi utama VPN antara lain sebagai berikut[8].

a. *Confidentially* (Kerahasiaan)

   Dengan digunakannnya jaringan publik yang rawan pencurian data, maka teknologi VPN menggunakan sistem kerja dengan cara mengenkripsi semua data yang lewat melauinya. 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 Intergrity* (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.

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 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.

### 2.2.4 OpenVPN Acces Server

OpenVPN merupakan aplikasi open-source untuk membuat *Virtual Private Network* (VPN), dimana aplikasi tersebut dapat membuat koneksi point-to-point tunnel yang telah terenkripsi. OpenVPN menggunakan *private* keys, certificate, atau username-password untuk melakukan autentikasi dalam membangun koneksi, dimana untuk enkripsi OpenVPN sendiri menggunakan SSL/TLS yang dimana pembuatan certificate SSL-nya dilakukan oleh OpenSSL yang telah disediakan oleh Linux. Cara kerja OpenVPN adalah sebelumnya pada kedua sisi (server client) harus memiliki jalur internet yang permanen. Apabila perusahaan memiliki router maka router tersebut harus dikonfigurasi firewall-nya agar dapat mencegah akses terhadap jaringan didalamnya dan juga harus dikonfigurasi agar OpenVPN dapat melewati router tersebut.

OpenVPN Access Server adalah sebuah solusi sofware yang mendukung penuh fitur SSL yang mengintegrasikan kemampuan server OpenVPN, kemampuan manajemen perusahaan dan paket *software*

OpenVPN Client yang mengakomodasi Windows, MAC, dan OS Linux. OpenVPN Access Server menggunakan AES-256-GCM secara default[9]. OpenVPN Access Server mendukung berbagai konfigurasi, termasuk akses remote yang aman ke jaringan internal dan atau sumber daya jaringan pribadi serta aplikasi dengan kontrol akses (OpenVPN.net). OpenVPN Access Server mempunyai kelebihan dalam penggunaanya karena menggunakan antarmuka sistem berbasis web, karena itu OpenVPN Access Server relatif mudah di konfigurasi dan gunakan. Dan juga disisi Client jika dengan OpenVPN-Access Server ini Client tidak perlu repot meng-copy file key dan certificate karena client hanya cukup menggunakan browser memasukan alamat VPN Server kemudan Login, setelah login client hanya perlu *download* file berbentuk exe yang di dalamnya sudah disertakan file key dan certificate kemudain menjalankan file exe tersebut untuk menginstal dan mengkonfigurasi OpenVPN client secara otomatis[10].

### 2.2.5 Parameter Pengujian

1. *Download*

   Seberapa cepat menarik data dari server di internet ke perangkat client. Sebagian besar koneksi dirancang untuk mengunduh lebih cepat daripada mengunggah, karena sebagian besar aktivitas online, seperti memuat halaman web atau *streaming* video, terdiri dari unduhan.

2. *Upload*

   Seberapa cepat mengirim data dari perangkat client ke internet. Kecepatan unggah yang cepat sangat membantu saat mengirim file besar melalui email, atau menggunakan obrolan video untuk berbicara dengan orang lain secara online.

3. *Latensi*

   *Delay* (Latency) merupakan waktu yang dibutuhkan data untuk menempuh jarak dari asal ke tujuan. *Delay* dapat dipengaruhi oleh jarak, media fisik, congesti atau juga waktu proses yang lama.