BAB II
TINJAUAN PUSTAKA

2.1 Tinjauan Pustaka

Penelitian ini didasarkan pada peninjauan dari hasil penelitian sebelumnya, yaitu Pengembangan Aplikasi *Backup dan Restore* secara Automatisasi Menggunakan SDLC untuk Mencegah Bencana (Andry, 2017). Manfaat penelitian ini adalah untuk membantu individu ataupun organisasi agar terhindar dari kegagalan sistem, kerusakan *file* atau gangguan lainnya. *Backup* menurut penelitian ini adalah sebuah proses penduplikasian data ke media yang berbeda dan terpisah, dimana nantinya hasil dari penduplikasian tersebut akan digunkan untuk pemulihan data jika terjadi kerusakan. *Backup* yang dilakukan dalam penelitian ini adalah *backup* yang dilaksanakan secara berkala dan berkelanjutan untuk menghindari kehilangan data yang dapat merugikan individu ataupun organisasi. Hasil dari penelitian tersebut adalah aplikasi *backup* dan *restore* secara automatisasi dapat melakukan *backup* dengan baik.

Penelitian tentang perancangan sistem otomatisasi *backup* data pada STMIK TIME Medan (Wijaya, Robet, & Robin, 2015), memaparkan tentang *backup* data secara otomatis untuk menjaga keamanan data di STMIK TIME Medan. *Backup* dalam penelitian ini mengacu pada menyalin data, dimana data yang sudah disalin dapat di-*restore* kembali apabila terjadi kehilangan data. Tujuan utama dari *backup* data yang ada di STMIK TIME Medan adalah mengembalikan data yang hilang akibat bencana alam dan mengembalikan data yang hilang akibat kesalahan penghapusan atau korupsi data.

Penelitian selanjutnya tentang Replikasi Basis Data pada Sistem Pengolahan Data Akademik Universitas Katolik Santo Thomas (Silitonga, 2014). Replika menurut penelitian ini adalah suatu tindakan meng-*copy* atau penduplikasian data dari satu tempat ke tempat lain secara *realtime.* Data yang telah di replika atau diduplikat akan tersinkronisasi dengan data awal. Dengan adanya replikasi, data yang ada dapat didistribusikan ke lokasi yang berbeda dengan koneksi jaringan lokal maupun internet. Hasil dari penelitian ini adalah terjaminnya keamanan data akademik yang ada di Universitas Katolik Santo Thomas.

Penelitian selanjutnya yang berjudul Analisis Perbandingan Metode Replikasi *Server* untuk Kebutuhan Pemulihan Bencana (Studi Kasus Sistem Informasi Geografis Perusahaan XYZ) menjelaskan tentang perbandingan metode replikasi *server* yang ada di perusahaan XYZ. Metode replikasi *server* ada 3 yaitu *Physical to Physical, Physical to Virtual VMware Converter* dan *Physical to Virtual Baremetal Restore. Physical to Physical* adalah metode replikasi *server* dari *server* fisik ke *server* fisik yang mempunyai spesifikasi yang sama. *Physical to Virtual VMware Converter* adalah metode replikasi *server* dari *server* fisik ke *server virtual* dengan aplikasi *VMware*. *Physical to Virtual Baremetal Restore* adalah metode replikasi *server* dari *server* fisik ke *server virtual* melalui media penyimpanan *tape* (Azizah, Aknuranda, & Yahya, 2017).

Penelitian tentang *Enhancing Security Concerns in Cloud Computing Virtual Machines : (Case Study on Central Bank of Sudan)* menjelaskan tentang perbandingan *backup* data menggunakan *Symantec NetBackup, Veeam Backup and Replication* dan *Dell AppAssure*. Dari penelitian tersebut dapat diketahui

bahwa *Veeam Backup* adalah pilihan solusi terbaik untuk melakukan *backup* data dengan *server virtual* dibandingkan *software backup* yang lainnya (Hassan & Hilles, 2014).

Berdasarkan tinjauan pustaka di atas, maka ditampilkan tabel penelitian sebagai pembanding penelitian terdahulu terhadap sistem replikasi dan *backup server* yang akan dikembangkan (Lihat pada Tabel 1).

Tabel 1 Tinjauan Pustaka

Peneliti	Tahun	Kesimpulan Penelitian
Johanes Fernandes Andry	2017	*Backup* adalah sebuah proses penduplikasian data ke media yang berbeda dan terpisah, dimana nantinya hasil dari penduplikasian tersebut akan digunkan untuk pemulihan data jika terjadi kerusakan. *Backup* harus dilaksanakan secara berkala dan berkelanjutan untuk menghindari kehilangan data yang dapat merugikan individu ataupun organisasi. Hasil dari penelitian ini merupakan *backup* dan *restore* data yang berjalan dengan baik.
Edi Wijaya, Robet & Robin	2015	*Backup* data mengacu pada menyalin data, dimana data yang sudah disalin dapat di-*restore* kembali apabila terjadi kehilangan data. *Backup* data memiliki 2 tujaun yaitu untuk mengembalikan data yang hilang akibat bencana alam atau mengembalikan data yang hilang akibat kesalahan penghapusan atau korupsi data.
Parasian D.P. Silitonga	2014	Replika adalah suatu tindakan meng-*copy* atau penduplikasian data dari satu tempat ke tempat lain secara *realtime.* Data yang telah di replika atau diduplikat akan tersinkronisasi dengan data awal. Dengan adanya replikasi, data yang ada dapat didistribusikan ke lokasi yang berbeda dengan koneksi jaringan lokal maupun internet.

Peneliti	Tahun	Kesimpulan Penelitian
Ulfa Khoirul Azizah, Ismiarta Aknuranda & Widhi Yahya	2017	Dalam analisa metode replikasi *server*, metode yang dipakai ada 3 yaitu *Physical to Physical*, *Physical to Virtual VMware Converter* dan *Physical to Virtual Baremetal Restore.*
Samah Sabir M. Hassan & Shadi M. S. Hilles	2014	Dalam penelitian ini, diketahui bahwa *Veeam Backup* adalah pilihan terbaik untuk *software backup* yang menggunakan *virtual server* dibandingkan dengan *Symantec NetBackup* dan *Dell AppAssure.*

Berdasarkan hasil penelitian terdahulu, peneliti akan membuat sebuah proyek replika dan *backup server* untuk membantu meningkatkan ketersediaan data yang terbukti berjalan baik seperti pada penelitian yang dilakukan oleh (Andry, 2017), (Wijaya et al., 2015), (Silitonga, 2014) dan dengan menggunakan konsep replika *server* yaitu *Physical to Virtual VMware Converter* yang dipaparkan oleh (Azizah et al., 2017) serta menggunakan *software backup* dan replikasi *Veeam Backup and Replication* (Hassan & Hilles, 2014).

2.2 Landasan Teori

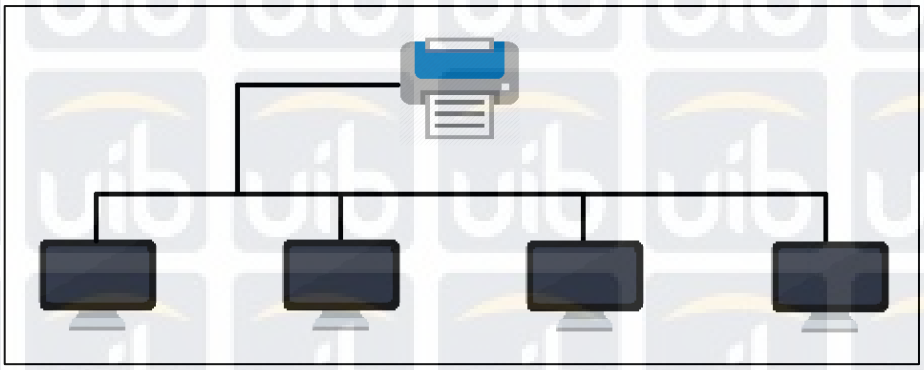
Dalam membuat sebuah replika dan *backup server*, penulis membuat sebuah landasan teori. Landasan teori ini adalah kumpulan dari teori-teori yang digunakan untuk memperkuat teori dalam penelitian penulis. Teori yang digunakan dalam penelitian ini adalah sebagai berikut:

2.2.1 Jaringan Komputer

Jaringan komputer adalah himpunan interkoneksi antara dua komputer tunggal ataupun beberapa komputer yang dihubungkan dengan media transmisi seperti kabel ataupun tanpa kabel yang disebut dengan *wireless* (Sari, Sudarsono, & Hayadi, 2013).

Data yang dibagikan sesama pengguna komputer adalah data yang dibawa oleh *transmitter* (pengirim) ke *receiver* (penerima). Data yang dikirim tersebut bergerak dari media transmisi kabel ataupun tanpa kabel, sehingga pengguna komputer dalam suatu jaringan dapat saling bertukar data atau file dan juga berbagi perangkat komputer seperti printer (Masykur & Karaman, 2016).

Pada umumnya, jaringan komputer yang kompleks diawali dari jaringan dengan bentuk yang sederhana. Jaringan komputer yang kompleks ini dapat menghubungkan banyak komputer, yang tentunya tidak didukung oleh hanya satu atau dua media transmisi, tetapi oleh banyak media dan peralatan komputer (lihat gambar 1).



Gambar 1 : Jaringan Komputer Sederhana

Local Area Network (LAN) adalah sebuah jaringan yang memiliki jangkauan area yang kecil dan dibatasi oleh ruang lingkup lingkungan saja (Sari et

al., 2013). LAN merupakan jaringan lokal yang biasanya digunakan untuk menghubungkan komputer pribadi dan *workstation* dalam area yang kecil seperti sebuah perusahaan (Wijaya et al., 2015). Jadi, dapat disimpulkan bahwa, LAN merupakan jaringan lokal yang memiliki jangkauan area yang relatif kecil dan digunakan untuk menghubungkan komputer pribadi dalam suatu lingkungan tertentu.

Kecepatan jaringan dipengaruhi oleh beberapa faktor yaitu: jumlah banyaknya pengguna, jenis media transmisi yang digunakan, kemampuan *hardware* yang terhubung, efisiensi *software* dan LAN *Port* dalam jaringan (Boavida, Triyono, & Sutanta, 2013). Kecepatan jaringan LAN dalam pengiriman data sangat tinggi. Kecepatan pengiriman data pada jaringan LAN umumnya berkisar antara 10-1000 Mbps. Jaringan LAN pada umumnya, banyak menggunakan media kabel sebagai media transmisi untuk mengirimkan data dari satu komputer ke komputer lainnya.

Metropolitan Area Network (MAN) adalah sebuah jaringan yang merupakan gabungan dari beberapa LAN. MAN menghubungkan komputer satu dengan lainnya yang berada pada jangkauan wilayah yang lebih luas dari LAN tetapi lebih sempit dari WAN dengan jangkauan antara 10-50 km. dalam pembuatan jaringan MAN diperlukan operator telekomunikasi sebagai penghubung antara jaringan komputer (Dedy Haryanto & Riadi, 2014).

Wide Area Network (WAN) adalah sebuah jaringan yang mencakup area yang berskala luas. Radius jaringan ini mencakup sebuah negara dan benua. Beberapa faktor yang mempengaruhi jaringan ini yaitu: *Bandwidth*, Teknologi, *Skalability, Support IP Based, Easy Configuration & Maintenance, Low Cost* dan

Security (Rosmiati, 2016). WAN berfungsi untuk menghubungkan jaringan LAN atau jaringan MAN yang memiliki jarak yang sangat jauh. Untuk menghubungkan jaringan ini diperlukan saluran telepon sebagai media penghubung (Wijaya et al., 2015). Singkatnya, WAN merupakan gabungan dari beberapa jaringan LAN atau MAN yang memiliki jangkauan jaringan yang luas yang saling terhubung ke internet. Jaringan WAN menggunakan alat komunikasi seperti modem dan jaringan internet untuk saling berhubungan satu sama lainnya

Peer to peer adalah jaringan yang kedua *client* dan *server*nya dapat menjalankan aturan *client* dan *server* dalam satu komputer. Dalam hal ini, baik *client* ataupun *server* dapat melakukan fungsi yang sama. *Client* dapat menjadi *server* dan *server* dapat menjadi *client*. Dikarenakan semua komputer dalam jaringan ini mempunyai fungsi yang sama, jaringan ini tidak memiliki pusat utama untuk mengontrol komputer. Pengguna dapat berbagi data dari komputernya sendiri dengan pengguna komputer lain didalam satu jaringan yang sama. Dalam jaringan ini, tidak ada komputer yang memiliki prioritas lebih tinggi dari yang lainnya, sehingga tidak memiliki batasan dalam berbagi dan mengakses data dengan komputer lain (Anwar & Riadi, 2013), lihat gambar 2.

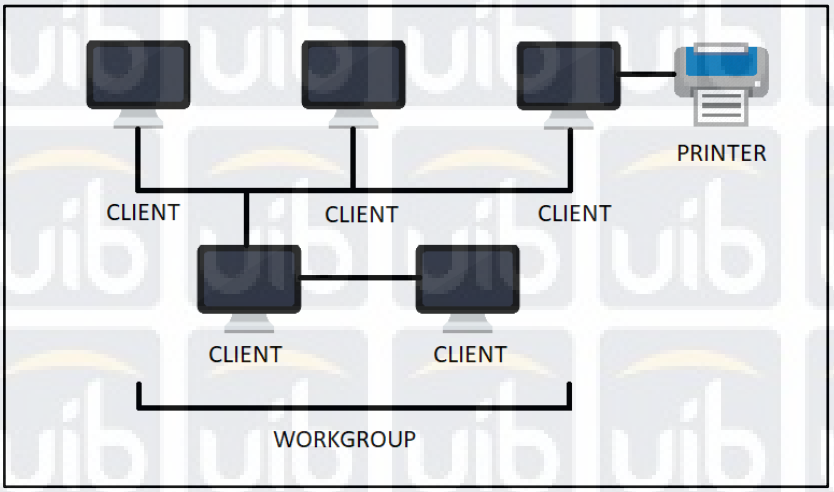
Keunggulan tipe jaringan *peer to peer* menurut Zunaidi, Andika, & Saniman (2014), yaitu:

1. Seluruh komputer yang terhubung dalam jaringan ini memiliki prioritas dan hak yang sama.
2. Biaya yang dibutuhkan lebih murah dikarenakan tidak menggunakan sebuah komputer *server*.

3. Kelancaran jaringan yang ada, tidak tergantung pada jaringan komputer *server*.

Sedangkan kelemahan jaringan *peer to peer* menurut Zunaidi et al. (2014), yaitu:

1. Sistem *troubleshooting* jaringan ini rumit, dikarenakan jaringan ini melibatkan seluruh komputer yang ada dalam jaringan untuk saling berkomunikasi.
2. Sistem keamanan jaringan tidak terpusat, melainkan ditentukan oleh pengguna komputer untuk menentukan keamanan fasilitas komputer yang digunakan.
3. Sistem *backup* tidak terpusat, melainkan terdapat pada masing-masing komputer dan *backup* pun dilakukan oleh masing-masing komputer.



Gambar 2: Jaringan *Peer to Peer*

Client adalah komputer pengguna layanan atau fasilitas dari *server* dan sebagai antar muka komputer dengan manusia. Sedangkan *server* adalah penyedia layanan atau fasilitas untuk digunakan oleh *client* yang terhubung dalam jaringan (Sari et al., 2013).

Hubungan antara *client* dan *server* dapat dikatakan sebagai *request-response.* Secara singkat yaitu *client* meminta informasi, dan *server* merespon dengan cara menyediakan informasi yang telah diminta oleh *client* atau dengan menolak permintaan *client* (lihat gambar 3).

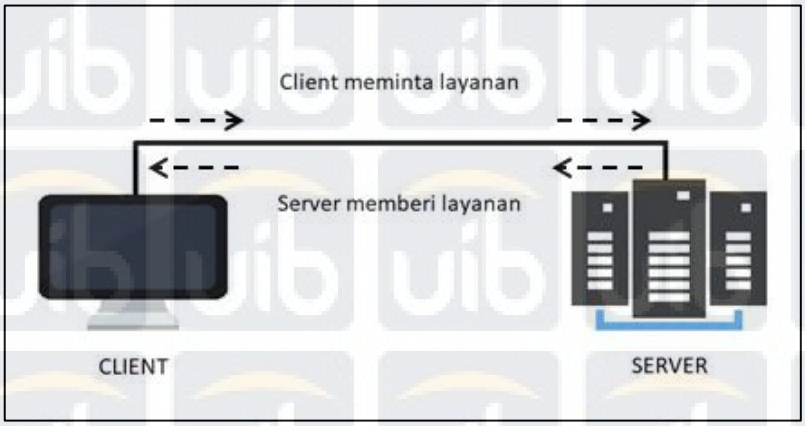
Keunggulan jaringan dengan tipe *client server* menurut Zunaidi et al. (2014), yaitu:

1. Komputer *server* berfungsi sebagai pusat data dan komputer *client* dapat mengambil data dari komputer *client* mana pun yang terhubung dalam jaringan. Jika pada salah satu komputer *client* terjadi kerusakan, pengguna masih dapat mengambil data dari komputer *client* yang lain.
2. Penyedian layanan dan pengelolaan fasilitas jaringan yang dilakukan komputer *server* membuat akses data lebih tinggi, tetapi komputer *server* tidak terbebani dengan aksesdata tersebut.
3. Sistem *backup* data yang ada dalam tipe jaringan ini lebih baik, karena *backup* data dilakukan secara terpusat dikomputer *server.* Jika terjadi kerusakan data di komputer *client,* maka masih terdapat *backup* data di komputer *server.*

Sedangkan kelemahan tipe jaringan *client server* menurut Zunaidi et al. (2014), yaitu:

1. Membutuhkan biaya yang mahal, dikarenakan komputer *server* harus memiliki kemampuan yang tinggi agar dapat memberikan layanan dan fasilitas bagi seluruh komputer *client* yang ada.

2. Kelancaran jaringan pada tipe jaringan ini bergantung pada komputer *server.* Jika terjadi masalah pada komputer *server,* maka seluruh jaringan yang ada akan mengalami gangguan.



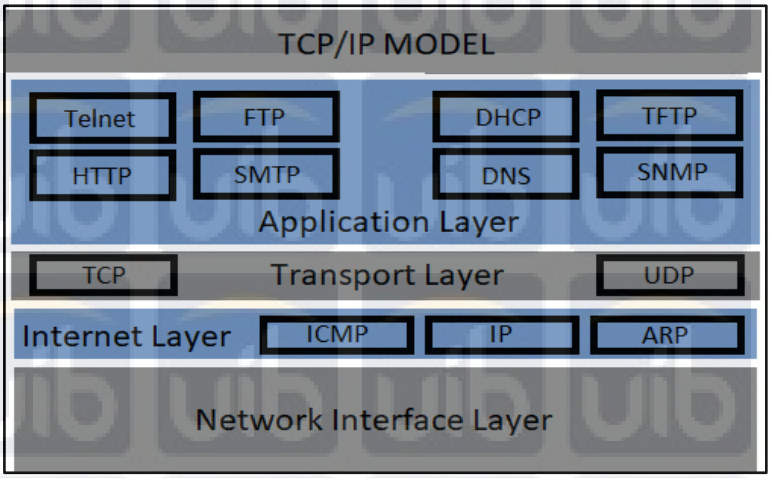
Gambar 3: *Client Server*

Dalam jaringan komputer, tentu saja ada media yang digunakan untuk menghubungkan jaringan agar dapat berinteraksi satu dengan yang lainnya atau sering dikenal dengan media transmisi. Media jaringan ini dapat berbentuk media kabel (*Wired Network*) dan non kabel (*Wireless Network*). Media jaringan dengan kabel dapat memanfaatkan berbagai bentuk kabel, seperti: kabel Coaxial, kabel STP, kabel UTP dan kabel *Fiber Optic* (Zunaidi et al., 2014). Sedangkan media jaringan tanpa kabel (*wireless*) memiliki 2 tipe jaringan yaitu: ad-hoc dan infrastruktur. Jaringan *wireless* ad-hoc adalah jaringan yang sangat sederhan dimana jaringan ini tidak memerlukan *access point* untuk saling terhubung. Sedangkan jaringan *wireless* infrastruktur adalah jaringan yang menggunakan *access point* untuk menghubungkan PC/laptop agar dapat saling berinteraksi (Wibowo, Rosmiati, & Sularsa, 2016).

TCP/IP (*Transmission Control Protocol/Internet Protocol*) adalah suatu standar atau aturan untuk tukar menukar data dan informasi dari satu komputer ke

komputer lainnya dalam sebuah komunitas internet (Wardoyo, Ryadi, & Fahrizal, 2014).

TCP/IP ini adalah protokol yang pada umumnya digunakan di dalam dunia jaringan. TCP/IP memungkinkan pengguna komputer berkomunikasi secara mudah melalui *platform* dan sebagai dasar untuk internet yang mendunia. TCP/IP merupakan kumpulan dari beberapa protokol (*protocol suite*). Pada dasarnya, TCP/IP tidak memiliki basis yang sama dengan OSI model, melainkan menggunakan basis model DARPA. TCP/IP hanya terdiri dari 4 lapisan yaitu *Network Interface Layer Protocol*, *Internet Layer Protocol*, *Transport Layer Protocol* dan *Application Layer Protocol* yang dapat dilihat pada gambar 4.



Gambar 4: TCP/IP Model

2.2.2 Internet

Internet adalah suatu jaringan yang dapat menghubungkan komputer satu dengan yang lainnya melalui suatu saluran dan *server* di seluruh belahan dunia. Internet ini dapat menghubungkan banyak komputer kedalam satu jaringan berupa komputer pribadi maupun komputer korporasi (Nurdin, 2015). Internet merupakan penerapan dan bagian dari WAN. Internet menggunakan TCP/IP sebagai protokol

untuk dapat bertukar data dan juga melayani permintaan layanan dari pengguna internet diseluruh bagian dunia (Wijaya et al., 2015). Jadi, dapat disimpulkan bahwa internet adalah sebuah penerapan dari jaringan WAN yang merupakan gabungan dari beribu-ribu jaringan yang ada di seluruh dunia.

Menurut Sari et al. (2013), ada beberapa jenis koneksi internet dilihat dari koneksi fisik, koneksi logika, IP *external*/*internal* dan IP dinamik/stakomputer.

1. Koneksi Fisik

   Yang termasuk dalam koneksi fisik yaitu *ethernet*, modem, ADSL, satelit, waveLAN. Dari segi konfigurasi, koneksi ini dapat dilihat sebagai *Point to Point* dan *Point to Multipoint*.
2. Koneksi Logika

   Yang ternasuk dalam koneksi ini yaitu IP *Address* dan *subnetting.*
3. IP *External*/*Internal*

   Yang dimaksud dengan IP *external* adalah IP yang sah untuk dipakai di jaringan internet sedunia dan IP *internal* adalah IP yang hanya boleh digunakan di jaringan intranet.
4. IP Dinamik/Stakomputer

   IP dinamik adalah IP komputer yang diberikan oleh ISP melalui DHCP dan akan berubah secara periodik sedangkan IP stakomputer adalah IP tetap yang diisi saat mengkonfigurasi jaringan.

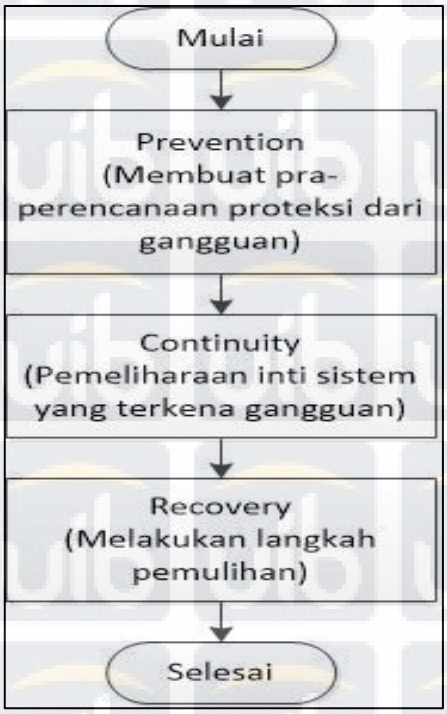
2.2.3 *Disaster Recovery Plan* (DRP)

Disaster atau bencana adalah kejadian yang bersifat merusak dengan waktu yang tidak dapat diprediksi dan tidak diharapkan. Berbagai bencana alam

menurut Putra, Sari, & Fairuzabadi (2017), adalah bencana alam yang disebabkan oleh kondisi geografis dan geologis, bencana yang disebabkan oleh faktor lingkungan dan sistem elektrik seperti kebakaran dan kerusakan jaringan listrik, serangan teroris, sistem atau perangkat yang rusak, kesalahan operasional akibat ulah manusia dan *virus*.

Menurut Saputro (2016), *Disaster Recovery Plan* merupakan suatu aturan atau prosedur yang dirancang untuk menangani kondisi darurat yang bertujuan untuk meminimalisir kerusakan terhadap fungsi-fungsi penting dalam suatu sistem. *Disaster Recovery Plan* berfokus pada penggunaan IT yang ditujukan untuk penyelamatan atau pemulihan sistem ataupun aplikasi dan infrastruktur komputer. Menurut Afif & Suryono (2013), *Disaster Recovery Plan* merupakan kemampuan organisasi dalam menghadapi becana dan gangguan dengan melakukan implementasi pemulihan fungsi kritis dalam organisasi. Menurut Azizah et al., (2017), *Disaster Recovery Plan* adalah rencana pemulihan cepat dari situasi darurat yang dihasilkan bencana dan hanya memberi dampak minimum pada organnisasi. Sedangkan menurut Putra et al. (2017), *Disaster Recovery Plan* adalah suatu perencanaan pemulihan bencana. Dari penjelasan sebelumnya, dapat disimpulkan bahwa *Disaster Recovery Plan* adalah perancangan pemulihan sistem secara cepat dan sesuai dengan prosedur suatu organisasi yang berfokus pada penggunaan IT dalam menghadapi situasi darurat yang disebabkan oleh bencana atau gangguan, bertujuan untuk meminimalisir kerusakan dan kerugian terhadap fungsi penting sistem serta menjamin kemampuan organisasi dalam menyelesaikan permasalahan yang terjadi dan memastikan kegiatan operasional organisasi dan perusahaan tetap berjalan sebagaimana mestinya.

Disaster Recovery Plan (DRP) menurut Afif & Suryono (2013), terdiri atas 3 fase perencanaan yaitu proteksi yang dilakukan pada saat pra-bencana (*prevention*), pengatasan bencana yang dilakukan pada saat terjadinya bencana (*continuity*) dan pemulihan yang dilakukan pada saat pasca bencana (*recovery*) yang dapat dilihat pada gambar 5 dibawah ini:



Gambar 5: Proses Perencanaan DRP

Berikut penjelasan proses perencanaan DRP diatas:

1. *Prevention* (pra-bencana)

   Pada fase ini, perusahaan membutuhkan pra-perencanaan proteksi seperti perencanaan pembuatan *server backup* dan *server* replika serta pelatihan untuk pemulihan (*recovery)* bagi organisasi dan perusahaan. Pada penelitian ini, penulis memakai bidang ini sebagai tahap proteksi data didalam *server*.

   Keuntungan yang dihasilkan dari fase ini adalah adanya kemampuan yang maksimal dari perusahaan untuk pulih dari bencana.

2. *Continuity* (pengatasan saat terjadi bencana)

   Dalam fase ini, perusahaan melakukan pemeliharaan inti sistem dan sumber daya perusahaan yang ada.

   Keuntungan yang dihasilkan dari fase ini adalah tetap berjalannya operasional perusahaan walaupun dalam keadaan terjadinya bencana.

3. *Recovery* (pasca bencana)

   Dalam fase ini, perusahaan melakukan langkah-langkah untuk pemulihan (*recovery*) sesuai dengan prosedur perusahaan sampai operasional perusahaan berjalan seperti biasanya.

   Keuntungan yang dihasilkan dari fase ini adalah kegiatan operasional perusahaan dapat berjalan normal setelah terjadinya bencana.

Dalam pembangunan *Disaster Recovery Plan*, terdapat beberapa proses yang bertahap. Dalam tahap pembangunan DRP biasanya tidak selalu sama karena tergantung pada kebutuhan dan tujuan pembuatannya. Menurut Yuliadi & Nugroho (2016), ada 4 tahapan umum yang biasanya dilakukan dalam proses pembangunan DRP dapat dilihat pada gambar 6 dibawah ini:

Gambar 6: Proses Pembangunan DRP

Berikut penjelasan proses pembangunan DRP diatas:

1. *Risk Assesment*

   Tahap ini merupakan tahap untuk mengidentifikasi ancaman-ancaman yang berkemungkinan terjadi dan menimbulkan resiko kerusakan dalam sebuah perusahaan. Dalam tahapan ini, perusahaan memperkirakan ancaman dan resiko yang akan timbul dari yang terkecil sampai yang terbesar sehingga nantinya dapat digambarkan cara pananganan atau solusi dari masalah tersebut.

2. *Priority Assesment*

   Tahap ini merupakan tahap untuk menyusun proses pemulihan sistem dengan berdasarkan prioritas. Dalam tahap ini, dibuat sebuah prosedur

dalam pemulihan sistem dengan mempertimbangkan data mana yang akan diselamatkan terlebih dahulu sesuai dengan tingkat kepentingan data bagi perusahaan. Proses pemulihan dalam fase ini juga disusun menurut prioritas proses yang dianggap lebih penting sehingga proses yang diutamakan adalah proses yang memiliki prioritas lebih dari proses yang lain.

3. *Recovery Strategy Selection*

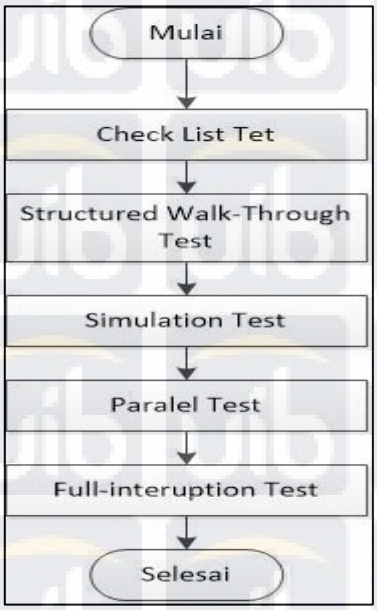
   Tahap ini merupakan tahap untuk mengidentifikasi strategi dan perancangan pemulihan (*recovery*) dengan tahapan yang jelas dan terstruktur. Tahap ini mencakup penyediaan fasilitas *backup* dan *recovery.* Kriteria-kriteria yang harus diperhatikan dalam memilih strategi pemulihan, yaitu strategi pemulihan harus memenuhi syarat dari tahapan sebelumnya, bersifat *cost effective* jika dibandingkan dengan resiko dan prioritasnya dan strategi yang dipilih harus dapat diterapkan dalam kondisi saat ini ataupun kondisi yang akan datang.

4. *Plan Documenting*

   Tahap ini merupakan tahap dokumentasi dari hasil tahap-tahap sebelumnya. Tahap ini tentunya sangat penting, tanpa adanya dokumentasi yang dapat menyimpan rancangan strategi yang telah dipilih, maka tahapan sebelumnya tidak berarti sama sekali dikarenakan tidak adanya dokumentasi sebagai pedoman yang pasti dalam strategi pemulihan.

Pengujian adalah tahap terpenting dari *Disaster Recovery Plan.* Dalam tahap ini akan dilakukan uji coba terhadap teori DRP yang sudah dirancang dan akan diterapkan dalam sebuah perusahaan. Pengujian ini harus dilakukan sesuai

dengan urutan prosedur yang telah disetujui, mengikuti standar yang ada dalam perusahaan dan disimulasikan dengan keadaan yang sebenarnya (Irfansyah, Saedudin, & Rahmat, 2018). Pengujian DRP terbagi menjadi lima bentuk yang dapat dilihat pada gambar 7 dibawah ini:



Gambar 7: Proses Pengujian DRP

Berikut penjelasan proses pengujian DRP diatas:

1. *Check List Test*

   Dalam tes ini, setiap unit manajemen dalam perusahaan akan memeriksa kembali apakah perencanaan DRP ini sesuai dengan prosedur yang ada dan apakah layak untuk dipakai oleh perusahaan.

2. *Structured Walk-Through Test*

   Dalam tes ini, setiap perwakilan dari unit manajemen akan melakukan pertemuan untuk membahas isi perencanaan secara keseluruhan. Tes ini bertujuan untuk memeriksa dan memastikan bahwa perencanaan DRP ini adalah perencanaan yang akurat dan dapat menunjukkan kemampuan

organisasi dalam menjalankan sistem *recovery* disetiap organisasi yang ada dalam perusahaan.

3. *Simulation Test*

   Dalam tes ini, semua orang yang terlibat dalam simulasi harus memandang bahwa keadaan darurat dalam simulasi adalah keadaan darurat yang sebenarnya. Tes ini dilakukan untuk mengetahui kesiapan setiap personil perusahaan dalam menangani keadaan darurat yang terjadi.

4. *Paralel Test*

   Dalam tes ini, simulasi yang dilakukan disesuaikan dengan tahap pemulihan secara keseluruhan. Tes ini berjalan paralel antara proses pemulihan dan proses kerja yang sebenarnya. Tujuan dari tes ini adalah untuk memastikan bahwa sistem utama berjalan dengan baik dalam lokasi *backup*, sama dengan sistem yang sebenarnya.

5. *Full-interuption Test*

   Dalam tes ini, bencana disimulasikan dengan sebenar-benarnya sehingga memiliki resiko yang sangat besar. Tetapi dalam tes ini akan terlihat kesiapan perusahaan dalam menangani bencana yang terjadi.

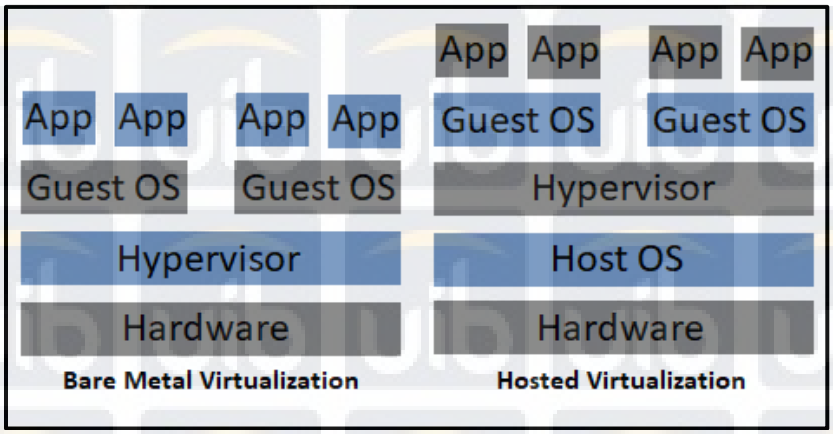
2.2.4 Virtualisasi

Virtualisasi merupakan teknik untuk membuat sesuatu yang berbentuk *virtual* (tidak nyata). Virtualisasi memungkinkan berjalannya sistem operasi dengan kapasitas kecil dan memungkinkan sebagian besar sumber daya pada perangkat keras komputer tidak sepenuhnya digunakan. Virtualisasi memungkinkan banyak aplikasi atau operasi dapat mengakses dan menggunakan

sumber daya yang sama. Hal ini sangat membantu dalam mengurangi kapasitas memori yang digunakan dan mengurangi biaya pada sistem jika dibandingkan dengan penggunaan memori perangkat keras pada umumnya (Sarddar & Bose, 2014).

Perangkat lunak virtualisasi memiliki kemampuan untuk membuat komputer secara *virtual*. Aplikasi virtualisasi dapat membuat sebuah *virtual machine* (VM) yang memungkinkan pengguna dapat menjalankan sebuah sistem komputer pada VM (Hernawan, 2013). *Virtual Machine* (VM) adalah sebuah penerapan perangkat lunak (*virtual*) dari mesin komputer fisik yang dapat menjalankan sistem sama persis dengan komputer secara fisik pada umumnya.

Terdapat dua jenis virtualisasi yaitu *bare metal* dan *hosted.* Perbedaan antara kedua virtualisasi ini terdapat pada tempat *hypervisor* pada susunan lapisan virtualisasi (lihat gambar 8). *Hypervisor* adalah lapisan perangkat lunak yang membuat perangkat keras tidak terlihat (abstrak) dan memungkinkan beberapa sistem operasi berjalan pada perangkat keras yang sama (Desai, Oza, Sharma, & Patel, 2013). *Bare metal virtualization* mempertahankan struktur yang ada dengan memuat perangkat keras langsung dengan *hypervisor. Hypervisor* tersebut kemudian dimuat dengan sistem operasi dan aplikasi yang diinginkan. Sedangkan *hosted virtualization* mempertahankan struktur dimana perangkat keras memiliki sistem operasi *host* seperti *Windows, Linux* atau *OS-X*. Kemudian memuat *hypervisor* ke dalamnya dan memuat sistem operasi diatas *hypervisor* tersebut (Anderson & Romney, 2014).



Gambar 8: Jenis Virtualisasi

Berikut perbedaan antara perangkat lunak virtualisasi dengan perangkat keras dalam bentuk fisik dari beberapa aspek menurut Sarddar & Bose (2014):

1. *Compatibility*

   Perangkat keras dan perangkat lunak virtualisasi memiliki mesin fisik yang sama. Mesin *virtual* dapat menjalankan sistem operasi dan aplikasi dengan sendirinya dan memiliki semua komponen dari perangkat keras. Oleh karena itu, semua komponen dari perangkat keras dan mesin *virtual* sepenuhnya bersifat kompatibel.

2. *Isolation*

   Meskipun mesin *virtual* dapat berbagi sumber daya dengan fisik komputer. Tetapi keduanya tetap terisolasi satu sama lain seperti halnya komputer fisik yang berbeda.

3. *Encapsulation*

   Mesin *virtual* pada dasarnya adalah wadah untuk perangkat lunak. Mesin *virtual* akan mengatur sumber daya perangkat keras *virtual*, sistem operasi dan semua aplikasi yang dikemas dalam satu paket. Misalnya, memindahkan mesin *virtual* dari satu lokasi ke lokasi lain dan menyalin perangkat lunak lainnya.

4. *Independent Hardware*

   Mesin *virtual* bersifat independen dari perangkat keras fisik yang mendasarinya. Misalnya, dapat mengonfigurasi mesin *virtual* pada perangkat keras dan komponen fisik dari komponen *virtual* yang benar-benar berbeda. *Server* fisik yang sama, setiap mesin *virtual* bahkan dapat menjalankan berbagai jenis sistem operasi.

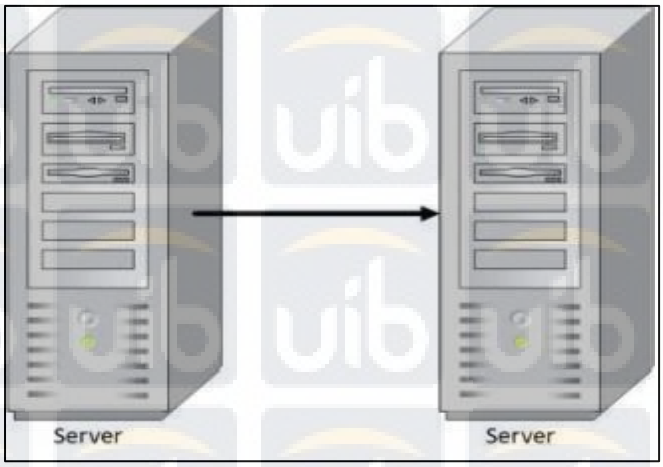
2.2.5 Replika *Server*

Replika menurut Lenti (2014), adalah suatu teknik penduplikasian data dari *data center* satu ke *data center* lainnya dan melakukan sinkronisasi antara data center awal dengan data center cadangan melalui koneksi jaringan lokal maupun internet. Menurut Basry & Sari (2014), replikasi *server* merupakan proses penyalinan data yang ada didalam sebuah *server* ke *server* lain yang berada di suatu lokasi tertentu. Jadi, replikasi *server* adalah proses penyalinan data didalam sebuah *server* ke *server* yang berada di lokasi berbeda dan sata yang disalin sudah tersinkronisasi.

Menurut Azizah et al. (2017), ada beberapa metode replikasi *server*, yaitu:

1. *Physical to Physical*

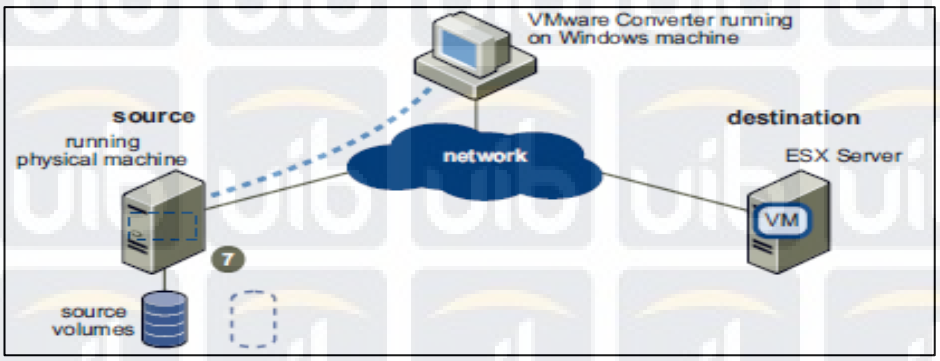
   Physical to Physical adalah metode replikasi *server* dari *server* fisik ke *server* fisik yang mempunyai spesifikasi yang sama (lihat gambar 9).



Gambar 9: *Physical to Physical*

2. *Physical to Virtual VMware Converter*

Physical to Virtual VMware Converter adalah metode replikasi *server* dari *server* fisik ke *server virtual* dengan aplikasi *VMware converter*. Dengan replikasi ini, mesin *virtual* yang ada secara otomatis tersinkronisasi dengan *server* tujuan (lihat gambar 10).

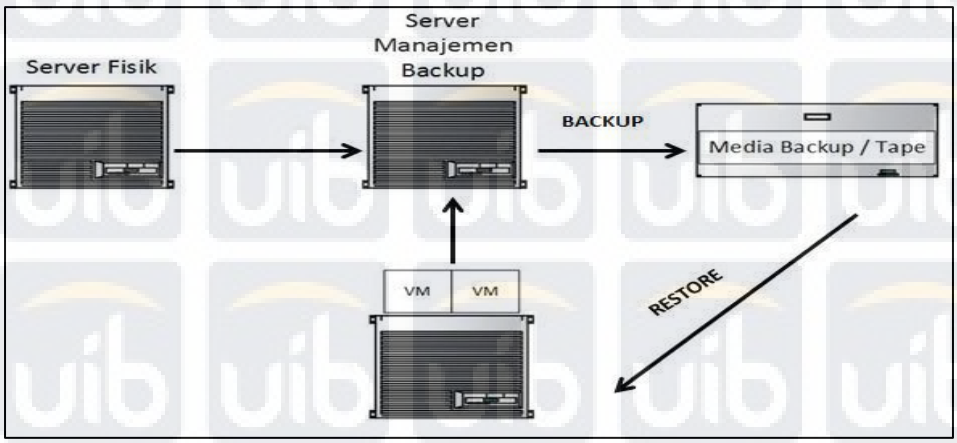


Gambar 10: *Physical to Virtual VMware Converter*

3. *Physical to Virtual Baremetal Restore*

Physical to Virtual Baremetal Restore adalah metode replikasi *server* dari *server* fisik ke *server virtual* melalui media penyimpanan *tape*. Cara kerja metode ini adalah mesin *virtual* akan menerima hasil *restore* data dari *server* fisik dengan melewati *server management backup* terlebih dahulu. *Server management backup* akan menentukan *rute* jalannya data pada

media *backup tape* yang tersedia untuk diteruskan atau di-*restore* ke mesin *virtual* (lihat gambar 11).



Gambar 11: *Physical to Virtual Baremetal Restore*

2.2.6 *Backup* dan *Recovery*

Backup menurut Yuliadi & Nugroho (2016) adalah proses penggandaan data kedalam media yang berbeda dari media asalnya. Menurut Saputro (2016), *backup* data merupakan kegiatan pengelola *database* untuk penyalinan sistem, data dan aplikasi. Menurut Wijaya et al. (2015), *backup* adalah penyalinan data dimana data yang telah disalin tersebut dapat di-*restore* kembali apabila terjadi kehilangan data. Dari beberapa pengertian tersebut, dapat disimpulkan bahwa *backup* adalah proses penyalinan atau penggandaan sistem, data dan aplikasi yang dapat di-*restore* kembali ketika terjadi kerusakan ataupun kehilangan pada data. *Backup* digunakan untuk dua tujuan utama, yaitu mengembalikan data yang mengalami kerusakan akibat bencana dan mengembalikan data setelah kesalahan penghapusan data.

Menurut Vašák (2017), *backup* terbagi menjadi beberapa kategori, yaitu berdasarkan fungsi, berdasarkan lokasi penyimpanan, berdasarkan arsitektur dan berdasarkan model penyebaran.

Beberapa cara *backup* berdasarkan fungsi, yaitu:

1. *Full Backup*

   Stategi *backup* ini dilakukan dengan cara mem-*backup* data secara keseluruhan, baik berupa folder, data, file ataupun aplikasi yang ada di dalam sistem. *Full backup* ini juga mem-*backup* data yang sudah pernah di-*backup* sebelumnya tanpa memilah apakah data tersebut sudah pernah di-*backup* atau tidak. Strategi ini biasanya digunakan dalam proses *backup* data pada saat memulai sebuah proses *backup* data awal. Sehingga strategi ini sangat diperlukan meskipun memakan waktu yang lama dan kapasitas yang besar.

2. *Incremental Backup*

   Streategi *backup* ini merupakan strategi *backup* yang hanya menyalin data yang berubah dari hasil *backup* terakhir, baik itu *full backup* ataupun *incremental backup.* Strategi ini dinilai lebih efisien dalam kapasitas media *backup* dan juga menghemat waktu dalam proses pem-*backup*-an.

3. *Differential Backup*

   Strategi *backup* ini merupakan strategi *backup* yang hanya menyimpan data yang berubah setelah *full backup* terakhir dilakukan. Data yang akan di-*restore* adalah data hasil dari *full backup* terakhir dan termasuk *differential backup* terakhir.

4. *Mirror Backup*

   Strategi *backup* ini merupakan penggandaan dari data yang akan di-*backup.* Waktu *backup* ini merupakan waktu *real (real time).* Kelemahan dari *backup* ini adalah jika *file* atau data yang berada di pusat data dihapus,

maka *file* yang ada di dalam *backup* ini juga akan ikut terhapus. Oleh karena itu, dalam sistem *backup* ini diperlukan kesadaran pengelola sistem *backup* jika terjadi penghapusan data secara tidak disengaja, sabotase ataupun invasi virus pada data. Selain itu, pada sistem *backup* ini tidak dapat diterapkan kompresi data dan perlindungan data berupa kata sandi pada *file.*

5. *Synthetic Backup*

   Strategi *backup* ini merupakan proses pembuatan *full backup* dengan melakukan *full backup* untuk langkah awal, lalu melanjutkan ke *incremental backup* untuk langkah selanjutnya. Biasanya, strategi *backup* ini dilakukan untuk kondisi *bandwidth* yang terbatas. Prosedur dalam *backup* ini disebut "sintetis" karena *backup* data yang dibuat tidak berasal dari data asli.

Tabel 2 Perbandingan *Backup* Berdasarkan Fungsi

Tipe Backup	Data yang Dibackup	Waktu Backup	Waktu Restore	Besar Penyimpanan
Full Backup	Semua Data	Lambat	Cepat	Tinggi
Incremental Backup	Data Baru atau Data yang Berubah	Cepat	Rata-Rata	Sangat Rendah
Differential Backup	Data Baru atau Data yang Barubah Setelah Full Backup Terakhir	Rata-Rata	Cepat	Rata-Rata
Mirror Backup	Data Baru atau Data yang Berubah	Sangat Cepat	Sangat Cepat	Sangat Tinggi
Synthetic Backup	Data Baru atau Data yang Barubah Setelah Full Backup Terakhir	Rata-Rata	Cepat	Rendah

Ada dua cara *backup* berdasarkan lokasi penyimpanan, yaitu :

1. *On-site Backup*

   On-site Backup atau *backup* ditempat merupakan strategi *backup* dengan media penyimpanan *backup* disimpan secara lokal. Media penyimpanan dihubungkan secara langsung atau melalui jaringan lokal.

2. *Off-site Backup*

   Off-site Backup merupakan strategi *backup* dengan media penyimpanan *backup* data berada di lokasi geografis yang berbeda seperti gedung yang berbeda, kota yang berbeda atau penyimpanan *cloud.*

Ada dua pendekatan untuk *backup* berdasarkan arsitektur, yaitu :

1. *File-level Backup*

   Backup ini terdiri dari *file* spesifik dari lingkungan tertentu dengan kemungkinan untuk tidak menyertakan data sistem *file* tingkat tinggi seperti hak akses *file.*

2. *Image-level Backup*

Backup ini pada umumnya disebut *image-level backup* atau *block-level backup*, dan dapat disebut juga sebagai *bare metal backup/recovery* (BMR), *disaster recovery backup, volume-level backup, ghost backup,* atau *machine cloning. Backup* ini menyimpan *file/*gambar yang berisi salinan dari sistem operasi dengan seluruh data yang terkoneksi termasuk status sistem dan aplikasi konfigurasi pada waktu tertentu. *Backup* ini digunakan untuk komputer atau *virtual machine* (VM).

Ada tiga jenis *backup* berdasarkan model penyebaran, yaitu:

1. *Local Backup*

   Dalam *backup* ini, penyalinan data di simpan di lokasi penyimpanan lokal.
2. *Cloud Backup* (*online backup*)

   Backup ini mengirim data yang di-*backup* secara langsung ke *cloud* melalui jaringan privat ataupun publik. Data yang di-*backup* tersimpan di penyedia *cloud* atau *Cloud Service Provider* (CSP) seperti AWS, *Azure* atau *Google*.
3. *Hybrid Cloud Backup*

   Backup ini merupakan campuran dari *local backup* dan *cloud backup. Backup* ini terdiri dari alat penyimpanan yang menyimpan hasil dari *full backup* dan *incremental backup* yang dilakukan setelah *full backup.* Data yang di-*backup* pertama-tama disimpan secara lokal dan kemudian direplikasi ke *cloud* (CSP).

Recovery (pemulihan) adalah proses pengembalian *backup* ke sistem awal setelah terjadinya kerusakan (Saputro, 2016). *Backup* dan *recovery* merupakan

hal yang berbeda satu sama lain tetapi saling berkaitan. *Backup* berfungsi untuk menyalin data sebelum terjadinya bencana atau gangguan dan merupakan sebuah pencegahan, sedangkan *recovery* berfungsi untuk memulihkan keadaan suatu sistem dari gangguan dan *recovery* dilakukan setelah terjadinya bencana.

Menurut Azizah et al. (2017), ada beberapa parameter yang menentukan bagusnya proses *recovery* yang berjalan, yaitu:

1. RTO (*Recovery Time Objective*)

   Durasi yang dibutuhkan untuk menyalakan kembali sistem yang mengalami kerusakan dikarenakan gangguan.

2. WRT (*Work Recovery Time*)

   Waktu yang dibutuhkan untuk memverifikasi sistem dan data, yang dilihat dari tersedianya sistem dan aplikasi yang berjalan dengan baik.

3. MTD (*Maximum Tolerable Downtime*)

   Waktu maksimum sebuah perusahaan menoleransi ketidakadaan sistem untuk perusahaan. Semakin kritis fungsi sistem perusahaan maka MTD akan semakin kecil.

2.3 Aplikasi

Aplikasi yang penulis gunakan dalam pembuatan proyek Kerja Praktek ini adalah *VMware vSphere* dan *Veeam Backup and Replication.*

2.3.1 *VMware vSphere*

VMware vSphere adalah sebuah *platform* berbasis *cloud computing* dari *VMware*. *VMware vSphere* berfungsi untuk mengubah pusat data menjadi sebuah insfrastruktur komputer yang dapat diukur. *VMware vSphere* memanfaatkan

virtualisasi untuk mengubah pusat data menjadi *cloud* sederhana (Desai et al., 2013).

Ada 4 komponen yang membentuk *VMware vSphere* menurut Ghorpade, Bennur, Acharya, & Kamatchi (2015) yang dapat dilihat di gambar 12, yaitu :

1. *Infrastructure Services*

   Infrastructure Services adalah serangkaian layanan yang disediakan untuk mengalokasikan sumber daya perangkat keras atau infrastruktur. *Infrastructure Services* dikategorikan menjadi 3, yaitu *VMware vCompute, VMware vStorage dan VMware vNetwork*. *VMware vCompute* adalah kemampuan untuk menggabungkan sumber daya server yang berbeda dan menetapkan sumber daya server tersebut ke aplikasi. *VMware vStorage* adalah rangkaian teknologi yang memungkinkan penggunaan dan manajemen penyimpanan secara efisien di lingkungan virtual. *VMware vNetwork* adalah rangkaian teknologi yang menyederhanakan dan meningkatkan jaringan di lingkungan virtual.

2. *Application Services*

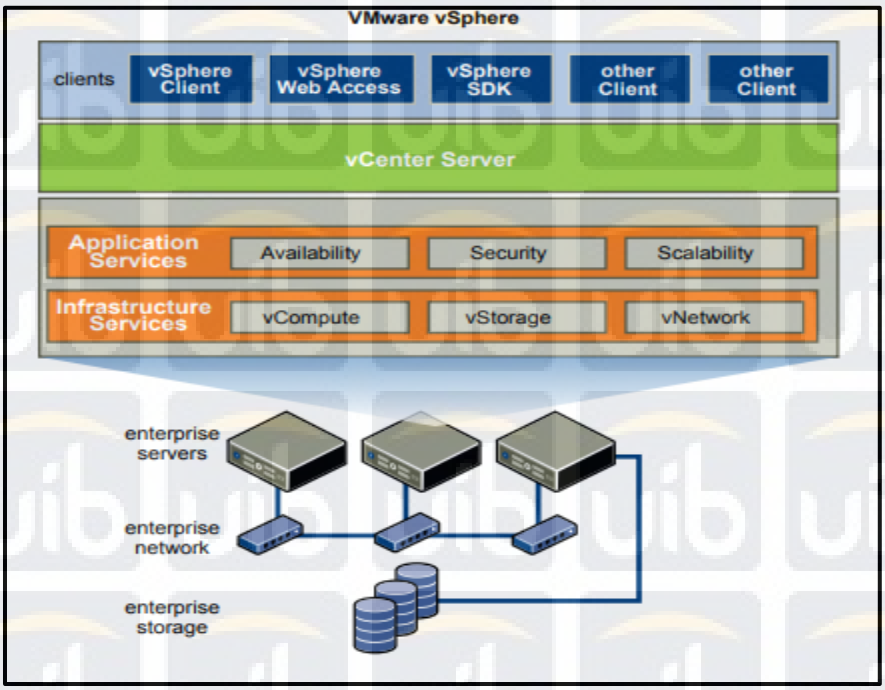
   Application Services adalah serangkaian layanan yang disediakan untuk memastikan ketersediaan, keamanan dan skalabilitas utuk aplikasi.

3. *VMware vCenter Server*

   VMware vCenter Server menyediakan kendali dari pusat data. IT menyediakan layanan pusat data penting seperti kontrol akses, kinerja pemantauan dan konfigurasi.

4. *Clients*

Clients atau pengguna dapat mengakses *VMware vSphere data center* melalui aplikasi *client* seperti *vSphere Client* atau *Web Access* melalui *browser Web.*



Gambar 12: Komponen *VMware vSphere*

2.3.2 *Veeam Backup & Replication*

Veeam Backup & Replication adalah aplikasi *backup* yang dikembangkan oleh Veeam. Aplikasi *backup* ini dibangun dalam *VMware vSphere* dan *Microsoft Hyper-V Hypervisors*. Perangkat lunak ini menyediakan fungsi *backup*, *recovery* dan *replication* untuk mesin *virtual* (Vašák, 2017).

Veeam Backup & Replication beroperasi dalam virtualisasi. Aplikasi ini mem-*backup* mesin *virtual* dalam bentuk gambar dengan menggunakan *snapshot hypervisor* untuk mengambil data mesin *virtual*. *Backup* yang dilakukan dapat berupa salinan lengkap dari gambar mesin *virtual* atau hanya menyimpan tambahan blok data yang berubah sejak *backup* terakhir dilakukan. Penambahan

data yang di-*backup* dibuat menggunakan mekanisme pelacakan blok data yang bertambah atau berubah dari data awal (*Changed Block Tracking/CBT*). *Veeam Backup & Replication* menyediakan verifikasi pemulihan otomatis untuk *backup* dan replika. Program memulai mesin *virtual* langsung dari *backup* atau replika di lingkungan pengujian yang terisolasi dan menjalankan pengujian terhadap mesin *virtual* tersebut. Selama verifikasi, gambar mesin *virtual* tetap dalam keadaan *read-only*. Mekanisme CBT ini juga dapat digunakan untuk mengatasi *troubleshooting* atau menguji *patch* dan *upgrade.*