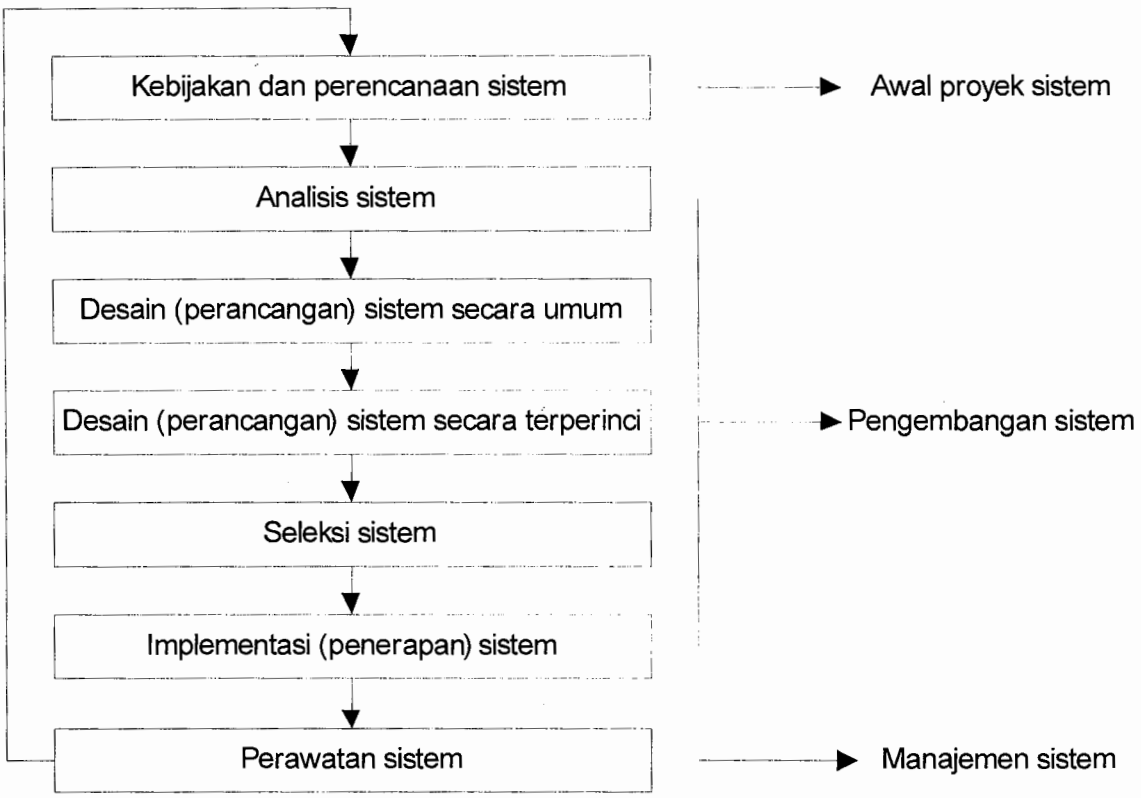
BAB II

LANDASAN TEORI

2.1. Sistem Informasi

Sistem informasi adalah aplikasi komputer untuk mendukung operasi dari suatu organisasi: operasi, instalasi, dan perawatan komputer, perangkat lunak, dan data. Suatu sistem informasi merupakan sekumpulan *hardware, software, brainware,* prosedur dan atau aturan yang diorganisasikan secara integral untuk mengolah data menjadi informasi yang bermanfaat guna memecahkan masalah dan pengambilan keputusan. Sistem Informasi diartikan pula satu kesatuan data olahan yang terintegrasi dan saling melengkapi yang menghasilkan output baik dalam bentuk gambar, suara maupun tulisan. Dalam suatu sistem informasi terdapat sekumpulan komponen pembentuk sistem yang mempunyai keterkaitan antara satu komponen dengan komponen lainnya yang bertujuan menghasilkan suatu informasi dalam suatu bidang tertentu. Dalam sistem informasi diperlukannya klasifikasi alur informasi, hal ini disebabkan keanekaragaman kebutuhan akan suatu informasi oleh pengguna informasi. Kriteria dari sistem informasi antara lain, fleksibel, efektif dan efisien. Siklus hidup pengembangan informatika sistem informasi dapat dilihat pada gambar 2.1:



Gambar 2.1 Siklus Hidup Pengembangan Sistem

2.1.1 Pengertian Sistem Informasi

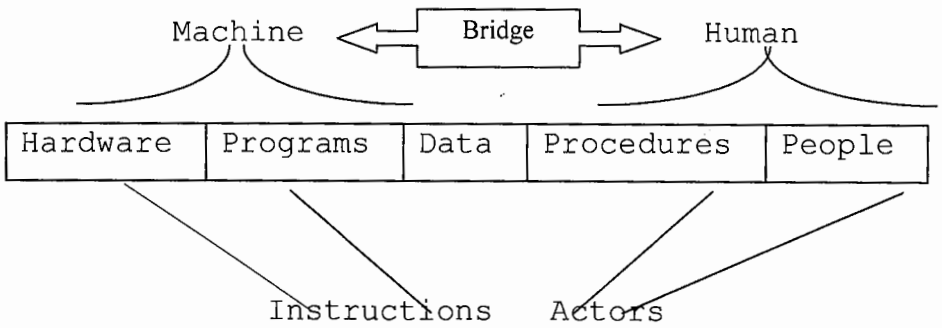
Sistem Informasi bisa diartikan dari kata-kata yang menyusunnya yaitu "Sistem" dan "Informasi". Beberapa pengertian tentang Sistem :

> *"Sistem merupakan kumpulan elemen yang saling kesatuan untuk mencapai tujuan* (Oetomo, 2002)."

> *"Sebuah sistem adalah sekelompok dua atau lebih komponen-komponen yang saling berkaitan (interrelated) atau subsistem-subsistem yang bersatu untuk mencapai tujuan yang sama (common purpose)* (Hall, 2001)."

Sistem adalah suatu himpunan komponen atau variabel yang terorganisasi, saling berinteraksi, saling bergantung satu sama lain dan terpadu. Sebuah sistem terdiri dari komponen-komponen yaitu pekerjaan, kegiatan, misi atau bagian-bagian system yang dibentuk untuk mewujudkan tujuan. Informasi adalah sesuatu yang nyata atau setengah nyata yang dapat mengurangi derajat ketidakpastian tentang suatu keadaan atau kejadian. Kualitas informasi tergantung dari tiga hal yaitu akurat, tepat waktu, dan relevan. Informasi memiliki nilai strategis guna memacu perkembangan bisnis dalam upaya unggul di dalam kompetisi.

Ada lima komponen sistem informasi yaitu *hardware*, *programs*, *data*, *procedures*, dan *people*. Hubungan kelima komponen sistem informasi tersebut dapat dilihat pada gambar 2.20 berikut :



Gambar 2.2 Lima komponen sistem informasi

Suatu Sistem Informasi melibatkan orang-orang pada berbagai tingkat di dalam sebuah organisasi, komputer, program, dan prosedur serta personil untuk mengoperasikan

sistem. Lingkungan adalah faktor eksternal terhadap sistem, ia mencakup semua yang berada di luar pengendali sistem. Sistem Informasi membantu mengendalikan organisasi, sistem informasi harus mempunyai umpan balik bagi unjuk kerja mereka serta harus dikendalikan. Sistem informasi memiliki banyak bagian-bagian khusus.

2.1.2 Kualitas Sistem Informasi

Agar berguna maka informasi harus didukung oleh tiga hal yaitu tepat nilainya atau akurat (*accurate*), tepat waktu (*timeliness*), dan tepat kepada orangnya atau relevan (*relevance*). Keluaran (*output*) yang tidak didukung oleh ketiga hal yang disebut di atas tidak dapat dikatakan sebagai informasi yang berguna, tetapi merupakan sampah (*garbage*) (Jogiyanto, 1999:10). Pengertian dari tiga hal pendukung informasi agar berguna:

Akurat, berarti informasi harus bebas dari kesalahan-kesalahan dan tidak menyesatkan.

Tepat waktu, berarti informasi yang datang pada penerima tidak boleh terlambat atau tepat pada waktunya.

Relevan, berarti informasi tersebut harus mempunyai manfaat untuk pemakainya.

2.2. Sistem Informasi Travel (SoftTravel)

Sistem informasi Travel (SoftTravel) adalah sistem yang akan membantu pihak perusahaan dalam mengelola data secara cepat dan akurat untuk dijadikan informasi yang berguna dalam waktu yang singkat. Data

yang dikelola aplikasi ini berupa data harga, jadwal , data pelanggan, data mitra, data karyawan, data transaksi, data file, data schedule event, data kantor, dan data tour yang di simpan dalam suatu basis data, yang nantinya akan dipakai dalam proses penjualan.

Pemanfaatan informasi yang sudah diolah oleh aplikasi ini akan sangat membantu dalam perkembangan perusahaan seperti :

1. Informasi karyawan akan membantu dalam pengelolaan dan manajemen pegawai dalam perusahaan.
2. Informasi harga dan jadwal kapal/pesawat akan sangat membantu pada saat konsultasi dengan pelanggan, sehingga karyawan akan lebih cepat memberikan saran dan alternatif pilihan yang akan memudahkan pelanggan menentukan pilihan sesuai kebutuhannya.
3. Pengelolaan pelanggan akan membantu dalam mencari informasi detail tentang setiap pelanggan, seberapa sering dia melakukan pembelian, tempat mana aja yang sering di kunjunginya yang nantinya semua informasi tersebut akan berguna dalam strategi pemasaran perusahaan.
4. Informasi mitra akan membantu dalam mencari informasi secara cepat tentang mitra perusahaan seperti alamat, no telepon, dan lain sebagainya.

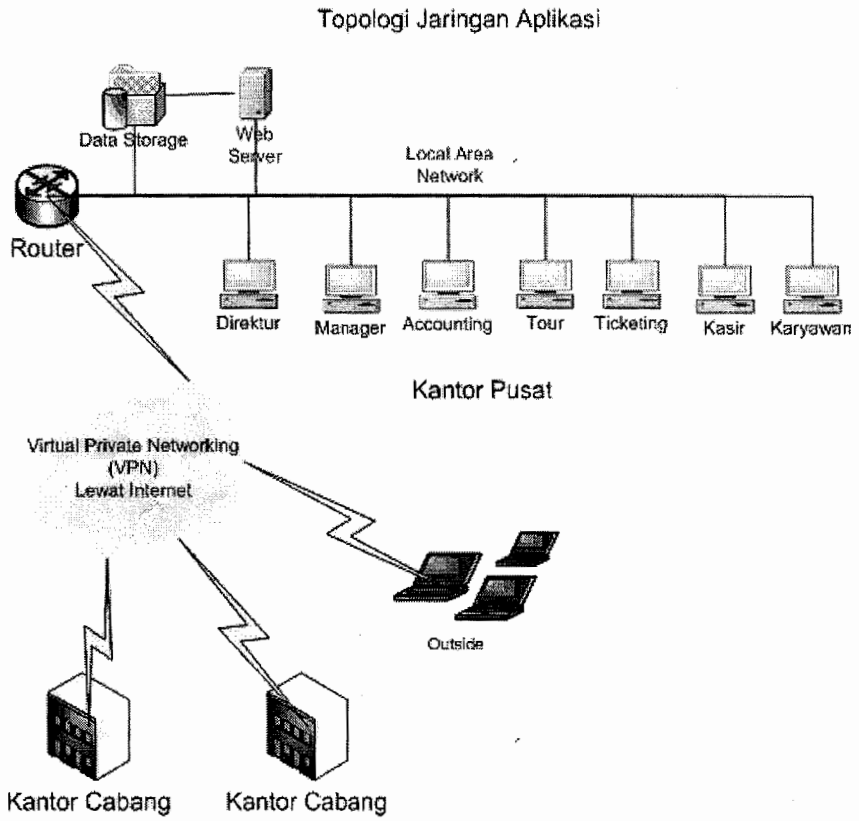
5. Informasi Jadwal Acara (Schedule event) dan Data File membantu Pengelolaan jadwal acara perusahaan (schedule event) dan pengelolaan file document.
6. Pengelolaan jadwal bertujuan memudahkan perusahaan dalam mengelola event (acara) sehingga antara event satu dengan yang lain tidak bertabrakan dan informasi event dapat dengan mudah diakses oleh setiap cabang, sehingga tidak perlu memberitahukan kepada semua cabang secara manual. Sedangkan pengelolaan *file document* memudahkan dalam mencari, menyimpan, mengirim dan mengakses document antar departemen atau bagian unit yang sebagian terpisah secara fisik yang membutuhkan, sehingga menambah efisiensi waktu dan tenaga dalam melakukan pengiriman file .
7. Data *Tour* akan sangat membantu dalam pengelolaan Paket *tour* yang ingin disusun oleh perusahaan agar sesuai dengan strategi pemasaran yang diterapkan. Data Kantor akan mempermudah dalam menyimpan segala informasi tentang perusahaan dan cabang-cabangnya.
8. Data transaksi akan membantu dalam memberikan informasi keuangan perusahaan seperti pengeluaran dan pemasukan sehingga perusahaan dapat dengan mudah mendapatkan informasi untuk menentukan strategi pengembangan perusahaan.

9. Membuat laporan kini tidak lagi menyita banyak waktu dan tenaga, karena dengan aplikasi ini nantinya akan sangat membantu dalam melakukan laporan keseluruhan secara cepat dan mudah. Aplikasi ini memberikan kebebasan bagi perusahaan untuk merancang dan menentukan sendiri jenis dan bentuk laporan dengan mudah seperti laporan keuangan, laporan transaksi, dan lain-lain sehingga sesuai dengan keinginan perusahaan.

Aplikasi ini menangani pengelolaan data antara kantor pusat dan cabang-cabangnya dengan membangun virtual private networking antara kantor pusat dan cabang-cabangnya sehingga datanya terpusat, yang akan memudahkan pengelolaan dan pemeliharaan data. Jaringan dengan menggunakan teknologi VPN akan mengurangi biaya dalam membangun dan merawat jaringan antara kantor pusat dengan kantor-kantor cabang dan dengan menerapkan teknologi enkripsi dan *authentication* akan menjamin keamanan data yang dikirim. Dengan membangun jaringan dengan data terpusat maka akan semakin mudah memonitor dan mengelola semua cabang-cabang yang ada karena semua data yang masuk secara *real time*.

Sistem aplikasi ini berbasis *web* dan *desktop*, baik *web* dan *desktop* memiliki fungsi yang sama. Aplikasi *web* akan digunakan oleh kantor-kantor cabang yang terpisah fisik dengan kantor pusat jika jaringan tidak memungkinkan untuk pemakaian *desktop base*, seperti

memiliki *latency* yang besar atau digunakan oleh departemen yang sedang berada di luar kantor supaya dapat melakukan pekerjaan di luar kantor tetapi bisa berinteraksi dengan data yang ada di kantor sehingga tercapai efisiensi kerja, atau digunakan oleh komputer yang memiliki sistem operasi (OS) yang tidak di support oleh aplikasi berbasis *desktop* (*Windows*), sedangkan aplikasi *desktop* digunakan oleh *user* yang bekerja dengan memanipulasi data yang besar sehingga membutuhkan respon yang cepat.



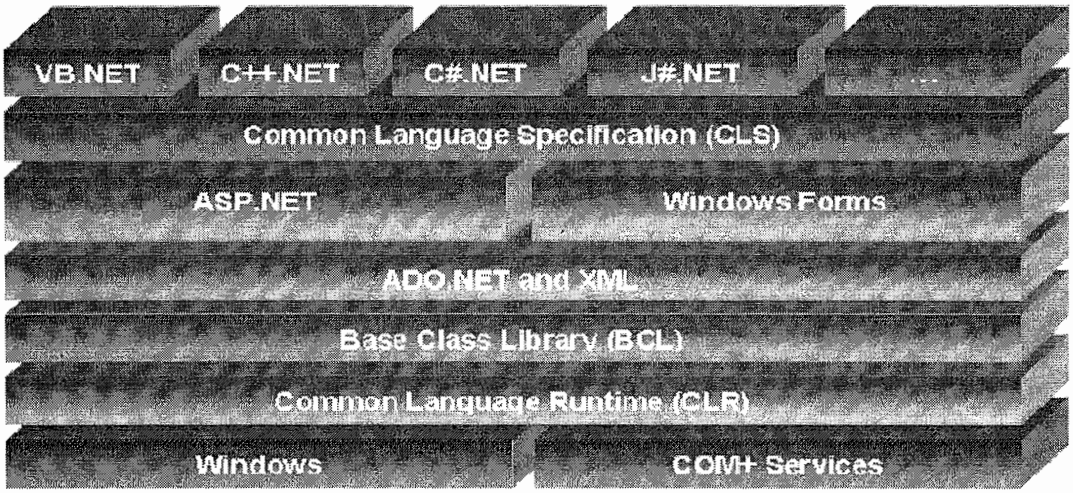
Gambar 2.3 Topologi Jaringan Aplikasi

2.3. .NET Framework

.NET Framework adalah lingkungan untuk membangun, deploying atau menyebarkan, dan menjalankan *sevices Web* dan aplikasi lainnya. *.NET Framework* disusun oleh dua komponen utama yaitu *Common Language Runtimes* (runtime bahasa umum) dan *.NET Framework Class Library* (pustaka *class .NET Framework*).

Secara sederhana *.NET Framework* adalah platform tunggal dimana semua orang dapat mengembangkan aplikasi menggunakan suatu sistem yang mirip dengan JVM (*Java Virtual Machine*). Hanya berbeda dengan Java, tidak ada penghalang bahasa dengan *.NET* sehingga aplikasi dapat dikembangkan menggunakan bahasa : VB, C++, C#, J#, dan bahasa-bahasa pemrograman lain yang kompatibel dengan *.NET Framework*. Tujuan dari *.NET Framework* adalah :

1. Menyediakan lingkungan pemrograman berorientasi objek
2. Menyediakan lingkungan untuk menjalankan suatu kode yang meminimalkan konflik saat software *deployment*/disebarkan dan *versioning*/tentang versi
3. Menyediakan lingkungan untuk menjalankan suatu kode yang menjamin keamanan saat kode dijalankan
4. Menyediakan lingkungan untuk menjalankan suatu kode yang dapat mengeliminasi masalah performa dari lingkungan *scripted* dan *interpreted*
5. Membuat pengembang memiliki pengalaman yang konsisten dalam berbagai tipe aplikasi seperti aplikasi berbasis *Windows* dan aplikasi berbasis *Web*



Gambar 2.4 Arsitektur .NET Framework

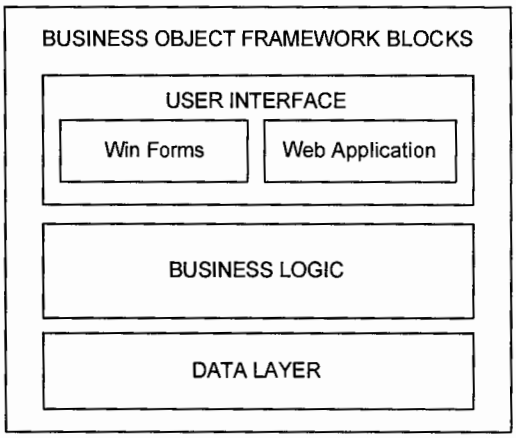
(*msdn.microsoft.com*)

2.4. Business Object Framework

Tanpa sebuah arsitektur, sebuah aplikasi mengabaikan sifat *maintainability* (tingkat kemudahan sistem software untuk dimodifikasi, diperbaiki atau ditingkatkan performance-nya/tune), fleksibilitas (tingkat kemudahan sistem software untuk dikembangkan lebih lanjut dan diintegrasikan dengan sistem lain), dan skalabilitas (tingkat kemampuan sistem software dalam menangani data yang besar/ beban yang berat) serta menjadi terlalu kaku untuk bertahan. Bahkan pembuat *software* sendiri akan mengalami kesulitan untuk mendeteksi *bug* atau memperbaiki kode aplikasi tersebut. Tidak adanya kerangka yang baik menghasilkan kode yang bersifat *monolithic* (satu kesatuan) dan memaksa sistem didesain dalam satu *form* dasar. Ketika dihadapkan dengan logika bisnis (*business logic*) yang sebenarnya dan akses ke data terbatas pada *form*, akan mengakibatkan penerapan *object oriented*

(orientasi objek) tidak bisa dilakukan dan menghasilkan penulisan kode yang sama berulang-ulang. Apabila *business rules* (aturan bisnis) dalam aplikasi harus dirubah atau akses ke data harus dirubah, maka setiap kode yang sama harus dirubah dan dites kembali.

Aplikasi yang mempunyai arsitektur yang baik memiliki batasan-batasan yang memisahkan antara data akses, *business logic* (logika bisnis) dan *user interface* ke dalam *layer-layer* (lapisan-lapisan) yang terpisah. Setelah terpisah, setiap *layer* (lapisan) dapat dengan mudah disentralistik dan dipakai ulang (*reuse*) kembali daripada mengulang kode yang sama. Dengan menggunakan *business object framework* memungkinkan setiap pengembang atau pembuat *software* menjadi lebih cepat dan efisien dalam membuat aplikasi yang benar yaitu dibagi ke dalam *layer* atau lapisan data akses, *business logic* (logika bisnis) dan *user interface*.



Gambar 2.5 Business Object Framework Blocks

(*www.codeproject.com*)

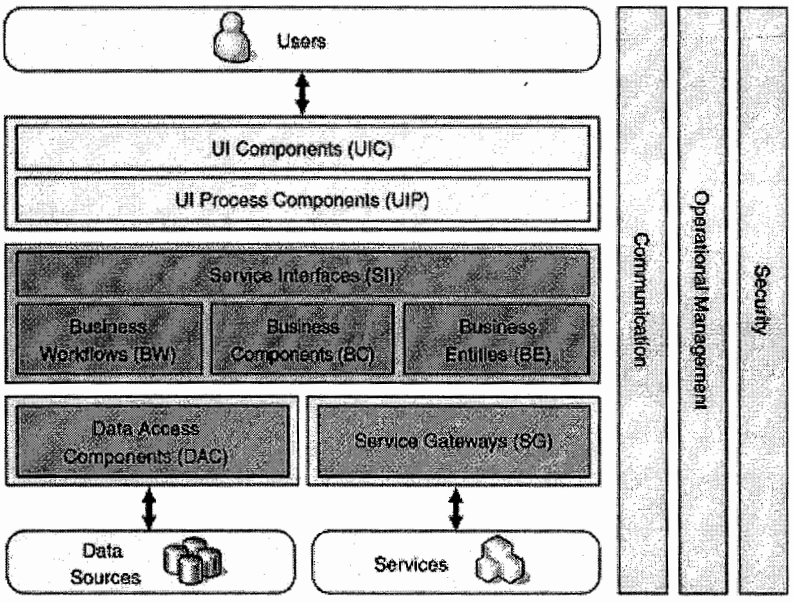
2.4.1 Perbandingan arsitektur *layering* dan arsitektur *tiers*

Sebuah *tier* didefinisikan sebagai sebuah aplikasi terpisah dari modul-modul aplikasi lain berdasarkan proses dan/atau jaringan (*network*) tertentu sedangkan *layering* didefinisikan sebagai pemisahan secara *logic* dalam satu kesatuan. Contoh *one-tier* model seperti Microsoft Access yang sudah menjalankan semua *layering* dalam satu kesatuan proses pada satu komputer. Contoh *two-tier* model seperti aplikasi *client-server* yang mempunyai dua *tier* yang berjalan pada dua komputer. Aplikasi yang memiliki lebih dari dua *tier* melibatkan banyak proses dan banyak komputer. Menambahkan *tiers* dalam suatu aplikasi dapat meningkatkan kompleksitas, penurunan *maintainability* dan menyebabkan permasalahan pada kinerja karena memperbesar *latency* ketika data dikirim dari satu *tier* ke *tier* lain melalui jaringan (*network*). Akan tetapi dalam beberapa kasus aplikasi memerlukan tambahan *tier* karena membutuhkan *scalability* yang tinggi (contoh : melayani > 500 *clients*) dan untuk faktor keamanan (*security*).

Tanpa memperhitungkan jumlah *tier* yang digunakan, arsitektur *layering* yang benar wajib bagi setiap aplikasi. Sebuah arsitektur yang memisahkan aplikasi menjadi beberapa lapisan yang mempunyai keunggulan *simplicity* (kesederhanaan), *scalability* (tingkat kemampuan sistem software dalam menangani data yang besar/ beban yang berat), *maintainability* (tingkat kemudahan sistem software untuk dimodifikasi, diperbaiki

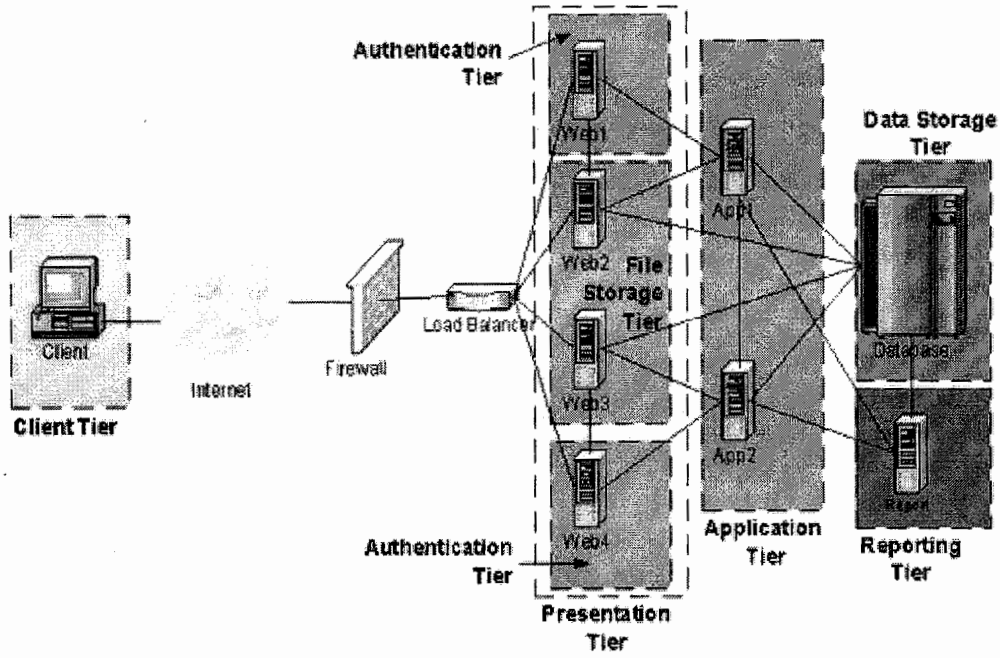
atau ditingkatkan *performance*-nya/*tune*) dan *code reuse* (pemanfaatan kode yang sudah ada). *Business object framework* memiliki 3 *layer* aplikasi *framework* dan dengan menggunakannya, secara otomatis mendapat keuntungan dalam efisiensi waktu dan tenaga.

Terdapat banyak pilihan *framework* untuk jenis ini khususnya yang berjalan pada lingkungan .NET diantaranya CSLA .NET yang dikembangkan oleh Rockford Lhotka (www.lhotka.net), StrataFrame yang dikembangkan oleh perusahaan MicroFour (www.strataframe.net), IdeaBlade Framework yang dikembangkan oleh perusahaan IdeaBlade (www.ideablade.com), XAF Framework yang dikembangkan oleh perusahaan DevExpress (www.devexpress.com). Untuk aplikasi yang akan dibuat oleh penulis dipilih XAF Framework.



Gambar 2.6 Layered Architecture

(msdn.microsoft.com)



Gambar 2.7 N-Tier architecture

(msdn.microsoft.com)

2.5. Jaringan Komputer

Jaringan komputer adalah sebuah sistem yang terdiri atas komputer dan perangkat jaringan lainnya yang bekerja bersama-sama untuk mencapai suatu tujuan yang sama. Tujuan dari jaringan komputer adalah:

1. Membagi sumber daya: contohnya berbagi pemakaian *printer*, *CPU*, *memori*, *harddisk*
2. Komunikasi: contohnya surat elektronik, *instant messaging*, *chatting*
3. Akses informasi: contohnya *web browsing*

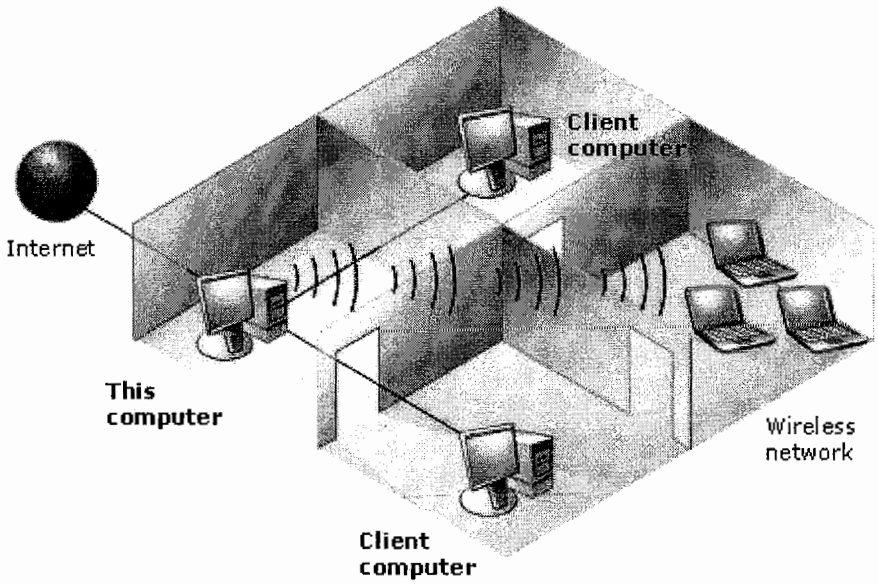
Agar dapat mencapai tujuan yang sama, setiap bagian dari jaringan komputer meminta dan memberikan layanan (service). Pihak yang meminta layanan disebut klien (client) dan yang memberikan layanan disebut pelayan (server). Arsitektur ini disebut dengan sistem client-server, dan digunakan pada hampir seluruh aplikasi jaringan komputer.

Klasifikasi Berdasarkan jangkauan penggunanya:

2. *intranet*
3. *extranet*
4. *Internet*

2.5.1 Intranet

Intranet (*Internal Network*) mulai didengung-dengungkan pada pertengahan tahun 1995 oleh beberapa penjual produk jaringan yang mengacu pada kebutuhan informasi dalam bentuk *Web* di dalam perusahaan. Intranet merupakan jaringan komputer dalam perusahaan yang menggunakan komunikasi data standar seperti dalam Internet. Artinya, semua fasilitas *Internet* dapat digunakan untuk kebutuhan dalam perusahaan (atau dalam suatu organisasi). Dengan kata lain, *Intranet* dapat dikatakan ber-*internet* dalam lingkungan yang terbatas.



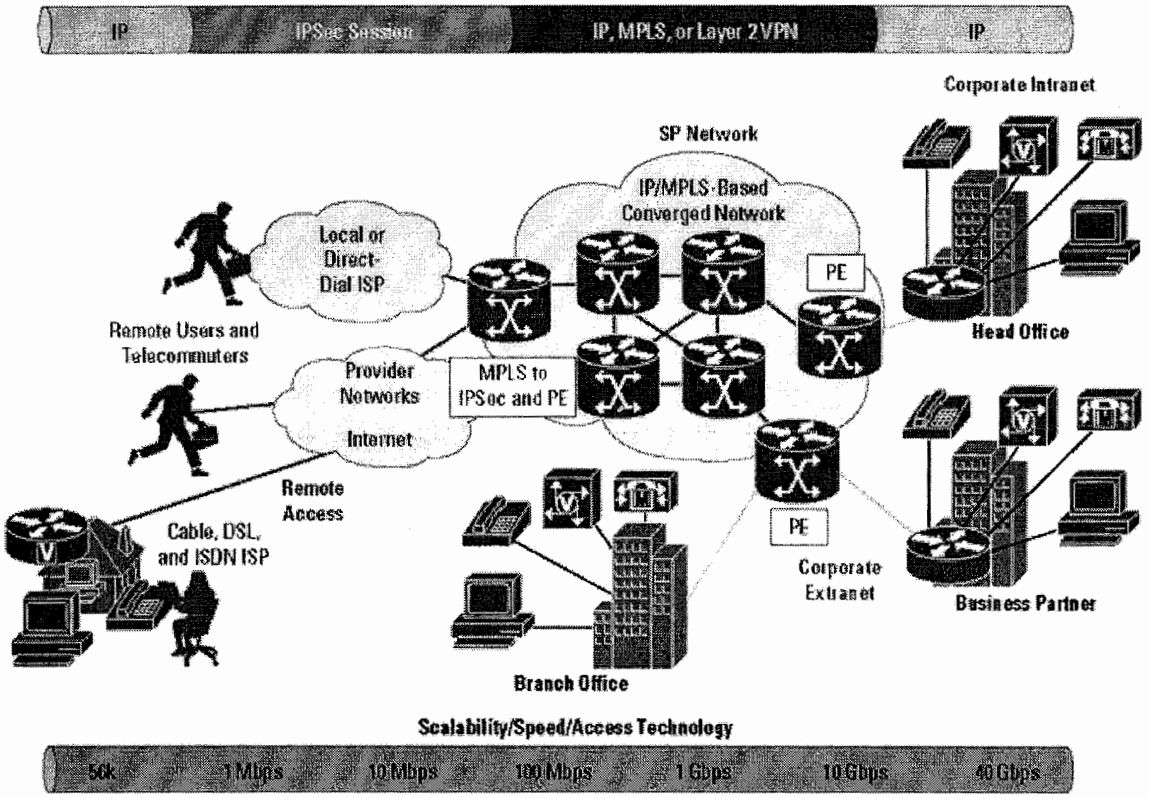
Gambar 2.8 Topologi Jaringan Intranet

(msdn.microsoft.com)

2.5.2 *extranet*

Extranet adalah istilah yang mengacu pada suatu *intranet* yang secara parsial bisa diakses oleh pihak luar yang memiliki otorisasi. Dari sisi posisinya *intranet* berada dibalik *firewall* dan hanya bisa diakses oleh user yang menjadi anggota dari perusahaan atau organisasi yang bersangkutan. Tetapi kebalikannya dengan *extranet*.
Extranet menyediakan beragam *level* akses kepada pihak luar. Anda bisa mengakses *extranet* hanya jika memiliki *username* dan *password* yang *vaild*, dan identitas Anda menentukan bagian-bagian mana dari *extranet* yang bisa diakses.

Extranet sangat penting arti dan kegunaannya bagi para mitra bisnis dalam hal pertukaran informasi.



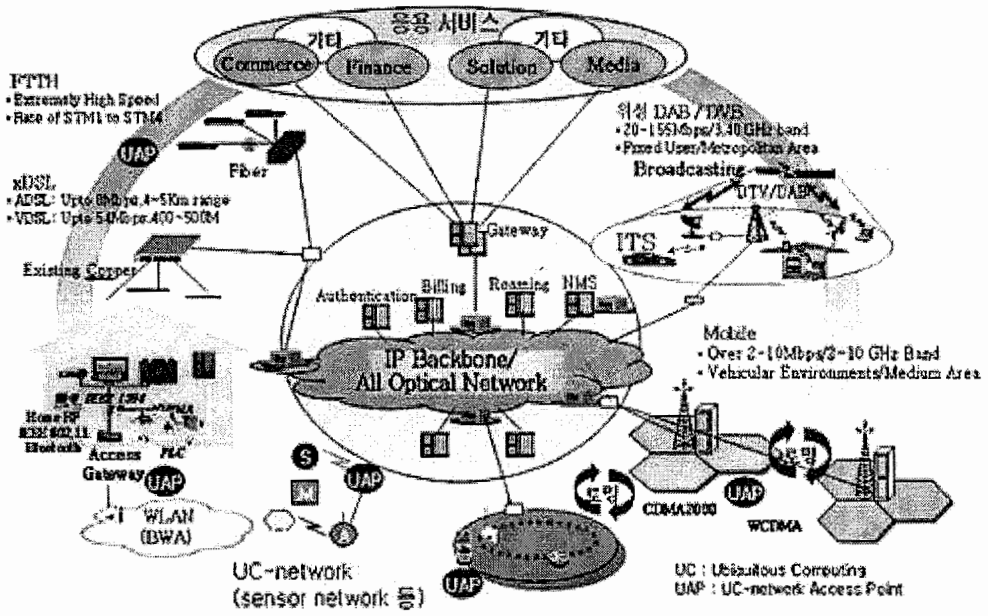
Gambar 2.9 Topologi Jaringan *Ekstranet*

(www.technet.com)

2.5.3 *Internet*

Secara umum, teknologi yang digunakan antara *Internet*, *Extranet* dan *Intranet* adalah sama. Namun demikian terdapat perbedaan antara *Internet* dengan *Intranet* dilihat dari perspektif jangkauan dan penggunaannya. Pada *Internet*, lingkupnya adalah global, komunikasi lewat saluran telekomunikasi publik, dan penggunanya bisa siapa saja tanpa membedakan posisi seseorang dalam kaitannya

dengan isi informasi. Pada *Intranet* dan *extranet*, cakupannya lebih terbatas, yakni di dalam organisasi. Hubungannya antar kelompok kerja atau departemen di dalam perusahaan, penggunaannya oleh komunitas yang sudah ditentukan.



Gambar 2.10 Topologi Jaringan Internet

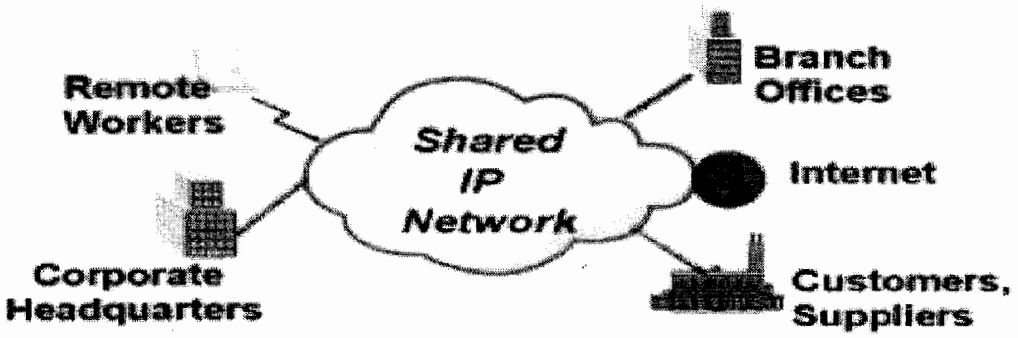
(*www.learnethernet.com*)

2.6. Virtual Private Network (VPN)

Virtual private network (VPN) berkembang pada saat perusahaan besar memperluas jaringan bisnisnya, namun mereka tetap dapat menghubungkan jaringan lokal (*private*) antar kantor cabang dengan perusahaan mitra kerjanya yang berada di tempat yang jauh. Perusahaan juga ingin memberikan fasilitas kepada pegawainya (yang memiliki hak akses) yang ingin terhubung ke jaringan lokal milik

perusahaan di manapun mereka berada. Perusahaan tersebut perlu suatu jaringan lokal yang jangkauannya luas, tidak bisa diakses oleh sembarang orang, tetapi hanya orang yang memiliki hak akses saja yang dapat terhubung ke jaringan lokal tersebut.

Implementasi jaringan tersebut dapat dilakukan dengan menggunakan *leased line*. Namun biaya yang dibutuhkan untuk membangun infrastruktur jaringan yang luas menggunakan *leased line* sangat besar. Di sisi lain perusahaan ingin mengoptimalkan biaya untuk membangun jaringan mereka yang luas. Oleh karena itu VPN dapat digunakan sebagai teknologi alternatif untuk menghubungkan jaringan lokal yang luas dengan biaya yang relatif kecil, karena transmisi data teknologi VPN menggunakan media jaringan publik yang sudah ada (misalnya internet).



Gambar 2.11 Topologi Jaringan VPN

2.6.1 Definisi Virtual Private Network (VPN)

VPN merupakan suatu jaringan komunikasi lokal yang terhubung melalui media jaringan publik. Infrastruktur publik yang paling banyak digunakan adalah internet. Untuk memperoleh komunikasi yang aman (*private*) melalui internet, diperlukan protokol khusus untuk mengatur pengamanan datanya.

Perusahaan / organisasi yang ingin membuat *wide area network* (WAN) dapat menggunakan VPN sebagai alternatif dalam implementasinya. Penggunaan *leased line* sebagai implementasi WAN membutuhkan investasi yang sangat besar. Dibutuhkan pengeluaran ribuan dolar (USD) setiap bulannya untuk memperoleh hak istimewa menggunakan kabel yang tak dapat digunakan oleh perusahaan / organisasi / orang lain.

2.6.2 Keuntungan menggunakan VPN

Ada beberapa keuntungan yang dapat diperoleh dengan menggunakan VPN untuk implementasi WAN. **Pertama,** jangkauan jaringan lokal yang dimiliki suatu perusahaan akan menjadi luas, sehingga perusahaan dapat mengembangkan bisnisnya di daerah lain. Waktu yang dibutuhkan untuk menghubungkan jaringan lokal ke tempat lain juga semakin cepat, karena proses instalasi infrastruktur jaringan dilakukan dari perusahaan / kantor cabang yang baru dengan ISP (*internet service provider*) terdekat di daerahnya. Sedangkan penggunaan *leased line* sebagai WAN akan membutuhkan waktu yang lama untuk membangun jalur koneksi khusus dari kantor cabang yang

baru dengan perusahaan induknya. Dengan demikian penggunaan VPN secara tidak langsung akan meningkatkan efektivitas dan efisiensi kerja.

Kedua, penggunaan VPN dapat mereduksi biaya operasional bila dibandingkan dengan penggunaan *leased line* sebagai cara tradisional untuk mengimplementasikan WAN. VPN dapat mengurangi biaya pembuatan jaringan karena tidak membutuhkan kabel (*leased line*) yang panjang. Penggunaan kabel yang panjang akan membutuhkan biaya produksi yang sangat besar. Semakin jauh jarak yang diinginkan, semakin meningkat pula biaya produksinya. VPN menggunakan internet sebagai media komunikasinya. Perusahaan hanya membutuhkan kabel dalam jumlah yang relatif kecil untuk menghubungkan perusahaan tersebut dengan pihak ISP terdekat.

Media internet telah tersebar ke seluruh dunia, karena internet digunakan sebagai media komunikasi publik yang bersifat terbuka. Artinya setiap paket informasi yang dikirimkan melalui internet, dapat diakses dan diawasi bahkan dimanipulasi, oleh setiap orang yang terhubung ke internet pada setiap saat. Setiap orang berhak menggunakan internet dengan syarat dia memiliki akses ke internet. Untuk memperoleh akses ke internet, orang tersebut dapat dengan mudah pergi ke warnet (warung internet) yang sudah banyak tersebar di Indonesia. Oleh karena itu untuk memperoleh komunikasi yang aman, perlu protokol tambahan yang khusus dirancang untuk mengamankan data yang dikirim melalui internet, sehingga data tersebut hanya dapat diakses oleh pihak tertentu saja.

Penggunaan VPN juga dapat mengurangi biaya telepon untuk akses jarak jauh, karena hanya dibutuhkan biaya telepon untuk panggilan ke titik akses yang ada di ISP terdekat. Pada beberapa kasus hal ini membutuhkan biaya telepon SLJJ (sambungan langsung jarak jauh), namun sebagian besar kasus cukup dengan biaya telepon lokal. Berbeda dengan penggunaan *leased line*, semakin jauh jarak antar terminal, akan semakin mahal biaya telepon yang digunakan.

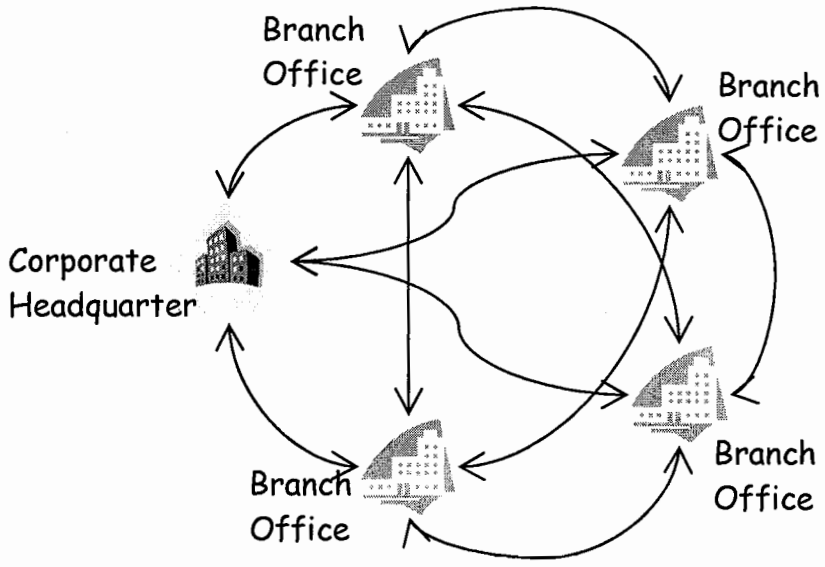
Biaya operasional perusahaan juga akan berkurang bila menggunakan VPN. Hal ini disebabkan karena pelayanan akses *dial-up* dilakukan oleh ISP, bukan oleh perusahaan yang bersangkutan. Secara teori biaya operasional ISP yang dibebankan kepada perusahaan bisa jauh lebih kecil daripada biaya operasional akses *dial-up* tersebut ditanggung perusahaan itu sendiri karena biaya operasional ISP itu ditanggung bersama-sama oleh ribuan pelanggan ISP tersebut.

Ketiga, penggunaan VPN akan meningkatkan skalabilitas. Perusahaan yang tumbuh pesat akan membutuhkan kantor cabang baru di beberapa tempat yang terhubung dengan jaringan lokal kantor pusat. Bila menggunakan *leased line*, penambahan satu kantor cabang membutuhkan satu jalur untuk membangun WAN. Penambahan satu kantor cabang baru lagi (dua kantor cabang) akan membutuhkan dua tambahan jalur, masing-masing ke kantor pusat dan ke kantor cabang terdahulu. Jika mereka memiliki kantor cabang yang ke-3, dibutuhkan enam jalur untuk menghubungkan semua kantor. Jika ada empat kantor

cabang, maka dibutuhkan 10 jalur seperti terlihat pada gambar 2.

Berbeda dengan penggunaan *leased line*, penambahan satu kantor cabang hanya membutuhkan satu jalur, yaitu jalur yang menghubungkan kantor cabang yang baru dengan ISP terdekat. Selanjutnya jalur dari ISP akan terhubung ke internet yang merupakan jaringan global. Dengan demikian penggunaan VPN untuk implementasi WAN akan menyederhanakan topologi jaringannya.

Keempat, VPN memberi kemudahan untuk diakses dari mana saja, karena VPN terhubung ke internet. Sehingga pegawai yang *mobile* dapat mengakses jaringan khusus perusahaan di manapun dia berada. Selama dia bisa mendapatkan akses ke internet ke ISP terdekat, pegawai tersebut tetap dapat melakukan koneksi dengan jaringan khusus perusahaan. Hal ini tidak dapat dilakukan jika menggunakan *leased line* yang hanya dapat diakses pada terminal tertentu saja.



Gambar 2.12 Jumlah jalur *leased line* untuk 5 kantor

(www.bebas.vlsm.org)

Kelima, investasi pada VPN akan memberikan peluang kembalinya investasi tersebut (ROI = *return on investment*) yang lebih cepat daripada investasi pada *leased line*. Berdasarkan artikel "*Delivering Profitable Virtual Private LAN Services - Business Case White Paper*" bulan November 2003, telah dilakukan studi kasus pada kota berukuran medium di Amerika Utara. Artikel tersebut menunjukkan bahwa dengan beberapa asumsi parameter yang disimpulkan pada tabel 1, VPN dapat mengembalikan nilai investasi dalam 2.1 tahun. Bahkan dengan peningkatan penetrasi pasar dan perubahan kecenderungan pelanggan untuk menyewa *bandwidth* yang besar akan mempercepat jangka waktu ROI, yaitu dalam 1 tahun.

Assumptions Parameter		2.1 Year Payback	1 Year Payback
Market Penetration		12.50%	15%
Year 1 Adoption Rate		4%	8%
# of Sites per Medium Enterprise		5	8
Subscriber BW % of Total Subs by BW	1.5Mbps	5.0 %	5.0 %
	6Mbps	45.0 %	20.0 %
	10Mbps	35.0 %	45.0 %
	45Mbps	10.0 %	10.0 %
	100Mbps	5.0 %	20.0 %

Tabel 2.1. Perbandingan parameter yang menentukan jangka waktu ROI

2.6.3 Kerugian menggunakan VPN

VPN juga memiliki kelemahan yaitu **pertama**, VPN membutuhkan perhatian yang serius pada keamanan jaringan publik (internet). Oleh karena itu diperlukan tindakan yang tepat untuk mencegah terjadinya hal-hal yang tidak diinginkan seperti penyadapan, *hacking* dan tindakan *cyber crime* pada jaringan VPN.

Kedua, ketersediaan dan performansi jaringan khusus perusahaan melalui media internet sangat tergantung pada faktor-faktor yang berada di luar kendali pihak perusahaan. Kecepatan dan keandalan transmisi data melalui internet yang digunakan sebagai media komunikasi jaringan VPN tidak dapat diatur oleh pihak pengguna jaringan VPN, karena *traffic* yang terjadi di internet melibatkan semua pihak pengguna internet di seluruh dunia.

Ketiga, perangkat pembangun teknologi jaringan VPN dari beberapa vendor yang berbeda ada kemungkinan tidak dapat digunakan secara bersama-sama karena standar yang ada untuk teknologi VPN belum memadai. Oleh karena itu

fleksibilitas dalam memilih perangkat yang sesuai dengan kebutuhan dan keuangan perusahaan sangat kurang.

Keempat, VPN harus mampu menampung protokol lain selain IP dan teknologi jaringan internal yang sudah ada. Akan tetapi IP masih dapat digunakan VPN melalui pengembangan IPSec (*IP Security Protocol*).

2.6.4 Jenis Implementasi VPN

2.6.4.1 *Remote access* VPN

Pada umumnya implementasi VPN terdiri dari 2 macam. Pertama adalah *remote access* VPN, dan yang kedua adalah *site-to-site* VPN. *Remote access* yang biasa juga disebut *virtual private dial-up network* (VPDN), menghubungkan antara pengguna yang *mobile* dengan *local area network* (LAN).

Jenis VPN ini digunakan oleh pegawai perusahaan yang ingin terhubung ke jaringan khusus perusahaannya dari berbagai lokasi yang jauh (*remote*) dari perusahaannya. Biasanya perusahaan yang ingin membuat jaringan VPN tipe ini akan bekerjasama dengan *enterprise service provider* (ESP). ESP akan memberikan suatu *network access server* (NAS) bagi perusahaan tersebut. ESP juga akan menyediakan *software* klien untuk komputer-komputer yang digunakan pegawai perusahaan tersebut.

Untuk mengakses jaringan lokal perusahaan, pegawai tersebut harus terhubung ke NAS dengan men-*dial* nomor telepon yang sudah ditentukan. Kemudian dengan menggunakan *software* klien, pegawai tersebut dapat terhubung ke jaringan lokal perusahaan.

Perusahaan yang memiliki pegawai yang ada di lapangan dalam jumlah besar dapat menggunakan *remote access* VPN untuk membangun WAN. VPN tipe ini akan memberikan keamanan, dengan mengenkripsi koneksi antara jaringan lokal perusahaan dengan pegawainya yang ada di lapangan. Pihak ketiga yang melakukan enkripsi ini adalah ISP.

2.6.4.2. *Site-to-site* VPN

Jenis implementasi VPN yang kedua adalah *site-to-site* VPN. Implementasi jenis ini menghubungkan antara 2 kantor atau lebih yang letaknya berjauhan, baik kantor yang dimiliki perusahaan itu sendiri maupun kantor perusahaan mitra kerjanya. VPN yang digunakan untuk menghubungkan suatu perusahaan dengan perusahaan lain (misalnya mitra kerja, *supplier* atau pelanggan) disebut **ekstranet.** Sedangkan bila VPN digunakan untuk menghubungkan kantor pusat dengan kantor cabang, implementasi ini termasuk jenis **intranet** *site-to-site* VPN.

2.6.5. Metode Pengamanan Jaringan VPN

Seperti telah dijelaskan sebelumnya, teknologi jaringan VPN menggunakan internet sebagai media transmisi data ke tempat yang dituju. Oleh karena itu pengamanan transmisi data melalui internet menjadi hal yang sangat substansial untuk diperhatikan agar diperoleh komunikasi yang aman.

Beberapa metode pengamanan data yang dapat dilakukan pada teknologi jaringan VPN antara lain dengan menggunakan *firewall*. Pengamanan bisa juga dilakukan dengan melakukan enkripsi pada data yang akan dikirim melalui internet. Selain itu, data dapat juga dikirim menggunakan protokol khusus yang aman untuk transmisi data melalui internet (IPSec). Alternatif lain pengendalian keamanan jaringan VPN adalah dengan menggunakan metode AAA server yang akan memeriksa autentikasi, autorisasi dan merekam segala sesuatu yang dilakukan pengguna pada suatu jaringan.

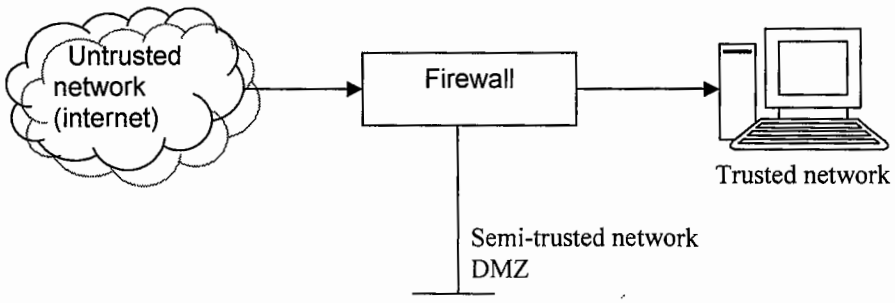
2.6.5.1. *Firewall*

Firewall merupakan sekumpulan komponen yang diletakkan antara dua jaringan. Komponen tersebut terdiri dari komputer, *router* yang dirancang sebagai *buffer* antara jaringan publik dan jaringan internal (*private*). Fungsi dari *firewall* adalah untuk membatasi akses ke jaringan internal yang terhubung ke jaringan publik (misal internet). Akses ke jaringan tersebut hanya diperbolehkan bagi orang-orang yang memiliki autorisasi terhadap jaringan tersebut. Arsitektur *firewall* dapat dilihat pada gambar 3.

Komponen utama pembangun *firewall* adalah

1. metode yang digunakan
2. aturan kebijakan keamanan jaringan (*policy*)
3. mekanisme autentikasi

Pada saat ini terdapat dua jenis metode *firewall* yang umum digunakan yaitu *packet filtering router* dan *proxy server*.



Gambar 2.13 Arsitektur *firewall*

(www.bebas.vlsm.org)

2.6.5.2. Enkripsi

Enkripsi merupakan teknik untuk mengamankan data yang dikirim dengan mengubah data tersebut ke dalam bentuk sandi-sandi yang hanya dimengerti oleh pihak pengirim dan pihak penerima data. Teknik enkripsi pada komputer berdasarkan pada perkembangan ilmu kriptografi. Dahulu kriptografi banyak digunakan pada bidang militer. Tujuannya adalah untuk mengirimkan informasi rahasia ke tempat yang jauh. Namun saat ini enkripsi telah banyak digunakan untuk aplikasi-aplikasi seperti informasi kartu kredit, PIN (*personal identity number*), informasi tabungan di bank dan lain sebagainya. Enkripsi yang

banyak digunakan saat ini adalah enkripsi kunci simetris dan enkripsi kunci publik.

2.6.5.2.1 Kunci Simetris

Pada enkripsi menggunakan kunci simetris, setiap komputer memiliki kunci rahasia (kode) yang dapat digunakan untuk mengenkripsi informasi sebelum informasi tersebut dikirim ke komputer lain melalui jaringan. Kunci yang digunakan untuk mengenkripsi data sama dengan kunci yang digunakan untuk mendekripsi data. Oleh karena itu, kunci tersebut harus dimiliki kedua komputer.

Kunci harus dipastikan ada pada computer penerima. Artinya pengirim harus memberitahu kunci yang digunakan pada penerima melalui orang yang dipercaya. Selanjutnya informasi yang akan dikirim, dienkripsi menggunakan kunci tersebut. Sehingga penerima bisa mendekripsi, dan mendapatkan informasi yang diinginkan. Contoh sederhana kunci simetris mengganti huruf yang sebenarnya dengan 2 huruf di bawahnya. Misalnya "A" menjadi "C" dan "B" menjadi "D". Kunci tersebut harus diketahui oleh penerima. Jika penerima tidak memiliki kunci, informasi tersebut tidak ada gunanya. Pada enkripsi ini, pihak penerima mengetahui kunci pihak pengirim.

2.6.5.2.2 Kunci Publik

Enkripsi kunci publik menggunakan kombinasi kunci privat dan kunci publik. Kunci privat hanya diketahui oleh pihak pengirim informasi. Sedangkan kunci publik dikirim ke pihak penerima. Untuk mendekripsi informasi,

pihak penerima harus menggunakan kunci public dan kunci privat miliknya. Kunci privat penerima berbeda dengan kunci privat pengirim, dan hanya penerima saja yang mengetahuinya.

Enkripsi kunci publik memerlukan perhitungan yang besar. Akibatnya sebagian besar sistem menggunakan kombinasi kunci public dan kunci simetri untuk proses enkripsi data. Pada saat dua komputer akan berkomunikasi secara aman, komputer A akan membuat kunci simetris dan dikirim ke komputer B menggunakan enkripsi kunci publik. Setelah itu kedua komputer dapat berkomunikasi menggunakan enkripsi kunci simetris. Setelah proses komunikasi tersebut selesai, kunci simetris untuk sesi tersebut dibuang. Jika kedua komputer ingin membentuk sesi komunikasi yang aman lagi, kunci simetris untuk sesi tersebut harus dibuat lagi. Dengan demikian setiap akan membentuk suatu sesi, kunci simetris baru akan dibuat.

Algoritma kunci publik dibuat berdasarkan algoritma "*hashing*". Kunci publik dibuat berdasarkan nilai "*hash*" yang diperoleh. Ide dasar enkripsi kunci publik adalah perkalian dua bilangan prima yang menghasilkan bilangan prima yang baru. Contohnya diberikan pada tabel di bawah ini.

Angka masukan	Algoritma "hashing"	Nilai "hash"
10667	Masukan x 143	1525381

Tabel 2.2. Algoritma "*hashing*'

Angka masukan merepresentasikan informasi yang akan dikirim. Nilai "*hash*" merupakan representasi informasi yang telah dienkripsi. Dari hasil di atas dapat ditunjukkan bahwa nilai "*hash*" 1525381 sangat sulit untuk dicari faktor-faktor bilangan primanya kalau tidak memiliki kuncinya. Namun kalau kuncinya (pengali) diketahui, sangat mudah untuk mendapatkan informasi aslinya. Algoritma kunci publik yang sebenarnya jauh lebih rumit dari contoh ini. Contoh ini adalah ide dasar munculnya algoritma kunci publik.

Kunci publik umumnya menggunakan algoritma yang lebih kompleks, dan nilai "*hash*" yang sangat besar mencapai 40-bit atau bahkan 128-bit. Jika nilai "*hash*" dibangun menggunakan 128-bit, akan ada 2^{128} kombinasi yang muncul. Nyaris tidak mungkin untuk memecahkan enkripsi ini tanpa ada kuncinya.

2.6.5.3. AAA Server

AAA server, singkatan dari *authentication*, *authorization* dan *accounting*, merupakan program *server* yang bertugas untuk menangani permintaan akses ke suatu komputer dengan menyediakan proses autentikasi, otorisasi dan akunting (AAA). AAA merupakan cara yang cerdas untuk mengendalikan akses ke suatu komputer, menerapkan kebijakan, memeriksa penggunaan komputer dan menyediakan informasi yang diperlukan untuk keperluan tagihan (pembayaran). Kombinasi proses ini sangat efektif untuk menyediakan manajemen dan keamanan jaringan.

Proses pertama yang dilakukan adalah autentikasi, yaitu proses untuk mengidentifikasi pengguna. Proses ini bekerja berdasarkan kenyataan bahwa setiap pengguna memiliki beberapa kriteria yang unik untuk masing-masing pengguna. Biasanya proses ini dilakukan dengan meminta pengguna untuk memasukkan *user name* dan *password*-nya. Jika masukan pengguna sesuai dengan data yang ada di *database*, pengguna tersebut berhak mengakses komputer / jaringan. Namun bila masukan ini gagal, pengguna tersebut tidak bisa mengakses komputer / jaringan tersebut.

Setelah proses autentikasi, setiap pengguna harus memiliki otorisasi untuk melakukan tugas-tugas tertentu. Sebagai contoh, setelah pengguna tersebut masuk ke jaringan yang dituju, pengguna tersebut mencoba untuk memberikan beberapa perintah pada jaringan tersebut. Proses otorisasi akan menentukan apakah pengguna tersebut dapat memberikan perintah seperti yang diinginkan atau tidak. Sehingga otorisasi dapat didefinisikan sebagai proses untuk menerapkan kebijakan untuk menentukan aktivitas, sumber dan layanan apa saja yang dapat diperoleh suatu pengguna. Biasanya proses otorisasi juga dilakukan pada saat proses autentikasi.

Proses terakhir adalah akunting yang berfungsi untuk menghitung jumlah *resource* yang digunakan setiap pengguna pada saat akses dilakukan, diantaranya waktu yang digunakan, atau besarnya data yang dikirim atau diterima selama akses berlangsung. Proses ini dilakukan berdasarkan informasi yang ada pada catatan (*log*) masing-masing pengguna. Catatan ini dapat digunakan untuk

mengendalikan otoritas masing-masing pengguna, analisis kecenderungan pengguna, mengamati pemanfaatan *resource*, dan perencanaan.