Terbit *online* pada laman web jurnal : http://teknosi.fti.unand.ac.id/

Jurnal Nasional Teknologi dan Sistem Informasi

| ISSN (Print) 2460-3465 | ISSN (Online) 2476-8812 |

Artikel Penelitian

Pembangunan *Auto Backup* SQL *Database Server* Menggunakan Raspberry Pi : Studi Kasus

Dwiny Meidelfi[a], *Hidra Amnur*[a], *Novri*[a]

[a]*Jurusan Teknologi Informasi Politeknik Negeri Padang, Kampus Limau Manis, Padang*

INFORMASI ARTIKEL

Sejarah Artikel:
Diterima Redaksi: 17 Maret 2018
Revisi Akhir: 29 Desember 2018
Diterbitkan *Online*: 31 Desember 2018

KATA KUNCI

Auto backup SQL database,
Raspberry Pi,
rsync

KORESPONDENSI

Telepon: +62813 8551 5030
E-mail: dwinymeidelfi@pnp.ac.id

A B S T R A C T

Pembangunan *auto backup* SQL *database server* bertujuan untuk menutupi kelemahan pada *database Server* jurusan Teknologi Informasi Politeknik Negeri Padang. Server ini menanggulangi kemungkinan terjadinya kerusakan data, kehilangan data atau kerusakan media penyimpan database. Raspberry Pi adalah mikro komputer yang digunakan sebagai *backup server*. Spesifikasi yang minim dapat digunakan secara optimal untuk membangun *backup server* karena tidak banyak sumber daya yang sia-sia. *Backup database* dilakukan dengan cara menggabungkan beberapa fungsi dari komponen sistem linux rsync dan crond Job. Rsync digunakan untuk proses pengiriman data dari database server ke *backup serv*er dan crond job digunakan untuk melakukan penjadwalan terhadap proses backup. Proses backup menggunakan komponen linux ini memiliki kemungkinan kegagalan backup yang minim karena rsync akan mengulangi setiap proses backup yang gagal atau kerusakan data hasil pengiriman.

1. PENDAHULUAN

Jurusan Teknologi Informasi (TI) merupakan salah satu jurusan di Politeknik Negeri Padang yang serius dalam mengikuti perkembangan teknologi informasi. Penggunaan teknologi hampir memenuhi setiap aspek pekerjaan di jurusan, diantaranya adalah penggunaan website, presensi perkuliahan, digital informasi, siaktif, kuesioner, perpustakaan dan inventaris jurusan TI. Dalam perencanaannya penggunaan teknologi informasi akan dikembangkan untuk seluruh aspek, sesuai dengan perkembangan teknologi dan kebutuhan jurusan.

Sistem informasi berbasis web merupakan salah satu teknologi yang sudah familiar digunakan di jurusan TI. Perkembangan yang selalu update, tersedia tenaga ahli dibidangnya, dan pengelolaan yang mudah menjadi alasan teknologi ini banyak digunakan di jurusan TI. Selain itu, sistem informasi berbasis web juga dikembangkan oleh tugas akhir mahasiswa. Hal ini berdampak terhadap penggunaan dan perkembangan teknologi informasi di jurusan TI.

Database memiliki peran paling penting dalam sebuah sistem informasi. Database terdiri dari kumpulan informasi yang disimpan di dalam komputer secara sistematik dan menggunakan program komputer untuk input dan output data. Format data yang disimpan berupa karakter, angka, huruf, foto, video dan audio. Pada umumnya, aplikasi atau sistem informasi *client-server* yang memiliki cakupan yang cukup besar dan data yang besar, sehingga *database* ditempatkan pada server khusus.

Pemanfaatan sistem informasi menggunakan web dan *database* memiliki ancaman yang dapat menimbukan kerugian bagi pengguna. Serangan virus, kerusakan perangkat, *human error*, dan serangan *hacker* dapat menimbulkan kerugian bagi penggunanya. Kehilangan *database* merupakan resiko yang paling buruk dalam pemanfaatan sebuah sistem informasi.

Saat ini, administrator sistem informasi jurusan TI Politeknik Negeri Padang melakukan *backup database* terhadap setiap perubahan data yang dilakukan, dan ada beberapa *database* dilakukan *backup* setiap hari. Setelah dilakukan berulang-ulang, cara ini masih menyisakan kelemahan yang harus ditanggulangi. Kelemahannya terdapat pada ketersediaan waktu, dan pekerjaan rutin yang harus dilakukan karena *database* dapat terjadi berubah setiap waktu.

https://doi.org/10.25077/ TEKNOSI.v4i3.2018.130-137

Attribution-NonCommercial 4.0 International. Some rights reserved

2. TINJAUAN PUSTAKA

2.1. Database

Database diartikan sebagai kumpulan data yang terintegrasi dan diatur sedemikian rupa sehingga data tersebut dapat dimanipulasi, diambil dan dicari secara tepat [1]. Selain berisi data, *database* juga berisi metadata. Metadata adalah data yang menjelaskan tentang struktur data itu sendiri. Sebagai contoh, dapat memperoleh informasi tentang nama-nama kolom dan tipe data yang ada pada sebuah tabel. Data nama kolom dan tipe yang ditampilkan tersebut disebut metadada. Motode *Backup Database* adalah kegiatan menyalin file atau *database*, sehingga salinan tersebut dapat digunakan untuk memulihkan data asli yang rusak karena berbagai sebab.

Pertumbuhan data yang tersimpan pada harddisk web sebagai data online berbanding lurus dengan pertambahan informasi yang disajikan, maka dibutuhkan antisipasi bilamana terjadi kerusakan data. Sekitar 70% bisnis mengalami kehilangan data akibat berbagai kecelakaan, seperti tidak sengaja terhapusnya data, kegagalan sistem, virus, kebakaran atau bencana lainnya, hal ini akan meransang pertumbuhan layanan backup data.

Dalam strategi backup dan recorvery data beberapa metode yang dapat digunakan yaitu [2]:

a. Backup Penuh (*Full Backup*)

Full backup adalah proses menyalin semua data termasuk folder ke media lain. Jika full backup ini dilakukan setiap hari, maka full backup totalnya dapat dilakukan seminggu sekali. Proses backup data ini membutuhkan waktu lebih lama karena akan menyalin semua dan setiap harinya dan membutuhkan media penyimpanan yang sangat besar. Hasil full backup ini lebih cepat dan mudah saat operasi restore.

b. Backup Peningkatan (*Incremental Backup*)

Incremental Backup adalah menyalin semua data yang berubah sejak terakhir kali melakukan full backup. Metode *incremental backup* membutuhkan semua file *incremental backup* agar *database* dapat direstore secara lengkap. Proses *backup* ini dapat dilakukan setiap hari sedangkan *backup* totalnya dapat dilakukan seminggu sekali. Oleh karena data yang dibackup adalah data yang sudah mengalami perubahan, maka waktu backup pun menjadi lebih cepat. Hal ini dimungkinkan ukurannya dan media penyimpanan pun lebih kecil, akan tetapi waktu yang dibutuhkan untuk proses *restore* lebih lama.

c. Backup Cermin (*Mirror Backup*)

Mirror backup sama dengan *full backup*, tetapi data tidak didapatkan atau dimanfaatkan (dengan format .tar .zip, atau yang lain) dan tidak bisa dilindungi dengan password. Mirror backup adalah metode backup yang paling cepat bila dibandingkan dengan metode lain, karena menyalin data dan folder ke media tujuan tanpa melakukan pemadatan. Tetapi hal itu menyebabkan media penyimpannya harus cukup besar.

2.2. Bash Linux Crontab

Crontab adalah sebuah perintah yang sangat berguna untuk menjalankan tugas-tugas yang terjadwal, sehingga akan mengurangi waktu administrasi. Selain crontab, ada juga perintah lain seperti anacron dan at. Anacron digunakan untuk melakukan penjadwalan suatu perintah untuk komputer yang tidak selalu menyala terus-menerus. Anacron menggunakan interval waktu harian, mingguan, dan bulanan. Sedangkan perintah at menjalankan suatu tugas sekali pada satu waktu, namun yang sering digunakan adalah crontab, karena lebih serbaguna, dan dapat diatur untuk berjalan pada sembarang interval waktu.

Dalam melakukan adminitrasi sistem, pengaturan cron dilakukan melalui file crontab, yang berisi jadwal waktu dan script yang harus dieksekusi. System Linux memiliki file crontab default, yaitu /etc/crontab, yang akan menjalankan beberapa script pada waktu yang telah ditentukan, misalnya setiap jam, harian, mingguan, dan bulanan.

Terdapat dua buah file yang menentukan user mana yang bisa menggunakan crontab: /etc/cron.allow dan /etc/cron.deny. Biasanya, hanya ada file cron.deny pada sistem, dan jika file ini ada, dan terdapat nama user didalamnya (satu user per baris), maka user tersebut tidak diperbolehkan menggunakan perintah crontab. Jika terdapat file cron.allow, maka hanya user yang namanya terdapat pada file ini yang diperbolehkan menggunakan perintah crontab. Pada file crontab, terdapat enam field untuk setiap entry, dan masing-masing field dipisahkan oleh spasi atau tab. Lima field pertama menentukan kapan perintah akan dijalankan. Field ke-enam adalah perintah yang akan dijalankan. Sebagai contoh script yang digunakan dalam crontab adalah sebagai berikut:

```
# min (0-59) hours  (0-23)   day(1-31)
  Month (1-12) dow (0-6) command
  34 2 * * *   sh   /root/backup.sh [3]
```

2.3. Raspberry Pi

Raspberry Pi merupakan sebuah komputer yang berukuran kecil yang dapat digunakan seperti sebuah Personal Computer (PC). Layaknya sebuah PC, Raspberry Pi membutuhkan Operating System (OS) agar dapat digunakan. OS ini disimpan dalam Secure Digital (SD) Card yang digunakan juga untuk media penyimpanan data seperti halnya hard disk. OS yang digunakan untuk Raspberry Pi merupakan varian dari OS Linux. Raspberry Pi digunakan sebagai web server yang akan melayani permintaan pengguna melalui web browser berupa tampilan halaman web yang telah ditanamkan dalam modul Raspberry Pi dengan web server yang dipilih untuk digunakan adalah web server apache, karena mudah dalam konfigurasi, mendukung untuk ditanamkan dalam modul Raspberry Pi dan dapat digunakan secara gratis. Tampilan halaman web yang ditampilkan tersebut digunakan sebagai antarmuka untuk mengontrol peralatan berupa lampu dan pompa air listrik. Selain digunakan sebagai web server, modul Raspberry Pi ini juga berfungsi untuk berkomunikasi dengan modem PLC menggunakan komunikasi serial.

Beberapa dari perangkat ini sangat lah penting, yang lainya bersifat opsional. Dalam pengoperasian Raspberry Pi sama saja dengan PC standart, membutuhkan keyboard untuk memasukan perintah, sebuah display dan sebuah power supply. Raspberry Pi membutuhkan sebuah perangkat penyimpanan menggunakan SD Card yang biasa digunakan pada digital kamera. SD card akan dikonfigurasi sedemikian rupa sehingga terlihat seperti harddisk untuk processor Raspberry Pi. Raspberry Pi akan melakukan booting (membuat sistem operasi ke RAM) dari SD card dengan

cara yang sama sperti komputer desktop boot up ke windows dari harddisk. Perangkat penting yang ditambahkan untuk pengoperasian Raspberry Pi [4]:
a. SD card yang berisi sistem operasi linux.
b. Keyboard USB dan monitor (dengan HDMI/DVI).
c. Power supply.
d. Kabel video graphic.

2.4. Keamanan Jaringan Komputer

Keamanan jaringan komputer sebagai bagian dari sebuah sistem informasi menjadi sangat penting untuk menjaga validasi dan integritas data serta menjamin ketersediaan layanan bagi penggunanya. Sistem harus dilindungi dari segala macam serangan dan usaha-usaha penyusupan atau pemindaian oleh pihak yang tidak berhak. Komputer yang terhubung kedalam jaringan mengalami ancaman keamanan yang lebih besar dari pada host yang tidak terhubung kemana-mana.

Dengan mengendalikan network security, resiko tersebut dapat dikurangi. Namun network security biasanya bertentangan dengan network acces, karena bila network acces semakin mudah, network security makin rawan. Bila network security makin baik, network access semakin tidak nyaman. Satu jaringan didesain sebagai komunikasi data highway dengan tujuan meningkatkan akses ke sistem komputer, semantara keamanan didesain untuk mengontrol akses. Penyediaan network security adalah sebagai aksi penyeimbang antara open acces dengan security [5].

a. Kendali Akses (Acces Control)
Kendali akses adalah sebuah kebijakan. Biasanya di implementasikan sebagai sebuah komponen hardware atau software, yang digunakan untuk membolehkan atau menolak user mengakses sumber daya yang terdapat dalam sebuah sistem komputer. Kendali akses hanya membolehkan user yang berhak saja yang dapat mengkases sumber daya dalam komputer. Dengan kendali akses kita dapat membatasi hak akses seorang user kedalam sistem untuk mengerjakantugas-tugas tertentu saja. Sehingga masing-masing user hanya dapat mengakses sumber daya yang ada dalam sistem komputer sesuai dengan hak yang diberikan kepada user tersebut. Ada 3 jenis metode access control yang biasanya diterapkan dalam sebuah organisasi untuk mengamankan akses user atau komputer kesumber daya yang ada dalam organisasi tersebut. Ketiganya yaitu : MAC (Mandatory Access Control), DAC (Discretionary Access Control) dan RBAC (Role-Based Access Control) [6].

b. Autentikasi (Authentication)
Autentikasi merupakan sebuah proses yang mem-verifikasi apakah *user* atau komputer yang mencoba untuk mengkases sumber daya dalam sistem komputer benar-benar user atau komputer yang sah atau tidak. *User* atau komputer diijinkan untuk mengakses sebuah sistem komputer dan seluruh sumber daya didalamnya jika sudah diautentikasi oleh komputer yang bersangkutan. Dalam mengamankan sistem komputer dari *user* yang tidak berhak maka diperlukan mekanisme autentikasi yang kuat [6].
c. Audit (Auditing)
Auditing adalah proses untuk melacak kegiatan-kegiatan, kesalahankesalahan, dan percobaan akses dan autentikasi ke dalam sebuah sistem komputer. Dengan *auditing* dapat membantu untuk mengidentifikasi kelemahan data yang ada dalam sistem komputer sehingga dapat menerapkan kebijakan keamanan yang tepat untuk sistem komputer. Audit sendiri terdiri dari berbagai macam jenis, yaitu: *System Auditing Functions, System Scanning Auditin, Logs File Auditin.* dan *Non-Essential Services Auditing* [6].

d. SSH (Secure Shell)
SSH (*secure shell*) adalah protokol jaringan yang berada pada lapisan aplikasi pada protokol jaringan TCP/IP. SSH memfasilitasi sistem komunikasi yang aman diantara dua sistem yang menggunakan arsitektur klien-server dengan menyediakan kerahasiaan dan integritas data melalui teknik enskripsi dan deskripsi yang dilakukan secara otomatis dalam koneksinya. SSH membutuhkan otentifikasi user berupa kunci umum dan *password* yang terenskripsi. SSH digunakan untuk mengendalikan komputer jarak jauh (*remote*), mengirim file, membuat terowongan yang terenskripsi (*tunneling/port forwading*) dan lain-lain. *Port forwarding* menyediakan kemampuan untuk mengkonversi koneksi TCP yang tidak aman ke koneksi SSH aman untuk pengalihan koneksi dari satu IP ke IP lain, sehingga seolah-olah klien menghubungi IP tujuan secara langsung. *Port forwarding* melalui *ssh* membentuk sambungan yang aman antara komputer lokal dengan komputer remote melalui layanan yang disampaikan [7].

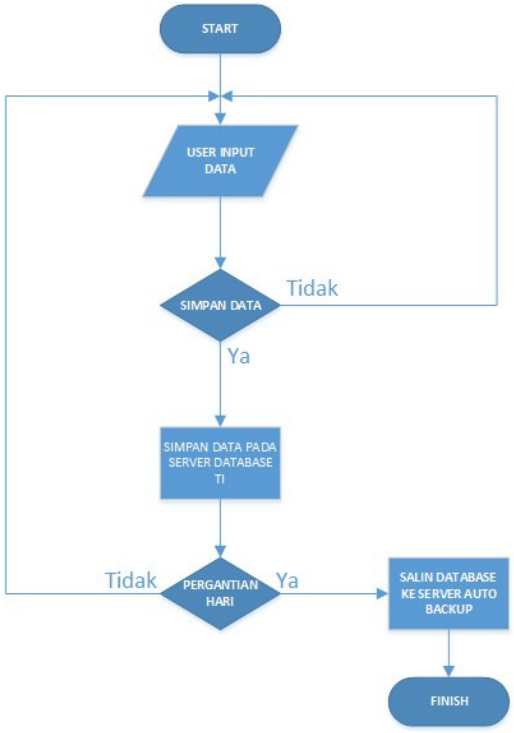
3. METODOLOGI

3.1. Flowchart

Proses analisis, merancang, mendokumentasikan atau mengelola suatu proses dibutuhkan flowchart untuk menyelesaikan beberapa permasalahan. Pada rancangan ini flowchart mewakili algoritma, alur kerja atau proses yang menunjukan langkah-langkah dengan simbol yang memiliki fungsi tersendiri. Simbol yang dihubungkan dengan panah menunjukan alur kerja dari sistem. Dalam rancangan ini flowchart menggambarkan solusi terhadap permasalah yang akan diselesaikan dalam implementasi. Presentasi rancangan sistem terdapat pada Gambar 1.

Proses membuat, membaca, mengubah dan menghapus data dilakukan pada sistem informasi jurusan TI, selanjutnya disimpan pada database server. Proses perubahan data ini dapat dilakukan setiap saat oleh user maupun administrator. Perubahan setiap data merupakan bagian penting dari database maka data yang update harus tersedia setiap waktu.

Setiap sistem memiliki kelemahan pada dua sisi yaitu hardware dan software. Kelemahan Database Server pada aspek hardware berupa kerusakan perangkat seperti harddisk penyimpanan. Pada sisi software kelemahan terdapat pada kehilangan data oleh berbagai penyebab seperti kegagalan sistem, kesengajaan maupun kesalahan pengguna. Dalam menanggulangi kelemahan-kelemahan ini dibutuhkan Backup Server yang melakukan pencadangan data yang dapat digunakan setiap saat dibutuhkan.



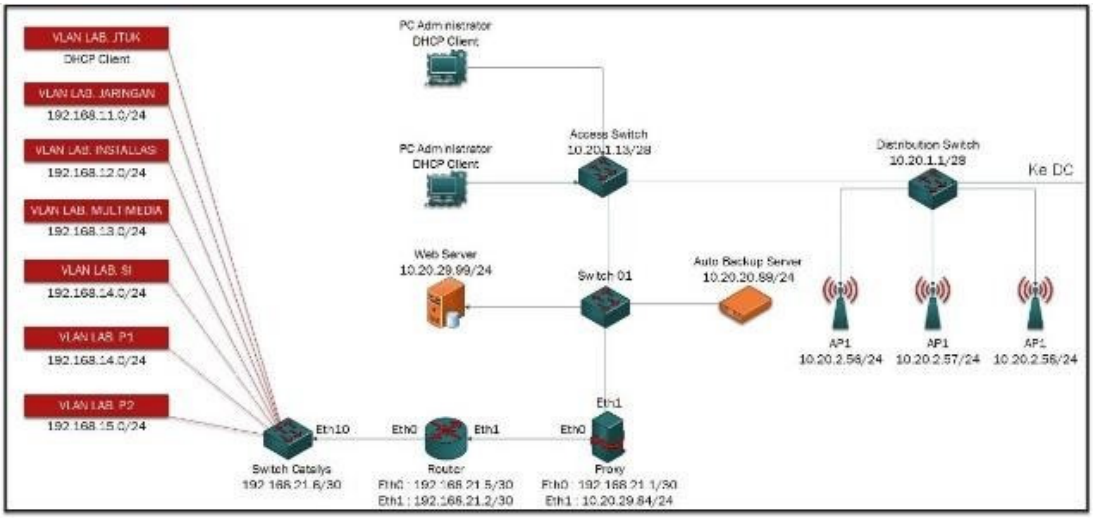
Gambar 1. Flowchart

Pencadangan data harus disesuaikan dengan kebutuhan dan spesifikasi perangkat yang digunakan. Manajemen Backup Database diatur berdasarkan besar kapasitas penyimpanan yang digunakan pada Backup Server dan perubahan data pada masing-masing database. Maka backup database tidak dilakukan secara bersamaan pada masing- masing database sehingga penyimpanan tersedia untuk daftar backup dengan waktu yang panjang.

3.2. Rancangan Topologi Jaringan

Rancangan topologi jaringan ini tidak merubah fungsi awal dari masing- masing perangkat atau pengalamatan jaringan yang sudah ada. Backup Server dihubungkan dengan switch 01 dengan alamat IP 10.20.29.89/24 sekelas dengan alamat IP Database Server yang mempunyai alamat IP 10.20.29.99/24. Penempatan perangkat dan pengalamatan IP Backup Server dapat dilihat pada Gambar 2.

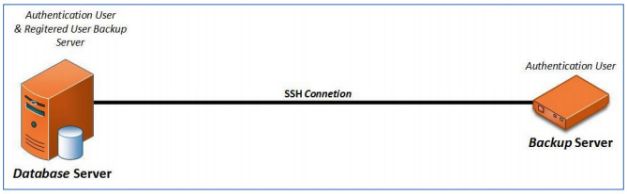
Penempatan dan pengalamatan IP seperti Gambar 2 bertujuan memudahkan dalam membangun koneksi jaringan antara Backup Server dengan Database Server. Keuntungan yang dihasilkan berupa mudah dalam melakukan transfer data sehingga mengurangi kemungkinan kegagalan pengiriman data, serta menjaga keamanan jaringan..



Gambar 2. Rancangan topologi jaringan

3.3. Rancangan Keamanan Jaringan

Proses pengiriman dan penerimaan data merupakan proses kerja dari *Database* Server dengan *Backup* Server. Dalam pengiriman data perlu dirancang keamanannya agar data yang dikirim tetap utuh sampai ketujuan tanpa terjadinya kerusakan atau kekurangan data. Gambar 3 merupakan rancangan keamanan server dan koneksi *Auto Backup Database*.



Gambar 3. Rancangan keamanan perangkat dan koneksi server

Dua aspek yang dilindungi pada rancangan keamanan ini adalah hak akses dan sistem koneksi. Dalam pembatasan hak akses dalam bentuk pembuatan sebuah *user* pada masing-masing server menggunakan otentikasi yang telah tersedia pada sistem operasi *linux* pada umumya. Sedangkan pada sistem koneksi berupa akses, pengiriman dan penerimaan data menggunakan *port* SSH didukung *enskripsi rsa-key. Enskripsi* dan hak akses ini hanya bisa dibangun oleh dua perangkat yang masing-masing menggunakan *port* SSH seperti yang dilakukan pada Gambar 3.

3.4. Manajemen File Backup

Setiap *file* yang dilakukan *backup* diatur jadwal dan nama *file* agar data tersimpan sesuai kebutuhan dan efektif dalam melakukan *backup.* Jadwal pelaksanaan *backup database dbsiaktif, kuesionerpbm* dan *web_ti* direncanakan seperti Tabel 1.

Tabel 1. Penjadwalan *backup database*

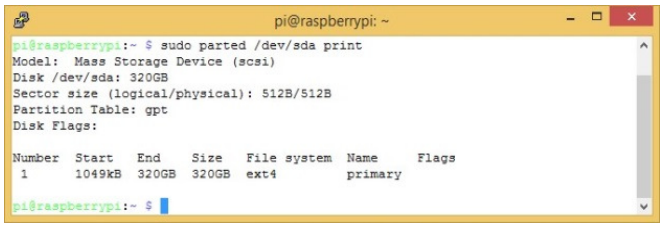
No	*Nama Database*	*Waktu Backup*	*Nama File*
1	*dbsiaktif*	*Pukul 02:01 setiap hari*	*dbsiaktif_<tgl>.sql*
2	*kuesionerpbm*	*Pukul 02:02 setiap hari*	*kuesionerpbm_<tgl>.sql*
3	*web_ti*	*Pukul 02:03 setiap minggu*	*Web_ti_<tgl>.sql*

Masing-masing *database* akan menjalankan proses *backup* dengan waktu yang berbeda-beda. Hal ini bertujuan menanggulangi kesibukan server dalam melakukan proses yang banyak dalam satu waktu. Sehingga dapat dikurangi kemungkinan dalam kegagalan proses *backup*. Nama *database* yang melakukan proses *backup* terdiri dari nama database, diikuti tanggal *backup* dan format data. Penamaan *database* ini akan membantu aspek manajemen *backup* data seperti membuat daftar data yang terstruktur pada masing-masing *database,* menghindari kemungkinan data ditimpa oleh *file* baru dan *database* dapat diseleksi berdasarkan tanggal *backup*.

4. HASIL DAN PEMBAHASAN

4.1. Membuat Penyimpanan Backup Database

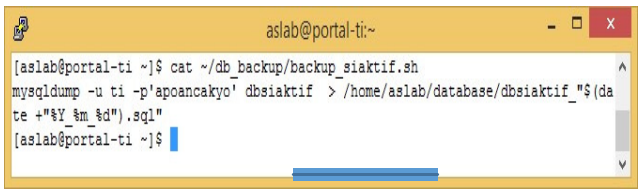
Eksternal Disk 320 Gb yang digunakan sebagai penyimpanan Backup Database. Penggunaan ruang penyimpanan data yang besar membantu melakukan Backup Database dalam jumlah yang banyak, sehingga maintenence server dapat dilakukan dalam rentang waktu yang panjang. Gambar 4 adalah disk yang digunakan untuk penyimpanan Backup Database.



Gambar 4. Penyimpanan Backup Database

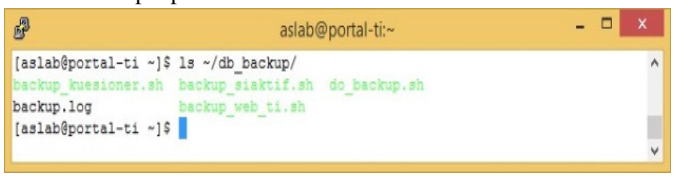
4.2. Membangun Auto Backup Database

Format data default dari database MySQL adalah .db dan untuk proses import/eksport, file yang dibutuhkan pada aplikasi phpMyadmin dengan file dengan format .sql. Selain itu, file .sql akan sangat efektif digunakan sebagai file backup karena file .sql sudah melalui proses compress sehingga kapasitas file menjadi lebih kecil. Pada linux CentOS file .db dari MySQL dirubah menjadi file .sql dengan perintah seperti Gambar 5.



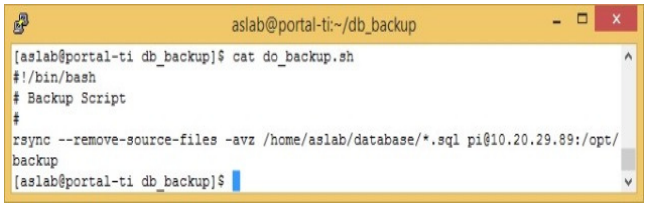
Gambar 5. Eksport database menjadi format .sql

Perintah eksport pada Gambar 5 merupakan perintah khusus untuk database dbsiaktif. Mysqldump merupakan format perintah untuk eksport database yang diikuti dengan –u (username) –p (password). Sedangkan karakter setelah tanda “>” merupakan lokasi penyimpanan file. Nama file dibuat diikuti dengan tahun, bulan dan tanggal dengan tujuan tidak ada penimpaan data pada setiap proses eksport. Hal yang sama dilakukan pada database yang lain, proses eksport database kuesionerpbm dibuat pada file backup_kuesioner.sh dan proses eksport database web_ti dibuat pada file backup_web_ti.sh. Daftar file eksport database terdapat pada Gambar 6.



Gambar 6. Daftar file bash eksport database

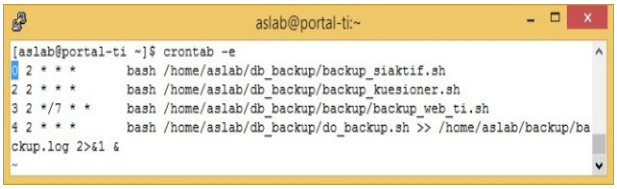
Proses kedua dalam menjalankan backup database yaitu membuat file do_backup.sh yang difungsikan sebagai perintah backup dari Database Server ke Backup Server. File ini berisikan perintah seperti Gambar 7.



Gambar 7. Perintah backup database

File do_backup.sh berisikan perintah transfer semua file dengan format .sql dari direktori /home/aslab/database/ Database Server ke direktori /opt/backup/ pada Backup Server. File ini berisikan perintah rsync –avz untuk transfer file, dan menggunakan –remove-source-files yang merupakan perintah untuk menghapus files sumber jika transfer file sudah berhasil. Pemanfaatan perintah ini sangat membantu proses pelaksanaan Backup Database, karena proses backup akan menjadi lebih efektif dan efisien tanpa harus takut kegagalan pengiriman data dan ada penumpukan data pada Database Server maupun pada Backup Server.

Setelah file untuk proses eksport dan backup dapat dijalankan maka dilakukan penjadwalan pada bash linux crontab. Proses penjadwalan dilakukan dengan menjalankan perintah crontab –e dan mengisikan script seperti Gambar 8.



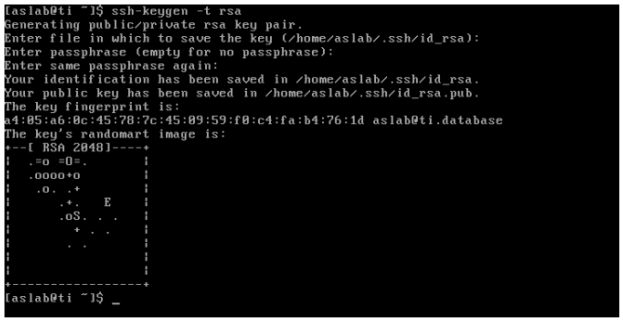
Gambar 8. Penjadwalan pada crontab

Attribution-NonCommercial 4.0 International. Some rights reserved

Pada Gambar 8 dilakukan pemanggilan file proses yang telah dibuat sebelumnya. Daftar penjadwalan 1 dan 2 merupakan proses eksport database yang dilakukan setiap jam 2 setiap hari namun pada menit yang berbeda. Menjalankan perintah eksport dimenit yang berbeda bertujuan untuk membagi kesibukan server dalam pelaksanaan eksport. Eksport database dbsiaktif dan kuesionerpbm dilakukan setiap hari. Sedangkan untuk database web_ti hanya dilakukan sekali seminggu sesuai dengan kondisi jarangannya perubahan data pada database web_ti. Pada daftar penjadwalan keempat aktifitas backup akan dijalankan dan direkap pada file backup.log sehingga proses backup dapat dilakukan monitoring.

4.3. Manajemen Keamanan Server dan Jaringan

Keamanan hak akses server dan koneksi server dibangun menggunakan *port* SSH. Pada *port* ini tersedia sebuah komponen standar dengan nama *sshkeygen* yang terdapat pada sistem komputer. Setiap komputer yang menggunakan port ini dapat menggunakan layanan *otentikasi* dari *ssh-keygen.* Perintah untuk mengaktifkan *ssh-keygen* dilakukan seperti Gambar 9.



Gambar 9. Aktifasi *ssh-keygen*

Perintah *ssh-keygen* yang diaktifkan membuat 2 buah *file* yaitu *id.rsa.pub* dan *id_rsa* pada *direktori /home/aslab/.ssh* seperti Gambar 10.

Gambar 10. File id_rsa.pub

Perintah *ssh-keygen* mengasilkan sebuah kunci SSH dengan panjang bit minimun 768 *bit* dan panjang *bit default* 2048 bit. Pada *database* server *rsakeygen* yang dibangun menghasilkan kunci seperti Gambar 11.

Gambar 11. Kunci *rsa-keygen Database* Server

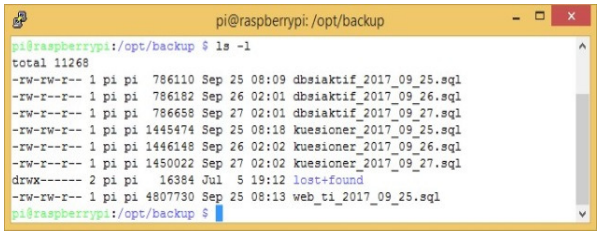
Kunci SSH ini digunakan untuk membangun koneksi yang aman antara *Database* Server dengan *Backup* Server. Pada implementasi ini difungsikan sebagai *otentikasi* hak akses dan *otentikasi* tansfer *file.* Dalam membangun proses *auto backup* kunci SSH ini disimpan pada *file authorized_key* dan digunakan akun (*pi*) pengguna *Backup* Server yang dikonfigurasi secara permanen. Isi *file* authorized_key pada *backup* server adalah kunci SSH *database* server seperti pada Gambar 12.

Gambar 12. Isi *file* authorized_key

Saat *Database* Server meminta koneksi kepada *Backup* Server baik koneksi *login* atau transfer data maka SSH *Backup* Server akan memeriksa *file authorized_key* untuk memeriksa kecocokan kunci SSH. Apabila kunci SSH permintaan koneksi cocok maka koneksi dapat dilanjutkan dan jika kunci SSH tidak cocok maka koneksi ditolak.

4.4. Hasil

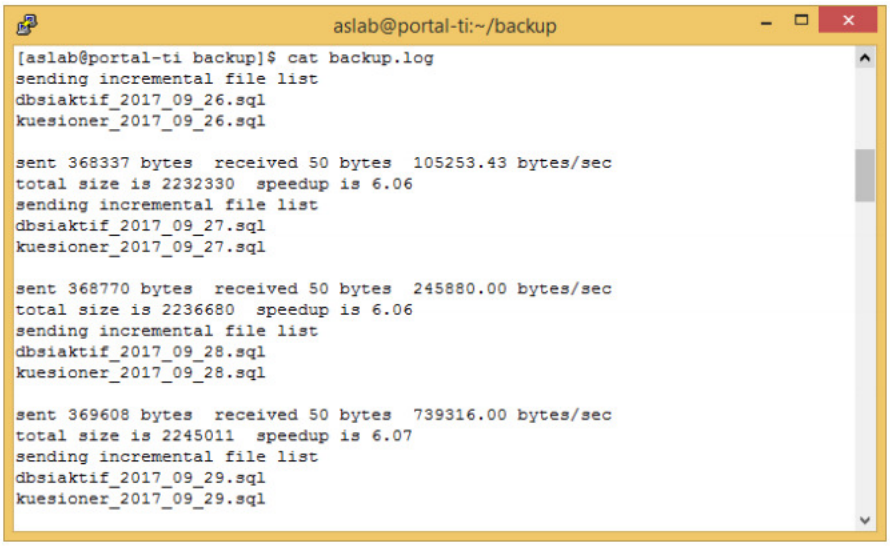
Implementasi Auto Backup SQL Database Server dimulai pada tanggal 25 September 2017. Keberhasilan backup dapat dilihat dari kondisi file yang ada pada direktori /home/aslab/database server database TI dan pada direktori /opt/backup pada Backup Server. Keberhasilan proses backup dilihat pada direktori /opt/backup Backup Server seperti Gambar 13.



Gambar 13. Isi file direktori /opt/backup Backup Server

Pada Gambar 13 dapat dilihat database yang berhasil dilakukan proses backup dan diberi nama file yang diikuti tanggal backup. Database dbsiaktif dan kuesioner memiliki file backup pada tanggal 25-27 September 2017. Hal ini karena backup database ini dikonfigurasi setiap hari, sedangkan database web_ti hanya dilakukan sekali dalam seminggu. Selain melihat file backup pada Backup Server, aktifitas backup dapat dilihat pada backup.log yang tersimpan pada direkroti /backup.

Laporan proses backup pada tanggal 25-27 September dapat dilihat pada Gambar 14.



Gambar 14. Isi *file backup.log*

Pada Gambar 14 dapat dilihat bahwa *database* berhasil melalui proses *backup*. Pengelompokan *log* aktifitas *backup* per hari dipisahkan satu spasi kebawah. Masing-masing laporan perhari memiliki beberapa kriteria berbeda yang dapat dilihat pada Tabel 2.

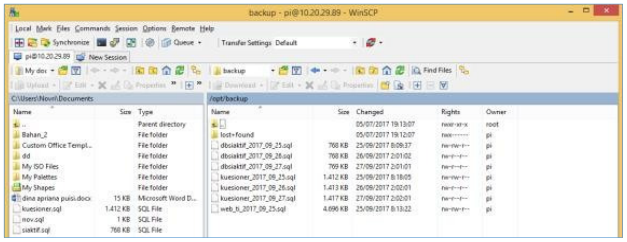
Tabel 2. Perbandingan proses *backup*

No	Tanggal *Backup*	Data *Size*	Kecepatan *Backup*
1	25/09/2017	368337 bytes	105253.43 bytes/sec
2	26/09/2017	368770 bytes	245880.00 bytes/sec
3	27/09/2017	369608 bytes	739316.00 bytes/sec

Proses *backup* yang telah dilakukan selama 3 hari memiliki perbedaan besar data dan kecepatan data yang menjalani proses *backup*. Besar data berubah setiap hari disebabkan karena ada penambahan data pada *database*. Sedangkan kecepatan *backup* database dipengaruhi konektifitas server antara kedua server, jika konektifitas semakin bagus maka semakin besar data dapat dikirim dalam satu detik.

Database yang berhasil melakukan *backup* dapat diakses/*download* menggunakan protocol SFTP (*Secure File Transfer Protocol*) yang merupakan gabungan dari fungsi FTP dan SCP. FTP (*File Transfer* Protocol) adalah protokol yang menyediakan layanan transfer *file* antara komputer dan SCP merupakan singkatan dari *Secure Copy* berfungsi untuk proses transfer data dengan menggunakan protokol SSH. SFTP menjadi penghubung server dengan *host* menajdi lebih aman karena koneksi yang *terenskripsi*. Mengakses *Backup* Server pada *host* yang menggunakan sistem operasi windows dapat dilakukan menggunakan aplikasi WinSCP data FileZilla.

Akses *host* terhadap *Backup* Server akan terhubung jika *otentikasi* berupa*user* dan *password* sesuai. Pada halaman *login* isikan alamat IP *backup* server, *username* dan *password* maka akan tampil isi dari *direktori home backup* server seperti Gambar 15.



Gambar 15. Hasil Backup Database

Pada daftar file backup, database dbsiaktif dan database kuesioner sudah ada 2 file yang dibedakan dengan nama tanggal. Sedangkan database web_ti hanya ada 1 daftar, hal ini karena database web_ti melalui proses backup dilakukan satu kali dalam 7 hari.

5. KESIMPULAN

Kesimpulan yang dapat diambil dari membangun Auto Backup SQL Database Server adalah sebagai berikut:

a. Backup Server jurusan Teknologi Informasi dapat dibangun dan dioperasi dengan baik menggunakan Raspbian Jessie pada Raspberry Pi.
b. Linux Crontab dapat digunakan untuk penjadwalan auto backup database dan berbagai penjadwalan proses lainnya.
c. Prose backup database dilakukan berdasarkan perencanaan manajemen file yang telah disesuaikan dengan kebutuhan backup agar ruang disk penyimpanan dimanfaatkan dengan optimal.
d. SSH aman digunakan untuk proses remote server dan transfer file antara satu komputer dengan komputer lain.
e. Kecepatan proses backup database jurusan Teknologi Informasi dipengaruhi koneksi antara Database Server dengan Backup Server.
f. Penggunaan aplikasi rsync sebagai aplikasi backup database memiliki kemungkinan kegagalan backup yang minim karena rsync akan mengulang proses backup pada setiap file yang rusak/tidak terkirim.
g. Backup database Server jurusan Teknologi Informasi menghasilkan data dengan format .sql, dan data ini dapat

https://doi.org/10.25077/ TEKNOSI.v4i3.2018.130-137
Attribution-NonCommercial 4.0 International. Some rights reserved

dilakukan proses eksport/import seperti pada pemanfaat database pada umumnya.

DAFTAR PUSTAKA

[1] R. Budi, *Belejar Otodidak Membuat Database Menggunakan MySQL*. Bandung: Informatika, 2011.

[2] P. Bidang and S. Informasi, "Metode Manajemen Backup Data Sebagai Upaya," vol. 13, no. 1, pp. 22–27, 2012.

[3] P. E. Suparwita, "Implementasi Sistem Backup Otomatis Virtual Private Server Dengan Crontab," *Jurnal Elektronika Ilmu Komputer*, vol. Vol I, pp. 29-34, 2012.

[4] I. P. Haryo, S. Nugroho dan D. Utomo, "Penggunaan Raspberry Pi Sebagai Web Server Pada Rumah Untuk Sistem Pengendalian Lampu Jarak Jauh dan Pemantauan Suhu," *Techne Jurnal Ilmiah Elektronika*, vol. 13, pp. 111-124, 2014.

[5] D. Purwanto dan R. D. Dana, "Sistem Kemanan Jaringan Model Client Server Menggunakan Enskripsi Data (MD5) Pada Dinas Kesehatan Kota Cirebon," *ICT,* vol. 13, pp. 1-15, 2015.

[6] M. R. Arief, "Autentikasi, Kendali Akses, Audit Sistem Keamanan Jaringan Komputer," *Dasi,* vol. 11, pp. 73-76, 2010.

[7] H. Jusuf, "Penggunaan Secure Shell (SSH) Sebagai Sistem Komunikasi Aman Pada Web Ujian Online," *ICT JURNAL*, vol. 2, pp. 75-85, 2015

BIODATA PENULIS

Dwiny Meidelfi
Merupakan staf pengajar tetap pada Program Studi Teknologi Rekayasa Perangkat Lunak Jurusan Teknologi Informasi Politeknik Negeri Padang. Matakuliah yang diampu diantaranya basis data, pemrograman visual, dan rekayasa perangkat lunak.

Hidra Amnur
Merupakan staf pengajar tetap pada Program Studi Teknik Komputer Jurusan Teknologi Informasi Politeknik Negeri Padang. Matakuliah yang diampu diantaranya Sistem Operasi dan Administrasi Sistem.

Novri
Merupakan lulusan pendidikan diploma tiga pada jurusan Teknologi Informasi Politeknik Negeri Padang