BAB II

LANDASAN TEORI

2.1 Jaringan Komputer

Jaringan komputer adalah suatu himpunan interkoneksi sejumlah *computer autonomous*. Dalam bahasa populer dapat dijelaskan bahwa jaringan komputer adalah kumpulan beberapa komputer yang saling terhubung satu sama lain melalui media perantara (Sofana, 2013). Media perantara dapat melalui kabel maupun tanpa kabel (*nirkabel*). Informasi berupa data akan mengalir dari satu komputer ke komputer lainnya sehingga masing-masing komputer yang terhubung tersebut dapat bertukar data atau berbagi perangkat keras.

2.1.1 Klasifikasi Jaringan Komputer

Lingkup sistem jaringan komputer melibatkan beberapa sub sistem yang terdiri sebagai berikut :

1. Berdasarkan geografisnya, jaringan komputer terbagi menjadi: LAN (*Local Area Network*) dan MAN (*Metropolitan Area Network*), atau WAN (*Wide Area Networ*k).
2. Berdasarkan fungsi, terbagi menjadi jaringan *client-server* dan jaringan *peer-to-peer*.
3. Berdasarkan topologi jaringan, jaringan komputer dibedakan meliputi topologi bus, bintang, cincin, mesh, pohon dan linier.

4. Berdasarkan distribusi sumber informasi/data meliputi jaringan terpusat dan jaringan terdistribusi.
5. Berdasarkan media transmisi data meliputi jaringan nirkabel dan jaringan berkabel (*wired network*).

2.2 Keamanan Data pada Jaringan Komputer

Keamanan jaringan adalah kumpulan piranti yang dirancang untuk melindungi data ketika transmisi terhadap ancaman pengaksesan, pengubahan, dan penghalangan oleh pihak yang tidak memiliki kewenangan (Sadikin, 2012).

2.2.1 Layanan keamanan jaringan

Lembaga internasional yang bernama Internasional *Telecommunication Union – Telecommunication Standaritation Sector* (ITU-T) mendefinisikan beberapa jenis layanan (*services*) dan mekanisme (*mechanism*) keamanan jaringan. Layanan keamanan jaringan didefinisikan berdasarkan kebutuhan yang harus disediakan untuk memenuhi permintaan terhadap keamanan jaringan. Berikut jenis-jenis layanan keamanan jaringan berdasarkan ITU-T pada dokumen X.800 (ITU, 1991) yaitu meliputi

1. Otentikasi

   Merupakan layanan yang memastikan kepastian dan keaslian data terhadap identitas sebuah entitas yang terlibat pada komunikasi data.

2. Kendali Akses

   Merupakan layanan keamanan jaringan yang menghalangi penggunaan tidak terotorisasi terhadap sumber daya.

3. Kerahasiaan Data

   Kerahasiaan data adalah layanan keamanan jaringan yang memproteksi data tertranmisi terhadap pengungkapan oleh pihak yang tidak berwenang.

4. Keutuhan Data

   Keutuhan data adalah layanan kemanan jaringan yang memastikan bahwa data yang diterima oleh penerima adalah benar-benar sama dengan data yang dikirim oleh pengirim.

5. *Non-Repudiation*

   Non-repudiation merupakan layanan keamanan jaringan yang menghindari penolakan atas penerimaan/pengiriman data yang telah terkirim.

6. Ketersediaan

   Layanan ketersediaan adalah layanan sistem yang membuat sumber daya sistem tetap dapat diakses dan digunakan ketika ada permintaan dari pihak yang berwenang.

2.2.2 Mekanisme Keamanan Jaringan

Untuk mewujudkan layanan keamanan jaringan pengembang sistem dapat menggunakan mekanisme keamanan jaringan. Menurut

ITU-T, ada beberapa jenis mekanisme keamanan jaringan yang meliputi :

1. *Enciphermen*

   Enciphermen merupakan mekanisme keamanan jaringan yang digunakan untuk menyembunyikan data. Mekanisme ini dapat menyediakan layanan kerahasiaan data meskipun dapat juga digunakan untuk layanan lainnya. Untuk mewujudkan mekanisme e*nciphermen* dapat menggunakan teknik kriprografi dan steganografi.

2. Keutuhan Data

   Mekanisme keutuhan data digunakan untuk memastikan keutuhan data pada unit data atau pada suatu aliran (*stream*) data unit. Cara yang digunakan adalah dengan menambahkan nilai penguji (*check value*) pada data asli. Jadi ketika sebuah data akan dikirim nilai penguji dihitung secara bersamaan. Penerima dapat menguji apakah ada perubahan data atau tidak dengan cara menghitung nilai penguji data yang terkirim dan membandingkan nilai penguji yang dihitung dengan nilai penguji yang dikirim bersamaan dengan data asli. Bila sama penerima dapat menyimpulkan data tidak berubah.

3. *Digital Signature*

   Digital signature merupakan mekanisme keamanan jaringan yang menyediakan cara bagi pengirim data untuk

"menandatangani" secara elektronik sebuah data dan penerima dapat memverifikasi "tanda tangan" itu secara elektronik. Digital Signature ditambahkan pada data unit dan digunakan sebagai bukti sumber pengirim dan menghindari pemalsuan tanda tangan.

4. *Authentication Exchange*

   Mekanisme ini memberikan cara agar dua entitas dapat saling meng-otentikasi dengan cara bertukar pesan untuk saling membuktikan identitas.

5. *Traffic Padding*

   Traffic Padding menyediakan cara unutk pencegahan analisis lalu lintas data pada jaringan yaitu dengan menambah data palsu pada lalu lintas data.

6. *Routing Control*

   Routing Control menyediakan cara untuk memilih dan secara terus menerus mengubah alur pada jaringan komputer antara pengirim dan penerima. Mekanisme ini menghindarkan komunikasi dari penguping.

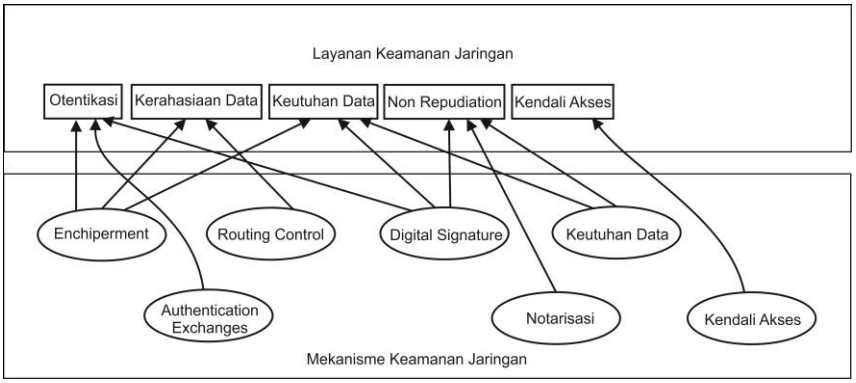
7. Notarisasi

   Notarisasi menyediakan cara untuk memilih pihak ketiga yang terpercaya sebagai pengendali komunikasi antara pengirim dan penerima.

8. Mekanisme Kendali Akses

   Mekanisme kendali akses memberikan cara bagi pengguna untuk memperoleh hak akses sebuah data. Misalnya dengan tabel relasi pengguna dan otoritasnya.

Hubungan antara mekanisme dan layanan keamanan jaringan diilustrasikan oleh Gambar 2.1. Gambar tersebut menjelaskan bahwa untuk mewujudkan sebuah layanan keamanan jaringan dibutuhkan mekanisme yang tepat dan tidak semua mekanisme keamanan jaringan digunakan untuk mewujudkan sebuah layanan keamanan jaringan.



Gambar 2.1 Hubungan antara mekanisme layanan dan keamanan jaringan (ITU, 1991)

2.3 Kriptografi

2.3.1 Sejarah

Kriptografi berasal dari bahasa yunani yaitu *crypto* yang berarti rahasia dan *graphia* yang artinya tulisan. Sejarah penulisan tertua dapat ditemukan pada peradaban Mesir kuno, yakni 4000 tahun yang lalu. Bangsa Mesir menggunakan ukiran rahasia yang disebut dengan *hieroglyph* untuk menyampaikan pesan kepada orang yang berhak. Jenis tulisan ini bukanlah bentuk tulisan standar yang digunakan dalam penulisan sebuah pesan (Ariyus, 2008)

Gambar 2.2 Tulisan yang Menggunakan *Hieroglyph* (Ariyus, 2008)

2.3.2 Algoritma Kriptografi

Kriptografi pada awalnya dijabarkan sebagai ilmu yang mempelajari bagaimana menyembunyikan pesan. Namun pada pengertian modern kriptografi adalah ilmu yang bersandarkan pada teknik matematika untuk berurusan dengan keamanan informasi

seperti kerahasiaan, keutuhan data dan otentikasi entitas (Sadikin, 2012).

2.3.3 Sistem Kriptografi

Sistem kriptografi terdapat 5 bagian yaitu :

1. *Plaintext*

   Merupakan pesan atau data dalam bentuk aslinya yang dapat terbaca.

2. *Secret Key*

   Merupakan masukan bagi algoritma enkripsi yakni nilai yang bebas terhadap teks asli dan menentukan hasil keluaran algoritma enkripsi.

3. *Chipertext*

   Merupakan hasil teks asli setelah dienkripsi. Chipertext dapat dianggap sebagai pesan dalam bentuk tersembunyi. Algoritma yang baik akan menghasilkan chipertext yang terlihat acak.

4. Algoritma Enkripsi

   Algoritma enkripsi memiliki 2 masukan teks asli dan kunci rahasia. Algoritma enkripsi melakukan transformasi terhadap teks asli sehingga menghasilkan *chipertext*.

5. Algoritma Dekripsi

   Algoritma deskripsi memiliki 2 masukan teks sandi dan kunci rahasia. Algoritma deskripsi akan memulihkan kembali

chipertext menjadi teks asli bila kunci rahasia yang dipakai algoritma deskripsi sama dengan kunci rahasia yang dipakai algoritma enkripsi.

2.3.4 Mekanisme Algoritma Kriptografi

Berikut mekanisme yang berkembang pada kriptografi modern yaitu (Sadikin, 2012) :

a. Fungsi *Hash*

Fungsi *hash* sering disebut dengan hash atau satu arah. Fungsi *hash* adalah fungsi yang memetakan pesan dengan panjang sembarang ke sebuah teks khusus yang disebut *message digest* dengan panjang tetap. Fungsi hash pada umumnya digunakan untuk membuat sidik jari dari suatu pesan.

b. Algoritma Simetri

Pada algoritma ini sering disebut dengan algoritma klasik karena memiliki kunci yang sama untuk kegiatan enkripsi dan dekripsi. Contoh penggunaan algoritma ini adalah si penerima pesan harus diberitahu kunci dari pesan tersebut agar dapat mendeskripsi pesan yang dikirim. Keamanan dari algoritma ini terletak pada kunci yang diberikan, jika kunci tersebut diketahui oleh orang lain maka orang tersebut dapat melakukan enkripsi dan deskripsi terhadap pesan tersebut.

Contoh algoritma simetri :

- *Data Encryption Standard* (DES)
- RC2, RC4, RC5, RC6
- *International Data Encryption Algrithm* (IDEA)
- *Advanced Encrption Standard* (AES)
- *One Time Pad* (OTP)
- A5

c. Algoritma asimetri

Algoritma ini sering disebut dengan algoritma kunci *public* dengan arti kata kunci yang digunakan untuk melakukan enkripsi dan dekripsinya berbeda. Pada algortima ini kunci terbagi menjadi dua bagian yaitu :

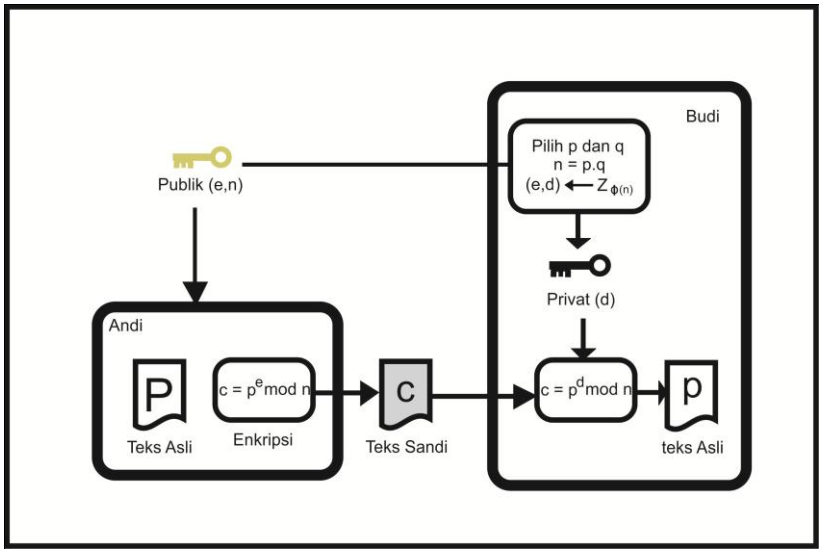
- Kunci umum atau *public key* dimana kunci ini dapat diketahui oleh orang lain atau bersifat umum.
- Kunci pribadi atau *private key* adalah kunci yang dirahasiakan atau hanya boleh diketahui oleh satu orang.

2.4 RSA (*Rivest Shamir Adleman*)

Dari sekian banyak algoritma kriptografi kunci-publik yang pernah dibuat, algoritma yang paling popular adalah algoritma RSA (Ariyus, 2008). Algoritma ini melakukan pemfaktoran bilangan yang besar. Oleh karena alasan tersebut, RSA dianggap aman. Untuk membangkitkan dua kunci, dipilih dua

bilangan prima acak yang besar. Algoritma RSA dibuat oleh 3 orang peneliti dari MIT (*Massachussets Institute of Technology*) pada tahun 1976 yaitu Ron Riverst, Adi Shamir, dan Leonard Adleman.

RSA mengekspresikan teks asli yang dienkripsi menjadi blok-blok yang mana setiap blok memiliki nilai bilangan biner yang di beri simbol “n”, blok teks asli “M” dan blok teks kode “C”. untuk melakukan enkripsi pesan “M” , pesan dibagi kedalam blok-blok numerik yang lebih kecil dari pada “n” (data biner dengan pangkat terbesar) jika bilangan prima yang panjangnya 200 digit, dapat ditambah beberapa bit 0 di kiri bilangan untuk menjaga agar pesan tetap kurang dari nilai “n”.



Gambar 2.3 Sistem RSA (Sadikin, 2012)

2.4.1 Pembangkitan Kunci RSA

Untuk menggunakan RSA terlebih dahulu pendekripsi (Budi) membangkitkan sepasang kunci yaitu kunci *public* dan kunci *privat*. (Sadikin, 2012). Hal pertama yang dilakukan algoritma pembangkit

kunci adalah membangkitkan 2 bilangan prima besar. Pembangkitan bilangan prima besar menggunakan algoritma pengujian bilangan prima misalnya algoritma Miller-Rabin. Berikut langkah-langkah untuk pembangkitan kunci RSA :

1. Bangkitkan bilangan prima p dan q ……. (2.1)
2. $n = p \times q$ …… (2.2)
3. $\emptyset(n) = (p-1) \times (q-1)$ …….. (2.3)
4. $e \overset{R}{\leftarrow} Z_{\emptyset(n)}$ dengan $\gcd(e, \emptyset(n)) = 1$ ……. (2.4)
5. $d = e^{-1}\ pada\ Z_{\emptyset(n)}$ ……... (2.5)
6. $K_{publik} = (e,n),\ K_{privat} = d$ ……..…… (2.6)

Agar sistem kriptografi RSA aman diperlukan bilangan prima yang besar sehingga n = p x q sangat sulit untuk difaktorisasi. Direkomendasikan besar p dan q adalah 512 bit sehingga n berukuran 1024 bit.

2.4.2 Proses Enkripsi RSA

Setelah kunci publik K_{publik} dibangkitkan oleh pendekripsi (Budi) maka sembarang orang dapat menggunakan kunci publik untuk mengirim pesan teks sandi ke Budi. Algoritma enkripsi RSA menggunakan fungsi eksponensial dalam modular n (Sadikin, 2012). Berikut langkah enkripsi RSA :

Input : $K_{publik} = (e,n), P \in Z_n$

Output : $C \in Z_n$

$C = P^e mod\ n$ {Gunakan algoritma $Square$ dan $Multiply$} ….. (2.7)

2.4.3 Proses Dekripsi RSA

Jika Budi mendapatkan teks sandi yang dienkripsi dengan kunci public Budi maka Budi dapat menggunakan kunci privatnya untuk mengembalikan teks sandi menjadi teks asli (Sadikin, 2012). Berikut rumus deskripsi RSA :

Input : $K_{privat} = d, K_{publik} = (e, n), C \in Z_n$

Output : $P \in Z_n$

$P = C^d\ mod\ n$ …….. (2.8)

2.4.4 Bukti Sistem Kriptografi RSA

Fungsi deskripsi RSA dapat dibuktikan yang merupakan *invers* (kebalikan) fungsi enkripsi RSA dengan menggunakan *teorema euler* (Sadikin, 2012). Hubungan parameter *d* di kunci privat dan *e* di kunci publik dapat ditulis sebagai berikut:

$e.d \equiv 1\ mod\ \emptyset(n)$ ……... (2.9)

Oleh karena itu, dengan aritmatika modular dapat ditulis sebagai :

$e.d \equiv t\emptyset(n+1)$ ……..... (2.10)

Dengan integer $t \geq 1$. Fungsi enkripsi RSA mengembalikan $C = P^e\ mod\ n$, jadi deskripsi RSA dapat dihitung sebagai:

$P = C^d\ mod\ n$ ……..…. (2.11)

$= P^{e.d} mod\ n$

$$= P^{t\emptyset(n)+1} \, mod \, n$$

$$= P^{t\emptyset(n)}.P \, mod \, n$$

$$= 1^{t}.P \, mod \, n \text{ dengan Teorema Euler}$$

$$= P \, mod \, n$$

Oleh karena itu, algoritma deskripsi RSA merupakan *invers* enkripsi RSA.

2.5 AES (*Advanced Encryption Standard*)

AES merupakan sistem penyandian blok yang bersifat *non-feistel* karena algoritma ini menggunakan komponen yang selalu memiliki *invers* dengan panjang blok 128 bit (Sadikin, 2012). Kunci AES dapat memiliki panjang 128, 192 dan 256 bit. Penyandian AES menggunakan proses berulang yang disebut dengan ronde. Jumlah ronde tergantung pada panjang kunci yang digunakan. Setiap ronde membutuhkan kunci ronde dan masukan dari ronde berikutnya. Kunci ronde dibangkitkan berdasarkan kunci yang diberikan.

Relasi antara jumlah ronde dan panjang kunci sebagai berikut:

Tabel 2.1 Jumlah Ronde dan Panjang Kunci (Sadikin, 2012)

Panjang kunci AES (bit)	Jumlah Ronde (Nr)
128	10
192	12
256	14

2.5.1 Proses Enkripsi AES

Proses enkripsi AES merupakan transformasi terhadap state. Sebuah teks dalam blok (128 bit) terlebih dahulu akan diorganisir sebagai state. Enkripsi AES adalah transformasi terhadap state yang dilakukan secara berulang dalam beberapa ronde (Sadikin, 2012).

Pada awalnya teks asli akan direorganisasi sebagai sebuah state. Kemudian sebelum ronde 1 dimulai blok teks asli dicampur dengan kunci ronde ke-0 transformasi ini disebut dengan AddRoundKey. Setelah itu, ronde ke-1 sampai dengan ronde ke-(Nr-1) dengan Nr adalah jumlah ronde menggunakan 4 jenis transformasi yaitu subytes, Shiftrows, mixcoloumns, dan addroundkey. Pada ronde terakhir yaitu ronde ke-Nr dilakukan transformasi serupa dengan ronde lain namun tanpa transformasi mixcoloumns.

2.5.2 Proses Dekripsi AES

Secara ringkas algoritma dekripsi AES merupakan kebalikan algoritma enkripsi AES. Deskripsi AES menggunakan transformasi dasar yang digunakan pada algoritma enkripsi AES. Setiap transformasi dasar AES memiliki transformasi invers, yaitu invsubbytes, invshiftrows, dan invmixcolomns (Sadikin, 2012).

2.6 PHP (PHP *Hypertext Preprocessor*)

PHP merupakan bahasa pemrograman *server side scripting* yang menyatu dengan HTML untuk membuat halaman web yang dinamis (Arief,

2011). Secara khusus, PHP dirancang untuk membentuk web dinamis artinya dapat membentuk suatu tampilan berdasarkan permintaan terkini. Bahasa pemrograman ini berbasis open source, semua pengguna bebas membuat, menyebarluaskan dan mendistribusikan programnya asal tidak mengambil hak cipta dari PHP tersebut.

Kelebihan dari bahasa pemrograman PHP adalah mendukung semua sistem operasi dari microsof windows, linux, machintosh dan lain sebagainya. Pada dasarnya bahasa pemrograman ini hampir sama dengan bahasa pemrograman C/C++ karena terdapat perintah yang sama seperti “printf”, kemudian CGI (*Common Gateway Interfaces*), dan PERL. PHP juga mendukung teknik pemrograman berorientasi obyek. Untuk membuat aplikasi berbasis web dengan PHP dapat menggunakan aplikasi bawaan seperti notepad, wordpad dan adobe dreamweaver.

2.7 Basis Data

Basis data terdiri dari 2 kata yaitu basis dan data dimana basis dapat diartikan sebagai markas atau gudang dan data adalah representasi fakta dunia nyata yang mewakili suatu objek seperti manusia (pegawai, siswa, pembeli), barang, peristiwa, konsep, keadaan dan sebagainya yang diwujudkan dalam bentuk angka, huruf, teks, gambar, bunyi atau kombinasinya (Fathansyah, 2012).

2.7.1 Sistem Basis Data

Sistem adalah sebuah tatanan yang terdiri atas sejumlah komponen fungsional yang saling berhubungan dan secara bersama-sama bertujuan untuk memenuhi suatu proses tertentu. Jadi sistem basis data adalah sistem yang terdiri atas kumpulan tabel data yang saling berhubungan dan sekumpulan program yang memungkinkan beberapa pemakai dan atau mengakses dan memanipulasi tabel-tabel data tersebut (Fathansyah, 2012).

2.7.2 Bahasa Basis Data

DBMS merupakan perantara bagi pemakai dengan basis data dalam disk. Cara berinteraksi antara pemakai dengan basis data diatur dalam suatu bahasa khusus yang ditetapkan oleh perusahaan pembuat DBMS. Contoh basis data adalah SQL, dBase, QUEL. Sebuah basis data biasannya dapat di pilah ke dalam dua bentuk yaitu :

a. *Data Definition Language* (DDL)

   DDL merupakan struktur basis data yang menggambarkan skema basis data secara keseluruhan dan didesain dengan bahasa khusus. Dengan bahasa, dapat membuat tabel baru, membuat indeks, mengubah tabel, menentukan struktur penyimpanan tabel dan sebagainya. Hasil dari kompilasi perintah DDL adalah kumpulan tabel yang disimpan dalam file khusus yang disebut kamus data.

b. *Data Manipulation Language* (DML)

DML merupakan bentuk bahasa basis data yang berguna untuk melakukan manipulasi dan pengambilan data pada suatu basis data. Manipulasi data dapat berupa

- Penambahan data baru ke suatu basis data,
- Penghapusan data dari suatu basis data dan
- Pengubahan data di suatu basis data.

2.8 MYSQL

MySql adalah salah satu jenis database server yang digunakan untuk membangun aplikasi web menggunakan database sebagai sumber dan pengolahan datanya (Arief, 2011). MySql didistribusikan secara gratis dibawah lisensi GPL *(General Public License)* dimana setiap orang bebas untuk menggunakan MySql, akan tetapi tidak boleh dijadikan produk turunan yang bersifat komersial.

Kelebihan MySql antara lain :

a. Portabilitas. MySql dapat berjalan stabil pada berbagai sistem operasi seperti *Windows, Linux, FreeBSD, Mac Os X Server, Solaris, Amiga,* dan masih banyak lagi.
b. *Open Source.* MySql didistribusikan secara *open source*, dibawah lisensi GPL sehingga dapat digunakan secara cuma-cuma.
c. *Multiuser*. MySql dapat digunakan oleh beberapa user dalam waktu yang bersamaan tanpa mengalami masalah atau konflik.

d. *Performance tuning*. MySql memiliki kecepatan yang menakjubkan dalam menangani *query* sederhana, dengan kata lain dapat memproses lebih banyak SQL per satuan waktu.

e. Jenis Kolom. MySql memiliki tipe kolom yang sangat kompleks, seperti *signed / unsigned integer, float, double, char, text, date, timestamp,* dan lain lain.

f. Perintah dan Fungsi. MySql memiliki operator dan fungsi secara penuh yang mendukung perintah *Select* dan *Where* dalam perintah *(query).*

g. Keamanan. MySql memiliki beberapa lapisan sekuritas seperti level *subnetmask*, nama *host*, dan izin akses *user* dengan sistem perizinan yang mendetail serta sandi terenkripsi.