BAB II
LANDASAN TEORI

2.1 Definisi Biometrik

Pada dasarnya setiap manusia, memiliki sesuatu yang unik yang berbeda dengan manusia lainnya. Inilah yang menimbulkan gagasan untuk menjadikan keunikan tersebut sebagai identitas diri. Hal ini perlu didukung oleh teknologi yang secara otomatis bisa mengidentifikasi/mengenali seseorang. Teknologi Biometrik adalah sistem yang menjembatani kebutuhan tersebut dengan menggunakan bagian tubuh manusia sebagai kepastian pengenalan. Bagian tubuh manusia yang digunakan antara lain sidik jari, mata dan wajah seseorang. Teknologi biometrik merupakan teknologi yang digunakan untuk menunjukkan keaslian *(authentication)* dari individu yang melakukan akses terhadap aset organisasi. *Authentication* adalah konsep yang menunjukkan bahwa hanya mereka yang diijinkan saja *(authentic)* yang dapat mempunyai akses terhadap aset organisasi atau hal hal yang bersifat *confidential* lainnya.

Secara umum ada tiga model *authentication* yang digunakan dalam mengamankan aset sebuah organisasi (Liu & Silverman 2004) yaitu: (1) *Something you have (possession):* kunci atau kartu identitas (2) *Something you know (knowledge):* password, PIN atau kata kunci yang digunakan untuk melakukan suatu akses kedalam asset organisasi (3) *Something you are (biometrik):* teknologi *biometrik security*. Teknologi *biometrik* yang merupakan pendekatan *something you are* dan merupakan pendekatan yang paling akurat,

(Chandra and Calderon 2003 pg54, Ax-S Biometrik 2005). Tarigan (2005 pg96), menyebutkan keunggulan biometrik adalah: (1) Sulit untuk dimanipulasi karena menggunakan konsep *something you are* (2) Memungkinkan dilakukan *audit trial* terhadap setiap kejadian yang ada, dimana melalui *biometrik security* dapat diketahui: siapa yang melakukan akses terhadap aset organisasi *(who)*, dimana *(where)* dan kapan *(when)* individu tersebut melakukannya (3) Mencegah individu yang tidak mempunyai otorisasi untuk melakukan akses terhadap aset organisasi. Kebocoran sangat mungkin terjadi, jika menggunakan *password (something you know)* atau kartu *(something you have)*, dimana kartu yang dimiliki individu dapat dipinjamkan kepada individu yang lain atau hilang dan ditemukan oleh individu yang tidak mempunyai otorisasi (4) Sebagai solusi untuk kelemahan konsep *something you know,* yaitu adanya kemungkinan individu tidak dapat mengingat kembali *password* atau PIN untuk melakukan akses.

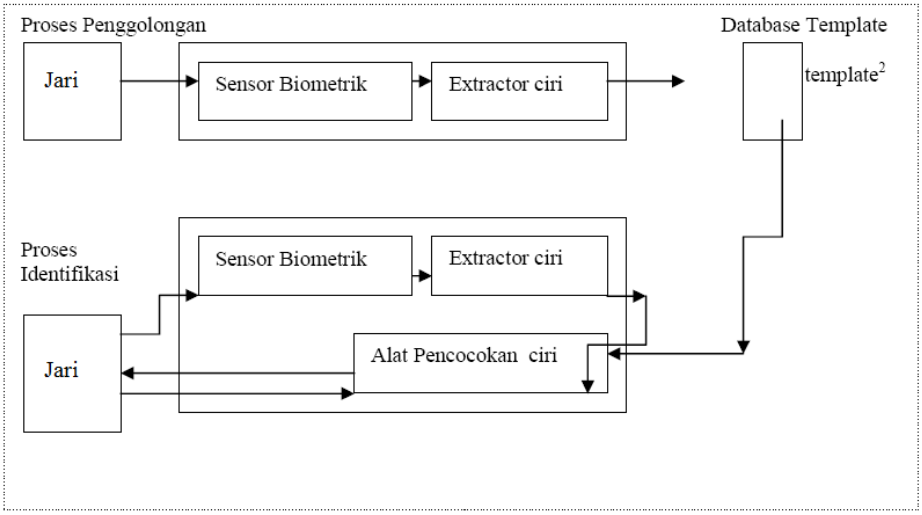
Lebih lanjut Tarigan mengungkapkan Biometrik merupakan sistem yang membaca bagian tubuh manusia untuk mengenali keaslian *(authentication)*, dimana teknologi ini menggunakan bagian yang unik dan tetap dari tubuh manusia seperti sidik jari, selaput pelangi mata / iris maupun wajah yang disimpan dalam database teknologi biometrik (Liu & Silverman (2004) pg 27-32). Mekanisme kerja dari teknologi ini adalah mencocokkan antara data yang diterima melalui *biometric reader* dengan apa yang ada dalam database sistem biometrik atau dengan kata lain membandingkan data yang sudah didefinisikan *(predifined data)* dengan data sekarang *(presented data)*. Dari perspektif ekonomi, teknologi *biometrics security* tidak lagi tergolong investasi yang mahal,

karena harga aplikasi biometrik sudah mulai terjangkau oleh hampir semua lapisan organisasi, jika dibandingkan beberapa tahun sebelumnya.

Menurut Sarwoko (2006, pg 2) Mekanisme sistem biometrik dapat digambarkan dengan beberapa fase, pertama fase penggolongan (enrollment). Pada fase ini masukan akan di pindai (scan) oleh sensor biometrik, yang merupakan representasi karakteristik digital. Selanjutnya fase pencocokan, dalam fase ini inputan database akan dicocokkan dengan identifikasi data. Dapat dimungkinkan adanya reduksi, sehingga dihasilkan representasi digital. Hasil ini akan diproses dengan ekstraktor ciri untuk menghasilkan suatu representasi yang ekspresif dalam bentuk template. Bergantung aplikasinya template dapat disimpan dalam database di sistem biometrik atau dapat direkam pada kartu magnetik (atau smartcard). Sedang pada fase pengenalan, karakteristik individu dibaca oleh pembaca biometrik (reader). Selanjutnya dikonversi dengan format digital, untuk diproses sebagai ekstraktor cirri (template). Hasil template ini selanjutnya dicocokkan dengan identifikasi individu. Lihat gambar 2.1.

Sistem biometrik belumlah sempurna, karena suatu saat masih dapat melakukan kesalahan dengan menerima impostor sebagai invidu yang juga valid (terjadi kesalahan pencocokan), sebaliknya terjadi penolakan terhadap individu yang valid (terjadi kesalahan ketidakcocokan). Untuk menjamin terhindarnya kesalahan seperti itu, sesuai referensi [34] memadukan ciri biometrik wajah dengan ucapan, serta dari referensi [35] memadukan biometrik wajah dengan ciri tanda-tangan. Selain itu dalam penerapannya ukuran database template sangatlah besar, bahkan dalam database perbankan pusat pernah terjadi bottleneck saat proses identifikasi [36]. Sistem biometrik yang ideal, diharapkan mempunyai

karakteristik sebagai berikut : pertama aspek universal, artinya ciri ini dapat berlaku secara umum (bahwa setiap manusia mempunyai karakteristik), kedua aspek unik (tidak ada dua manusia yang mempunyai karakteristik yang sama), ketiga haruslah bersifat permanen (karaktristik personal yang tidak berubah-ubah) dan terakhir dapat dihimpun (collectable), karakteristik ini mudah disajikan oleh sensor dan mudah dikuantisasikan dan dikuantifikasikan.



Gambar 2.1 Mekanisme Sistem Biometrik

Selain beberapa hal yang harus diperhatikan dari mekanisme ini adalah masalah kinerja (dalam mekanisme ini akurasi sistem, kecepatan, kehandalan) perlu mempertimbangkan adanya resource, faktor-faktor operasional dan pengembangan, dsb. Hal ini akan berpotensi sebagai kendala teknis. Selain itu adalah akseptabilitas (daya terima pengguna) akan mendorong keyakinan user terhadap akurasi dan kecepatan. Serta aspek circumvention yaitu aspek kemudahan sistem yang tidak bergantung alat, mekanisme operasional, dsb.

2.2 Sistem Proteksi Aplikasi

2.2.1 Dongle

Dongle merupakan sebuah alat berukuran kecil yang biasanya dihubungkan ke perangkat komputer dengan tujuan memberikan limitasi tertentu kepada sebuah aplikasi yang dijalankan di komputer tersebut. Sejarah dongle dapat dilacak sejak akhir periode 1970an, dimana pada saat itu untuk menghubungkan sebuh *device* dengan komputer masih menggunakan *port pararel*. Berbeda dengan kondisi saat ini yang sudah menggunakan *USB*. Bentuk dongle yang sekarang umum digunakan sangat mirip dengan *USB Flash Drive* yang sudah umum digunakan sebagai media penyimpanan data.

Gambar 2.2 Contoh dongle tahun ’70 yang menggunakan port pararel

Gambar 2.3 Contoh dongle yang sekarang umum digunakan

2.2.2 Build-in Unique Identity

Pada umumnya pada setiap alat-alat yang menjadi elemen dari sebuah komputer terdapat nomor identitas dari pabrik masing-masing alat tersebut. Nomor tersebut umumnya sudah dalam format tersendiri yang disusun identik untuk setiap alat di seluruh dunia. Beberapa contoh yang ada adalah :

- Serial Number Processor
- Serial Number Harddisk
- Serial Number Motherboard
- Network Interface

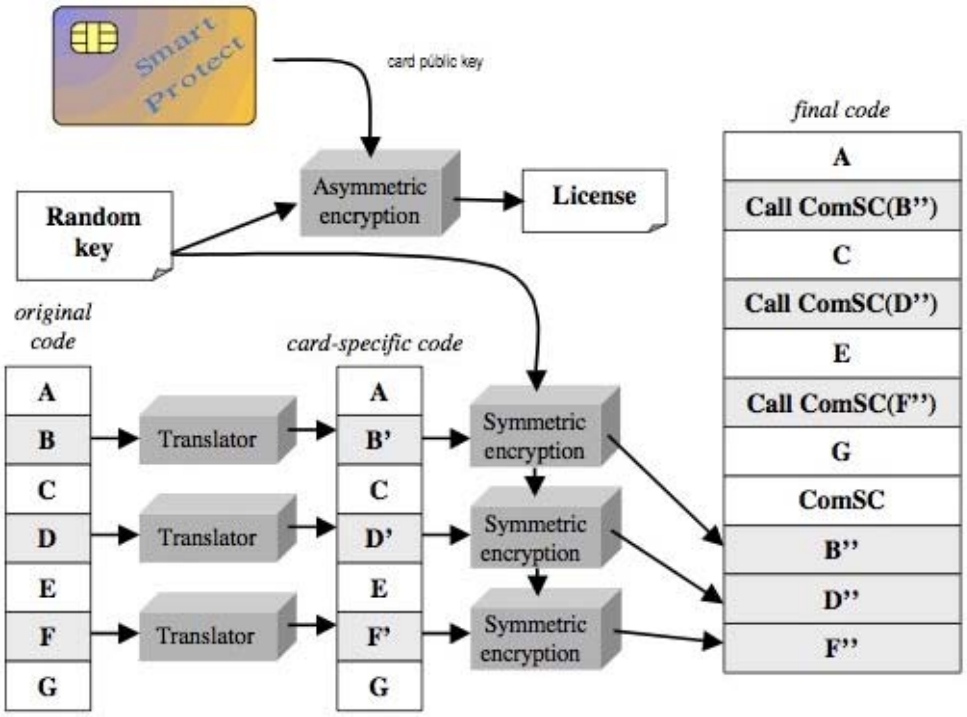
Sementara itu, *MAC Address* (*Media Access Control Address*) merupakan istilah yang digunakan untuk menyebut nomor serial dari *Network Interface*. Didesain dengan menggunakan 12 digit nomor hexadecimal, sebagai contoh : 00-21-5D-F4-85-16. Tanda pemisah setiap

2 digit merupakan tambahan dari *operating system* yang digunakan oleh komputer yang membaca nomor tersebut.

2.2.3 MCU Smartcard

MCU smartcard merupakan semua smart card yang berisi aplikasi/*function*. Kelebihannya jika terjadi pembajakan aplikasi, maka aplikasi yang dibajak tidak dapat digunakan sepenuhnya, hal ini dikarenakan ada modul/function yang tidak terdapat didalam aplikasi yang dibajak, melainkan ada didalam MCU smartcard.

MCU smart card ini mempunyai operating system dan memori sendiri. Programmer dapat memasukkan *source code*-nya kedalam MCU Smart Card ini yang nantinya akan di-*compile* dan dijalankan di dalam MCU Smart Card itu sendiri. Pada saat softwarenya dijalankan dan ingin menjalankan function tertentu, maka sistem akan memanggil *function* tersebut dari dalam dongle, dalam MCU Smart Card itu. Untuk membajak atau menduplikasikannya tidak mudah, karena program itu tidak lengkap tanpa coding yang ada di dalam MCU Smart Card yang mengakibatkan program tidak dapat dijalanlan. Saat ini, MCU Smart Card sudah banyak dijadikan standar untuk Credit Card di bank bank luar negeri dan mulai digunakan di beberapa bank di Indonesia.



Gambar 2.4 Proses *Code Transformation* menggunakan Smart Card

2.3 Mekanisme Proteksi

Saat ini ada beberapa mekanisme proteksi yang tersedia di pasar, diantaranya:

1. Secara software, penggunaan nomor seri aplikasi

    a. Online (Daring // Dalam Jaringan)

    - Sistem proteksi mempergunakan pengecekan nomor seri aplikasi secara online, meningkatkan pengamanan sistem dan jaminan selalu mendapatkan perbaharuan informasi/aplikasi;
    - Kelebihan: pembobolan terhadap mekanisma proteksi lebih susah, karena sistem mempergunakan pairing key

(*private key* dan *public key*) atau PGP (*pretty good privacy*);

- Kelemahan: sangat tergantung kepada koneksi internet, secara tidak langsung membatasi perkembangan pangsa pasar, karena hanya dapat dipergunakan pada wilayah yang telah memiliki koneksi internet.

b. Offline (Laring // Luar Jaringan)

- Sistem verifikasi serial number dilakukan oleh aplikasi dan dan disimpan pada computer yang telah terinstalah aplikasi;
- Kelebihan: tidak butuh koneksi internet, verifikasi cepat, penjualan alat bisa sebanyak mungkin;
- Kelemahan algoritma pengecekan serial number ada didalam aplikasi, sehingga mengakibatkan kemungkinan untuk terjadinya pembajakan terhadap aplikasi lebih besar.

2. Secara hardware, penggunaan alat tambahan seperti *dongle*

- Proteksi mempergunakan dongle, adalah dengan menambahkan sebuah alat yang memiliki identitas unik yang dihubungkan secara lansgung dengan perangkat yang akan dijual, penggunaan *dongle* bisa pada 2 bagian, 1 pada mesin biometric dan/atau pada komputer yang menjalankan aplikasi;
- Kelebihan: tidak membutuhkan koneksi internet, verifikasi cepat, sistem proteksi sulit untuk dibobol;

- Kekurangan: akan ada biaya tambahan seperti pembelian *dongle*, perawatan dongle, *team support* untuk dongle, distribusi dan pergantian dongle.

2.4 Sistem Verifikasi

Mesin biometrik pada saat ini seluruhnya memiliki Network Interface sebagai media untuk menerima dan mengirim data ke komputer server dan pengguna mesin baik berupa kabel maupun non-kabel (*wireless*). Sehingga menggunakan Mac Address dalam sistem untuk menentukan apakah sebuah alat diperoleh secara resmi ataupun tidak merupakan pilihan yang tepat.

2.4.1 Komunikasi Data

Komunikasi data antara mesin sidik jari dan komputer server memiliki beberapa hal yang harus kita perhatikan, antara lain :

Protokol

Protokol merupakan format data tertentu untuk mengirim dan menerima data antara 2 buah Network Interface, atau pada umumnya disebut *bahasa* Network Interface. Seperti manusia yang setiap suku nya memiliki bahasa sendiri, Network Interface pun demikian, setiap alat yang digunakan menggunakan bahasa yang telah ditentukan oleh Operating System yang diinstall. Sebagai contoh :

- TCP / IP
- Apple Talk
- NETBUI

- BITTORRENT
- IBM Data Link Control

Packet data

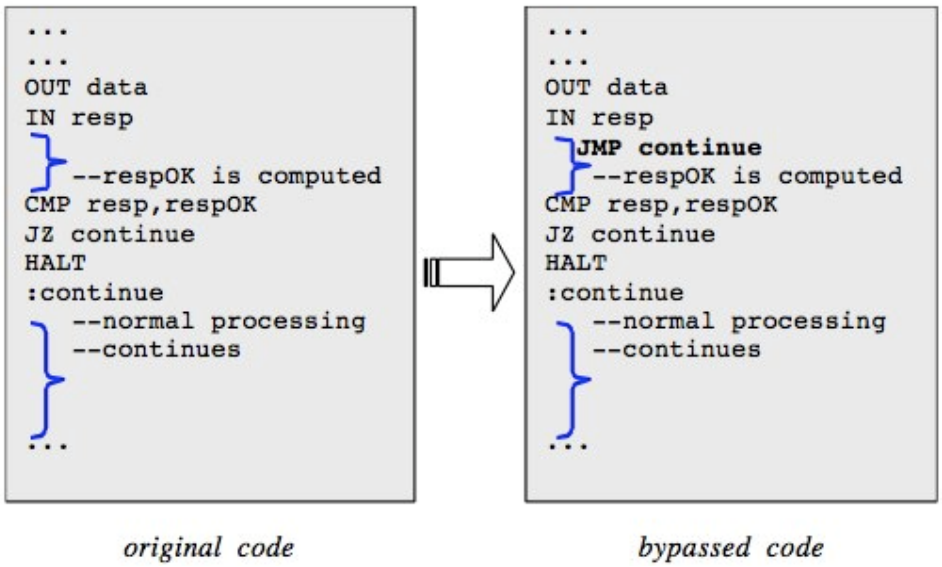
Setiap kata yang disebutkan oleh manusia memiliki arti sendiri, tapi apabila kata-kata tersebut dirangkai menjadi sebuah kalimat maka makna dari kata tersebut terkadang menjadi berubah / lebih luas. Demikian pula dengan Network Interface, setiap data yang dikirim oleh Network Interface memiliki arti. Tapi data tersebut akan lebih bermanfaat / memiliki arti lebih ketika dikirim dalam bentuk sebuah packet data.

2.5 Kompresi

Untuk mencegah adanya pihak lain menangkap data yang dikirim oleh Network Interface, pada umumnya sebelum data tersebut dikirim terdapat proses kompresi data yang membuat data tidak dapat dibaca tanpa menggunakan metode untuk de-kompresi data tersebut (Encyclopedia of Biometrics,2009, section B,22).

Kompresi juga dapat dipergunakan dalam sistem proteksi aplikasi untuk mempersulit cracker dalam melakukan *reverse engginering*. Cara kerjanya adalah sebagai berikut ini, aplikasi yang ada dibangun mempergunakan bahasa pemrograman tingkat tinggi, yang selanjutnya di *compile* menjadi bahasa mesin *(file executable*), setelah proses *compile* selesai, maka hasil compile tersebut akan di kompres mempergunakan aplikasi khusus, ketika akan aplikasi akan di ekseskusi, maka aplikasi akan melakukan proses dekompresi (extract) pada memory komputer dan kemudian menjalankannya. File *executable* yang telah

dikompres inilah yang menyebabkan para *cracker* kesulitan untuk melakukan proses reverse engginering karena file executable yang telah di kompress hanya bisa di decompress (extract) melalui apliksi executable itu sendiri. Proses *reverse engginering* dipergunakan oleh cracker untuk mengetahui letak kode verifikasi yang berfungsi untuk validasi aplikasi, begitu posisi code telah diketahui maka cracker dengan mudah dapat membuat *patch* untuk mem bypass fungsi pengecekan.



Gambar 2.5 *reverse engginering* untuk melewati sistem pengecekan

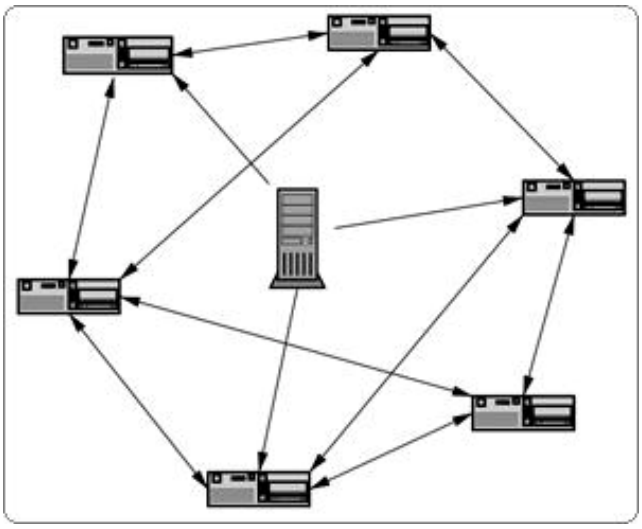
2.6 Sistem Pembaharuan Aplikasi

Semakin berkembangnya bisnis proses, mekanisme, cara kerja dan jumlah user, diperlukan sebuah sistem pembaruan terhadap sistem aplikasi jika terdapat update atau perbaikan aplikasi. sistem pembaharuan aplikasi ini harus bisa berfungsi secara mandiri tanpa interaksi user dalam penyebarannya. Beberapa

sistem yang mungkin dapat diterapkan dalam sistem pembaharuan aplikasi adalah

Peer 2 Peer

P2P banyak dipergunakan untuk share file terbuka di internet aplikasi p2p seperti kazaa, napser atau gnutella , konsep peer to peer ini dapat dipergunakan dalam sistem pembaharuan aplikasi dengan modifikasi agar sistem peer to peer yang dibangun menjadi closed circuit (hanya berfungsi dengan sistem yang kita kembangkan).

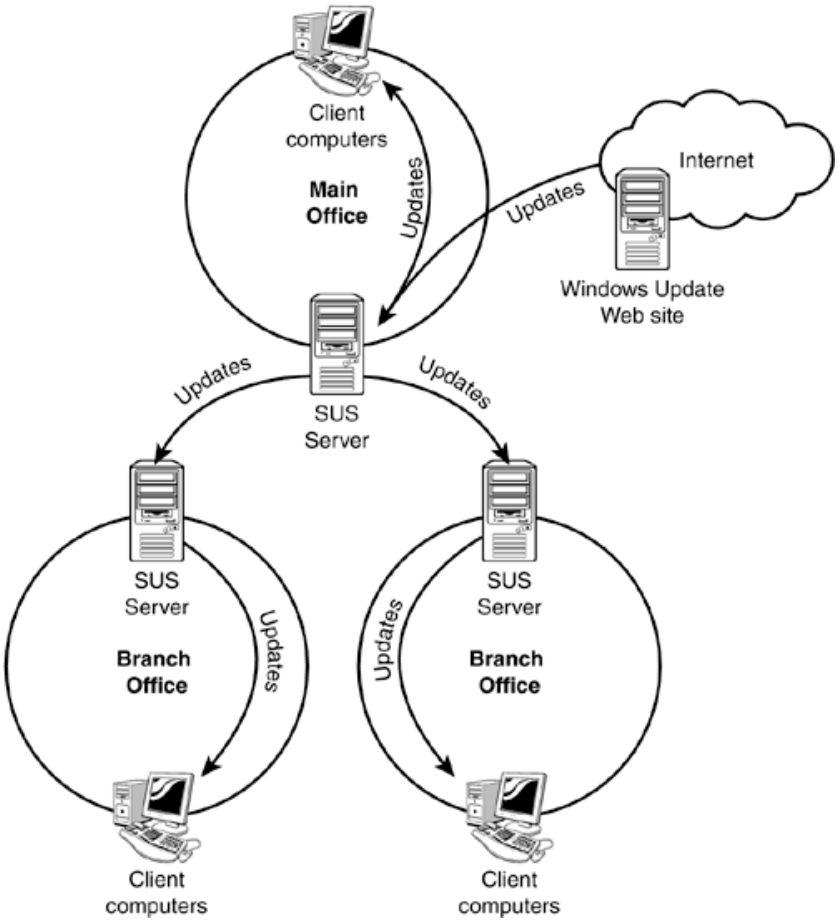


Gambar 2.6 Cara kerja torrent

Sistem P2P mempergunakan konsep desentralisasi jaringan dimana aplikasi (paket aplikasi) tersebar dijaringan internet tanpa adanya server pusat yang menyediakan. keuntungan dalam penggunaan sistem P2P adalah, kita tidak perlu menyediakan kapasitas penyimpanan dan bandwith yang besar untuk menangani update request dari user-user yang ada.

Distributed Update Server

Distributed Update Server merupakan konsep sharing file dengan menggunakan beberapa server yang diletakkan pada lokasi yang berbeda, setiap request yg dilakukan terhadap server akan dialihkan ke server yang pada saat itu sedang *idle* dan memiliki lokasi terdekat dengan user.

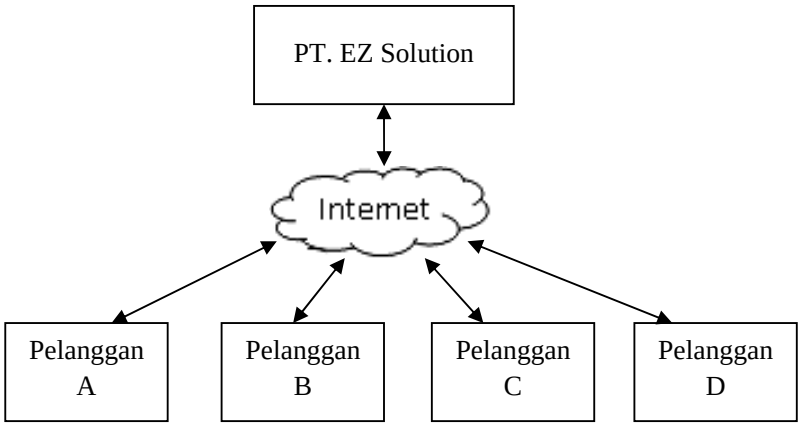


Gambar 2.7 cara kerja ***Distributed Update Server***

Centralized Update Server

Konsep ini mirip dengan Distributed Update Server, hanya saja disini hanya digunakan 1 lokasi server. Karena hanya 1 lokasi ketika diperlukan maintenance

akan jauh lebih mudah, Kelemahan nya adalah diperlukan spesifikasi server yang tinggi dan bandwith yang besar untuk melayani banyak customer & tidak memiliki backup.



Gambar 2.8 cara kerja ***Centralized Update Server***

2.7 Sistem Aplikasi Komputer

Aplikasi komputer atau biasa disebut dengan perangkat lunak merupakan suatu program komputer yang berfungsi untuk melakukan tugas tugas khusus seperti; membuat dokumen, memanipulasi foto, membuat laporan keuangan, mencatat transaksi. Berikut ini contoh beberapa Sistem aplikasi komputer dibagi berdasarkan jenisnya

a. Aplikasi hiburan, seperti: winamp, powerdvd

b. Aplikasi Pendidikan

c. Aplikasi Bisnis

d. Aplikasi Khusus

e. Aplikasi Produktivitas

2.8 Aplikasi mesin biometrik

Dalam aplikasinya, mesin biometrik selain pada absensi karyawan, dapat juga dipergunakan pada;

- Autentikasi terhadap perangkat elektronik seperti, komputer dan telepon untuk menggantikan atau sebagai pelengkap *password*
- Pengamanan terhadap lokasi lokasi tertentu yang hanya dapat dimasuki oleh orang yang tertentu melalui system access control doorlock
- Surviliance camera yang di lengkapi dengan system biometric pengenal wajah yang dapat membantu pihak yang membutuhkan dalam mencari atau mendeteksi orang yang di cari.

2.9 Perbandingan dengan penelitian yang telah ada

Peneliti	Tahun	Topik Penelitian			
		Biometrics	MAC Address	Security	network
Chandra and Calderon	2003	√			
Liu & Silverman	2004	√			
Sarwoko	2006	√			
Alan MacCormack	2003			√	
Antonio Maña, Ernesto Pimentel	2000			√	
Liu, Simon & Silverman, Mark	2005	√		√	
Fanglu Guo and Tzi-cker Chiueh	2006		√		√

Tabel 2.1 perbandingan dengan penelitian yang telah ada

Peneliti melakukan penelitian ini untuk melakukan sistem identifikasi mesin biometric dengan penerapan MAC Address. Berdasarkan tabel diatas, kami menyimpulkan bahwa penelitian ini belum pernah dilakukan sebelumnya.