PENYIMPANAN DATA BERBASIS CLOUD SEBAGAI MITIGASI BENCANA KERUSAKAN DATA

Asril Basry
Fakultas Teknik, Program Studi Sistem Informasi
Universitas Persada Indonesia YAI Jakarta
Email: basrya@hotmail.com

ABSTRAK

Mitigasi dalam mengurangi risiko kerusakan data dimana bencana yang dimaksud seperti terjadi kebakaran , bencana alam , perang dll sehingga dapat menyebabkan kerusakan pada infrastruktur teknologi informasi dalam hal ini adalah media penyimpanan data. Salah satu strategi yang dilakukan suatu perusahaan adalah membuat perencanaan mitigasi kerusakan dengan memanfaatkan teknologi penyimpanan data yang berbasiskan *cloud*. Adapun *cloud storage* merupakan salah satu bagian dari cloud computing yang dilakukan oleh pihak penyedia layanan ini atau *internet provider*. Perusahaan harus memiliki strategi penyimpanan data berbasiskan *cloud* dengan menyalin atau *back up* data kedalam *cloud storage* dengan diupdate atau dimutakhirkan secara berkala sehingga jika suatu kondisi terjadi bencana yang menyebabkan tidak berfungsinya fasilitas dan infrastruktur teknologi informasi dalam hal ini media penyimpanan data (*data storage*) , maka perusahan dapat melanjutkan pengolahan data dengan menggunakan data yang disimpan dalam penyimpanan data yang berbasiskan *cloud*, adapun dalam penyimpanan data yang berbasiskan *cloud* tetap menjamin terhadap keamanan dan kerahasian data perusahaan.

Kata kunci: mitigasi, strategi, pemulihan, bencana, penyimpanan awan, keamanan.

ABSTRACT

Mitigation for Data Loss disaster which is fire , geographical fenomena and war etc, are able to destroy information technology infrastructure especially data storage . One of several strategies that the company plan to create data mitigation using cloud storage tecknology. The cloud storage is a part of cloud computing that is provided by other parties or internet provider. The company must has the strategy of data saving using cloud storage to copy or back up data into cloud storage and continue for regularly data updating. if the disaster will be occured and all facilities and IT infrastructure will be malfunction such as data storage, so The company will continue their data processing using back up data in cloud storage that it can guarantee the company data to be safety and confidentiality.

Keywords: *mitigation, strategy, recovery, disaster, cloud storage, safety.*

1. PENDAHULUAN

1.1 Latar Belakang

Dalam suatu jaringan komputer di suatu perusahaan terutama di perusahaan besar dan multi nasional , mitigasi bencana kerusakan data merupakan sesuatu strategi yang sangat penting dalam menghadapi kejadian bencana yang tidak diharapkan terhadap infrastruktur teknologi informasi. Apabila hal ini tidak dilakukan maka perusahaan akan mendapat kesulitan untuk melanjutkan proses pengolahan data dan bias memungkinkan dapat dapat mengakibatkan bisnis di perusahaan akan terhenti (*business interruption*). Dalam suatu insiden dimana suatu misanya suatu kebakaran terhadap sebuah server-room dimana berada didalamnya semua server- menghancurkan semua yang ada didalamnya termasuk semua server dan infrastruktur pendukungnya seperti router, switches, jaringan kabel termasuk media penyimpanan data atau data *storage* dan apapun – semuanya tak tersisa sama sekali , sehingga perlu diadakan pemulihan terhadap infrastruktur yang tidak berfungsi tadi.

Data merupakan suatu yang sangat penting sehingga untuk pemulihan agar bisa beroperasinya pengolahan data dan diakses oleh pemakai atau user bisa menggunakan teknologi komputasi awan dimana data perusahan yang disimpan di suatu provider penyedia layanan *cloud storage* dan dapat direstore sehingga proses pegolahan data dapat dilanjutkan seperti sebelum terjadinya bencana [1].

1.2 Perumusan masalah

Perusahaan sudah seharusnya mengelola infrastruktur sistem dan melindunginya terhadap segala macam bentuk ancaman dan bahaya yang mengganggu jalannya pengoperasian dan pengolahan data serta juga mengelola sistem mitigasi bencana kerusakan data dan *business continuity planning* [2] setelah pasca bencana terhadap segala macam bentuk kerusakan dan kehilangan data dalam hal adanya bencana tersebut.

Dalam membuat perencanaan pemulihan bencana terhadap infrastruktur teknologi informasi terutama kerusakan terhadap penyimpanan data (*data storage*) dibutuhkan suatu teknologi yang dapat mengatasi jika kerusakan terhadap penyimpanan data dan melakukan pemulihan segera (*data recovery*) sehingga proses pengolahan data tidak terhenti

1.3 Tujuan

Adapun tujuan dari mitigasi bencana kerusakan data diutamakan untuk mengatur dan mementukan suatu cara yang terstruktur untuk membuat keputusan jika suatu kejadian atau insiden yang mengganggu terjadi selain itu adalah untuk mengurangi ketidaktahuan dari perusahaan dan meningkatkan kemampuan perusahaan untuk sehubungan dengan bencana tersebut. Sesungguhnya, ketika suatu peristiwa yang mengganggu terjadi, perusahaan tidak akan mempunyai kemampuan untuk menciptakan dan melaksanakan suatu rencana pemulihan dengan segera. Oleh karena itu, jumlah perencanaan dan pengujian yang telah dilakukan sebelumnya akan menentukan kemampuan perusahaan tersebut dalam menangani pemulihan bencana terhadap teknologi informasi,.Tujuan tujuan dari rencana pemulihan bencana meliputi:

1 Melakukan proteksi dan perlindungan di perusahaan dari kegagalan penyediaan layanan jasa Komputer.
2 Memperkecil risiko keterlambatan suatu perusahaan dalam pegolahan data
3 Menjamin pengoperasian pegolahan data secara normal pasaca terjadinya bencana
4 Menggunakan suatu teknologi penyimpanan data online (*cloud storage*) diluar sistem penyimpanan data perusahaan [3].

2. PEMBAHASAN

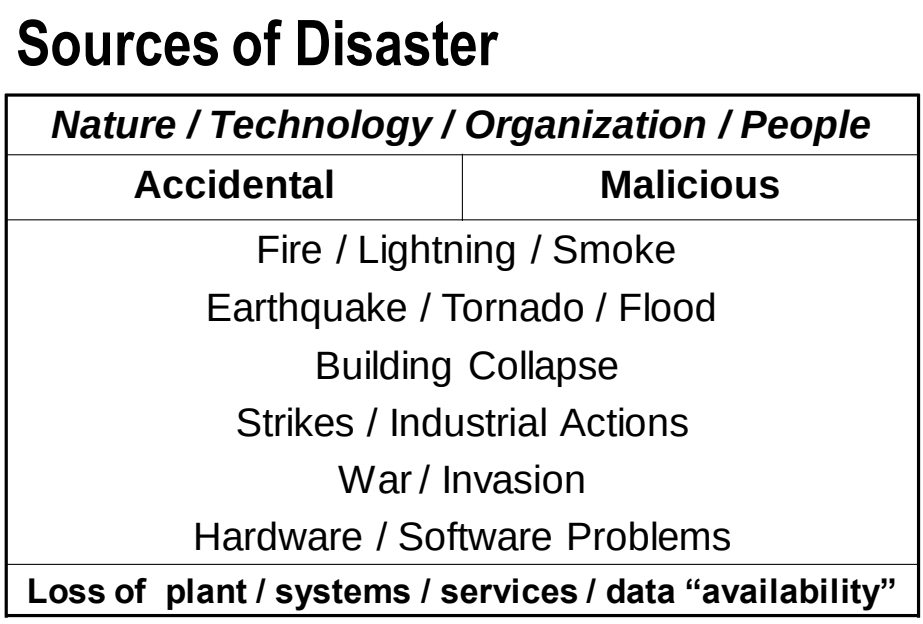
Mengirim data backup secara berkala ke tempat penyimpanan diluar ruang server disatu lokasi perusahaan (*offsite storage*) merupakan hal yang sering dilakukan oleh suatu perusahaan. Dengan tersedianya mesin server di tempat terpisah (dari server room yang terbakar atau rusak) maka bisa melakukan restore data ke mesin atau infrastruktur cadangan agar memungkinkan pemakai bisa mulai melanjutkan pekerjaannya dalam batas minimum agar bisa operasional saja. Proses inilah yang disebut bagian dari *Disaster Recovery* (DR) [4]. Saat terjadi bencana atau disaster kerusakan tidak hanya melanda ruang server tetapi juga tempat penyimpanan back-up data (*offstorage*) [5]

2.1 Strategi Pencegahan Dan Mitigasi Risiko

Dalam mitigasi bencana kerusakan data seharusnya juga mencakup strategi encegahan yang meliputi metoda-metoda yang harus diambil untuk menghindari potensi terjadinya suatu bencana terhadap infrastruktur teknologi informasi.

Selain itu dalam membuat perencanaan pemulihan bencana juga harus mengenali sumber sumber dari bencana seperti terlihat pada gambar 1. Berdasarkan dari sumber sumber diatas dapat dilakukan mitigasi dari resiko dan biasanya di-implementasikan sepanjang temuan potensi resiko. Berikut adalah contoh-contoh strategi pencegahan :

1. Backup dapat dilakukan dengan harian, mingguan, dan bulanan dan data disimpan offsite. Alasan disimpan terpisah atau offsite adalah kalau disimpan ditempat / di gedung yang sama, jika terjadi bencana seperti contohnya kebakaran , banjir , perang maka perusahaan kehilangan semuanya tidak hanya software dan aplikasi berikut juga dengan infrastruktur lainnya termasuk penyimpanan data atau *data storage*.
2. Memperbaiki dan mengelola dengan dengan baik keamanan data dan infrastruktur termasuk perlindungan terhadap firewall System yang bisa merupakan ancaman dari pihak luar sistem atau internet.



Gambar 1. Sumber – Sumber Bencana [8]

2.2 Risiko Sistem Data

Risiko sistem data berhubungan dengan penguunaan infrastruktur secara bersamaan seperti networks, file servers dan perangkat lunak aplikasi yang akan berdampak pada pengoperasian dan penggunaan komputer di perusahaan atau organisasi , kerusakan pada infrastruktur komputer termasuk penyimpanan data membutuhkan waktu yang lama dan tentunya dengan biaya yang cukup besar, untuk itu perlu dibuatkan kategori dari risiko sistem data sebagai berikut :

1. Data communication network
2. Telecommunication systems and network
3. Shared servers
4. Virus
5. Data backup/storage systems
6. Software applications and bugs

2.3 Menentukan Efek Dan Dampak Dari Bencana

Saat kita telah melakukan analisa terhadap risiko bencana dan selanjutnya menentukan efek dari bencana dan dampaknya terhadap pengoperasian dan penggunaan komputer di perusahaan atau organisasi, misalnya seperti gambar 2 dimana terjadi bencana gempa bumi atau *earthquake* dapat mengakibatkan kerusakan dari sistem data termasuk kerusakan media penyimpanan data (*data storage*) dan merupakan suatu yang sangat kriris apabila data sudah rusak dan tidak dapat digunan sehingga dapat memungkinkan pengolahan data menjadi berhenti serta bukan tidak mungkin bisnis diperusahaan menjadi terhenti *(Business interruption*)

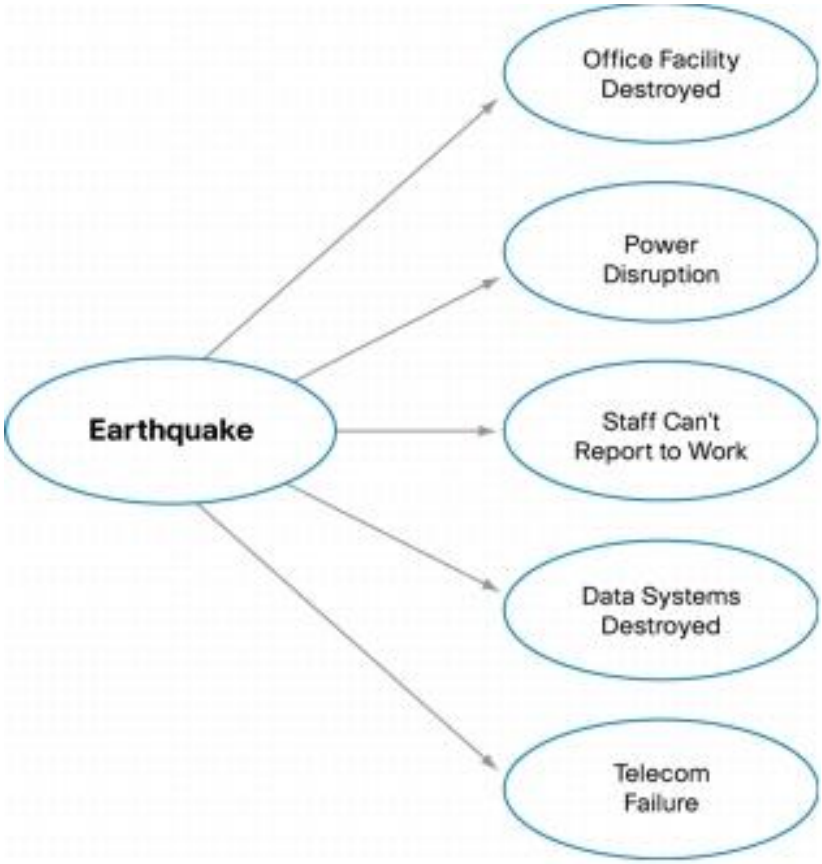
2.4 Prosedur Pemulihan Data

Perencanaan pemulihan bencana sebaiknya memiliki rincian prosedur untuk melakukan *restore system* atau *system components* sehingga pengoperasian teknologi informasi di perusahaan dapat normal kembali. Proses untuk melakukan pemulihan data terhadap pelayanan teknologi informasi adalah sebagai berikut :

1. Memberikan notifikasi dan pemberitahuan tentang Kerusakan kepada pemakai
3. Mendapatkan tempat bekerja dan infrastrukturnya
4. Mendapatkan dan install H/W beserta komponennya
5. Mendapatkan dan load backup data
6. Restore sistem operasi and software aplikasi

7. Restore sistem data dan load backup data
8. Melakukan test system functionality termasuk security controls
9. Melakukan koneksi sistem ke network atau jaringan luar lainnya

Untuk menghindari masalah saat situasi darurat pasca bencana diharapkan dibuatkan dokumentasi dari prosedur ini dengan format yang sederhana dan dilengkapi dengan langkah langkah untuk menjalankan prosedur pemulihan pencana teknologi informasi



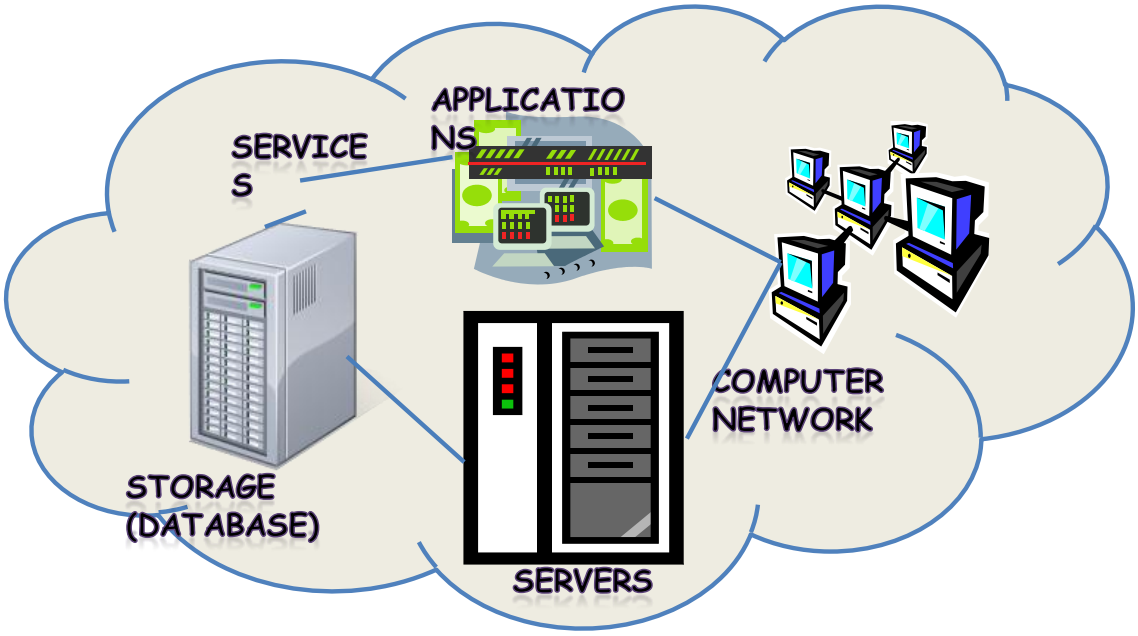
Gambar 2. Dampak Bencana Gempa Bumi [8]

2.5 Komputasi Awan

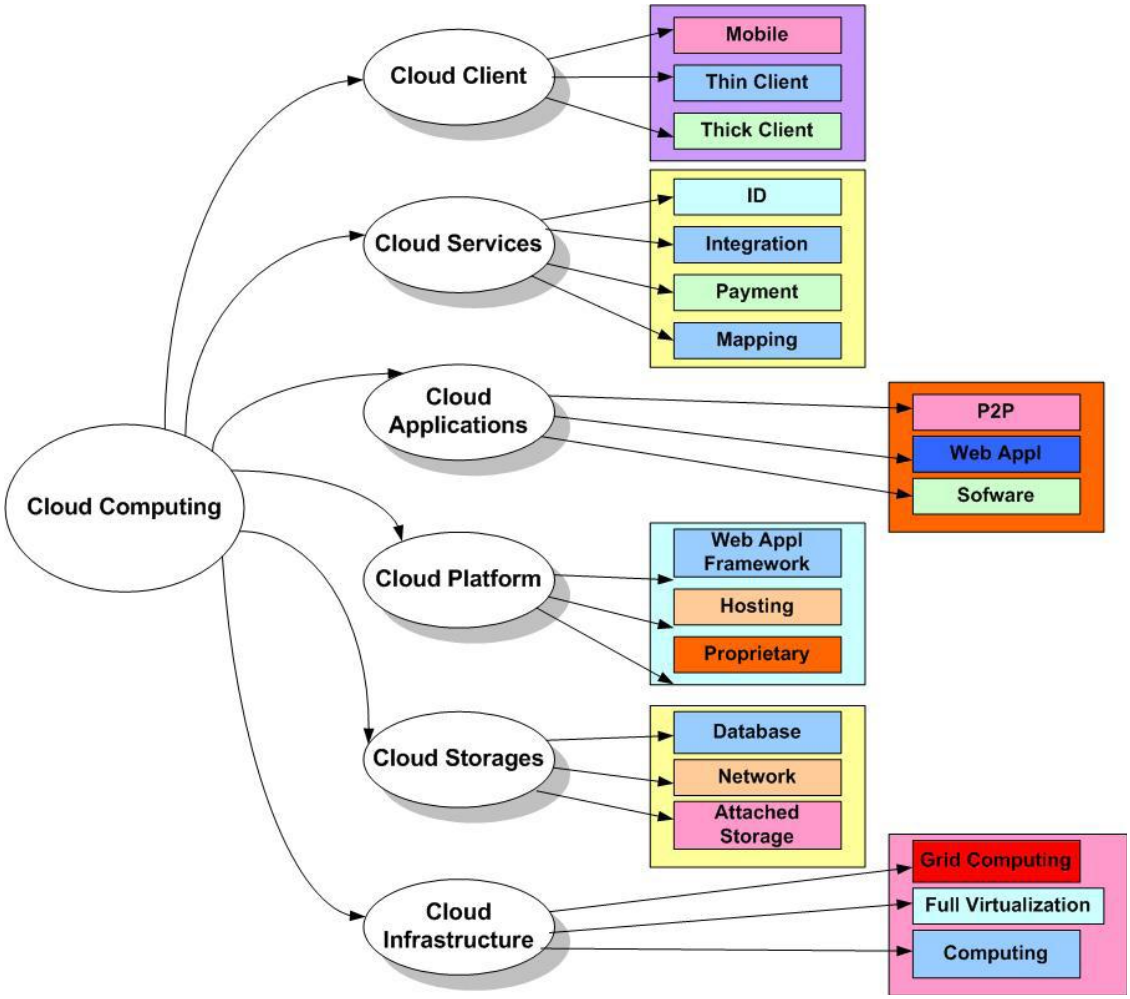
Cloud computing atau komputasi awan dimana data data layanan berada pada sumberdaya yang digunakan bersama (*shared resources*) dalam suatu pusat data dengan menggunakan internet. Komputasi awan merupakan teknologi yang memanfaatkan layanan menggunakan pusat server yang disediakan oleh suatu *provider* dan bersifat *virtual* [6] dengan tujuan pemeliharaan data Komputasi awan atau *cloud computing* dengan menggunakan suatu provider yang dapat memberikan pelayanan terhadap penggunaan perangkat lunak (*software*) , penyimpanan data (*data storage*) , Jaringan (*network*) serta komputasi data menggunakan server termasuk penggunaan Web [7]. (Gambar 3).

Salah satu layanan yang diberikan oleh *cloud computing* adalah *cloud storage* (Gambar 4). *Cloud storage* atau dikenal dalam bahasa baku penyimpanan awan adalah sebuah layanan penyimpanan data online yang terintegrasi dan tersinkronisasi melalui internet dan dapat di akses dengan menggunakan berbagai platform (OSX, iOS, Windows, WindowsMobile, Android, Linux, Blackberry, Symbian dan lain-lain). Komputasi awan menjadi buah bibir di dunia IT beberapa tahun belakangan ini beberapa pemain besar dunia IT lainnya seperti: Cisco, Oracle , Google, Microsoft hingga Amazon turut andil memperkenalkan produk terbaru mereka di dalam peta persaingan komputasi awan.

Penulis mengusulkan untuk melakukan back up data menggunakan *cloud storage* dimana menyalin data atau back up data dapat dilakukan dengan frekwensi harian , mingguan atau bulanan. Dimana jika terjadi suatu bencana terhadap teknologi informasi makan proses pemulihannya atau recovery dapat menggunakan data yang disimpan pada *cloud storage*,



Gambar 3. Konfigurasi Komputasi Awan [9]



Gambar 4. *Cloud Storages* [9]

3. KESIMPULAN

Dalam pembahasan penyimpanan data berbasiskan *cloud* dimana data merupakan suatu aset yang sangat penting diperusahaan sudah seharusnya perusahaan memberikan perlindungan sangat baik serta paling utama adalah perusahaan dapat melakukan pemulilhan kembali operasional pengolahan data tanpa kehilangan data berharga jika terjadi suatu bencana (*disaster*). Untuk itulah perusahaan harus mengembangkan startegi pencegahan terjadi kerusakan terhadapa penyimpanan data dan mitigasi risiko terhadap kerusakan data serta memiliki sistem perencanaan pemulihan bencana atau *disaster recovery planning* di suatu perusahaan

Perusahaan harus mengetahui tingkat risiko data serta dampak bila terjadi kerusakan atau bencana terhadap data , adapun penyimpanan berbasis *cloud* serta diikuti dengan perencanaan pemulihan data jika terjani bencana kerusakan data memberikan suatu kerangka kerja untuk mencegah serta membuat suatu penyelamatan / *recovery* data dari segala macam bencana baik yang berskala kecil maupun besar. Strategi penyimpanan berbasis *cloud* dan mitigasi bencana kerusakan data memberikan daftar yang sudah dibuat dan koordinasi dari langkah-langkah yang perlu dilakukan untuk meminimalkan akibat dari suatu bencana dan membantu perusahaan dalam mempercepat pemulihan sistem.

Dalam upaya penangan pemulihan bencana , penulis mengusulkan untuk menggunakan teknologi penyimpanan berbasis *cloud* dimana data –data disalin atau *back up* menggunakan penyimpanan data berbasiskan *cloud* yang merupakan salah satu pelayanan dari komputasi awan yang disediakan oleh *internet provider* , sehingga jika terjadi bencana data tersebut bisa dilakukan proses *restore* sehingga pengolahan data dapat dilanjutkan

DAFTAR PUSTAKA

[1] Carroll, M., Merwe, A., & Kotzé, P. Secure Cloud Computing Benefits , Risks and Controls. IEEE. 2011.

[2] Hasibuan, Z., Kurniawan, A., & Budiarto, R. (2010) "*Multi-Format Concept based Information Retrieval using Data Grid*.", Journal of Advanced Computing and Application Volume 1, Issue 1

[3] CSO Group (2010) , "Mitigating Security Risk In Cloud. Available ata : http://eval.*Symantec.com/mktginfo/enterprise/white papares/b-cso group mitigating securityRisk in cloud WP.en-us.pdf* [Retrieved on 2015-10-02 07:10 AM].

[4] L.A. Worbel ,"*Disaster Recovery Planning for Telecommunications*, ," *:* Artech House (US), 1990.

[5] Sun Microsystems Inc (2009), "Introduction to cloud computing Architecture ", http://www.sun.com/featured-articles/cloudcomputing.pdf, white papar, first edition June 2009: 1-32

[6] Hartic, K (2008), "What is cloud computing ? cloud computing journal available at: http://cloudcomputing.sys-con.com/node/579826," [diakses 09 September 2015]

[7] R. Frinkel, R. Taylor, R. Bolles, R. Paul, "An overview of AL, programming system for automation," *in Proc. Fourth Int. Join Conf Artif.Intel.*, pp. 758-765, Sept. 3-7, 2006.

[8] Saad Haj Bakry, *PhD, CEng, FIEE*, "Contigency and recovery Planning," *Presentation in network security*, pp. 758-765, Sept. 3-7, 2006.

[9] Rittinghouse, JW , & Ransome JF, 2010, "*Cloud computing Implementation , Management & Security*," New York : Taylor and Francis Group.