DISASTER RECOVERY STRATEGY MENGGUNAKAN *SOFTWARE* BACULA DENGAN METODE *INCREMENTAL BACKUP-RESTORE*

DISASTER RECOVERY STRATEGY USING SOFTWARE BACULA WITH INCREMENTAL BACKUP-RESTORE METHOD

Aditya Shofwan Zulma[1], M Teguh Kurniawan[2], Adityas Widjajarto[3]

[1,2,3]Prodi S1 Sistem Informasi, Fakultas Rekayasa Industri, Universitas Telkom
[1]adityazulma@student.telkomuniversity.ac.id, [2]teguhkurniawan@telkomuniveristy.ac.id, [3]adtwjrt@telkomuniversity.ac.id

Abstrak

Data merupakan informasi yang harus ditangani dan dikelola secara baik. Pengelolaan data tersebut menggunakan sistem penyimpanan data yang terpusat (*data center*). Untuk mendukung layanan data, *data center* harus memiliki mitigasi bencana dengan menerapkan *Disaster Recovery Strategy* (DRS). DRS harus berkaitan dengan *business continuity plan* (BCP) untuk mencegah terjadinya hal yang tidak terduga untuk kelangsungan proses bisnis organisasi. Strategi yang dilakukan untuk menghindari masalah yang terjadi adalah dengan melakukan *data backup* dan *restore*. *Data backup* dan *restore* dapat dilakukan melalui jaringan komputer dengan menggunakan *software remote backup system*. Proses *data backup* dan *restore* menggunakan metode *incremental backup-restore*. Sebuah sistem *backup* merupakan komponen penting dalam banyak infrastruktur sistem komputer dan *data center* sebagai pemulihan dari kehilangan data dan merupakan bagian paling penting dari *disaster recovery strategy*. Penelitian ini bertujuan untuk mengetahui bagaimana pengaruh dari proses *data backup* dan *restore* secara *remote* terhadap integritas data dan kecepatan proses data. Analisis parameter untuk mengukur integritas data adalah *hash* MD5 *checksum* dan *digital signature*. Sedangkan untuk parameter kecepatan proses data yaitu *throughput* dan waktu *delay*. Hasil penelitian ini adalah analisis integritas data dan kecepatan proses data sebelum melakukan proses *data backup* dan setelah proses *data restore*. Analisis integritas data dilakukan pada dua parameter yaitu *hash* MD5 dan *digital siganture* yang memiliki hasil integritas yang sama pada pengujian datanya. Sedangkan pada analisis kecepatan proses data dibagi menjadi dua yaitu *throughput* dan waktu *delay* yang keduanya memiliki hasil yang berbeda karena beberapa faktor.
Kata kunci: *Disaster Recovery Strategy, Data Center, Backup, Restore, Incremental Backup-Restore*.

Abstract

Data is the information that must be handled and managed properly. The data management uses a data center. To support the data services, the data center must have disaster mitigation by applying Disaster Recovery Strategy* (DRS). DRS *have to relate with business continuity plan* (BCP) *to prevent unexpected things for the continuity of the organization's business process. The strategy that has been done to avoid the problems is to perform data backup and restore. Data backup and restore can be done through a computer network by using software remote backup system. The process of data backup and restore uses incremental backup-restore method. A backup system is an important component in many computer system infrastructure and data center as recovery from the data loss and the most important part of a disaster recovery strategy. The research aims to find out how is the influence of data backup process and restore process remotely toward the data integrity and data process speed. The parameter analysis that used to measure the data integrity is hash* MD5 *checksum and digital signature. While for the parameter of data process speed is throughput and delay time. The result of the research is analysis of data integrity and data process speed before do the data backup process and after process of data restore. The analyze of the data integrity are performed on two parameters, namely hash* MD5 *and digital siganture that have the same integrity result in the data test. While the analysis of data process speed is divided into two, namely throughput and delay time which both of them have the different results due to several factors.
Keywords*: *Disaster Recovery Strategy, Data Center, Backup, Restore, Incremental Backup-Restore

1. Pendahuluan

Data merupakan salah satu informasi yang harus ditangani dan dikelola secara baik. Solusi untuk pengelolaan data saat ini dengan menggunakan sistem penyimpanan data terpusat atau sering disebut *data center*. *Data center* adalah peralatan elektronik utama yang digunakan untuk melakukan pengolahan data, tempat penyimpanan data, dan menjadi tempat peletakan alat-alat komunikasi [1]. *Data center* sebagai penyedia layanan data tentunya harus memiliki pengelolaan operasional yang

aman, yaitu sudah mementingkan aspek keamanan baik keamanan fisik maupun keamanan data yang terdapat dalam *data center* tersebut. Tetapi dalam operasionalnya, *data center* dapat mengalami beberapa masalah atau insiden yang tidak terduga seperti bencana alam, sistem elektrik, serangan dari *hacker*, *virus* dan *worm*. Masalah tersebut dapat mengakibatkan operasional dari *data center* terganggu bahkan mengalami kerusakan perangkat [2]. Dari masalah tersebut, *data center* dalam mendukung layanan data harus memiliki mitigasi (pencegahan) dengan menerapkan *Disaster Recovery Strategy* (DRS). *Disaster recovery strategy* merupakan strategi dengan melakukan mitigasi untuk mengurangi dampak jika terjadi masalah atau insiden [3]. Pada *data center,* mitigasi dilakukan pada *Disaster Recovery Center* (DRC). *Disaster recovery center* adalah tempat lokasi data pengganti yang menyimpan semua data dari *data center*. *Disaster recovery strategy* pada DRC dilakukan untuk menghindari masalah atau insiden dan untuk menjalankan *business continuity* (BC) dari suatu organisasi. *Business continuity* merupakan bagian dari *business continuity plan* (BCP). Dalam hal ini BCP merupakan salah satu bagian dari DRS untuk mencegah terjadinya hal yang tidak terduga pada proses bisnis organisasi. Salah satu hal yang bisa dilakukan pada DRS adalah dengan menerapkan sistem *data backup* dan *restore*.

Backup dan *restore* adalah kegiatan menyalin dari *file* sistem atau bagian dari *file* sistem (data) yang disimpan pada suatu media penyimpanan yang dapat digunakan sewaktu-waktu untuk melakukan *data restore* jika dibutuhkan [4]. *Data backup* dan *restore* dapat dilakukan melalui jaringan komputer dengan menggunakan *software* tertentu yang disebut *remote backup system*. Tetapi sebagai bagian dari BCP, data yang berada dalam proses *backup* dan *restore* harus masuk dalam kriteria *security model* CIA (*Confidentiality, Integrity,* dan *Availability*). *Confidentiality* dan *integrity* memastikan data asli dalam proses *backup* dan *restore* tidak ada modifikasi dari faktor apapun [5]. *Availability* menjaga waktu dalam hal *recovery point objective* (RPO) dan *recovery point objective* (RTO) sebagai salah satu acuan pada BCP. Oleh karena itu, dalam penelitian ini penulis melakukan *disaster recovery strategy* dengan mengacu pada *business continuity plan*. Penelitian dilakukan dengan membuat suatu sistem *data backup* dan *restore* secara *remote* menggunakan *software* Bacula dengan metode *incremental backup-restore*. Kemudian akan dilakukan analisis terhadap kecepatan proses data dan integritas data dalam proses *data backup* dan *restore* tersebut.

2. Tinjauan Pustaka

2.1 *Data Center*

Data center merupakan bangunan atau bagian dari bangunan yang memiliki fungsi utama sebagai ruang komputer dan area pendukungnya [6]. *Data center* merupakan fasilitas yang digunakan sebagai tempat layanan data dan menjadi sumber informasi digital yang dikirimkan. Sebagai fasilistas layanan data, *data center* harus memiliki kriteria-kriteria sebagai berikut [7]:

1. *Availability*
   Data center harus dapat beroperasi dengan memberikan layanan secara terus menerus dan berkelanjutan. Beberapa layanan beserta komponennya sedapat mungkin mendekati *zero-failure*, yang berarti setiap operasi dan layanan yang diberikan harus dalam keadaan baik dan normal.
2. *Scalability* dan Fleksibility
   Data center sebagai penyedia layanan data harus mampu beradaptasi dengan perkembangan teknologi saat ini. *Data center* juga harus dapat menyesuaikan dengan kebutuhan penyimpanan data yang diperlukan secara cepat.
3. *Security*
   Data center tentu menyimpan berbagai data dan aset yang berharga bagi suatu organisasi seperti data karyawan, data keuangan, data operasional, dan data penting lain. Oleh karena itu untuk menjaga data dan aset berharga tersebut, data center harus memiliki sistem keamanan yang sangat baik dan aman.

2.2 *Business Contuinity*

Business Continuity (BC) adalah suatu proses dalam melanjutkan bisnis suatu perusahaan atau organisasi dalam keadaan normal maupun abnormal [8]. *Business continuity* merupakan bagian dari *Business Continuity Plan* (BCP) untuk mencegah terjadinya hal yang tidak terduga pada proses bisnis organisasi. *Business continuity* saat ini penting diterapkan oleh perusahaan atau organisasi karena letak geografis Indonesia yang rawan mengalami bencana alam yang dapat terjadi secara tidak terduga.

Business continuity plan dapat diartikan sebagai perencanaan yang dapat mempertahankan kelangsungan fungsi proses bisnis saat terjadi gangguan dan setelah gangguan. Dalam ilmu jaringan, BCP dieratkan dengan proses dari *disaster recovery strategy* pada perusahaan yang mempunyai fungsi dalam menjalankan *data center* dan bahkan perusahaan penyedia layanan *data center*. *Business Continuity Plan* dapat menjadi acuan untuk menentukan SLA (*Service Level Agreement*) pada *disaster recovery strategy* sebagai *disaster recovery as a service*.

2.3 *Disaster Recovery Strategy*

Disaster Recovery Strategy (DRS) adalah proses pemindahan layanan dan sistem *data center* yang sedang mengalami gangguan atau masalah ke tempat *data center* alternatif (*disaster recovery center*). *Disaster recovery strategy* merupakan strategi yang sudah direncanakan untuk menjamin kelangsungan proses layanan data yang diberikan jika terjadi masalah. Rencana tersebut adalah solusi yang efektif jika digunakan untuk melakukan pemulihan (*recovery*) layanan [4].

Rencana untuk melakukan DRS dilakukan jika terjadi suatu masalah tertentu, seperti hilang atau putusnya akses ke *data center*, *data center* secara tiba-tiba tidak bisa memproses layanan data, dan terputusnya hubungan *data center* dengan jaringan lokal maupun internet.

2.4 *Disaster Recovery Center*

Disaster Recovery Center (DRC) merupakan suatu fasilitas yang berfungsi sebagai *backup plan* untuk mengambil alih fungsi dari *data center* ketika terjadi masalah atau gangguan agar layanan yang diberikan *data center* tetap beroperasi. DRC memiliki fungsi untuk mengurangi risiko terhadap *data center* yang mengalami masalah dan meningkatkan ketersediaan layanan yang diberikan [9]. *Disaster recovery center* dalam proses *disaster recovery center* dikaitkan artikan dalam *disaster recovery as a service*, dimana DRC harus bisa menjadi bagian dari *business continuity plan*. Berikut hal-hal yang harus diperhatikan dalam *disaster recovery as a service* [10]:

1. *Recovery Point Objective* (RPO)
   Recovery Point Objective adalah waktu yang diperlukan dalam terjadinya kehilangan data. RPO merupakan lama waktu dari data yang ditoleransi untuk hilang ketika terjadi suatu gangguan. RPO erat kaitannya dengan DRC sebagai layanan proses *backup*.
2. *Recovery Time Objective* (RTO)
   Recovery Time Objective adalah waktu yang diperlukan *service provider* dalam memulihkan layanannya. RTO menjadi hal yang kritikal karena dikaitkan dalam berapa lama suatu layanan yang mengalami gangguan dapat berjalan normal kembali.
3. *Performance*
   Dalam menjaga performa dari layanan, DRC harus dimanfaatkan sebaik mungkin dalam menjaga data yang di-*backup* dari *data center*. DRC harus bisa menjamin bahwa proses *backup* yang dilakukan dapat melindungi data primer dari *data center*.
4. *Consistency*
   Konsistensi diperlukan dalam DRC dalam menjamin konsistensi data yang digunakan ketika DRC digunakan. Konsistensi dalam DRC diantara konsistensi aplikasi, konsisten data, dan konsistensi pada waktu tertentu.

2.5 *Backup* dan *Restore*

Backup adalah salinan dari suatu informasi data (*file* maupun direktori) yang disalin dari media penyimpanan internal komputer ke dalam media penyimpanan eksternal seperti USB *disk, harddisk* eksternal, atau *compact disk*. Informasi data yang dimaksud dapat berupa *file* data, aplikasi, sistem, aplikasi, dan *database*. *Backup* sangat diperlukan karena merupakan cadangan dari data utama **[**11**]**.

Restore adalah pengembalian atau pemulihan data dari penyimpanan data cadangan ke dalam penyimpanan data internal atau aslinya. *Restore* dapat dilakukan jika sebelumnya telah dilakukan *data backup*. Tujuan dari *restore* adalah mengembalikan suatu data yang dibutuhkan jika data tersebut mengalami masalah seperti hilang atau rusak [4].

2.6 *Software* Bacula

Bacula adalah sebuah *backup software* terpopuler bagi perusahaan ke-3 menurut Google Trends. Bacula merupakan program *backup* melalui jaringan yang bersifat *open source* (dapat digunakan secara bebas) yang digunakan sebagai *data backup* dan *restore* secara *remote*. Bacula merupakan program *backup* jaringan tingkat lanjut yang memungkinkan pengelolaan penyalinan data, pengindeksan *file* (*indexing*), *data restore*, verifikasi data, dan penjadwalan *backup* antara sistem komputer yang ada. Sistem *backup* Bacula membutuhkan setidaknya masing-masing komponen berikut [12], antara lain:

1. *Director Daemon* (*Director*)
   Merupakan aplikasi utama yang berguna untuk mengontrol proses *backup* dan *restore* yang dilakukan oleh *file daemon* dan *storage daemon*.
2. *Storage Daemon* (SD)
   Merupakan aplikasi yang berguna untuk melakukan baca dan tulis (*read & write*) pada perangkat penyimpanan data yang digunakan untuk *backup*.
3. *File Daemon* (FD)
   Merupakan aplikasi yang berada pada *client* yang membutuhkan data untuk disalin akan keperluan *backup*. Aplikasi ini juga bertanggung jawab untuk melakukan kompresi dan enkripsi data.
4. *Catalog* (*Database*)

Merupakan layanan yang berguna untuk melakukan pengindeksan dan menjaga *database* dari *file* yang didukung. *Database* tersebut disimpan dalam *database* MySQL.

5. Bacula *Console*
   Merupakan sebuah aplikasi berbasis *command line interface* (CLI) yang digunakan oleh pengguna bacula untuk berinteraksi dan mengontrol bacula. Pada *console*, pengguna dapat melakukan akses pada *backup director*, memeriksa status proses *backup* atau *restore*, tes koneksi ke *client* dan *store* (status), dan *execute restore*.

2.7 Kriptografi

Kriptografi (*cryptography*) berasal dari bahasa Yunani yaitu dari kata *kryptós* yang memiliki arti tersembunyi dan *gráphein* yang memiliki arti sesuatu yang tertulis atau tulisan, sehingga kriptografi dapat disebut sebagai sesuatu yang tertulis secara tersembunyi atau rahasia [13].

Kriptografi dapat dihubungkan dengan *security model* CIA (*Confidentially, Integrity,* dan *Availability*) karena model tersebut dapat menjadi parameter umum dalam menilai baik dan buruk keamanan dalam suatu jaringan. Berikut ada empat tujuan mendasar kriptografi yang juga merupakan aspek keamanan *security model* CIA [5], yaitu:

1. Kerahasiaan (*Confidentially*)
   Kerahasiaan adalah layanan yang berguna untuk menjaga isi dari sebuah informasi dari pihak lain kecuali yang memiliki otoritas atau kunci khusus untuk membuka infomasi yang terenkripsi.
2. Integritas Data (*Data Integrity*)
   Integritas erat hubungannya dengan menjaga data atau informasi dari perubahan data dari pihak lain yang tidak berwenang. Untuk menjaga integritas data, suatu sistem harus memiliki kemampuan untuk mendeteksi manipulasi data atau informasi antara lain, penyisipan, penghapusan, dan pensubsitusian informasi lain ke dalam data yang sebenarnya.
3. Autentikasi (*Authentication*)
   Autentikasi berhubungan dengan identifikasi atau pengenalan secara sistem maupun informasi itu sendiri. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri dan mengenal satu sama lain. Informasi yang dikirimkan harus diautentikasi keaslian, isi data, dan waktu pengiriman.
4. Non-repudiasi (*Non-Repudiation*)
   Non-repudiasi atau nirpenyangkalan adalah suatu usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman dan terciptanya suatu informasi oleh pengirim atau pembuat informasi.

2.8 *Quality of Service*

Quality of Service (QoS) adalah suatu metode untuk pengukuran dalam jaringan dan pendefinisian karakteristik dari suatu layanan dalam jaringan. QoS pada dasarnya ditentukan oleh kualitas dalam jaringan yang diukur [14]. Qos memiliki beberapa parameter yaitu *packet loss, jitter, throughput,* dan *delay*.

1. *Throughput*
   Throughput merupakan parameter yang berupa kecepatan (*rate)* transfer data yang efektif dan diukur dalam bps. *Throughput* merupakan jumlah total kedatangan paket yang berhasil di *monitoring* selama interval waktu tertentu dibagi oleh durasi interval waktu tersebut [14]. Kategori *throughput* menurut TIPHON *standards* ditunjukkan pada Tabel 1.

Tabel 1 Kategori *Throughput*

Kategori *Throughput*	*Throughput* (%)
Sangat Bagus	100
Bagus	75
Sedang	50
Buruk	<25

Untuk mendapatkan nilai *throughput* dapat menggunakan rumus berikut:

$$Throughput = \frac{\text{Total Ukuran Paket}}{\text{Waktu Pengiriman}}$$

2. *Delay*
   Delay adalah waktu yang dibutuhkan data dalam menempuh jarak asal ke tujuan. Ada beberapa hal yang dapat mempengaruhi *delay* diantaranya yaitu oleh media fisik yang digunakan, jarak, *congestion*, dan waktu proses yang lama [14]. Kategori *delay* menurut TIPHON *standards* ditunjukkan pada Tabel 2.

Tabel 2 Kategori *Delay*

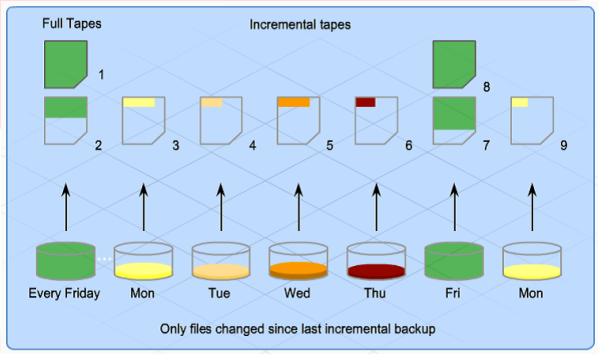
Kategori *Delay*	*Delay* (bps)
Sangat Bagus	<150
Bagus	150 s/d 300
Sedang	300 s/d 450
Buruk	>450

Untuk mendapatkan nilai *delay* dapat menggunakan rumus berikut:

$$Delay = \frac{\text{Waktu Pengiriman}}{\text{Total Jumlah Paket}}$$

2.9 *Incremental Backup-Restore*

Incremental backup-restore adalah salah satu metode *backup* yang digunakan dengan menyalin semua data atau sebagian data yang telah berubah sejak *backup* terakhir dilakukan. Prinsip dari metode ini adalah melakukan *backup* dari metode *backup* sebelumnya (*full backup* atau *differential backup)* [11].

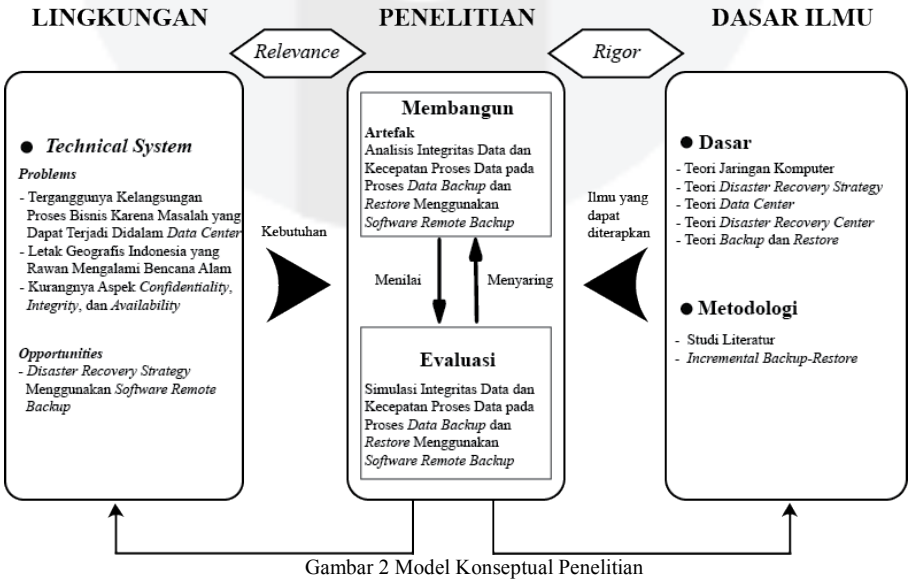


Gambar 1 *Incremental Backup* [9]

3. Metode Penelitian

3.1 Model Konseptual

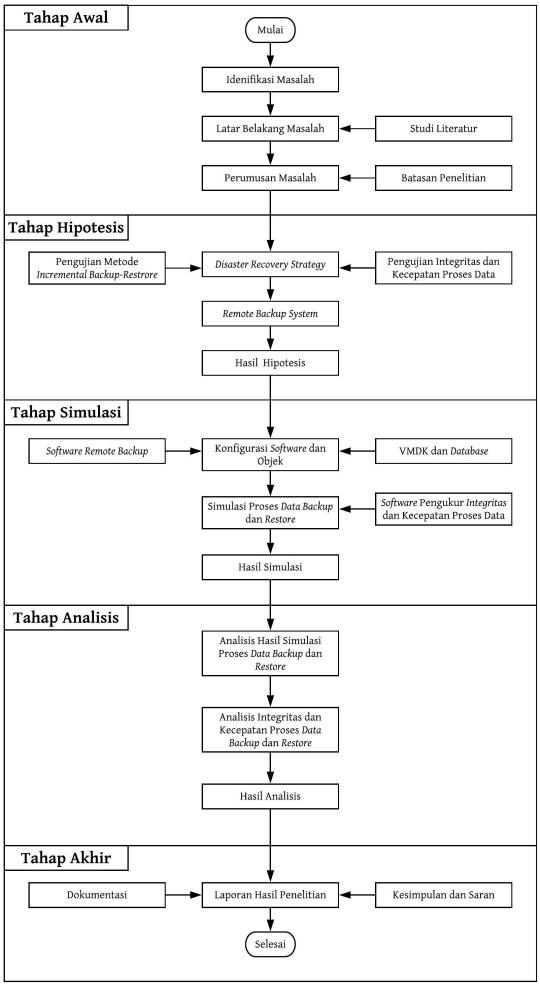
Metodologi penelitian merupakan suatu kerangka atau asumsi yang ada dalam melakukan elaborasi penelitian atau sederhananya metodologi penelitian merupakan langkah-langkah yang ada dalam penelitian. Metodologi penelitian dapat berupa kerangka atau model konseptual yang digunakan dalam penelitian [15]. Metode konseptual adalah model yang bersifat analitis dengan memberikan komponen-komponen produk yang akan dikembangkan serta keterkaitan antar komponen [16]. Proses model konseptual sangat dibutuhkan kepastian untuk memntukan ruang lingkup dan tingkatan model secara detail. Pada penelitian ini, model konseptual yang digunakan dijelaskan pada Gambar 2.



Gambar 2 Model Konseptual Penelitian

3.2 Sistematika Penelitian

Sistematika pemecahan masalah merupakan bagian yang menjelaskan tentang tahapan-tahapan yang akan dilakukan dalam penelitian ini. Tahapan dimulai dari identifikasi masalah sampai tahapan akhir yaitu laporan hasil penelitian. Sistematika tahapan-tahapannya adalah sebagai berikut:



Gambar 3 Sistematika Penelitian

4. Hasil dan Analisis

4.1 Analisis MD5 *Checksum*

Analisis MD5 *checksum* yaitu analisis dalam melihat *hash* MD5 pada objek *backup* VMDK sebelum proses *data backup* dan setelah proses *data restore*. Analisis tersebut didasarkan pada hasil dari pengujian integrtias data.

Tabel 3 Hasil Autentikasi MD5 *Checksum*

File VMDK	Autentikasi
ClientHost.plist	*Verified* OK
ClientHost.vmsd	*Verified* OK
ClientHost.nvram	*Verified* OK
ClientHost.vmx	*Verified* OK
ClientHost.vmxf	*Verified* OK
startMenu.plist	*Verified* OK
Virtual Disk-s001.vmdk	*Verified* OK
Virtual Disk-s002.vmdk	*Verified* OK
Virtual Disk-s003.vmdk	*Verified* OK
Virtual Disk-s004.vmdk	*Verified* OK
Virtual Disk-s005.vmdk	*Verified* OK
Virtual Disk-s006.vmdk	*Verified* OK
Virtual Disk-s007.vmdk	*Verified* OK
Virtual Disk-s008.vmdk	*Verified* OK

File VMDK	Autentikasi
Virtual Disk-s009.vmdk	*Verified* OK
Virtual Disk-s010.vmdk	*Verified* OK
Virtual Disk-s011.vmdk	*Verified* OK
Virtual Disk-s012.vmdk	*Verified* OK
Virtual Disk-s013.vmdk	*Verified* OK
Virtual Disk-s014.vmdk	*Verified* OK
Virtual Disk-s015.vmdk	*Verified* OK
Virtual Disk-s016.vmdk	*Verified* OK
Virtual Disk-s017.vmdk	*Verified* OK
Virtual Disk-s018.vmdk	*Verified* OK
Virtual Disk-s019.vmdk	*Verified* OK
Virtual Disk-s020.vmdk	*Verified* OK
Virtual Disk-s021.vmdk	*Verified* OK
Virtual Disk-s022.vmdk	*Verified* OK
Virtual Disk-s023.vmdk	*Verified* OK
Virtual Disk-s024.vmdk	*Verified* OK
Virtual Disk-s025.vmdk	*Verified* OK
Virtual Disk-s026.vmdk	*Verified* OK
Virtual Disk-s027.vmdk	*Verified* OK
Virtual Disk-s028.vmdk	*Verified* OK
Virtual Disk-s029.vmdk	*Verified* OK
Virtual Disk-s030.vmdk	*Verified* OK
Virtual Disk-s031.vmdk	*Verified* OK
Virtual Disk-s032.vmdk	*Verified* OK
Virtual Disk.vmdk	*Verified* OK
vmware-0.log	*Verified* OK
vmware-1.log	*Verified* OK
vmware-2.log	*Verified* OK
vmware.log	*Verified* OK

Analisis dari MD5 *checksum* dalam pengujian integritas data yaitu, pertama seluruh *file* VMDK berstatus *Verified* OK yang artinya tidak ada perubahan *hash* MD5 pada data sebelum proses *data backup* dan dan setelah *data restore*. Selama proses *data backup* dan *restore* seluruh data tetap ada sebagaimana semula tanpa ada data yang termodifikasi atau data hilang. Hasil pengecekan *hash* MD5 telah memenuhi unsur *security model triad* terutama *integrity* karena tidak ada perubahan informasi pada data. Oleh karena itu dalam pengujian integritas MD5 *checksum* dapat menjadi salah satu acuan dalam SLA sebagai kelangsungan bisnis perusahaan dalam DRS.

4.2 Analisis *Digital Signature*

Analisis *digital signature* yaitu analisis dalam mengetahui tanda RSA *key* pada *file* target (tabel) dalam objek *database* sebelum proses *data backup* dan setelah proses *data restore*. Analisis tersebut didasarkan pada hasil dari pengujian integrtias data.

Tabel 4 Kategori *Delay*

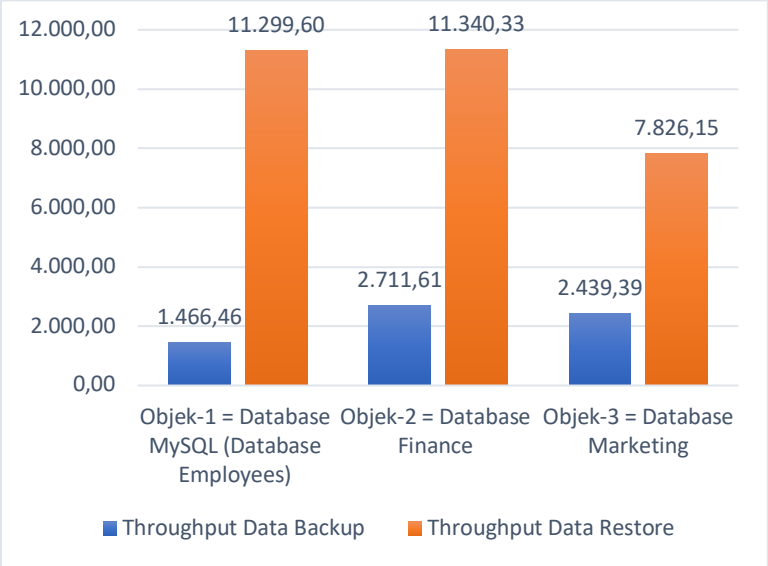
Objek *Backup*	*Public key*	*Digest File*	*File Target*	Autentikasi
Database MySQL (*Database Employees*)	*public1 .pem*	*digest1.bin*	*titles.frm*	*Verified* OK
Database Finance	*public2 .pem*	*digest2.bin*	*tax.frm*	*Verified* OK
Database Marketing	*public3 .pem*	*digest3.bin*	*transactions .frm*	*Verified* OK

Analisis dari *digital signature* dalam pengujian integritas yaitu seluruh target *file* tabel dalam *database* berstatus *Verified* OK yang artinya tidak ada perubahan data yang terjadi sebelum proses *data backup* maupun setelah *data restore*. Status tersebut dapat diartikan bahwa tabel *database* target tidak mengalami penambahan, pengurangan atau kehilangan data selama proses terjadi.

Integritas menggunakan *digital signature* telah memenuhi *security model triad* yaitu *confidentiality* (keamanan data hanya pada yang memiliki otoritas), *integrity* (tidak ada perubahan informasi pada data), dan *authentication* (isi data telah diautentikasi keasliannya). *Digital signature* bisa dikatakan lebih handal dari pada *hash* MD5 karena menggunakan keamanan data menggunakan enkripsi *asymmetic key*. Hasil dari pengujian integritas *digital signature* tersebut dapat menjadi acuan yang handal dalam SLA sebagai kelangsungan bisnis perusahaan dalam proses DRS.

4.3 Analisis *Throughput*

Berikut hasil dari perhitungan *throughput* dalam satuan KBps:



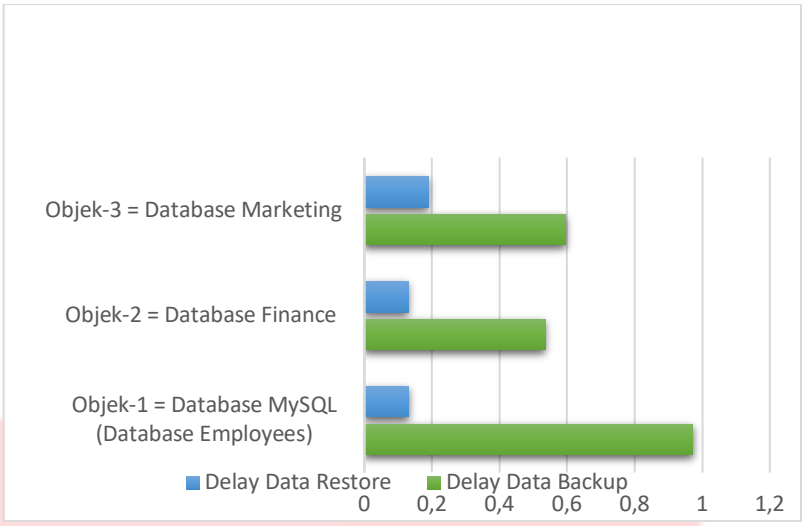
Gambar 4 Grafik Diagram *Throughput*

Berdasarkan Gambar 4 analisis dari perhitungan *throughput* dalam pengujian kecepatan proses data yaitu kecepatan *throughput* pada proses *data restore* lebih cepat daripada proses *data backup*. Hal tersebut dapat terjadi karena fitur dalam *software* bacula yang menjadikan semua data terlebih dahulu dikompresi dalam bentuk GZIP. Tetapi *throughput* dari setiap proses *backup* 1-3 dan *restore* 1-3 berbeda-beda. Perbedaan dapat terjadi karena beberapa faktor, diantaranya: sistem dan aplikasi perangkat, spesifikasi perangkat, media transmisi, tipe dan ukuran data, dan besar *bandwidth* dalam jaringan.

Perhitungan *throughput* menjadi penting karena dapat memenuhi *security model* CIA yaitu *availability* dalam hal kecepatan yang menjamin ketersediaan data saat dibutuhkan. Selain itu dengan hasil perhitungan nilai *throughput*, pengujian *data backup* dan *restore* lebih baik diimplementasikan pada skenario pengujian maupun sistem *backup* dan *restore* yang hampir sama seperti pada penelitian ini. Nilai *throughput* digunakan pada data yang berukuran kecil sampai sedang dan menggunakan metode *incremental*. Dikarenakan jika data berukuran besar, nilai *throughput* akan menjadi kurang atau tidak bisa memenuhi *availability* pada suatu layanan. *Throughput* dalam proses *data backup* dan *restore* juga menjadi hal penting dalam penggunakan metode *incremental backup-restore*. Hasil *throughput* dapat menjadi salah satu acuan untuk *recovery time objective* pada SLA dalam menjalankan *business continuity plan*.

4.4 Analisis Waktu *Delay*

Berikut hasil dari perhitungan waktu *delay* dalam satuan ms:



Gambar 5 Grafik Diagram Waktu *Delay*

Berdasarkan Gambar V-2 analisis dari perhitungan waktu *delay* dalam pengujian kecepatan proses data yaitu waktu *delay* yang didapatkan dalam semua proses *data backup* dan *restore* kurang dari 1ms. Hal tersebut terjadi karena pada pengujian sistem menggunakan topologi lokal yang langsung terhubung tanpa ada hambatan dari jaringan luar (internet). Jika topologi terhubung dengan jaringan luar dan setiap *site router* terhubung dengan internet untuk saling berkomunikasi, maka waktu *delay* pada semua proses *data backup* dan *restore* ditambahkan dengan waktu *delay* internet sebesar 50ms yaitu berkisar antara 50,1ms – 50,9ms. Mengacu waktu *delay* pada TIPHON *standards*, *delay* yang didapatkan termasuk dalam kategori sangat bagus karena *delay* kurang dari 150ms. Menggunakan waktu *delay* dan kategori *delay* tersebut, pengujian *data backup* dan *restore* dapat diimplementasikan ke dalam banyak skenario pengujian maupun sistem *backup* dan *restore* dengan instrumen fisik dan program yang sama atau lebih baik.

Perhitungan waktu *delay* dapat memenuhi konsep *security model* CIA yaitu *availability* CIA dalam hal performa dan konsistensi layanan yang menjamin ketersediaan data saat dibutuhkan. Waktu *delay* dalam proses *data backup* dan *restore* berkaitan dengan metode *incremental backup-restore*. Kaitan tersebut yaitu dalam hal seberapa besar *data backup* atau jumlah paket yang dikirimkan dalam proses *data backup* dan *restore*. Hasil waktu dapat menjadi salah satu acuan untuk *recovery point objective* pada SLA dalam menjalankan *business continuity plan*.

5. Kesimpulan dan Saran

5.1 Kesimpulan

Berdasarkan penelitian *Disaster Recovery Strategy* Menggunakan *Software* Bacula Dengan Metode *Incremental Backup*-Restore, dapat disimpulkan bahwa:

1. Proses *data backup* dan *restore* secara *remote* dilakukan dengan metode *incremental backup-restore* menggunakan *software* Bacula. Pada proses *data backup* dilakukan ketika terdapat penambahan data baru sejak terakhir dilakukan *full data backup* dengan level *Incremental*. Sedangkan pada proses *data restore* dilakukan setelah proes *data backup* dengan metode *incremental* menggunakan fitur seleksi *JobID.*
2. Pengaruh terhadap integritas data dan kecepatan proses *data backup* dan *restore* menggunakan metode *incremental* adalah:
   a. Pengujian *data backup* dan *restore* dengan metode *incremental* pada objek yang telah ditentukan. Pengujian dilakukan terhadap integritas data dibagi menjadi dua yaitu *hash* MD5 dan *digital siganture* yang memiliki hasil integritas yang sama pada pengujian datanya. Sedangkan pada kecepatan proses data dibagi menjadi dua yaitu *throughput* dan waktu *delay* yang keduanya memiliki hasil yang berbeda karena beberapa faktor.
   b. Berdasarkan pengujian dan analisis integritas data menggunakan parameter *hash* MD5 pada objek *backup* sistem operasi berupa VMDK menunjukkan hasil *hash* yang sama sebelum proses *data backup* dan setelah *data restore*. Sedangkan untuk parameter *digital signature* menggunaka RSA *key* pada objek *backup database* MySQL menunjukkan hasil *Verified* OK yang artinya selama proses *data backup* dan *restore* tidak ada modifikasi atau perubahan pada data. Kedua hasil tersebut memenuhi *model security* CIA untuk digunakan sebagai acuan SLA dalam mendukung kelangsungan bisnis organisasi.
   c. Berdasarkan pengujian dan analisis kecepatan proses data menggunakan parameter QoS *throughput* dan waktu *delay* pada objek *backup database* yaitu durasi waktu yang pada *data restore* lebih cepat dibandingkan dengan *data backup.* Pada parameter *throughput* memiliki hasil rata-rata *rate backup* yaitu 2.205,82 KBps, dan rata-rata *rate restore* yaitu 10.155,36 KBps. Sedangkan pada parameter waktu *delay* memiliki hasil rata-rata *delay backup* yaitu 0,7001 ms dan rata-rata *delay restore* yaitu 0,150 ms.
   d. Metode *incremental* pada pengujian dilakukan pada objek *backup database* MySQL. Metode tersebut mempengaruhi jumlah ukuran data yang juga berpengaruh terhadap parameter *throughput* dan waktu *delay* pada analisis kecepatan proses data.
   e. Hasil pengujian *thoughput* dan waktu *delay* bersifat tidak absolut karena dipengaruhi banyak faktor seperti: sistem dan aplikasi perangkat, spesifikasi perangkat keras yang digunakan, media transmisi, tipe dan ukuran data, dan besar *bandwidth* yang didapatkan.

6. Daftar Pustaka

[1] H. Geng, Data Center Handbook, John Wiley & Sons., 2015.

[2] C. Hendy, "Secure Operation Data Center menurut TIA-942-A," 2016.

[3] B. Syahputra, Strategi Backup dan Recovery Data pada Disaster Recovery Center, Jakarta, 2008.

[4] L. Ashdown, "Backup and Recovery Concepts," 2001.

[5] CompTIA, CompTIA Security+ (Student Edition), London: gtslearning, 2014.

[6] Telecommunication Industry Assosiation, TIA-942 Standard, Telecommunication Industry Assosiation, 2012.

[7] I. Caesar, "Analisis dan Perancangan Power Management Data Center Berdasarkan Tiering Level di Pemerintahan Kabupaten Bandung Menggunakan Standar TIA-942 dengan Metode PPDIOO Life-Cycle Approach," 2017.

[8] Humdiana, "Perancangan Business Continuity Plan: Studi Kasus Pada PT.PAM," 2014.

[9] Wijasena, "Sekilas Tentang Disaster Recovery Center (DRC)," 2011. [Online]. Available: http://www.ristinet.com/index.php?ch=8&lang=&s=d393cfd993bce4dd308ab1356deb47ff&n=227.

[10] Garibaldi, "5 Hal Yang Harus Diperhatikan Dalam Memilih Disaster Recovery-As-A-Service-Yang Tepat," 2014. [Online]. Available: https://blog.indonesiancloud.com/2014/06/08/5-hal-yang-harus-diperhatikan-dalam-memilih-disaster-recovery-as-a-service-yang-tepat/#.Wvg9_i-B28o.

[11] P. G. Kusuma, "Analisis Backup dan Sinkronisasi Data Otomatis," 2012.

[12] Eric, "What is Bacula?," 2011. [Online]. Available: http://www.bacula.org/5.1.x-manuals/en/main/main/What_is_Bacula.html.

[13] R. Nuansa, "Enkripsi dan Kriptografi," 2016.

[14] R. Wulandari, "Analisis QoS (Quality of Service) Pada Jaringan Internet," 2016.

[15] Z. A. Hasibuan, "Metodologi Penelitian pada Bidang Ilmu Komputer dan Teknologi Informasi," 2007.

[16] T. M. Endaswara, Pengembangan Media Pembelajaran Bahasa Berbasis Lingkungan dan Teknologi, DIKSI, 2015.