

BAB II

LANDASAN TEORI

II.1. Implementasi

Implementasi adalah suatu tindakan atau pelaksanaan rencana yang telah disusun dengan cermat dan rinci. Implementasi ini biasanya selesai setelah dianggap permanen. Terkait dengan hal ini, berikut beberapa pengertian menurut para ahli. (<http://www.gurupendidikan.com/9-pengertian-implementasi-menurut-para-ahli/>).

Implementasi ialah sebuah proses untuk mewujudkan terlaksananya suatu kebijakan dan tercapainya kebijakan tersebut. Implementasi juga dimaksudkan untuk menjadi sarana untuk membuat sesuatu dan memberikan hasil yang bersifat praktis terhadap sesama. Jadi Implementasi itu berfungsi sebagai sebuah tindakan individu publik yang diarahkan pada tujuan serta ditetapkan dalam keputusan dan memastikan terlaksananya dan tercapainya suatu kebijakan serata memberikan hasil yang bersifat praktis terhadap sesama. (Lukman, 2015:146).

II.2. Keamanan

Masalah keamanan merupakan salah satu aspek terpenting dari sebuah sistem informasi. Masalah keamanan sering kurang mendapat perhatian dari para perancang dan pengelola sistem informasi. Masalah keamanan sering berada di urutan setelah tampilan, atau bahkan di urutan terakhir dalam daftar hal-hal yang dianggap penting. Apabila mengganggu performansi sistem, masalah keamanan sering tidak dipedulikan, bahkan ditiadakan. (Dony Arius, 2008).

Keamanan komputer meliputi empat aspek, antara lain:

1. *Authentication.*

Agar penerima informasi dapat memastikan keaslian pesan, bahwa pesan itu datang dari orang yang dimintai informasi. Dengan kata lain, informasi itu benar-benar datang dari orang yang dikehendaki.

2. *Integrity*

Keaslian pesan yang dikirim melalui jaringan dan dapat dipastikan bahwa informasi yang dikirim tidak dimodifikasi oleh orang yang tidak berhak.

3. *Non-repudiation*

Merupakan hal yang berhubungan dengan si pengirim. Pengirim tidak dapat mengelak bahwa dialah yang mengirim informasi tersebut.

4. *Authority*

Informasi yang berada pada sistem jaringan tidak dapat dimodifikasi oleh pihak yang tidak berhak untuk mengaksesnya.

5. *Confidentiality*

Merupakan usaha untuk menjaga informasi dari orang yang tidak berhak mengakses. Kerahasiaan ini biasanya berhubungan dengan informasi yang diberikan ke pihak lain.

6. *Privacy*

Lebih kearah data-data yang bersifat pribadi.

7. *Availability*

Aspek availabilitas berhubungan dengan ketersediaan informasi ketika dibutuhkan. sistem informasi yang diserang atau dijebol dapat menghambat atau meniadakan akses ke informasi.

8. *Access Control*

Aspek ini berhubungan dengan cara pengaturan akses ke informasi. Hal ini biasanya berhubungan dengan masalah otentikasi dan privasi. Kontrol akses seringkali dilakukan dengan menggunakan kombinasi *user id* dan *password* ataupun dengan mekanisme lain.

II.3. Basis Data (*Database*)

Database adalah sekumpulan file data yang saling berhubungan dan diorganisasikan sedemikian rupa sehingga memudahkan untuk mendapat dan memproses data. Lingkungan system database menekankan data yang tergantung (*idenpendent* data) pada aplikasi yang akan menggunakan data. Data adalah kumpulan fakta dasar (mentah) yang terpisah (Wahana komputer, 2006)

Menurut Adyanata Lubis (2016), Basis data merupakan gabungan *file* data yang dibentuk dengan hubungan/relasi yang logis dan dapat diungkapkan dengan catatan serta bersifat independen. Adapun basis data adalah:

“Tempat berkumpulnya data yang saling berhubungan dalam suatu wadah (organisasi/perusahaan) bertujuan agar dapat mempermudah dan mempercepat untuk pemanggilan atau pemanfaatan kembali data tersebut.”

Arti lain dari sistem basis data adalah:

“Suatu sistem penyusunan dan pengelolaan *record-record* dengan menggunakan komputer, dengan tujuan untuk menyimpan atau merekam serta memelihara data secara lengkap pada sebuah organisasi/perusahaan, sehingga mampu menyediakan informasi yang optimal yang diperlukan pemakai untuk kepentingan proses pengambilan keputusan.”

Dalam pembuatan dan penggunaan basis data terdapat empat komponen dasar sistem basis data, yaitu:

1. Data

Data yang digunakan dalam sebuah basis data, haruslah mempunyai ciri sebagai berikut:

- a. Data disimpan secara terintegrasi (*integrated*), yaitu *Database* merupakan kumpulan dari berbagai macam *file* dari aplikasi-aplikasi yang berbeda yang disusun dengan cara menghilangkan bagian-bagian yang rangkap (*redundant*).
- b. Data dapat dipakai secara bersama-sama (*shared*), yaitu masing-masing bagian dari database dapat diakses oleh pemakai dalam waktu yang bersamaan, untuk aplikasi yang berbeda.

2. *Hardware*

Terdiri dari semua peralatan perangkat keras komputer yang digunakan untuk pengelolaan sistem *database* , seperti

- a. Peralatan untuk penyimpanan, disk, drum, dll
- b. Peralatan *input* dan *output*
- c. Peralatan komunikasi data, dll

3. *Software*

Berfungsi sebagai perantara (*interface*) antara pemakai dengan data fisik pada *database*, dapat berupa:

- a. *Database Management System* (DBMS).
- b. Program-program aplikasi dan prosedur-prosedur yang lain, seperti Oracle, SQL Server, MySQL, dll

4. *User* (Pengguna)

Terbagi menjadi 3 klasifikasi:

- a. *Database Administrator (DBA)*, yaitu orang/*team* yang bertugas mengelola sistem *database* secara keseluruhan.
- b. *Programmer*, yaitu orang/*team* membuat program aplikasi yang mengakses *database* dengan menggunakan bahasa pemrograman.
- c. *End user*, orang yang mengakses *database* melalui terminal dengan menggunakan *query language* atau program aplikasi yang dibuat oleh *programmer*. (Adyanata Lubis , 2016)

Beberapa istilah-istilah pada database adalah:

1. *Table*

Sebuah tabel merupakan kumpulan data (nilai) yang diorganisasikan ke dalam baris (*record*) dan kolom (*field*). Masing-masing kolom memiliki nama yang spesifik dan unik.

2. *Field*

Field merupakan kolom dari sebuah *table*. *Field* memiliki ukuran *type* data tertentu yang menentukan bagaimana data nantinya tersimpan.

3. *Record*

Record merupakan sebuah kumpulan nilai yang saling terkait.

4. *Key*

Key merupakan suatu *field* yang dapat dijadikan kunci dalam operasi tabel. Dalam konsep database, *key* memiliki banyak jenis diantaranya *Primary Key*, *Foreign Key*, *Composite Key*, dll.

5. SQL

SQL atau *Structured Query Language* merupakan suatu bahasa (*language*) yang digunakan untuk mengakses database. SQL sering disebut juga sebagai *query*.

II.4. Kriptografi

Menurut Dony Ariyus (2008), Kriptografi berasal dari bahasa Yunani. Menurut bahasa tersebut kata kriptografi dibagi menjadi dua, yaitu *crypto* dan *graphia*. *Crypto* berarti *secret* (Rahasia) dan *graphia* berarti *writing* (tulisan)”. Menurut terminologinya, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan / data dikirim dari suatu tempat ke tempat yang lain.

Pada dasarnya komponen kriptografi terdiri dari beberapa komponen, seperti:

1. *Enkripsi*: merupakan hal yang sangat penting dalam kriptografi, merupakan cara pengamanan data yang dikirimkan sehingga terjaga kerahasiaannya.
2. *Dekripsi*: merupakan kebalikan dari enkripsi. Pesan yang telah dienkripsi dikembalikan ke bentuk asalnya. Algoritma yang digunakan untuk dekripsi tentu berbeda dengan yang digunakan untuk enkripsi.
3. *Kunci*: adalah kunci yang dipakai untuk melakukan enkripsi dan dekripsi. Kunci terbagi menjadi dua bagian, yaitu kunci rahasia (*private key*) dan kunci umum (*public key*).
4. *Ciphertext*: merupakan suatu pesan yang telah melalui proses enkripsi. Pesan yang ada pada teks-kode ini tidak bisa dibaca karena berupa karakter-karakter yang tidak mempunyai makna (arti).
5. *Plaintext*: sering disebut dengan *cleartext*. Teks-asli atau teks-biasa ini merupakan pesan yang ditulis atau diketik yang memiliki makna. Teks asli inilah yang diproses menggunakan algoritma kriptografi untuk menjadi *ciphertext* (teks-kode).
6. *Pesan*: dapat berupa data atau informasi yang dikirim (melalui kurir, saluran komunikasi data, dsb) atau yang disimpan di dalam media perekaman (kertas, *storage*, dsb).
7. *Cryptanalysis*: kriptanalisis bisa diartikan sebagai analisis kode atau suatu ilmu untuk mendapatkan teks-asli tanpa harus mengetahui kunci yang sah secara wajar. Jika suatu teks-

kode berhasil diubah menjadi teks-asli tanpa menggunakan kunci yang sah, proses tersebut dinamakan breaking code. Hal ini dilakukan oleh para kriptanalis. Analisis kode juga dapat menemukan kelemahan dari suatu algoritma kriptografi dan akhirnya dapat menemukan kunci atau teks-asli dari teks-kode yang dienkripsi dengan algoritma tertentu.

II.4.1. Sejarah Kriptografi

Menurut Dony Ariyus (2008), Kriptografi sudah digunakan oleh bangsa Mesir sejak 4000 tahun yang lalu, diperkenalkan oleh orang-orang Mesir lewat *hieroglyph*. Jenis tulisan ini bukanlah bentuk standar untuk menulis pesan.

Tulisan yang Hieroglyph

Arius, 2008)



zaman

suatu saat

Gambar II.1 Menggunakan

(Sumber: Dony

Dikisahkan, pada

Romawi Kuno, pada

Julius Caesar ingin

mengirimkan pesan rahasia kepada seorang jenderal dimedan perang. Pesan tersebut harus dikirimkan melalui seorang kurir. Karena pesan tersebut mengandung rahasia, Julius Caesar kemudian memikirkan bagaimana mengatasi nya. Ia kemudian mengacak pesan tersebut hingga menjadi suatu pesan yang tidak dapat dipahami oleh siapapun terkecuali oleh jenderal nya saja. Tentu sang jenderal telah diberi tahu sebelumnya bagaimana cara membaca pesan teracak

tersebut. Yang dilakukan Julius Caesar adalah mengganti semua susunan alphabet dari a, b, c, yaitu a menjadi d, b menjadi e, c menjadi f dan seterusnya.

II.5. Algoritma

II.5.1. Pengertian Algoritma

Menurut Ema Utami dan Suwanto Raharjo (2004), Algoritma merupakan urutan atau deskripsi langkah-langkah penyelesaian masalah yang tersusun secara logis, ditulis dengan notasi yang mudah dimengerti sedemikian sehingga langkah-langkah tersebut dapat dilaksanakan oleh pemroses.

II.5.2. Sejarah Algoritma

Ditinjau dari asal usul-usulnya, kata *Algoritma* mempunyai sejarah yang menarik. Kata ini muncul di dalam kamus *Webster* sampai akhir tahun 1957. Kata *algorism* mempunyai arti proses perhitungan dalam bahasa Arab. Algoritma berasal dari nama penulis buku Arab yang terkenal, yaitu Abu Ja'far Muhammad Ibnu Musa al-Khuwarizmi (al-Khuwarizmi dibaca oleh orang barat sebagai *algorism*). Kata *algorism* lambat laun berubah menjadi *algorithm*.

II.6. Algoritma Kriptografi

Algoritma kriptografi merupakan langkah-langkah logis bagaimana menyembunyikan pesan dari orang-orang yang tidak berhak atas pesan tersebut.

Algoritma kriptografi terdiri dari tiga fungsi dasar, yaitu:

1. *Enkripsi*

Merupakan hal yang sangat penting dalam kriptografi, merupakan pengamanan data yang dikirimkan agar terjaga kerahasiaannya. Pesan asli disebut *plaintext*, yang diubah menjadi kode-kode yang tidak dimengerti. Enkripsi bisa diartikan dengan cipher atau kode. Sama halnya dengan kita tidak mengerti akan sebuah kata maka kita akan melihatnya di dalam kamus atau daftar istilah. Beda halnya dengan enkripsi, untuk mengubah teks asli ke bentuk teks kode kita menggunakan algoritma yang dapat mengkodekan data yang kita inginkan.

2. *Dekripsi*

Merupakan kebalikan dari enkripsi. Pesan yang telah dienkripsi dikembalikan ke bentuk asalnya (teks-asli), disebut dengan dekripsi pesan. Algoritma yang digunakan untuk dekripsi tentu berbeda dengan algoritma yang digunakan untuk enkripsi.

3. *Kunci*

Yang dimaksud disini adalah kunci yang dipakai untuk melakukan enkripsi dan dekripsi. Kunci terbagi menjadi dua bagian, kunci rahasia (*private key*) dan kunci umum (*public key*).

II.6.1. Algoritma Knapsack

Algoritma Knapsack juga adalah algoritma kriptografi kunci-publik. Keamanan algoritma ini terletak pada sulitnya memecahkan persoalan knapsack (*Knapsack Problem.*). Knapsack artinya karung/kantong. Karung mempunyai kapasitas muat terbatas. Barang-barang dimasukkan ke dalam karung hanya sampai batas kapasitas karung saja. (Rinaldi Munir, 2004).

II.7. Java

Java merupakan bahasa pemrograman yang awalnya dikembangkan oleh James Gosling di Sun Microsystem. James Gosling, Mike Sheridan, dan Patrick Naughton memulai proyek untuk bahasa pemrograman Java awalnya adalah untuk industri televise interaktif, namun bahasa

Oak (nama awal dari Java) terlalu maju untuk teknologi televisi. Bahasa pemrograman ini menggunakan bahasa gabungan yang mirip dengan bahasa C dan C++.

Sun Microsystem merilis implementasi *public* pertama untuk Java 1.0 pada tahun 1991. Prinsip perilisannya adalah “*Write Once, Run Anywhere*”. Bahasa pemrograman ini menyediakan tingkat keamanan yang tinggi dan menyediakan *feature* untuk mengkonfigurasi keamanannya. Segera setelah perilisannya, banyak *web browser* yang memasukkan kemampuan untuk menjalankan *applet* dari Java yang membuat bahasa pemrograman ini segera populer. Dengan munculnya Java 2 (dirilis pada awalnya sebagai J2SE pada Desember 1998-1999), versi ini dibangun dengan memiliki konfigurasi diberbagai *platform*. J2EE ditargetkan untuk menangani aplikasi-aplikasi *enterprise*, J2ME ditargetkan untuk menangani aplikasi *mobile*, dan J2SE ditargetkan untuk aplikasi-aplikasi standard. Pada tahun 2006 untuk alasan pemasaran, Sun mengganti nama J2 untuk masing-masing edisi menjadi Java EE, Java ME, dan Java SE. (Aditya Kunto Wisnuraharja, 2013).

II.8. NetBeans

Netbeans merupakan salah satu *IDE* yang dikembangkan dengan bahasa pemrograman java. Netbeans mempunyai lingkup pemrograman java terintegrasi dalam suatu perangkat lunak yang di dalamnya menyediakan pembangunan pemrograman *GUI*, *text editor*, *compiler*, dan *interpreter*. *Netbeans* adalah sebuah perangkat lunak open source sehingga dapat digunakan secara grafis untuk keperluan komersil maupun nonkomersil yang didukung oleh *Sun MicroSystem*. (Atik Rusmayanti ; 2013 : 2-3)

II.9. Pengertian Client Server

Definisi *Client Server* menurut Rizal Qosidi (2010), menurut buku Yuswanto, yang berjudul Pemrograman Client Server Microsoft Visual Basic 6.0, menjelaskan bahwa: *server*

adalah komputer *database* yang berada di pusat, dimana informasinya dapat digunakan bersama-sama oleh beberapa *user* yang menjalankan aplikasi di dalam komputer lokalnya yang disebut dengan “*Client*”.

Menurut buku Ramadhan, SQL Server 2000 dan Visual Basic 6.0, menjelaskan bahwa: “*client* dan *Server* pada dasarnya tidaklah berarti dua buah komputer yang berbeda. *Client* dan *Server* adalah dua buah aplikasi yang berjalan dan saling berinteraksi satu sama lain sehingga aplikasi *Client* dan *Server* bisa saja berada bersama dalam satu buah komputer secara sekaligus”.

II.10. XAMPP

Menurut Satriawaty Mallu (2015), XAMPP dari *Apache*, *MYSQL*, *PHP* dan *Perl* adalah perangkat lunak bebas, yang mendukung banyak sistem operasi, merupakan kompilasi dari beberapa program. XAMPP memiliki arti sebagai berikut:

X: Program ini dapat dijalankan di banyak sistem operasi seperti *Windows*, *Linux*, *Mac OS* dan juga *Solaris*.

A: *Apache*, merupakan aplikasi *web server*. Tugas utama Apache adalah menghasilkan halaman *web* kepada user berdasarkan kode *PHP* yang dituliskan oleh pembuat *web*.

M : *MySQL* merupakan aplikasi *database server*, bahasa terstruktur yang digunakan untuk membuat dan mengelola *database* beserta isinya pengguna dapat memanfaatkan *MySQL* untuk menambahkan, mengubah, dan menghapus data yang berada dalam *database*.

P : *PHP*, bahasa pemrograman *web*. Bahasa pemrograman PHP merupakan bahasa pemrograman untuk membuat *web* yang bersifat *server-side scripting*.

P : *Perl* adalah bahasa pemrograman untuk segala keperluan, dikembangkan, pertama kali oleh Larry Wall di mesin *Unix*.

