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

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

Fachrul Hijriah Usman[1], M Teguh Kurniawan[2], Adityas Widjajarto3[3]

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

Abstrak

Dalam pengoperasian sebuah *data center* tidak pernah lepas dari berbagai gangguan yang disebabkan oleh berbagai macam faktor seperti bencana alam, kebakaran, *human error, virus, worm,* dan *fault system.* Kondisi tersebut dapat menyebabkan anomali pada proses bisnis yang sedang menggunakan data tersebut. Untuk itu diperlukan adanya sebuah *disaster recovery strategy* (DRS) sebagai strategi yang berfungsi untuk mendukung *business continuity,* salah satu bentuk strategi tersebut adalah dengan melakukan aktivitas *data backup* dan *data restore* menggunakan *remote backup system* pada sebuah *disaster recovery center*. Pada penelitian *disaster recovery strategy* menggunakan *software* bacula dengan metode *differential backup-restore* ini mendapatkan hasil bahwa integritas data yang telah ditransmisikan saat proses *data backup* dan *restore* identik atau tidak mengalami gangguan, keutuhan datanya terjaga dan telah memenuhi aspek *information security* berdasarkan CIA *Triad Model* dan pada kecepatan proses dengan parameter *throughput* pada *data backup* yang mengalami peningkatan, yaitu dari 2.337,038 KB/s hingga 3.237,748 KB/s dan pada proses *data restore* yang mendapatkan hasil yang fluktuatif, yaitu dari 9.574,797 KB/s, 10.539,896, dan 10.493,376 KB/s. Sedangkan pada waktu *delay* yang dihasilkan berkisar antara 50,145 ms – 50,513 ms pada proses *data backup* dan *restore,* hasil tersebut termasuk dalam kategori sangat baik dengan perolehan indeks 4 berdasarkan standar TIPHON. Hasil penelitian ini dapat menjadi referensi dalam membuat sebuah SLA terkait integritas data dan kecepatan proses *data backup* dan *restore* untuk mendukung *business continuity* pada suatu proses bisnis.

Kata Kunci : Pusat Data, DRC, DRS, Bacula, *Differential Backup-Restore,* CIA *Triad Model*, TIPHON.

Abstract

In the operation of a data center never escapes from various disturbance caused by various factors such as natural disaster, fire, human error, virus, worm, and system fault. Such conditions may cause anomalies in the business processes that are using the data. Therefore, a disaster recovery strategy* (DRS) *is required as a strategy to support business continuity, one of which is to perform data backup and data restore activities using a remote backup system in a disaster recovery center. In disaster recovery strategy research using bacula software with differential backup-restore method gets the result that the data integrity of data that has been transmitted during the process of data backup and restore is identical or not disturbed, the integrity of the data is maintained and has fulfilled the information security aspects of the* CIA *Triad Model and at the speed of the process with the parameters of throughput on the backup data that gets the increased results, i.e. from* 2.337.038 KB/s *up to* 3237.748 KB/s *and the data restore process that gets fluctuated results, i.e. from* 9,574,797 KB/s, 10,539,896 KB/s, *and* 10,493,376 KB/s. *While the resulting delay time ranges between* 50.145 ms - 50,513 ms *on the process of data backup and restore, the results are included in the category very well with the acquisition of index 4 based on* TIPHON *standards. The results of this study can be a reference in making an* SLA *related to data integrity and speed of data backup and restore process to support business continuity in a business process.

***Keywords*: *Data Center*, DRC, DRS, Bacula, *Differential Backup-Restore*, CIA *Triad Model*, TIPHON.**

1. Pendahuluan

Informasi adalah data yang telah diolah sedemikian rupa sehingga memiliki nilai berupa sebuah informasi yang dapat digunakan untuk berbagai kebutuhan, salah satunya adalah kebutuhan dalam proses bisnis [1]. Tingkat kebutuhan dan nilai informasi yang sangat tinggi menjadikan agar informasi tersebut harus tersimpan dalam suatu sistem yang memiliki tingkat keamanan yang tinggi sehingga terhindar dari berbagai gangguan. Data yang merupakan sumber dari sebuah informasi menjadikan sebuah data tersebut menjadi sebuah *asset* yang sangat penting untuk dijaga keamanannya, salah satu cara untuk menjaga keamanan data adalah dengan menerapkan pengelolaan yang baik dan benar. Pengelolaan tersebut dilakukan dengan cara menyimpan data secara terpusat sehingga data tersebut dapat dikelola maupun diakses dengan mudah oleh pemiliknya. Penyimpanan data secara terpusat tersebut dilakukan pada sebuah infrastruktur yang disebut *data center*. *Data Center* (DC) adalah ruangan yang berisi sebagian besar *server* dan penyimpanan data perusahaan terletak, beroperasi yang diatur oleh seorang *administrator* [2]. Dalam pengoperasiannya, sebuah DC tidak akan lepas dari berbagai gangguan seperti bencana alam yang disebabkan oleh berbagai faktor contohnya faktor geografis, kebakaran, *human error*, serangan pada sistem seperti *virus*, *worm*, dan *fault system* [3].

Oleh karena itu diperlukan adanya *disaster recovery strategy* (DRS) yaitu sebuah strategi yang berfungsi untuk melakukan pencadangan atau pemulihan yang mencakup fasilitas seperti perangkat fisik maupun *non*-fisik yang ada pada DC atau teknologi berupa *software* yang mendukung jalannya proses bisnis pada sebuah DC, hal ini dilakukan sebagai mitigasi atau pencegahan dari dampak yang mungkin terjadi ketika terjadi sebuah insiden *disaster* yang dilakukan pada sebuah infrastruktur yang disebut *disaster recovery center* (DRC). DRC merupakan sebuah fasilitas yang berguna untuk mengambil alih fungsi pada sebuah proses bisnis jika terjadi gangguan pada DC utama [4]. DRC digunakan sementara waktu selama dilakukannya pemulihan pada pusat data utama untuk menjaga *business continuity* (BC). Penerapan DRC adalah suatu kewajiban untuk diimplementasikan dalam rangka meminimalisasi kerugian finansial maupun non-finansial dan meningkatkan rasa aman dalam hubungan bisnis dengan para *stakeholder* terkait seperti *customer*, *supplier*, dan *investor*. Salah satu bentuk strategi tersebut adalah dengan melakukan aktivitas *data backup* dan *data restore* pada sebuah DRC. Bacula adalah sebuah *software* yang digunakan untuk mengelola *backup* dan *restore* data pada sebuah perangkat melalui sebuah jaringan, komponen yang bekerja pada *software* bacula yaitu, *bacula-director*, *storage-daemon*, *catalog*, dan *bacula-console* [5]. Tentunya sangat penting untuk menjaga data sebagai *asset* dari berbagai gangguan atau serangan sehingga diperlukan sebuah solusi yaitu *disaster recovery strategy* dengan menggunakan *software remote backup* bacula. Pada penelitian ini menggunakan metode *differential backup-restore* yang bertujuan untuk mengamati pengaruh metode yang digunakan pada integritas data dan kecepatan proses dengan parameter *throughput* dan *delay* sebagai *quality of service* pada proses *data backup* dan *restore.*

2. Tinjauan Pustaka

2.1 *Disaster Recovery Center*

Disaster Recovery Center (DRC) adalah kemampuan sebuah infrastruktur untuk melakukan kembali operasi secepatnya pada saat terjadi gangguan yang signifikan seperti bencana besar yang tidak dapat diduga sebelumnya. Fungsi dari adanya DRC adalah untuk meminimalkan kerugian finansial dan *non*-finansial dalam menghadapi kekacauan bisnis atau bencana alam yang meliputi fisik dan informasi berupa data penting perusahaan, serta meingkatkan rasa aman di antara *personel*, *supplier*, *investor*, dan *customer* [4].

Tujuan dari DRC adalah mengembalikan fungsi sistem dalam waktu yang singkat dan dengan risiko kehilangan data yang kecil sehingga proses bisnis tidak terganggu, sehingga tidak terjadi kerugian finansial dalam bisnis perusahaan [6]. Terdapat tiga tipe mode operasi pada sebuah *disaster recovery center*:

1. *Cold* DRC yaitu *data center* sebagai *backup* dalam kondisi mati dan akan diunduh dan dikonfigurasi hanya pada saat *data center* mengalami gangguan untuk pertama kali. *Data center* dapat dilakukan *backup-restore* bila diperlukan dan pada umumnya membutuhkan waktu pemulihan dalam hitungan jam.
2. *Warm* DRC yaitu *data center* sebagai *backup* dalam kondisi *standby* dan bila *data center* mengalami gangguan maka kondisi menjadi aktif. Pada *data center* cadangan *software* sudah terunduh dan proses terjadi secara otomatis menggunakan *cluster manager*. Pada umumnya dilakukan *backup* secara *mirror* menggunakan replikasi berbasis *disk* atau *shared disk* dan membutuhkan waktu pemulihan dalam hitungan menit.
3. *Hot* DRC yaitu *data center* sebagai *backup* dalam kondisi aktif. Pada *data center* cadangan *software* telah terunduh dan tersedia pada kedua *data center*. Pada umumnya melakukan *backup* data secara

real time dan kedua *data center* memiliki data yang identik. Membutuhkan waktu pemulihan dalam hitungan detik.

2.2 *Disaster Recovery Strategy*

Disaster Recovery Strategy (DRS) adalah strategi yang telah direncanakan untuk menjaga kelangsungan layanan pada sebuah proses bisnis jika terjadi bencana. Strategi tersebut merupakan solusi untuk melakukan *restore* terhadap layanan pada proses bisnis yang sedang terganggu. Strategi ini sangat mendukung keberlangsungan jalannya operasional pada sebuah *disaster recovery center.* DRS merupakan aktivitas untuk menentukan dan memilih strategi-strategi operasi pemulihan alternatif yang diperlukan untuk menjaga fungsi-fungsi organisasi yang vital [7].

2.3 *Business Continuity*

Business Continuity (BC) adalah proses otomatis atau *manual* yang dirancang untuk mengurangi ancaman terhadap fungsi penting ogranisasi sehingga menjamin kontinuitas layanan bagi operasi yang penting. BC didesain untuk melindungi proses bisnis vital dari kerusakan atau bencana yang terjadi secara alamiah atau perbuatan manusia dan kerugian yang ditimbulkan dari tidak tersedianya proses bisnis normal. Memiliki sebuah perencanaan BC dipandang sebagai sebuah jaminan kebijakan yang memberikan kontribusi pada "*good governance*" sebuah bisnis. Namun, tidak semua industri atau negara di dunia menyadari pentingnya nilai perencanaan BC. Di seluruh dunia, industri jasa keuangan adalah terdepan dibanding industri lainnya dalam persyaratan perencanaan BC yang *up to date* dan *tested*. Regulasi ini ditegakkan dengan audit internal maupun eksternal dan dalam kasus-kasus ekstrim dengan berbagai sanksi dan denda [8].

Proses suatu *business continuity plan* (BCP) akan memungkinkan perusahaan atau organisasi menemukan dan mengurangi (*reduce*) ancaman, menanggapi (*respond*) suatu peristiwa ketika terjadi, pemulihan (*recover*) dari dampak langsung suatu peristiwa atau bencana dan akhirnya mengembalikan (*restore*) operasi menjadi seperti semula. *Reduce*, *respond*, *recover*, dan *restore* ini lebih dikenal sebagai empat R pada BCP [8].

Dalam penyusunan *business continuity plan* (BCP) pada proses *risk assessment* dilakukan berdasarkan beberapa parameter, diantaranya yang memiliki keterkaitan dengan *disaster recovery* adalah *Recovery Time Objective* (RTO) dan *Recovery Point Objective* (RPO) [9].

Recovery Time Objective (RTO) merupakan total waktu yang dibutuhkan oleh penyedia layanan untuk melakukan pemulihan setelah terjadinya *disaster*. Sedangkan *Recovery Point Objective* (RPO) merupakan jumlah kehilangan data yang dapat ditoleransi atau diterima ketika terjadi *disaster* oleh penyedia layanan dalam waktu tertentu.

2.4 *Service Level Agreement*

Service Level Agreement (SLA) merupakan kontrak antara penyedia layanan dengan pengguna atau customer dalam memberikan jaminan *service level* yang di inginkan. SLA berfungsi sebagai sikap optimis oleh sebuah *provider* dalam memberikan sebuah layanan dan memberikan tingkat kepercayaan kepada pengguna dalam menikmati layanan yang gunakan [10].

2.5 *Differential Backup Method*

Differential backup adalah salah satu metode *backup* yang dibuat berdasarkan data pada sebuah *database* yang memiliki *update* sejak dilakukan *full backup*. Posisi di mana sebuah *database* disebut *differential backup* adalah setelah dilakukannya *full backup*.

Secara umum *differential backup* memiliki ukuran yang lebih kecil dan lebih cepat dibandingkan dengan *full backup*. Keuntungan utama dari metode ini adalah jika terdapat sebuah *database* yang berukuran sangat besar maka proses *backup* akan mengalami penghematan waktu dan ukuran yang signifikan saat dilakukannya proses *backup* [11]. Keuntungan *differential backup* yaitu:

1. Waktu yang dibutuhkan untuk melakukan *restore* akan lebih singkat jika dibandingkan dengan metode *incremental backup.*
2. Apabila terdapat aktivitas *backup* dengan metode ini maka data yang di *backup* akan semakin kecil ukurannya.
3. *Backup* akan terasa lebih cepat jika dibandingkan dengan metode *full backup* dan membutuhkan *temporary storage* yang lebih kecil jika dibandingkan dengan metode *full backup.*

Gambar 1 *Differential Backup* [8]

2.6 Bacula

Bacula adalah sebuah aplikasi *backup-restore* yang berfungsi untuk melakukan pengaturan *backup, recovery*, dan verifikasi data komputer melalui sebuah jaringan dari sebuah komputer yang berbeda atau pada satu komputer yang sama. *Software* ini mendukung berbagai media penyimpanan seperti *tape* dan *disk* serta cenderung lebih mudah digunakan karena berbagai macam *front end* untuk *software* ini. Bacula memiliki lisensi GNU *Version* 2 dan secara fungsi sama dengan aplikasi *propertary* lainnya seperti Legato Networker, dan ARCserverIT, oleh sebab itu *software* ini sangat cocok untuk perusahaan yang ingin melakukan *backup* secara berkala tanpa mengeluarkan banyak dana dalam pengoperasiannya [13]. *Software* bacula terdapat beberapa komponen yang memiliki fungsi yang berbeda-beda, antara lain [5]:

1. *Director Daemon* (*Director*)
   Merupakan *service program* yang membawahi semua *backup, restore*, verifikasi, dan operasi pengarsipan karena *daemon* ini berhubungan langsung dengan *daemon* yang lainnya.
2. *Storage Daemon* (SD)
   Merupakan aplikasi yang berguna untuk melakukan penyimpanan data-data yang akan di-*backup* dan berinteraksi dengan media penyimpanan data yaitu *physical backup media* atau *volume/disk* sehingga sering disebut sebagai *storage server*.
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 bertugas untuk melakukan pengelolaan indeks pada *file* yang telah di-*backup, log* dari aktivitas *job backup* atau *restore* ke dalam *database* sehingga sistem administrator dapat dengan mudah melakukan pengembalian data yang telah di-*backup*. *Database* tersebut disimpan dalam *database* MySQL, Postgresql, atau Sqlite.
5. Bacula *Console*
   Merupakan sebuah aplikasi berbasis *command line interface* (CLI) yang digunakan oleh sistem *administrator* untuk mengontrol bacula dan berkomunkasi dengan *daemon* bacula *director* dalam pengaturan konfigurasi. Bacula *console* terbagi menjadi tiga macam *interface* yang tersedia yaitu *text-based console interface, Qt-based interface*, dan *xwWidgest Graphical interface.*

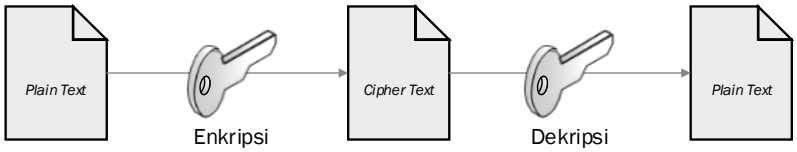
2.7 Kriptografi

Kriptografi merupakan ilmu mengenai teknik enkripsi, dimana data akan diacak menggunakan suatu kunci enkripsi menjadi sebuah data yang sulit dibaca oleh seseorang yang tidak memiliki kunci dekripsi. Dekripsi menggunakan kunci dekripsi untuk dapat membaca isi dari data yang telah dienkripsi sebelumnya. Proses enkripsi dilakukan menggunakan sebuah algoritma dengan beberapa parameter.

Algoritma dalam kriptografi biasanya tidak dirahasiakan, karena hal ini dinilai sesuatu yang kurang baik, akan tetapi yang menjadi kerahasian dalam sebuah kriptografi terletak pada beberapa parameter yang digunakan. Jadi kunci enkripsi ditentukan oleh parameter dan parameter yang menentukan kunci dekripsi yang harus dirahasiakan karena hal ini yang akan menjadi ekuivalen dengan kunci enkripsi. Berdasarkan kunci yang digunakan, kriptografi dibagi menjadi dua jenis, yaitu [14]:

1. Algoritma Simetris
   Algoritma ini disebut simetris karena mempunyai kunci yang sama dalam proses enkripsi maupun dekripsi, sehingga algoritma ini biasa disebut algoritma satu kunci atau kunci tunggal. Kunci pada algoritma ini bersifat rahasia atau *private key*, sehingga disebut juga algoritma *private key*. Beberapa contoh algoritma simetris yaitu DES dan AES.
2. Algoritma Asimetris
   Algoritma ini disebut asimetris karena mempunyai kunci yang berbeda antara enkripsi dan dekripsi.

Kunci yang digunakan untuk melakukan enkripsi adalah *public key*, sedangkan kunci yang digunakan untuk melakukan dekripsi adalah *private key*.



Gambar 2 Proses Enkripsi dan Dekripsi

Kriptografi memiliki tujuan yang merupakan aspek keamanan dari sebuah informasi, terdapat empat tujuan dasar dari ilmu kriptografi, yaitu [15]:

2. Kerahasian Data
   Menjaga isi dari sebuah informasi dari orang lain yang tidak memiliki otoritas terhadap sebuah informasi kecuali yang memiliki kunci untuk melakukan dekripsi terhadap informasi tersebut.
3. Integritas Data
   Integritas data merupakan representasi dari sebuah kualitas sebuah data, hal ini sangat penting karena komputer dan orang-orang menggunakan informasi untuk membuat sebuah keputusan dan mengambil tindakan, secara sederhana dalam istilah bisnis, integritas data adalah jaminan bahwa data konsisten, bersertifikat dan dapat menjadi rujukan [16].
4. Autentikasi
   Identifikasi atau pengenalan berdasarkan kesatuan sistem atau informasi itu sendiri. Pihak yang saling berkomunikasi harus saling memperkenalkan diri satu sama lain serta informasi yang dikirimkan melalui sebuah kanal harus diautentikasi keasliannya, baik dari isi data dan waktu pengiriman.
5. Non-repudiasi
   Suatu usaha untuk menghalangi terjadinya sebuah penyangkalan pada pengiriman dan terciptanya sebuah informasi oleh yang mengirimkan atau yang membuat informasi.

2.8 CIA *Triad Model*

Data yang merupakan sumber informasi dapat dikatakan aman apabila memenuhi tiga parameter yang dikenal dengan istilah CIA/AIC *Triad Model* atau *Confidentiality, Integrity, and Availability Triad Model* [9]:

1. *Confidentiality* atau kerahasiaan, artinya pada suatu informasi yang bersifat rahasia hanya dapat diakses oleh pihak tertentu saja.
2. *Integrity* atau integritas, artinya data yang disimpan, ditransmisikan memiliki keutuhan yang tidak berubah.
3. *Availability* atau ketersediaan, artinya informasi dapat diakses oleh pihak yang memiliki hak akses, baik itu unttuk melihat atau memodifikasi.

2.9 *Quality of Service*

Quality of Service (QoS) adalah adalah sebuah metode yang dapat digunakan untuk melakukan pengukuran terhadap kualitas sebuah jaringan dan salah satu cara untuk mendefinisikan karakteristik dan sifat pada sebuah layanan. Pada QoS terdapat beberapa parameter salah satunya adalah *throughput* dan *delay.*

Throughput adalah parameter yang menjelaskan mengenai kecepatan pengiriman data yang diukur dalam satuan bps (*bit per second*) [17]. Berikut adalah rekomendasi *Telecommunications and Internet Protocol Harmonization Over Networks* (TIPHON) mengenai nilai suatu *throughput*:

Tabel 1 Kategori *Throughput* (Sumber : TIPHON)

Kategori *Throughput*	*Throughput* (%)	*Indeks*
Sangat Bagus	100	4
Bagus	75	3
Sedang	50	2

Kategori *Throughput*	*Throughput* (%)	*Indeks*
Buruk	< 25	1

Untuk mendapatkan nilai *throughput* dapat menggunakan rumus berikut:

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

Sedangkan *delay* adalah waktu tunda sebuah paket saat dikirim dari *source* ke *destination* yang diukur dalam satuan ms (*millisecond*). Berikut adalah rekomendasi *Telecommunications and Internet Protocol Harmonization Over Networks* (TIPHON) mengenai nilai suatu *delay:*

Tabel 2 Kategori *Delay* (Sumber : TIPHON)

Kategori *Delay*	*Delay* (ms)	*Indeks*
Sangat Bagus	<150	4
Bagus	150 – 300	3
Sedang	300 – 450	2
Buruk	>450	1

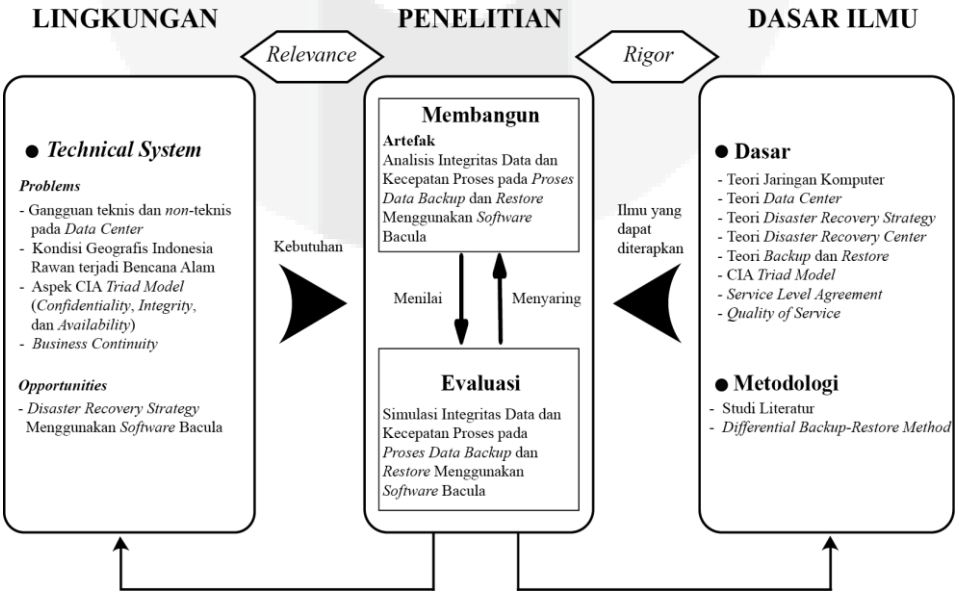
Untuk mendapatkan nilai *delay* dapat menggunakan rumus berikut:

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

3. Metode Penelitian

3.1 Model Konseptual

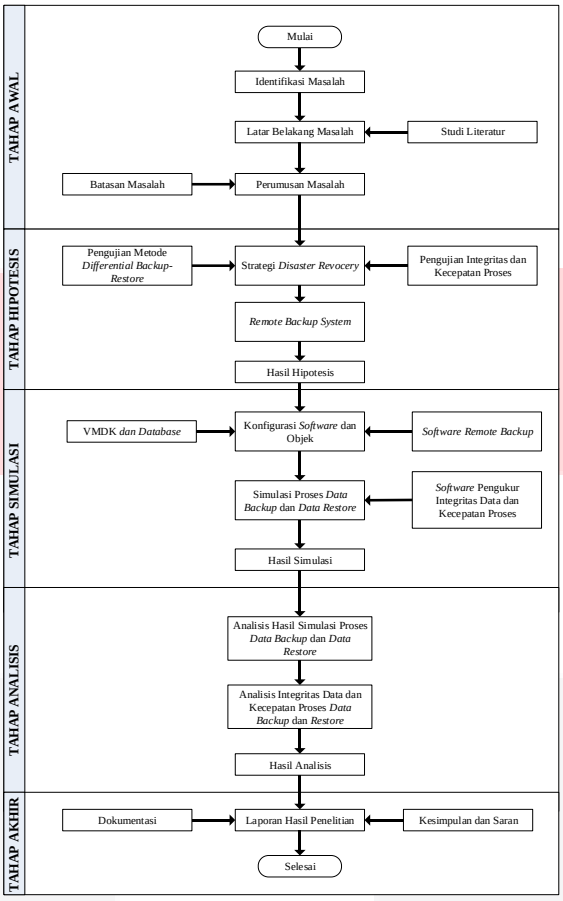
Model konseptual adalah deskripsi singkat mengenai bagaimana suatu sistem diorganisasikan dan bekerja [18]. Fungsi utama dari model konseptual sangat erat hubungannya dengan teori referensi atau literatur yang digunakan. Dengan bantuan model konseptual, peneliti dapat menunjukkan bagaimana melihat fenomena yang ada pada penelitiannya. Konsep-konsep teoritis yang digunakan untuk membangun model konseptual memberikan perspektif atau sebuah cara untuk melihat fenomena empiris [19]. Model konseptual yang ada pada penilitian ini adalah sebagai berikut:



Gambar 3 Model Konseptual Penelitian

3.2 Sistematika Penelitian

Sistematika penelitian terdiri dari beberapa langkah yang dilakukan selama pengerjaan penelitian ini yang bersifat terstruktur dan sistematis. Dimulai dari tahap awal identifikasi masalah hingga laporan hasil penelitian. Sistematika penulisan yang terdiri dari beberapa langkah dilakukan sebagai berikut:

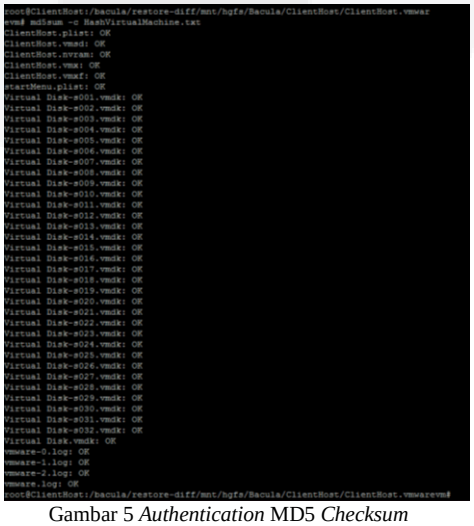


Gambar 4 Sistematika Penelitian

4. Hasil dan Analisis

4.1 Analisis MD5 *Checksum*

Berikut adalah hasil proses autentikasi dari skenario pengujian integritas data dengan target *backup* VMDK *ClientHost* menggunakan algoritma MD5:



Gambar 5 *Authentication* MD5 *Checksum*

Berdasarkan hasil pengujian skenario integritas data dengan target *backup* VMDK

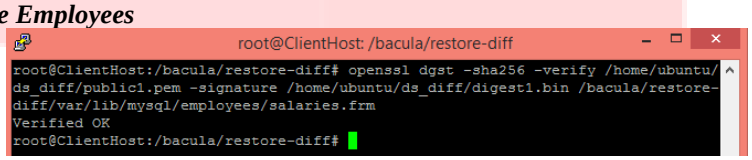
ClientHost, dapat dianalisis bahwa data pada VMDK *ClientHost* mendapatkan status verifikasi OK pada seluruh *file* yang ada di dalam direktori *ClientHost*, hal ini berarti *file* tetap dalam keadaan utuh atau *original*, dan tidak mengalami perubahan sejak dilakukan proses *data backup* hingga dilakukan proses *data restore*. Hasil tersebut memenuhi aspek *information security* berdasarkan *(Confidentiality, Integrity, and Availability Triad Model)* atau CIA *Triad Model*, di mana kerahasiaan data dari pihak yang tidak berwenang untuk mengakses data dapat diandalkan karena keutuhan data tidak mengalami modifikasi dengan status verifikasi yang dihasilkan seperti pada gambar selama menjalankan proses *data backup* dan *restore*, dan ketersediaan dari data yang telah berhasil di-*restore* ketika data dibutuhkan menunjukkan bahwa seluruh data tersebut tersedia dan dapat diakses oleh pihak yang berwenang saat diperlukan jika terjadi suatu kondisi abnormal pada DC.

Hasil pengujian tersebut tentunya dapat menjadi referensi untuk dijadikan sebuah *service level agreement* atau SLA untuk mendukung *business continuity* khususnya mengenai tingkat jaminan keamanan yang di-*provide* kepada *client* pada proses *data backup* dan *restore* dengan target *backup operating system* dan aplikasi dengan menggunakan metode *differential backup-restore*.

4.2 Analisis *Digital Signature* RSA

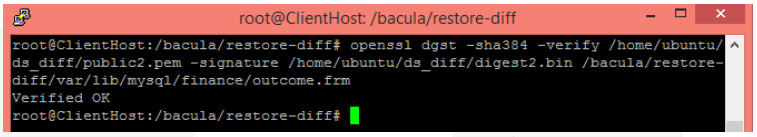
Berikut adalah hasil proses autentikasi dari skenario pengujian integritas data dengan target *backup* MySQL *database* menggunakan parameter *digital signature*:

Verify Database Employees



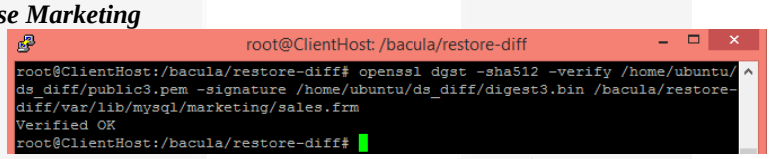
Gambar 6 *Database Employees Verified*

Verify Database Finance



Gambar 7 *Database Finance Verified*

Verify Database Marketing



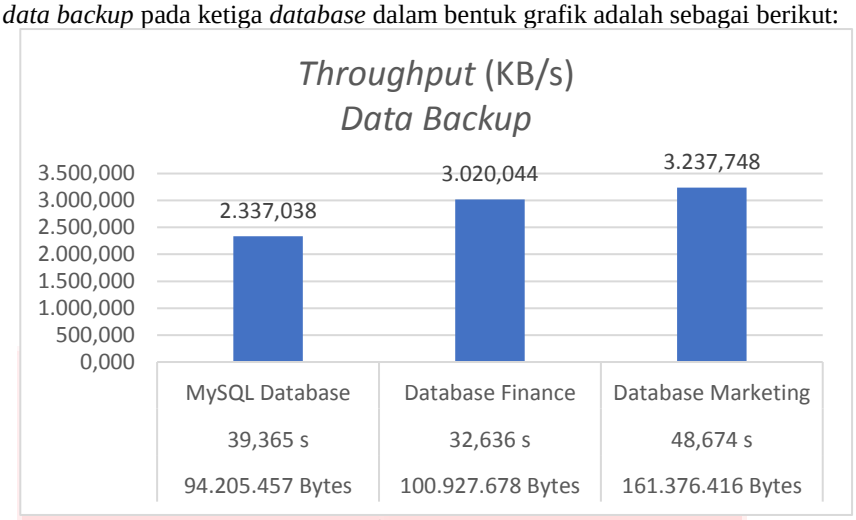
Gambar 8 *Database Marketing Verified*

Berdasarkan hasil pengujian dari skenario integritas data pada objek MySQL *database*, *database finance*, dan *database marketing*, dapat dilihat pada *input file* masing-masing *database* dan *signature* memiliki kesamaan dengan *output status* yang dihasilkan yaitu *verified OK*, status tersebut menandakan bahwa *database* yang telah berhasil di-*restore* tidak mengalami gangguan baik itu kerusakan data, kehilangan data, dan modifikasi berupa penambahan atau pengurangan data sejak *data backup* hingga *data restore* dilakukan. Pengujian tersebut memenuhi aspek *information security* berdasarkan *(Confidentiality, Integrity, and Availability Triad)* atau CIA *Triad Model*, di mana kerahasiaan data khususnya tabel data yang terdapat pada *database employees*, *finance*, dan *marketing* terjamin keamanannya dengan hasil verifikasi *integrity* yang tidak mengalami modifikasi, dan ketersediaan data yang dapat diandalkan ketika data ingin di-*restore*. Selain itu data yang telah di-*restore* juga telah diautentikasi keasliannya.

Menggunakan *digital signature* untuk menjaga integritas data lebih dapat diandalkan jika dibandingkan dengan *hash* MD5, karena *digital signature* melakukan pengamanan data dengan *asymetric key*. Hasil pengujian ini sangat penting bagi keberadaan data pada suatu organisasi, mengingat *database* menyimpan data secara terpusat dan sistematis sebagai sumber informasi bagi suatu organisasi dalam menjalankan proses bisnisnya, oleh karena itu *database* yang merupakan sebuah *asset* bagi suatu organisasi harus dijaga keamanannya. Hasil pengujian ini dapat menjadi referensi yang relevan untuk dijadikan sebuah *service level agreement* atau SLA untuk mendukung *business continuity* khususnya mengenai tingkat jaminan keamanan yang di-*provide* kepada *client* pada proses *data backup* dan *restore* pada target *backup* MySQL *database* dengan menggunakan metode *differential backup-restore*.

4.3 Analisis *Throughput Data Backup*

Hasil pengujian dari skenario kecepatan proses dengan parameter *throughput* pada saat dilakukan *data backup* pada ketiga *database* dalam bentuk grafik adalah sebagai berikut:



Gambar 9 Grafik *Throughput Data Backup*

Berdasakan hasil *data backup* pada pengujian objek-1 dengan target MySQL *database* yang menggunakan metode *default* yaitu metode *full backup*, menghasilkan nilai *throughput* pada *data backup* sebesar 2.337,038 KB/s. Sedangkan pada pengujian objek-2 dan objek-3 dengan target *database finance* dan *marketing* yang menggunakan metode *differential backup*, mengalami peningkatan nilai *throughput* yaitu dari 3.020,044 KB/s dan 3.237,748 KB/s.

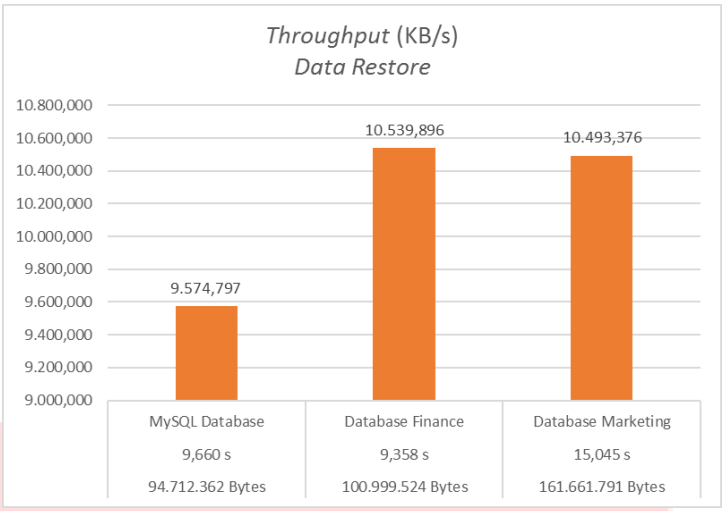
Hasil tersebut tergolong cepat karena sejak pengujian objek-1 hingga objek-3 dilakukan, *throughput* terus mengalami peningkatan pada proses transmisi data sebesar 683,006 KB/s pada pengujian objek-2 dan 217,704 KB/s pada pengujian objek-3. Selain itu dapat dilihat juga pada durasi waktu yang diperlukan untuk melakukan *data backup* yang fluktuatif, di mana pada pengujian objek-2 mengalami kecepatan tertinggi, yaitu sebesar 32,636 detik dalam melakukan *data backup*, sedangkan pada pengujian objek-1 dan objek-3 masing-masing membutuhkan waktu selama 39,365 dan 48,674 detik.

Hasil pengujian objek-2 tersebut dipengaruhi oleh metode *differential backup* yang digunakan, di mana hanya melakukan *backup* terhadap data yang baru ditambahkan, yaitu *database finance*, sedangkan pada pengujian objek-3 menjadi pengujian yang memerlukan waktu paling lama, kondisi tersebut disebabkan karena pada pengujian ini melakukan *backup* pada *database* yang baru ditambahkan yaitu *database marketing*, dan juga melakukan *backup* pada *database* pengujian objek-2, oleh karena itu durasi waktu yang dihasilkan tersebut dipengaruhi oleh besar ukuran data yang diproses, serta adanya proses kompresi terlebih dahulu dalam bentuk GZIP pada sistem bacula.

Nilai *throughput* merupakan hal terpenting khususnya terkait dengan aspek *availability* pada CIA *Triad Model*, karena hal tersebut menyangkut bagaimana kecepatan pemrosesan data pada saat sebuah data diperlukan. Dari pengujian yang telah dilakukan, terjadi peningkatan *throughput* pada setiap pengujian, sehingga dapat disimpulkan bahwa semakin besar ukuran data yang diproses, nilai *throughput* akan juga mengalami peningkatan, hasil pengujian tersebut dapat digunakan sebagai referensi dalam menentukan SLA terkait *throughput data backup* untuk mendukung BCP.

4.4 Analisis *Throughput Data Restore*

Hasil pengujian dari skenario kecepatan proses dengan parameter *throughput* pada saat dilakukan *data restore* pada ketiga *database* setelah dilakukan *data backup* dalam bentuk grafik adalah sebagai berikut:



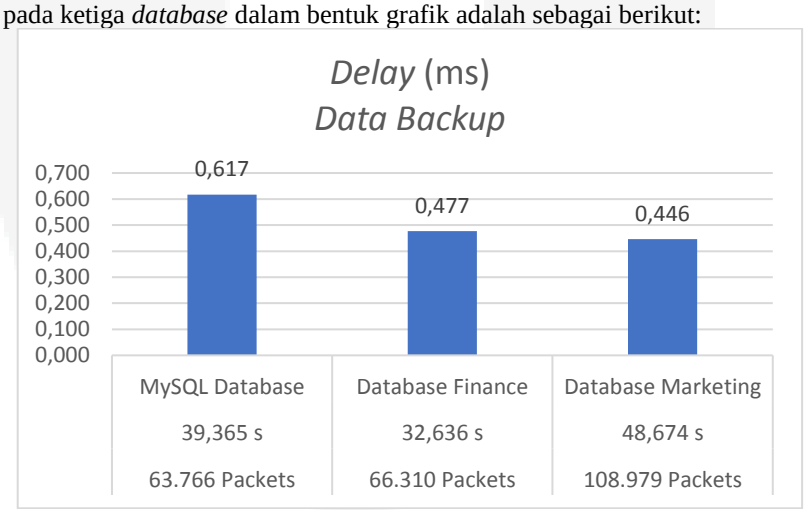
Gambar 10 Grafik *Throughput Data Restore*

Gambar 10 menunjukkan hasil *data restore* pada pengujian objek-1 dengan target MySQL *database*, menghasilkan nilai *throughput* sebesar 9.574,797 KB/s. Sedangkan pada pengujian objek-2 dan objek-3 dengan target *database finance* dan *marketing* mengalami kondisi fluktuatif cenderung menurun, yaitu sebesar 10.539,896 KB/s dan 10.493,376 KB/s. Kondisi fluktuatif tersebut juga terjadi pada durasi waktu yang dibutuhkan selama menjalankan *data restore.*

Dikarenakan ukuran data yang semakin besar pada pengujian objek-1, 2, dan 3, sehingga terlihat pada grafik hasil pengujian, yang menunjukkan penurunan pada *throughput* dan durasi waktu yang diperlukan lebih lama, tentunya hasil pengujian ini dapat menjadi acuan khususnya terkait RTO pada SLA, dan dapat menjadi pertimbangan yang cukup besar dalam memenuhi aspek *availability* pada CIA *Triad Model.*

4.5 Analisis *Delay Data Backup*

Hasil pengujian dari skenario kecepatan proses dengan parameter *delay* pada saat dilakukan *data backup* pada ketiga *database* dalam bentuk grafik adalah sebagai berikut:



Gambar 11 Grafik *Delay Data Backup*

Gambar 11 menunjukan hasil pengujian *delay* pada *data backup.* Pengujian objek-1 menghasilkan *delay* sebesar 0,617 ms dan pada pengujian objek-2 menghasilkan nilai 0,477 ms, sedangkan pada pengujian objek-3 menghasilkan nilai *delay* sebesar 0,446 ms. Ketiga pengujian tersebut menghasilkan waktu *delay* yang sangat kecil, hal ini disebabkan karena pada pengujian ini menggunakan topologi lokal yang langsung terhubung antara *BackupServer* dan *ClientHost*, sehingga tidak adanya hambatan seperti pada jaringan luar atau internet. Jika pada topologi pengujian diasumsikan terhubung oleh jaringan luar dengan *delay* sebesar 50 ms, maka seluruh hasil perhitungan tersebut ditambahkan dengan *delay* jaringan luar, sehingga asumsi rata-rata waktu *delay data backup* yang dihasilkan adalah 50,513 ms.

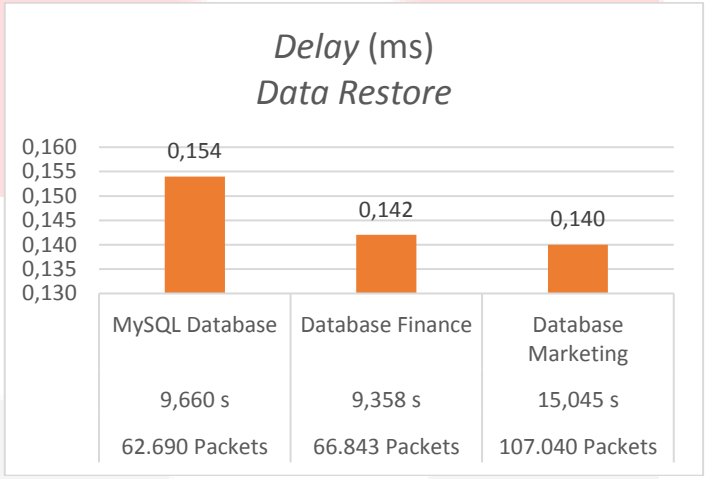
Seluruh hasil pengujian menunjukkan bahwa waktu *delay* yang dihasilkan termasuk dalam

kategori sangat baik, dengan perolehan indeks 4 berdasarkan standar TIPHON dengan *range* nilai *delay* <150 ms. Dengan hasil tersebut dapat disimpulkan bahwa pengujian ini dapat diimplementasikan pada banyak skenario pengujian *data backup* dan *data restore*, dengan tetap memperhatikan *instrument hardware* dan *software* yang digunakan harus sama atau lebih baik dari pengujian ini.

Waktu *delay* yang dihasilkan dapat memenuhi aspek *availability* pada CIA *Triad Model*, khususnya terkait performa ketersediaan data saat diperlukan dengan waktu *delay* yang semakin kecil. Kondisi tersebut dapat menjadi tolak ukur bagi suatu organisasi dalam menentukan RPO pada SLA untuk mendukung *business continuity*.

4.6 Analisis *Delay Data Restore*

Hasil pengujian dari skenario kecepatan proses dengan parameter *delay* pada saat dilakukan *data restore* pada ketiga *database* setelah dilakukan *data backup* dalam bentuk grafik adalah sebagai berikut:



Gambar 12 Grafik *Delay Data Restore*

Gambar 12 menunjukan hasil pengujian *delay* pada *data restore*. Pengujian objek-1 menghasilkan nilai *delay* sebesar 0,154 ms dan pada pengujian objek-2 menghasilkan nilai *delay* sebesar 0,142 ms, sedangkan pada pengujian objek-3 menghasilkan nilai *delay* sebesar 0,142 ms. Ketiga pengujian tersebut menghasilkan waktu *delay* yang sangat kecil, hal ini disebabkan karena pada pengujian ini masih menggunakan topologi lokal yang langsung terhubung antara *ClientHost* dan *BackupServer*, sehingga tidak adanya hambatan seperti halnya pada jaringan luar. Jika pada topologi pengujian diasumsikan terhubung oleh jaringan luar dengan waktu *delay* sebesar 50 ms, maka seluruh hasil perhitungan tersebut ditambahkan dengan waktu *delay* jaringan luar, sehingga asumsi rata-rata waktu *delay data restore* yang dihasilkan adalah 50,145 ms.

Hasil pengujian tersebut termasuk dalam kategori sangat baik, dengan perolehan indeks 4 berdasarkan standar TIPHON dengan nilai *delay* yang dihasilkan <150 ms. Waktu *delay* yang dihasilkan dapat memenuhi aspek *availability* pada CIA *Triad Model*, khususnya terkait performa ketersediaan data saat diperlukan dengan waktu *delay* yang semakin kecil. Kondisi tersebut dapat menjadi tolak ukur bagi suatu organisasi dalam menentukan SLA untuk mendukung *business continuity*.

Delay pada ketiga pengujian *data backup* dan *restore* menghasilkan waktu *delay* yang sangat kecil, sehingga dapat disimpulkan bahwa waktu yang diperlukan oleh sebuah paket dalam proses transmisi data pada *data restore* dapat diandalkan, karena meskipun total paket yang ditransmisikan mengalami peningkatan pada setiap pengujian, waktu *delay* yang dihasilkan semakin kecil.

5. Kesimpulan dan Saran

5.1 Kesimpulan

Berdasarkan penelitian *Disaster Recovery Strategy* menggunakan *Software* Bacula dengan Metode *Differential Backup-Restore*, dapat diambil kesimpulan sebagai berikut:

1. Proses *data backup* secara *remote* menggunakan *software* bacula dengan metode *differential* terjadi pada saat terdapat sebuah data yang baru ditambahkan atau berubah sejak dilakukannya *full backup*. Sedangkan proses *data restore* dengan menggunakan metode *differential* dapat dilakukan dengan

menjalankan perintah *restore* berdasarkan *JobId* pada bacula *director* setelah proses *data backup* dengan metode *differential* telah berhasil dilakukan.

2. Analisis integritas data dan kecepatan proses pada aktivitas *data backup* dan *restore* dengan metode *differential backup-restore* adalah sebagai berikut*:*
   a. Berdasarkan hasil pengujian skenario integritas data dengan parameter MD5 dan *digital signature* RSA pada target *backup-restore* sebuah *operating system* dan aplikasi berupa VMDK *ClientHost*, serta MySQL *database* tidak mengalami perubahan selama pengujian *backup* dan *restore* dilakukan sehingga hasil tersebut memenuhi aspek *information security* CIA *Triad Model* dan dapat menjadi referensi dalam merancang sebuah SLA untuk mendukung *business continuity*.
   b. Berdasarkan hasil pengujian skenario kecepatan proses *data backup* dan *restore* dengan parameter *throughput* pada target *backup-restore* yaitu MySQL *database* yang dilakukan sebanyak tiga kali pengujian dengan melakukan penambahan *database* disetiap pengujiannya, nilai *throughput* pada proses *data backup* pengujian objek-2 mengalami peningkatan sejak pengujian objek-1 sebesar 683,006 KB/s dan pada pengujian objek-3 sebesar 217,704 KB/s, sedangkan pada proses *data restore* menghasilkan nilai *throughput* yang fluktuatif, di mana pada pengujian objek-2 mengalami peningkatan sebesar 965,099 KB/s dan pada pengujian objek-3 mengalami penurunan sebesar 46,52 KB/s. Nilai *throughput* tersebut dapat menjadi referensi dalam merancang sebuah SLA khususnya mengenai *throughput* yang akan diterima *client* untuk mendukung *business continuity*.
   c. Berdasarkan analisis kecepatan proses *data backup* dan *restore* dengan parameter *delay* pada target *backup-restore* MySQL *database* yang dilakukan sebanyak tiga kali pengujian dengan melakukan penambahan *database* disetiap pengujiannya, waktu *delay* yang dihasilkan pada proses *data backup* dan *data restore* mengalami peningkatan, dimana waktu *delay* pada *data backup* pengujian objek-1, objek-2, dan objek-3 masing-masing menghasilkan *delay* sebesar 0,617 ms, 0,477 ms, dan 0,446 ms. Meskipun waktu *delay* yang dihasilkan tersebut telah dijumlahkan dengan asusmsi waktu *delay* jaringan luar sebesar 50 ms, waktu *delay* yang dihasilkan masih termasuk dalam kategori sangat baik dengan perolehan indeks 4 sesuai standar TIPHON. Waktu *delay* tersebut dapat menjadi referensi dalam merancang sebuah SLA khususnya mengenai waktu *delay* yang akan diterima *client* untuk mendukung *business continuity*.
   d. *Throughput* dan waktu *delay* yang dihasilkan tersebut bersifat tidak mutlak karena setiap pengujian yang dilakukan dipengaruhi oleh berbagai faktor yang ada pada suatu jaringan, seperti spesifikasi *hardware* yang digunakan, utilisasi pada jaringan yang digunakan, ukuran data, tipe data, jumlah pengguna, dan topologi jaringan yang digunakan pada saat pengujian.
   e. Durasi waktu yang dibutuhkan untuk melakukan proses *data restore* lebih cepat dibandingkan dengan melakukan proses *data backup*.
   f. Metode *differential* yang digunakan pada pengujian ini memiliki pengaruh terhadap ukuran data dan durasi waktu yang dibutuhkan untuk melakukan proses *data backup* dan *restore*. Di mana pada pengujian objek-2 yang menggunakan metode *differential* memiliki ukuran data yang lebih kecil pada proses *data backup* serta waktu yang lebih singkat jika dibandingkan dengan pengujian objek-1 yang menggunakan metode *full*.

5.2 Saran

Adapun saran yang dapat diberikan dari hasil penelitian dan analisis yang telah dilakukan adalah sebagai berikut:

1. Dalam melakukan pengujian disarankan menggunakan *hardware* yang memiliki spesifikasi yang identik antara DRC *site* dan DC *site.*
2. Ketika melakukan pengujian disarankan melibatkan jaringan luar atau internet pada topologi pengujian agar pengukuran dari hasil *throughput* dan *delay* dapat lebih akurat dan menghasilkan nilai yang mendekati kondisi asli jika diimplementasikan.
3. Backup dengan target sistem operasi dilakukan dalam periode tertentu sesuai dengan *update* pada sistem operasi serta membuat sistem operasi tersebut menjadi ISO agar *data backup* dan *data restore* dapat dilakukan dengan mudah.
4. Untuk penelitian selanjutnya dari segi *non*-teknis dapat dilanjutkan dengan fokus penyusunan suatu DRP dan SLA untuk mendukung BCP.

6. Daftar Pustaka

[1] A. Kadir, Pengenalan Sistem Informasi, Yogyakarta, 2003.

[2] M. &. C. Bullock, "Data Center Definition and Solutions," August 2014. [Online].

[3] Lintasarta, 2015 Oktober 2015. [Online]. Available: http://blog.lintasarta.net/article/operasional-perusahaan-jadi-lebih-mudah-dengan-server-data-center-terbaik/.

[4] F. Ridho, N. P. Yudho and R. H. P, "Disaster Recovery Center (DRC)," 14 November 2012. [Online]. Available: https://www.slideshare.net/fariderdotcom/disaster-recovery-center-and-disaster-recovery-plan.

[5] Eric, 08 Agustus 2011. [Online]. Available: http://www.bacula.org/5.1.x-manuals/en/main/main/What_is_Bacula.html.

[6] R. K. Rolen, "Global Journal of Computer Science and Technology Interdiciplinary," *Disaster Recovery Center Establishment for T4 Data Center to Run the IT System in Power Utilities* , p. 13, 2013.

[7] Certified Public Accountant, "Alternatif Recovery Strategy," 29-30 October 2009. [Online]. Available: https://simponi.mdp.ac.id/materi201020112/TI407/051041/TI407-051041-637-17.pdf.

[8] U. Solehudin, "Business Continuity and Disaster Recovery Plan," 2005. [Online]. Available: http://ftp.gunadarma.ac.id/linux/docs/v06/Kuliah/MTI-Keamanan-Sistem-Informasi/2005/128/128P-08-final1.0-disaster-recovery-and-business-continuity-plan.pdf.

[9] CompTIA+, CompTIA Security+ SY0-40I Official Study Guide Student Editon, London: gtslearning, 2014.

[10] Chandra, "Apa itu Service Level Agreement?," 08 Juni 2016. [Online]. Available: https://servernesia.com/1460/apa-itu-sla/.

[11] S. M. I Putu Agus Eka Pratama, "Jaringan Komputer," 2003. [Online]. Available: ftp://ftp.itb.ac.id/pub/ISO-IMAGES/.../presentasi-ittelkom.pdf.

[12] CloudBerry Lab, February 2017. [Online]. Available: https://www.cloudberrylab.com/incremental-backup-vs-differential-backup.aspx.

[13] Bacula.org, "Bacula," 2017. [Online]. Available: https://blog.bacula.org/what-is-bacula/supported-operating-systems/.

[14] M. Riadi, "Pengertian, Sejarah dan Jenis Kriptografi," 13 Januari 2014. [Online]. Available: https://www.kajianpustaka.com/2014/01/pengertian-sejarah-dan-jenis-kriptografi.html.

[15] A. Musfiroh, "Mas Tekno," 19 Oktober 2017. [Online]. Available: https://www.mastekno.com/pengertian-tujuan-dan-jenis-jenis-kriptografi-rumus-penyelesaian/.

[16] M. D.Sinaga, "Integritas Basis Data," 18 October 2017. [Online]. Available: dinus.ac.id/repository/docs/ajar/Integritas_Basis_Data.ppt.

[17] R. Wulandari, "Analisis QoS (Quality of Service) Pada Jaringan Internet (Studi Kasus : UPT Loka Uji Teknik Penambangan Jampang Kulon - LIPI)," *Jurnal Teknik Informatika dan Sistem Informasi*, pp. 163-164, 2016.

[18] J. Wiley and Sons, "Interaction Design," in *Beyond Human-Computer 2nd edition*, 2002, p. 22.

[19] J. Jonker, B. J.W., Pennink and S. Wahyuni, Metodologi Penelitian. Panduan Untuk Master Ph.D di bidang Manajemen, Jakarta: Salemba Empat, 2011.