IMPLEMENTASI REPLIKASI BASIS DATA DAN MODEL DISCRETIONARY ACCES CONTROL UNTUK KEAMANAN DATABASE STUDI KASUS SMK PLUS PRATAMA ADI BANJARAN

Widi Linggih Jaelani
Magister Teknik Informatika,
Program Pasca Sarjana, Universitas Langlangbuana
widijaelani@yahoo.co.id

Abstrak

Sistem ujian online merupakan sebuah proses ujian yang dilaksanakan secara komputerisasi dimana siswa mengerjakan soal tidak lagi berbasis kertas tetapi menggunakan computer sebagai media pelaksanaan ujian. Ketika ujian di laksanakan secara komputerisasi maka dibutuhkan sebuah system yang bekerja yang terdiri dari perangkat lunak dan database. Dalam sebuah database yang digunakan oleh sebuah system biasanya terjadi sebuah permasalahan yang disebabkan karena kesalahan pada saat melakukan disain pada database dan penentuan hak akses setiap user terhadap database. Dalam sebuah instansi, salah satu factor yang penting adalah bagaimanacara mengamankan data – data penting yang ada didalam instansi agar tidak bocor. Untuk mengamankan database dapat menggunakan beberapa teknik pengamanan database yang bisa diimplementasikan. Replikasi Basisdata dan Model Discretionary Acces Control dapat merupakan teknik pengamanan database yang bisa diimplementasikan didalam melakukan perancangan database. Model Discretionary Acces Control dapat membuat sebuah model acces control setiap user terhadap database dan Replikasi Database akan membuat sebuah replika dari database yang ada sehingga database yang diakses merupakan database hasil replika bukan database master. Dengan mengimplementasikan Model Discretionary Acces Control dan Replikasi Database maka database yang dipergunakan untuk system ujian online akan lebih aman dan lebih baik karena menunjang tiga aspek keamanan computer yang harus diperhatikan yaitu kerahasiaan data, keutuhan data, dan keberadaan data.

1. Pendahuluan

Basis data adalah kumpulan data yang saling berelasi. Data sendiri merupakan fakta mengenai objek, orang, dan lain-lain. Data dinyatakan dengan nilai (angka, deretan karakter, atau simbol) (Kadir. Abdul, (1999), Konsep dan Tuntunan Praktis Basis Data, Yogyakarta, Penerbit Andi). Seiring dengan perkembangan TI (Teknologi Informasi) saat ini, database sudah banyak dipergunakan oleh beberapa instansi ataupun lembaga sebagai sebuah sarana untuk menyimpan sebuah data termasuk di dunia pendidikan. Sekolah merupakan instansi yang turut serta dalam perkembangan teknologi (Anwar. Nuril, 2013, Analisa Arsitektur Client Server Menggunakan Database Terpusat (Studi Kasus Pada SMP Muhammadiyah Purwodadi Purworejo), Jurnal Sarjana Teknik Informatika, Universitas Ahmad Dahlan). Dibeberapa sekolah pengimplementasian teknologi sudah di implementasikan beberapa aspek baik diimplementasikan untuk peoses Penerimaan Peserta Didik Baru (PPDB), dan Pembelajaran online (e-learning) baik untuk proses pembelajaran, pemberian tugas, ataupun untuk ujian. Salah satu sekolah yang saat ini mengimplementasikan teknologi didalam proses pembelajarannya ialah SMK PLUS PRATAMA ADI BANJARAN. Saat ini disekolah tersebut pengimplementasian teknologi baru sebatas di Sistem Ujian saja baik untuk harian, tengah semester, dan akhir semester. Untuk PPDB tidak dilakukan secara khusus dikarenakan berkaitan dengan status sekolah yang swasta bukan sekolah negeri dan ketika akan siswa masuk ke sekolah tersebut tidak dilaksanakan seleksi terlebih dahulu. Dalam proses ujian online yang berlangsung ada sebuah sistem yang bekerja yang terdiri dari sebuah perangkat lunak dan database. Didalam proses ujian online database dipergunakan untuk melakukan penyimpanan data soal, data jawaban, data siswa, data nialai dan masih banyak lagi data yang lainnya. Database yang dipergunakan saat ini masih disimpan di satu buah server lokal yang ada di sekolah dan disain yang ada dapat menyebabkan ketidak amanan terhadap database yang dipergunakan oleh sistem ujian

online. Tetapi, masih banyak pihak yang kurang memperhatikan tingkat keamanan dari database yang dimilikinya padahal keamanan merupakan salah satu bagian terpenting dari sebuah sistem yang bisa menjaga keberlangsungan dari suatu bisnis proses yang ada.

Dalam database yang digunakan oleh sebuah Sistem biasanya terjadi sebuah permasalahan yang disebabkan oleh beberapa faktor seperti karena database hanya disimpan di satubuah serever sehingga jika terjadi gangguan baik berupa serangan ataupun masalah internal pada server maka akan menyebabkan data tidak dapat diakses. Kesalahan selanjutnya bisa terjadi pada saat melakukan disain pada database yang akan dipergunakan sehingga data yang ada didalam database menjadi tidak aman. Selain permasalah perancangan ada juga permasalahan yang disebabkan oleh tidak telitinya atau kurang tepat dalam menentukan hak akses setiap user terhadap sebuah database sehingga menyebabkan user bisa melakukan akses terhadap data yang tidak berhak diakses. Saat ini database sistem ujian online SMK Plus Pratama Adi masih disimpan di satu server dan penentuan akses kontrol untuk user terhadap database yang ada didalam sistem ujian online masih kurang efektif sehingga ada kemudahan untuk melakukan akses data yang bukan haknya. Kedua hal tersebut bisa menimbulkan beberapa kerentanan dari mulai server down sehingga database tidak bisa diakses total dan penyalahgunaan terhadap akses data karena kurangnya pengontrolan akses kedalam database. Sedangkan didalam suatu instansi, salah satu faktor yang penting adalah bagaimana cara mengamankan data-data penting yang ada didalam instansi tersebut agar tidak bocor atau agar dapat diamankan (Alamsyah. Ilham, 2013, Pengolahan Keamanan Database Pada Data Kepegawaian (Studi Kasus di PDAM Tirta Intan Kabupaten Garut), Jurnal Algoritma Sekolah Tinggi Teknologi Garut). Pada umumnya, suatu sistem memiliki database yang dilengkapi dengan keamanan yaitu berupa password. Tetapi jika password tersebut bisa dipecahkan atau diketahui oleh orang lain maka isi database yang bersifat rahasia dapat dibaca oleh orang lain yang tidak berkepentingan (Nathasia. Novi, 2011, Penerapan Teknik Kriptografi Stream Ciper Untuk Pengamanan Basis Data, ICT Reaserch Center UNAS, Universitas Nasional). Keamanan database server sangat diperlukan untuk menjaga data agar tidak digunakan oleh yang tidak punya otoritas terhadap data tersebut. Keamanan database timbul dari kebutuhan untuk melindungi data dari kehilangan dan kerusakan data, adanya pihak yang tidak diijinkan yang akan mengakses atau merubah data, perlindungan terhadap delay berlebihan yang disebabkan karena terlalu berlebihan mengakses dan menggunakan data, atau mengatasi gangguan denail of service. (Sugiantoro. Bambang, 2010, Analisa Keamanan Database Server Menggunakan Teknologi Virtual Private Database dan Notifikasi Database Server Menggunakan Agen Bergerak, Seminar Nasional Informatika 2010, Universitas Gajah Mada Yogyakarta).

Untuk menjaga keamanan dari sebuah database ada beberapa cara yang bisa dilakukan seperti :

1. Teknologi virtual private database (VPD)yang dimana memungkinkan kontrol akses mencapai baris yang spesifik dari database sehingga user dapat mengakses ke data yang digunakan (Sugianto. Bambang, 2010). Oracle Menyediakan metode logis dan elegan untuk menerapkan keamanan untuk data dalam tabel databaseyang dimana VPD dapat digunakan untuk menyediakan keamanan tingkat baris. Itu Dikutip dari pasal 11 dari Oracle Efektif Database 10g Keamanan oleh Desain, ditulis oleh David C. Knox (McGraw-Hill / Osborne, 2004; ISBN: 0072231300). Dalam hal ini pengguna berwenang untuk akses pada tingkat-SECRET berbeda di level sensitifitas SECRET, CONFIDENTIAL, dan UNCLASSIFIED. Data itu bercampur dalam tabel di berbagai tingkat sensitivitas (http://www.devshed.com/c/a/oracle/row-level-security-with-virtual-private-database/ diakses pada 21 Desmber 2016 jam 11:46) .
2. Replikasi Basis Data yang dimana replikasi merupakan sebuah teknik untuk melakukan copy dan pendistribusian data dengan objek database dari suatu database ke database lain kemudian melaksanakan singkronisasi antara database sehingga konsistensi data dapat terjamin (Hadiansyah. Tantan, 2009)
3. Agen Bergerak yang merupakan terobosan baru dalam perkembangan perangkat lunak. Agen merupakan entitas perangkat lunak yang didedikasikan untuk tujuan tertentu (Tri, 2001).
4. Basis Data Terdistribusi adalah jaringan dua atau lebih oracle database yang berbeda pada satu komputer atau lebih. Dimana sebuah aplikasi secara dapat bersamaan dapat mengakses atau memodifikasi data dalam

beberapa database dalam lingkungan terdistribusi tunggal (http://www.jejaring.web.id/homogen-sistem-basis-data-terdistribusi/ diakses pada 19 Desember 2016 jam 16 : 31)

5. Sistem Hak Akses merupakan kumpulan dari metode dan komponen yang dipergunakan untuk melindungi asset informasi. Akses kontrol digunakan untuk memastikan hanya orang yang berhak saja yang dapat melihat informasi. Kontrol akses memberikan kemampuan untuk mendikte mana informasi yang dapat dilihat atau dimodifikasi oleh user (Herdiansyah. Tantan, 2009)

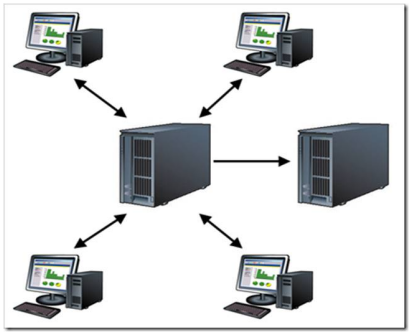
2. Tinjauan Pustaka

A. Replikasi Basis Data

Replikasi database adalah seperangkat teknologi yang digunakan untuk menyalin dan mendistribusikan data dari satu database ke database yang lain. Dan selanjutnya, mensinkronisasikan antar database untuk menjaga konsistensi. Dengan replikasi, data dapat didistribusikan ke lokasi yang berbeda dan pengguna yang jauh melalui LAN, WAN, Dial-up Connection, wireless connections, dan internet.

B. Kegunaan Replikasi Basis Data

Kegunaan Membuat backup dengan menggunakan replication memungkinkan didapatkan backup yang sempurna dari suatu database MySQL yang besar dan aktif tanpa melakukan penghentian dari server yang bersangkutan. Tanpa replikasi, backup akan memperlambat sistem dan ada kemungkinan data yang tidak konsisten, karena bisa saja satu tabel berubah sementara tabel lain yang berhubungan tidak berubah dan sedang di-backup. Mematikan server akan menjamin data yang konsisten, tetapi ini berarti menghentikan layanan pada pengguna dan sangat tidak diharapkan. Kadangkala penghentian ini tidak dapat dihindarkan, tetapi penghentian setiap hari tidak dapat diterima.



Gambar Replikasi Database (https://diskusikuliah.wordpress.com/2010/10/31/database-replication/ 21 desember 2016 21:35)

Gambar diatas merupakan deskripsi untuk Replikasi Database, jadi database yang ada di komputer “Server Master” sekaligus yang diakses oleh client, dimiliki juga oleh komputer “Server Slave”. sehingga dapat menghindari kemungkinan kehilangan data yang ada pada komputer Server Master”.

Metoda alternatif replikasi MySQL menjamin backup sempurna tanpa harus menghentikan server tiap hari. Replikasi merupakan konfigurasi sistem dimana server MySQL, yang dalam hal ini dinamakan master, menyimpan data dan menangani permintaan pengguna, sementara server MySQL yang lain, yang dinamakan slave server berisi copy dari data master dan melakukan semua SQL statement yang mengubah data di master, segera setelah master melakukannya. Dengan demikian backup dapat dilakukan secara periodik, misalnya seminggu sekali, pada server slave untuk mendapatkan backup yang sempurna. Setelah backup selesai, replikasi dapat dijalankan lagi dan slave akan secara otomatis melakukan query yang dilakukan master pada saat slave dimatikan. Fitur replikasi merupakan bagian dari MySQL.

Pada umumnya replikasi mendukung ketersediaan data setiap waktu dan dimanapun diperlukan. Keuntungan lainnya adalah Memungkinkan beberapa lokasi menyimpan data yang sama. Hal ini sangat berguna pada saat lokasi-lokasi tersebut membutuhkan data yang sama atau memerlukan server yang terpisah dalam pembuatan aplikasi laporan.

Aplikasi transaksi online terpisah dari aplikasi pembacaan seperti proses analisis database

secara online, data smarts atau data warehouse. Memungkinkan otonomi yang besar. Pengguna dapat bekerja dengan meng-copy data pada saat tidak terkoneksi. Kemudian melakukan perubahan untuk dibuat database baru pada saat terkoneksi. Data dapat ditampilkan seperti layaknya melihat data tersebut dengan menggunakan aplikasi berbasis Web.

C. Replikasi Basis Data Meningkatkan kinerja pembacaan

Membawa data mendekati lokasi individu atau kelompok pengguna. Hal ini akan membantu mengurangi masalah, karena modifikasi data dan pemrosesan query yang dilakukan oleh banyak pengguna karena data dapat didistribusikan melalui jaringan dan data dapat dibagi berdasarkan kebutuhan masing-masing unit atau pengguna.

D. Sistem Hak Akses

Dalam bahasa inggrisnya, hak akses ini dikenal dengan istilah 'privileges' Sistem Hak Akses merupakan kumpulan dari metode dan komponen yang dipergunakan untuk melindungi asset informasi. Akses kontrol digunakan untuk memastikan hanya orang yang berhak saja yang dapat melihat informasi. Kontrol akses memberikan kemampuan untuk mendikte mana informasi yang dapat dilihat atau dimodifikasi oleh user (Herdiansyah. Tantan, 2009). User dalam MySQL dapat dibuat dengan berbagai kombinasi hak akses yang dapat dibatasi. Apakah user tersebut dapat membuat, mengubah dan menghapus sebuah tabel, atau user tersebut kita batasi hanya untuk melihat tabel saja (perintah SELECT). Lebih jauh lagi, MySQL memiliki kemampuan untuk membatasi hak akses dari komputer mana MySQL Client dijalankan. Misalkan tabel jurusan_fisika, hanya dapat diakses dari komputer yang alamat IP-nya berasal dari jurusan fisika saja, sehingga membatasi hak akses mahasiswa fisika untuk melihat tabel jurusan pariwisata. Selain lokasi IP address, hak akses user dalam MySQL dapat dibatasi juga pada level tabel dan kolom tertentu saja. Misalkan dalam tabel mahasiswa terdapat kolom IPK yang harus dirahasiakan, maka kita bisa membatasi hak akses untuk kolom IPK dan membuka akses untuk kolom lainnya (http://www.duniailkom.com/tutorial-belajar-mysql-mengenal-superuser-root-dan-pengertian-privileges-mysql/ Diakses 20 January 2017 pada pukul 13:37).

E. Akses Kontrol dalam Database

Aspek keamanan dari database menjadi pemikiran utama dari banyak organisasi. Kebutuhan keamanan database menjadi penting karena nilai dari data yang disimpan sangat berharga bagi organisasi tersebut. Tidak semua data mempunyai nilai yang sama. Setiap bagian data mempunyai kepentingan dan nilai yang berbeda pula. Untuk itu diperlukan suatu metode pengaturan dari keamanan data. Hal ini penting karena untuk data dengan jumlah dan jenis yang besar diperlukan manajemen data yang baik. Untuk data dengan kapasitas volume data yang relatif kecil mungkin cukup dengan cara administrasi tunggal, dengan kata lain semua hak istimewa (privilege) dari data yang disimpan diatur oleh seorang adminstrator. Masalah akan muncul jika volume data berkembang menjadi sangat besar, maka manajemen dari data tersebut tidak cukup diatur oleh seorang administrator saja, karena itu diperlukan suatu teknik yang dapat digunakan untuk mengatur akses kontrol dari sebuah objek dalam sistem database.

F. Pengertian Akses Kontrol

Kontrol adalah sebuah mekanisme yang mengatur mana yang berhak dan tidak berhak melakukan akses terhadap sebuah objek. Kontrol bisa menjadi penjaga keamanan informasi dari serangan. Akses kontrol merupakan fitur-fitur keamanan yang mengontrol bagaimana pemakai sistem berkomunikasi dan berinteraksi dengan sistem dan sumber daya lainnya. Akses kontrol melindungi sistem dan sumber daya dari akses yang tidak berhak dan umumnya menentukan tingkat otorisasi setelah prosedur otentikasi berhasil dilengkapi. Akses adalah aliran informasi antara subjek dan objek. Sebuah subjek merupakan entitas aktif yang meminta akses ke suatu objek atau data dalam objek tersebut. Sebuah subjek dapat berupa pemakai, program, atau proses yang mengakses informasi untuk menyelesaikan suatu tugas tertentu. Ketika sebuah program mengakses sebuah file, program menjadi subjek dan file menjadi objek. Objek adalah entitas pasif yang mengandung informasi. Objek bisa sebuah entitas, data atau field pada tabel yang berada di dalam database.

G. Subjek dan Objek

Kontrol akses adalah semua yang mengatur tentang proses pengontrolan akses. Sebuah entitas yang meminta akses ke sebuah sumber daya disebut sebagai akses dari subjek. Sebuah subjek merupakan entitas yang aktif karena dia menginisiasi sebuah permintaan akses. Sebuah sumber daya yang akan diakses oleh subjek disebut sebagai objek dari akses. Objek dari akses merupakan bagian yang pasif dari

akses karena subjek melakukan akses terhadap objek tersebut. Jadi tujuan dari kebijakan kontrol akses adalah mengijinkan hanya subjek yang mempunyai otorisasi yang bisa mengakses objek yang sudah diijinkan untuk diakses. Hal ini mungkin juga ada subjek yang sudah mempunyai otorisasi tapi tidak mengizinkan akses terhadap spesifik objek tertentu.

H. Least Privilege

Organisasi-organisasi menggunakan beberapa kebijakan dalam menerapkan peraturan kontrol akses. Filosofi yang paling tidak aman (paling berbahaya) adalah memberikan hak akses kepada setiap orang secara default. Memang kelihatannya mudah akan tetapi hal ini mudah juga untuk dibobol. Jadi pada metode ini, kita harus memastikan bahhwa semua akses harus dibatasi karena administrasi yang buruk bisa menyebabkan lubang kemanan. Filosofi dari least privilege adalah sebuah subjek hanya diberikan hak sesuai dengan keperluannya tidak lebih. Least privilege membantu menghindari authorization creep, yaitu sebuah kondisi dimana sebuah subjek memiliki hak akses lebih dari yang sebenarnya dibutuhkan.

I. Model Akses Kontrol

Model akses kontrol sangat berfungsi dalam menentukan jenis kontrol akses yang diperlukan dalam mendukung kebijakan keamanan. Model akses kontrol ini menyediakan level konseptual dari kebijakan keamanan. Hal ini akan mengijinkan kita untuk melakukan pemetaan antara tujuan dan petunjuk dari kebijakan keamanan terhadap masalah yang spesifik. Penerapan akses kontrol pada subjek sistem (sebuah entitas aktif seperti individu atau proses) terhadap objek sistem (sebuah entitas pasif seperti sebuah file) berdasarkan aturan (rules). Model kontrol akses merupakan sebuah framework yang menjelaskan bagaimana subjek mengakses objek. Model ini menggunakan teknologi kontrol akses dan mekanisme sekuriti untuk menerapkan aturan dan tujuan suatu model.

Ada tiga tipe utama model kontrol akses yaitu mandatory, discretionary, dan role-based. Tiap tipe model memakai metode berbeda untuk mengkontrol bagaimana subjek mengakses objek dan mempunyai kelebihan serta keterbatasan masing- masing. Beberapa model dipakai secara eksklusif dan kadang-kadang model tersebut dikombinasikan sehingga mampu mencapai tingkat keperluan keamanan yang dibutuhkan.

1. Mandatory Access Control

Otorisasi suatu akses subjek terhadap objek bergantung pada label menunjukkan ijin otorisasi suatu subjek dan klasifikasi dari objek. Pada mandatory access control, pengguna dan pemilik data tidak memiliki banyak kebebasan untuk menentukan siapa yang dapat mengakses file-file yang dibuatnya. Pemilik data dapat mengijinkan pihak lain untuk mengakses file miliknya namun sistemlah yang membuat keputusan final dan dapat membatalkan kebijakan dari pemilik data. Model ini lebih terstruktur dan ketat serta berdasarkan label keamanan sistem. Pengguna diberikan ijin otorisasi dan data diklasifikasikan. Klasifikasi disimpan di label sekuriti pada sumber daya. Klasifikasi label menentukan tingkat kepercayaan pengguna yang harus dimiliki untuk dapat mengakses suatu file. Ketika sistem membuat keputusan mengenai pemenuhan permintaan akses ke suatu objek, keputusan akan didasarkan pada ijin otorisasi subjek dan klasifikasi objek. Aturan-aturan bagaimana subjek mengakses data dibuat oleh manajemen, dikonfigurasikan oleh administrator, dijalankan oleh sistem dan didukung oleh teknologi security.

2. Discretionary Access Control

Subjek memiliki otoritas, dengan batasan tertentu, untuk menentukan objek-objek apa yang dapat diakses. Contohnya adalah penggunaan daftar kontrol akses (access control list). Daftar kontrol akses merupakan sebuah daftar yang menunjuk pengguna-pengguna mana yang memiliki hak ke sumber daya tertentu. Misalnya daftar tabular akan menunjukkan subjek atau pengguna mana yang memiliki akses ke objek dan hak apa yang mereka punya berkaitan dengan objek tersebut. Kontrol akses triple terdiri dari pengguna, program, dan file dengan hubungan hak akses terkait dengan tiap pengguna. Tipe kontrol akses ini digunakan secara lokal, dan mempunyai situasi dinamis dimana subjek-subjek harus memiliki pemisahan untuk menentukan sumber daya tertentu yang diijinkan untuk diakses oleh pengguna. Ketika pengguna dengan batasan tertentu memiliki hak untuk merubah kontrol akses ke objek-objek tertentu, hal ini disebut sebagai user-directed discretionary access control. Sedangkan kontrol akses berbasis identitas (identity-based access control) adalah tipe kontrol akses terpisah berdasarkan identitas suatu individu. Dalam beberapa kasus, pendekatan hybrid juga digunakan, yaitu yang mengkombinasikan fitur-fitur user-based dan identity-based discretionary access control. Jika pengguna membuat suatu file, maka ia merupakan pemilik file

tersebut. Kepemilikan juga bisa diberikan kepada individu spesifik. Sistem yang menerapkan model discretionary access control memungkinkan pemilik sumber daya untuk menentukan subjek-subjek apa yang dapat mengakses sumber daya spesifik. Model ini dinamakan discretionary karena kontrol akses didasarkan pada pemisahan pemilik. Akses dibatasi berdasarkan otorisasi yang diberikan pada pengguna. Ini berarti bahwa subjek-subjek diijinkan untuk menentukan tipe akses apa yang dapat terjadi pada objek yang mereka miliki. Jika organisasi menggunakan model discretionary access control, administrator jaringan dapat mengijinkan pemilik sumber daya mengontrol siapa yang dapat mengakses file/sumber daya tersebut. Implemetasi umum dari discretionary access control adalah melalui access control list yang dibuat oleh pemilik, diatur oleh administrator jaringan, dan dijalankan oleh sistem. Dengan demikian kontrol ini tidak termasuk dalam lingkungan terkontrol yang terpusat dan dapat memberi kemampuan pada pengguna untuk mengakses informasi secara dinamis, kebalikan dari aturan yang lebih statis pada mandatory access control.

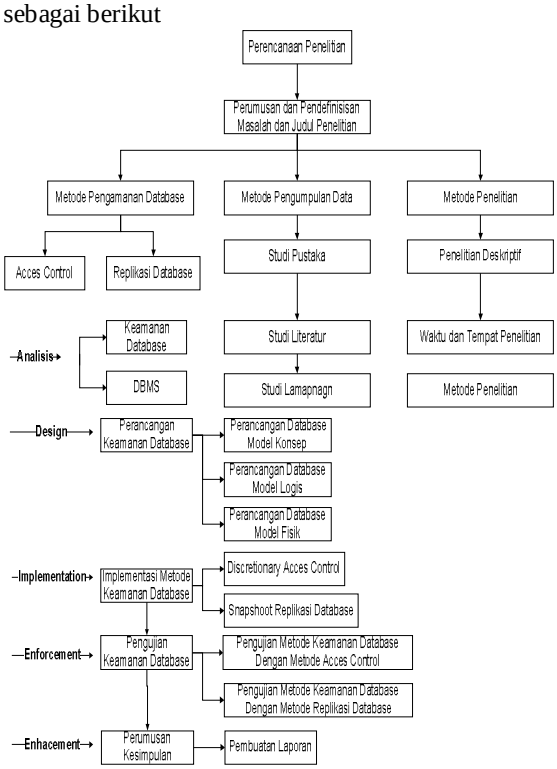
3. Non Discretionary (Role-Based) Access Control

Otoritas sentral menentukan subjek-subjek apa yang mempunyai akses ke objek-objek tertentu berdasarkan kebijakan keamanan organisasi. Kontrol akses bisa berdasarkan peran individu dalam suatu organisasi (role-based) atau tanggung jawab subjek dan tugasnya (task-based). Dalam organisasi dimana sering terdapat adanya perubahan/pergantian personel, non-discretionary access control merupakan model yang tepat karena kontrol akses didasarkan pada peran individu atau jabatan dalam suatu organisasi. Kontrol akses ini tidak perlu diubah saat individu baru masuk menggantikan individu lama. Tipe lain dari non-discretionary access control adalah kontrol akses lattice-based. Dalam model lattice (lapis tingkatan), terdapat pasanganpasangan elemen yang memiliki batas tertinggi terkecil dari nilai dan batas terendah terbesar dari nilai. Untuk menerapkan konsep kontrol akses ini, pasangan elemen adalah subjek dan objek, dan subjek memiliki batas terendah terbesar serta batas tertinggi terkecil untuk hak akses pada suatu objek. Selain itu terdapat model role-based access control yang juga sebagai non-discretionary access control. Model ini menerapkan seperangkat aturan terpusat pada kontrol untuk menentukan bagaimana subjek dan objek berinteraksi. Tipe model ini mengijinkan akses ke sumber daya berdasarkan peran yang pengguna tangani dalam suatu organisasi. Administrator menempatkan pengguna dalam peran dan kemudian memberikan hak akses pada peran tersebut (http://repository.usu.ac.id/bitstream/123456789/16384/3/Chapter%20II.pdf Diakses 20 januari 2017 pada pukul 14:03).

3. Metode Penelitian

A. Alur Metode Penelitian

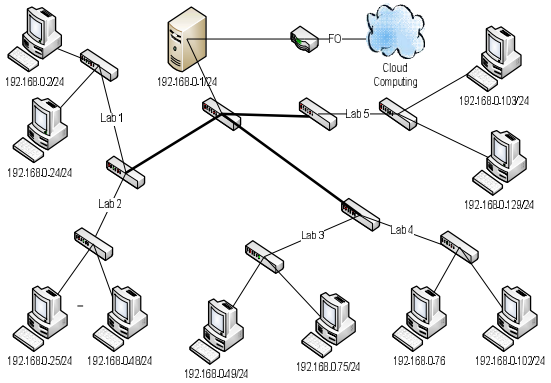
Penelitian yang dilakukan memiliki alur sebagai berikut



Gambar Alur Metode Penelitian

B. Analisis Sistem

Hasil yang diperoleh dari hasil observasi yang dilakukan pada Sistem ujian *online* di SMK Plus Pratama Adi menghasilkan sebuah gambaran Sistem saat ini. Berikut gambaran dari Sistem yang sedang digunakan saat ini :



Gambar Bentuk Sistem Ujian *Online* Smk Plus Pratama Adi

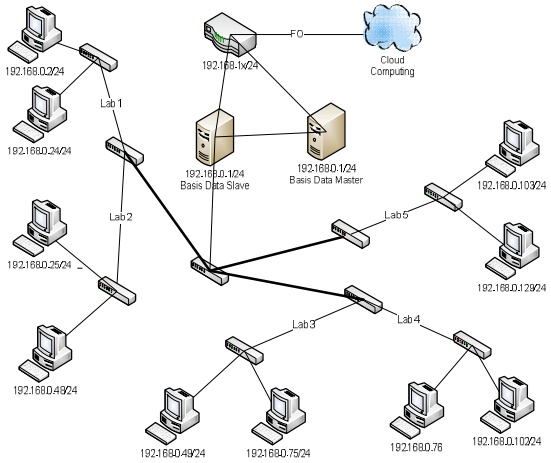
Hasil yang diperoleh dari hasil wawancara yang dilakukan di SMK Plus Pratama Adi Banjaran adalah sebagai berikut :

1. Pada awalnya pihak sekolah melaksanakan ujian berbasis kertas.
2. Karena ingin menjadi salah satu sekolah yang berbasis teknologi di wilayah kabupaten bandung maka pihak sekolah secara bertahap melakukan pengembangan terhadap Sistem pembelajaran yang ada.
3. Pengembangan yang pertama dilakukan dengan cara membuat sebuah Sistem ujian yang tadinya dilakukan berbasis kertas sekarang ujian dilakukan berbasis *online* walaupun Sistem yang dibuat masih sederhana.
4. Pihak sekolah menginkan sebuah Sistem yang dapat berjalan baik saat dipergunakan.
5. Pihak sekolah menginginkan adanya pengembangan Sistem yang tadinya dibuat sederhana menjadi sebuah Sistem yang baik dari sisi pengoperasian dan dari sisi keamanannya juga terutama keamanan data yang ada didalam Sistem ujian tersebut.
6. Sistem ujian *online* pertama kali dipergunakan pada tahun ajran 2015 – 2016.
7. Pada awal penggunaan Sistem yang dipergunakan masih belum mempergunakan model.
8. Ditahun ajaran 2016 – 2017 sistem yang dipergunakan dirubah karena dirasa Sistem yang pertama kurang maksimal.
9. Sistem yang kedua sudah mempergunakan model.
10. Sistem ujian dipergunakan pada saat Ujian Tengah Semester (UTS), Ujian Akhir Semester (UAS), dan ulangan harian.
11. Sistem dan *database* disimpan di *sever* local yang ada di sekolah.
12. Soal masih diinputkan oleh administrator dikarenakan Sistem masih dijalankan secara lokal.
13. Ketika siswa login disistem ujian *online* saat ini, siswa mash dapat melihat semua soal yang sudah di upload sehingga siswa bisa melakukan pengerjaan soal manapun.
14. Karena Sistem masih dalam tahap pengembangan untuk sementara Sistem diakses melalui jaringan local.
15. Soal disimpan di *database* yang disimpan di servel local.
16. Ketika *sever down* maka siswa tidak bias mengerjakan soal dan pihak kurikulum harus melakukan penjadwalan ulang.
17. Masih ditemukan kejadian informasi yang dikeluarkan Sistem tidak sesuai dengan ketentuan seharusnya seperti pada saat input soal pilihan ganda soal diiputkan beserta pilihan jawaban tetapi pada saat soal tersebut diakses terkadang pilihannya tidak muncul sama sekali.
18. Setelah ujian selesai masih ditemukan kejadian nilai siswa yang berubah tidak sesuai dengan hasil sebenarnya.

Siawa masih bias melakukan akses terhadap Sistem diluar jam ujian dan masih dapat mengerjakan soal walaupun soal yang tidak diperuntukan untuk siswa tersebut seperti siswa kelas X (sepuluh) masih dapat mengerjakan soal kelas XI (sebelas) dan XII (duabelas) sehingga menyebabkan terjadinya penumpukan data nilai didalam sistem.

C. Perancangan Sistem

Berikut ini merupakan gambaran bentuk Sistem yang dianjurkan dimana *databas* yang dapat diakses oleh siswa hanyalah *databas* slave dimana *databas* slave hanyabisa diakses dengan menggunakan jaringan local. Sedangkan *databas* master dapat diakses memalui layanan public.



Gambar Bentuk Perancangan Keamanan *Databas* Sistem Ujian *Online* SMK Plus Pratama Adi Banjaran

A. Replikasi Database

Replikasi merupakan suatu teknik untuk melakukan copy dan pendistribusian data dan objek-objek *databas* dari satu *databas* ke *databas* lain dan melaksanakan sinkronisasi antara *databas* sehingga konsistensi data dapat terjamin. Dengan menggunakan teknik replikasi ini, data dapat didistribusikan ke lokasi yang berbeda melalui koneksi jaringan lokal maupun internet. Replikasi juga memungkinkan untuk mendukung kinerja aplikasi, penyebaran data fisik sesuai dengan penggunaannya, seperti pemrosesan transaksi *online* dan DSS (Desiscion Support Sistem) atau pemrosessan *databas* terdistribusi melalui beberapa server. *Snapshoot replicarion databas* Mendistribusikan data yang dapat dilihat pada saat tertentu tanpa melakukan update. Replikasi ini membantu pada saat data sebagian besar statis dan tidak sering berubah, dapat menerima copy data yang telah melewati batas waktu yang ditentukan, dan datanya sedikit

Hasil penelitian observasi dan wawancara menunjukan adanya keterbatasan dalam hal pengelolaan keamanan pada *databas* yang ada pada Sistem ujian *online*. *Acces control* dan Replikasi *databas* yang diusulkan peneliti adalah dua buah teknik atau cara yang bias dilakukan untuk melakukan pengamanan *databas* supaya aspek Kerahasiaan (*Confidentaility),* Integritas (*Integrity),* keberadaan (*availiability)* dalam *databas* yang ada id Sistem ujian *online.* Dimana *Confidentaility* adalh elemen yang menjamin kerahasiaan data atau informasi, memastikan bahwasannya informasi hanya bias diakses oleh orang yang berwenang dan bisa menjamin kerahasiaan data yang dikirim, diterima, dan disimpan. *Integrity* adalah elemen yang menjamin bahwa data tidak dirubah tanpa adanya ijin pihak yang berwenang, menjaga keakuratan dan keutuhan informasi serta metode prosesnya untuk menjamin aspek *integrity* ini. *Availibility* adalah elemen yang menjamin bahwa data akan tersedia saat dibutuhkan, memastikan user yang berhak memperoleh informasi.

Table yang nantinya akan direplikasi adalah table yang berisi informasi dalam Sistem ujian *online*, yaitu informasi seputar ujian *online* baik berupa data soal, data nilai ataupun data lainnya yang berhubungan dengan proses ujian *online*. Untuk melakukan proses replikasi *databas* Sistem ujian *online* maka lakukanlah langkah – langkah dibawah ini. Langkah yang akan dijelaskan adalah langkah replikasi *databas* dengan teknik *Snapshoot Replication Databas* dengan menggunakan MySQL sebagai DBMS (*Databas Management* Sistem).

B. Acces Control

Seperti yang sudah dijelaskan sebelumnya, bahwa setiap user yang didaftarkan pada Sistem ujian *online* maka iduser tersebut akan menjadi iduser dalam MySQL. Berikut user basis data yang sudah ditentukan.

Tabel 5.17 User Basis Data Ujian *Online*

No	Deskripsi Tugas	User	Privilege	Keterangan
1	Entry data file materi	Guru	Create	
			Update	
			Delete	
2	Entry data jawaban	Siswa	update	Siswa hanya mengupdate jawaban yang sudah diisi siwa kedalam table bukan meng update keseluruhan data yang ada didalam table
3	Entry data kelas	Admin	Create	
			Update	
			Delete	
4	Entry data mata pelajaran	Admin	Create	
			Update	
			Delete	
5	Entry data modul	uru	Create	

			Update	
			Delete	
6	Entry data nilai	siswa	Update	Siswa tidak melakukan update langsung terhadap data yang ada didalam table tetapi data yang ada didalam table akan langsung terupdate sesuai dengan hasil yang didapat oleh siswa pada saat ujian
7	Entry data nilai soal esy	Guru	Update	Setelah memeriksa jawaban soal esai guru akan melakukan update data nilai siswa.
8	Entry data *online*	Siswa	Update	Data yang diupdate tidak langsung diupdate oleh siswa tetapi akan terupdate otomatis pada saat siswa login kedalam Sistem ujian *online*
9	Entry data pengajar	Admin	Create	
			Update	
			Delete	
10	Entry data quiz esai	Guru	Create	
			Update	
			Delete	
11	Entry data quiz pilihan ganda	Guru	Create	
			Update	
			Delete	
12	Entry data registrasi siswa	Admin	Create	
			Update	
			Delete	
13	Entry data siswa	Admin	Create	
			Update	
			Delete	
14	Entry data siswa sudah mengerjakan	Siswa	Update	Data siswa sudah mengerjakan akan terupdate secara otomatis pada saat siswa sudah beres mengerjakan soal
15	Entry data topik quis	Guru	Create	
			Update	
			Delete	

4. Hasil Dan Pembahasan

Pengujian keamanan akan dilakukan dengan cara melakukan sebuah serangan yang dengan target sasaran langsung mengakses ke dalam database sehingga penyerang akan melakukan perubahan data yang ada didalam database dan menyebabkan data yang ada didalam database menjadi berubah. Peermasalahan tersebut sering juga dikenal dengan istilah DOS dan selain ancaman yang berupa DOS ada juga ancaman yang berupa penyusupan yang dilakukan sehingga pelaku dapat masuk dengan menpergunakan salah satu username dan password milik salah satu user dan setelah berhasil masuk kedalam sistem maka pelaku akan melakukan perubahan data, penghapusan data, ataupun pencurian terhadap data. Untuk melakukan salah satu ancaman tersebut dapat dilakukan dengan cara menggunakan SQL Injection.

Injeksi SQL atau SQL Injection memiliki makna dan arti yaitu sebuah teknik yang menyalahgunakan sebuah celah keamanan yang terjadi dalam lapisan basis data sebuah aplikasi. Celah ini terjadi ketika masukan pengguna tidak disaring secara benar dari karakter-karakter pelolos bentukan string yang diimbuhkan dalam pernyataan SQL atau masukan pengguna tidak bertipe kuat dan karenanya dijalankan tidak sesuai harapan. Ini sebenarnya adalah sebuah contoh dari sebuah kategori celah keamanan yang lebih umum yang dapat terjadi setiap kali sebuah bahasa pemrograman atau skrip diimbuhkan di dalam bahasa yang lain.

SQL injection adalah jenis aksi hacking pada keamanan komputer di mana seorang penyerang bisa mendapatkan akses ke basis data di dalam sistem. SQL injection yaitu serangan yang mirip dengan serangan XSS dalam bahwa penyerang memanfaatkan aplikasi vektor dan juga dengan Common dalam serangan XSS.

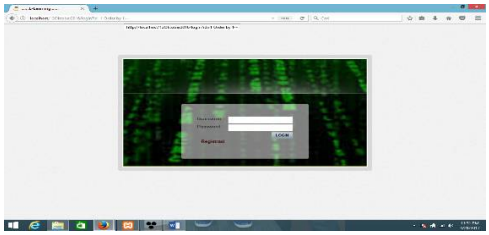
SQL injection exploits dan sejenisnya adalah hasil interfacing sebuah bahasa lewat informasi melalui bahasa lain . Dalam hal SQL injection, sebuah bahasa pemrograman seperti PHP

atau Perl mengakses *Database* melalui SQL query. Jika data yang diterima dari pengguna akhir yang dikirim langsung ke *Database* dan tidak disaring dengan benar, maka yang penyerang dapat menyisipkan perintah SQL nya sebagai bagian dari input.

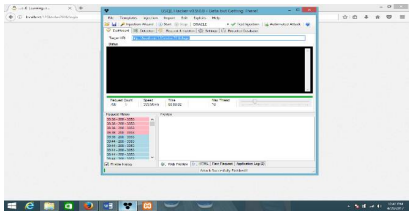
Pengujian keamanan dari *Database* Sistem ujian *online* akan dilakukan dengan menggunakan software Safe SQL Injection. Safe SQL Injector terkenal dengan kemudahan penggunaannya Safe3 SI menawarkan serangkaian fitur yang memungkinkan deteksi otomatis dan eksploitasi kelemahan SQL injection dan pengambilalihan *Database* server.

1. Tambahkan tanda ‘ dikahir url seperti pada gambar untuk melihat celah yang bisa di injection jika ada pesan *error* maka bisa di injection tapi hasil nya tidak ada seperti pada gambar dibawah ini.

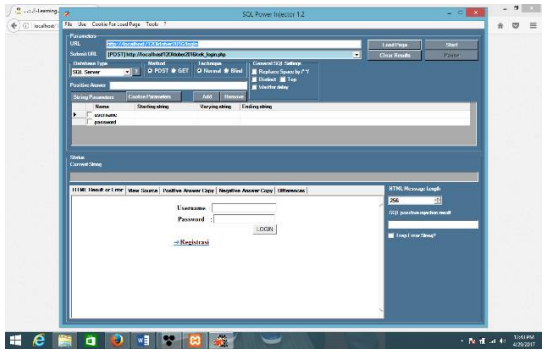
2. Selnajutnya masukan perintah **order by 1- -** untuk melihat ada berapa colom pada table tersebut jika ada pesan ***unkown column “ ”*** berarti pada kolom tersebut bisa kita masukan perintah sql tapi hasilnya nihil seperti pada gambar dibawah



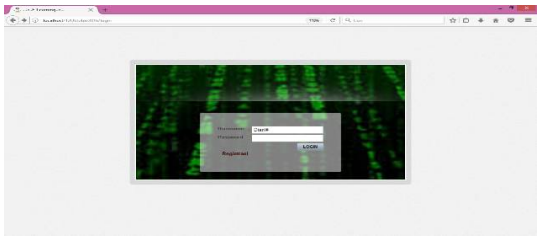
3. Setelah dicoba beberapa kali dengan berbagai macam teknik masih tetap tidak ada error
4. Masuka url web kedalam BSQL seperti Nampak pada layar



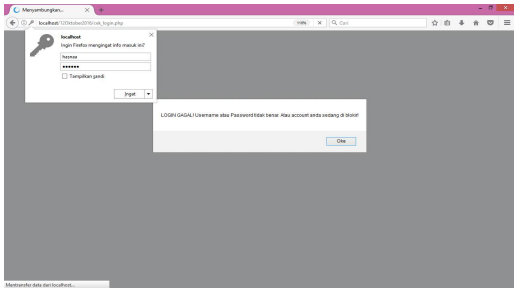
5. Tidak ada celah untuk dinjeksi
6. Security bisa dianggap sudah bagus.
7. Tes menggunakan sql Power Injection



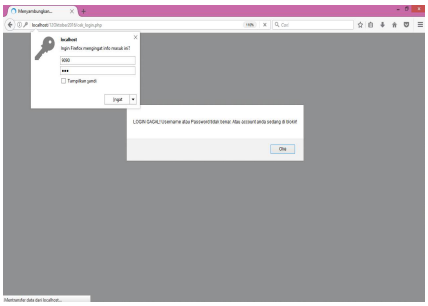
8. Masih tetap tidak muncul atau celah untuk mengijeksi query kedalam database system Tampilan halaman login



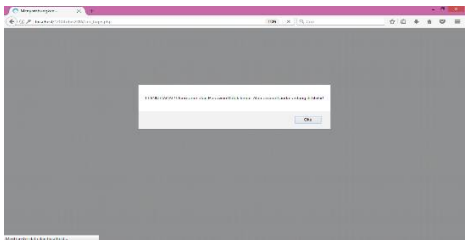
9. Pengujian acces control “Admin” jika 2 kali salah memasukan password maka akun akan diblokir percobaan pertama menggunakan akun dengan nama hanna berikut screenshootnya;



10. Pengujian acces control “Siswa” jika 2 kali salah memasukan password maka akun akan diblokir percobaan pertama dengan user id “9090” berikut screenshootnya;



11. Pengujian acces control “Guru” jika 2 kali salah memasukan password maka akun akan diblokir berikut screenshootnya;



Dari beberapa percobaan dan pengujian yang sudah dilakukan maka didapat hasil :

1. Sistem acces kontrol di level aplikasi untuk user guru dan siswa dapat memberikan protek keamanan yang cukup baik dapat terbukti bahwa ketika user dua kali salah melakukan login kedalam Sistem maka user tersebut langsung di blokir.
2. Sistem acces kontol di level *databas* untuk user guru dan siswa bisa mengontrol akses user kedalam *databas* sehingga setiap user tidak bisa seenaknya melakukan akses terhadap sembarang data yang ada didalam *databas*
3. Ketika dilakukan serangan dengan menggunakan SQL Injection sebanyak empat kali percobaan tidak ada percobaan yang berhasil menembus *databas* .

5. Kesimpulan Dan Saran

A. Kesimpulan

Berdasarkan uraian permaslahan, penelitian, dan pengujian yang dilakukan maka penulis dapat menyimpulkan sebagai berikut:

1. *Database* yang sudah dibuat dengan menggunakan teknik Replikasi Basis Data dan Model *Discretionary Acces Control* sudah bisa tahan terhadap serangan yang muncul
2. Dengan membuat pengaturan terhadap hak akses setiap user maka *database* yang ada menjadi lebih aman karena setiap user memiliki batasan terhadap pengaksesan data didalam *database* sehingga user tidak bisa melakukan akses data terhadap data yang tidak diperuntukan untuk user tersebut.
3. *Database* Sistem ujian online yang dirancang mempergunakan teknik standar yang sesuai dengan ilmu perancangan *database*. Teknik Replikasi Basis Data dan Model *Discretionary Acces Control* merupakan teknik pengamanan *database* yang bisa diimplementasikan pada saat akan melakukan perancangan *database* dan terbukti bahwa teknik Replikasi Basis Data dan Model *Discretionary Acces Control* dapat diimplementasikan untuk membuat sebuah rancangan *database* yang melakukan pengamanan terhadap *database* yang dirancang.
4. Solusi yang dikemukakan sudah cukup membantu ketika ada permasalahan serangan yang muncul terhadap *database*

B. Saran

Saran dari peneliti untuk sekolah ketika penelitian ini akan diimplementasikan kedalam Sistem ujian online oleh sekolah adalah :

1. Yang harus diperhatikan pertama kali adalah pengaturan akses control kedalam Sistem dan *database* janagan sampai pengelola salah menentukan akses control masing – masing user. Sehingga dengan demikian *database* yang dipergunakan bisa lebih terjaga keamanan data yang ada didalamnya.
2. Ketika akan mengimplementasikan rancangan keamanan *database* kedalam Sistem yang utuh, maka sebaiknya pihak sekolah menghubungi seorang web desainer untuk membuat sebuah tampilan Sistem yang lebih menarik dan lebih baik lagi.
3. Adanya pelatihan yang dilakukan untuk guru dan admin untuk menambah wawasan dan pengetahuan seputar keilmuan Teknologi Informasi dan Komunikasi.

C. Daftar Pustaka

Alamsyah. Ilham, 2013, Pengolahan Keamanan Database Pada Data Kepegawaian (Studi Kasus di PDAM Tirta Intan Kabupaten Garut), Jurnal Algoritma Sekolah Tinggi Teknologi Garut

Anwar. Nuril, 2013, Analisa Arsitektur Client Server Menggunakan Database Terpusat (Studi Kasus Pada SMP Muhammadiyah Purwodadi Purworejo), Jurnal Sarjana Teknik Informatika, Universitas Ahmad Dahlan

Hadiansyah. Tatan, 2009, Replikasi Basis Data dan Sistem Hak Akses Untuk Menjaga Keamanan Basis Data Studi Kasus : www.sukabumikota.go.id, Tesis, Universitas Langlangbuana

Kadir. Abdul, (1999), *Konsep dan Tuntunan Praktis Basis Data*, Yogyakarta, Penerbit Andi

Nathasia. Novi, 2011, Penerapan Teknik Kriptografi Stream Ciper Untuk Pengamanan Basis Data, ICT Reaserch Center UNAS, Universitas Nasional

Sugiantoro. Bambang, 2010, Analisa Keamanan Database Server Menggunakan Teknologi Virtual Private Database dan Notifikasi Database Server Menggunakan Agen Bergerak, Seminar Nasional Informatika 2010, Universitas Gajah Mada Yogyakarta

http://www.devshed.com/c/a/oracle/row-level-security-with-virtual-private-database/ diakses pada 21 Desmber 2016 jam 11:46

https://diskusikuliah.wordpress.com/2010/10/31/database-replication/ 21 desember 2016 21:35

https://csirt.bppt.go.id/wp-content/uploads/2014/06/Panduan-3-Keamanan-Database.pdf Diakses Pada 19 April 2017 Jam 18 : 00 Wib

http://www.jejaring.web.id/homogen-sistem-basis-data-terdistribusi/ diakses pada 19 Desember 2016 jam 16 : 31

http://repository.usu.ac.id/bitstream/123456789/16384/3/Chapter%20II.pdf Diakses 20 januari 2017 pada pukul 14:03

http://www.duniailkom.com/tutorial-belajar-mysql-mengenal-superuser-root-dan-pengertian-privileges-mysql/ Diakses 20 January 2017 pada pukul 13:37