Journal of Information System, Informatics and Computing

Vol.1 No.1 Agustus 2017
ISSN : 2597-3673 (Online)
ISSN : 2579-5201 (Printed)

JISICOM (Journal of Information System, Informatics and Computing)

PENGEMBANGAN TEKNOLOGI INFORMASI BERBASIS ACCESS ID CARD

Ifan Junaedi
Program Studi, Sistem Informasi ,STMIK JAYAKARTA Jakarta Indonesia
Jl. Salemba I No. 10-12A Jakarta 10430 Indonesia
Email: ifn1809jn@yahoo.co.id

ABSTRACT

Development information technology base on this Id-Card access very good for , Education , Institution And society in general that is this Id-Card very assisting in course of data proteksi and custody, because by wearing this Id-Card consecutively process administration at Institution, Education Or society . Where data considerably awake because not all user can use the the Id-Card except rightful claimant and is authoritative.

Keywords : Acces Id Card

Pengembangan teknologi informasi berbasis access Id-Card ini sangat berguna bagi , Pendidikan , Instansi dan masyarakat pada umumnya yaitu Id-Card ini sangat membantu dalam proses penjagaan dan proteksi data, karena dengan memakai Id-Card ini dapat dengan teratur proses administrasi pada Instansi, Pendidikan atau masyarakat . Dimana data dengan sangat terjaga karena tidak semua pemakai dapat menggunakan Id-Card tersebut kecuali yang berhak dan berwenang .

Kata kunci : *Acces Id Card*

Journal of Information System, Informatics and Computing
Vol.1 No.1 Agustus 2017
ISSN : 2597-3673 (Online)
ISSN : 2579-5201 (Printed)
JISICOM (Journal of Information System, Informatics and Computing)

1. PENDAHULUAN

Sebuah organisasi adalah kumpulan orang-orang yang bersinergi satu dengan yang lainnya dengan tujuan pencapaian sebuah visi dan misi yang telah diatur dan disepakati bersama.

Di Era globalisasi, persaingan yang dirasakan oleh organisasi-organisasi (perusahaan) terasa semakin ketat, baik menyangkut produk (barang dan jasa) maupun harga dan pasar yang semakin beragam, persaingan yang memerlukan modal yang tidak sedikit dan kemampuan untuk mengendalikannya.

Tidak terkecuali Di dunia pendidikan yang semakin terasa persaingannya, yang tidak hanya menyangkut kualitas pengajaran tetapi juga dituntut dengan berbagai fasilitas yang bertujuan agar komunitas kampus semakin merasa nyaman, aman, serta fasilitas yang memudahkan dan mempercepat proses, baik pengajaran maupun administrasi sehingga tercapainya efisiensi dan efektifitas waktu. Hal-hal tersebut menjadi kunci utama suksesnya dunia pendidikan yang bertujuan tercapainya kecerdasan bangsa seperti yang diamanatkan UUD ’45.

Agar tercapainya tujuan tersebut diperlukan sebuah system yang tepat dan pengaturan/pengendalian yang benar, dalam hal ini pengaturan akses terhadap peralatan atau tempat-tempat tertentu.

Pengaturan akses terhadap peralatan dan tempat-tempat tertentu semakin mendapat perhatian yang serius, baik perusahaan kecil, perusahaan multinasional maupun lembaga-lembaga pemerintahan dalam semua tingkatan tidak terkecuali dunia pendidikan dalam hal ini kampus.

Pengaturan orang-orang dan kewenangannya dalam sebuah organisasi biasanya dilakukan berdasarkan penggunaan kartu identitas seperti Surat Ijin Mengemudi (SIM), Kartu Perpustakaan, Kartu Kredit, kartu anggota atau kartu identitas pegawai. Kartu-kartu tersebut harus ditunjukkan kepada seseorang (seperti penjaga/security) atau digesekkan/didekatkan pada suatu alat pembaca yang menunjukkan dan memastikan bahwa pemegang kartu memiliki hak dan kewenangan tertentu. Dalam rangka pemenuhan peningkatan keamanan, industri mengembangkan teknologi (seperti pita magnetic, bar codes dan semacam chips) yang dapat dimasukkan dalam kartu. Kemudian kartu tersebut dapat digesekkan pada mesin pembaca pita magnetic, di scan melalui mesin pembaca barcode atau ditunjukkan melalui pembaca elektronik yang menggunakan radio frekuensi (RF) untuk otorisasi akses secara otomatis. Sebuah Personal Identification Number (PIN) dapat dimasukkan melalui keypad untuk menambah factor otentifikasi untuk memastikan bahwa pemegang kartu adalah benar-benar pemilik dari kartu

tersebut, teknologi ini diharapkan dapat mengurangi ongkos dan meningkatkan kenyamanan, meskipun masih ada titik lemah dari cara ini yaitu jika pemegang kartu adalah bukan pemilik kartu tersebut.

Perubahan dalam lingkungan kampus mengakibatkan meningkatnya masalah dalam identifikasi dan otentifikasi orang-orang yang berada dalam areal kampus. Perubahan pada sector pendidikan ini terasa cukup tinggi sehingga diperlukan sebuah system yang mampu mengidentifikasi perubahan yang terjadi secara simultan terutama terhadap asset dan informasi yang dimiliki oleh kampus. Peningkatan ukuran dan komplektisitas pada komunitas kampus dapat menyebabkan pengaksesan terhadap asset dan informasi kampus oleh orang-orang yang tidak berhak.

Langkah yang harus ditempuh untuk mengatasi hal tersebut adalah, pengenalan sebuah sistem identifikasi dalam mengakses asset atau informasi organisasi dalam hal ini kampus dan komunitasnya menggunakan suatu kartu identitas atau peralatan lain yang dapat dipercaya yang mengandung sistem intelligence yang terintegrasi.

Sebagai suatu alat yang diandalkan kartu tersebut harus mendukung beberapa aplikasi pengamanan untuk pemrosesan identitas pribadi, kewenangan dan hak akses dan termasuk perlindungan terhadap sistem cryptograpi dari informasi yang ada.

Diperlukannya suatu kartu yang dapat diandalkan didasari pada model pengaksesan yang baru yang memerlukan pemrosesan yang cepat, otentifikasi jati diri, minimalisasi resiko kesalahan. Model ini ditunjukkan dalam suatu blueprint untuk sistem identifikasi personal yang aman yang dapat memecahkan masalah mendasar dalam pengaturan pengaksesan yaitu bagaimana untuk mengetahui secara akurat dan tepat keterkaitan seseorang dengan hak dan kewenangan dalam suatu lingkungan dimana keputusan untuk pengaksesan harus dibuat, seperti sebuah kartu identitas yang “smart” atau cerdas yang dapat terdiri dari suatu pita magnetic, pita akses pintu gerbang, barcode, peralatan radio frekuensi, smart card chip dan teknologi pengamanan lainnya.

2. PERUMUSAN MASALAH

Rumusan Masalah adalah untuk mengetahui bagaimana cara kerja Pengembangan Teknologi Informasi berbasis Access ID-CARD dengan dunia nyata yaitu Pendidikan, Perusahaan serta masyarakat.

3. LINGKUP EKSPERIMEN

Berdasarkan pokok permasalahan yang telah dirumuskan maka ada beberapa

tujuan yang ingin dicapai diantaranya adalah

a. Untuk mengetahui secara akurat sikap dan respon masyarakat terhadap Pengembangan Teknologi Berbasis Acces Id Card
b. Untuk Mengimplemetasikan Pengembangan Teknologi Berbasis Acces Id Card dan mekanisme-mekanismenya kepada masyarakat
c. Untuk mempelajari dan memahami Pengembangan Teknologi Berbasis Acces Id Card secara umum dan mekanisme-mekanisme tambahan yang bisa diimplementasikan didalamnya.

Kegunaan yang dapat diambil diantaranya:

a. Untuk memberikan gambaran dan pengetahuan yang kongkrit kepada masyarakat tentang Pengembangan Teknologi Berbasis Acces Id Card
b. Sumbangan kepada institusi Pemerintahan, swasta maupun kampus-kampus untuk pembangunan Pengembangan Teknologi Berbasis Acces Id Card

4. KAJIAN PUSTAKA

4.1 Deskripsi Teoritis

Card atau ID-Raed merupakan alat bantu elektronik yang mampu melakukan pemprosesan data dan mampu menerima input , memproses data menumimpan data dengan perintah-perintah dari hasil pengolahan san menyediakan output berupa informasi yang dibutuhkan oleh pemakai dengan sistem pengamanan data secara fisik diharapkan dapat mengambil satu data dan menghasilkan data yang dibutuhkan secara akurat serta data tersebut tidak mungkin akan ditampilkan jika bukan pemiliknya yang akan memproses data tersebut.

5. PEMBAHASAN

Pertimbangan Keamanan. Untuk mengurangi resiko akibat akses yang dilakukan oleh orang-orang yang tidak berhak atau membebaskan diri dari ancaman, sistem yang mengendalikan akses masuk kedalam perusahaan harus menjadi pertimbangan yang serius. Perancangan sistem keamanan ini dimulai dengan pembuatan kartu termasuk komponen yang harus ada dalam sistem tersebut seperti jaringan, database, software, hardware, kamera, mesin pembaca dan kartu itu sendiri, pemrosesan sistem seperti prosedur penjagaan dan proteksi data yang berada dalam sistem serta selama proses transmisi.

Perancang sistem akan mempertimbangkan tingkat pengamanan

yang bagaimana yang harus diimplementasikan berdasarkan lingkungan yang ada disekitar sistem dan perkiraan akan adanya ancaman serangan terhadap system ;

5.1 Keamanan dari Kartu

Kartu berjenis smart card dapat digunakan untuk menghindakan dari pemalsuan kartu, penggunaan kartu diluar kewenangannya dan menghindarkan pemakaian kartu dari oaring yang tidak berhak. Smart card memiliki berbagai macam kemampuan yang berupa software dan hardware yang dapat mendeteksi dan bereaksi terhadap kemungkinan pemalsuan dan dapat mengkounter serangan yang mungkin dilakukan, didalam smart card terdapat sensor-sensor terhadap voltase, frekuensi, cahaya dan temperatur; filter yang memakai sistem clock; pengacakam memori, catu daya yang konstan dan perancangan chip yang bagus untuk menghindari analisa secara visual, micro probing atau manipulasi chip. Jika smart card akan digunakan untuk melakukan verivikasi identitas secara manual, dapat ditambahkan kemampuan pengamanannya pada smart card tersebut, seperti jenis huruf yang khas, warna tinta dan penggunaan warna yang beragam, micro pinting sistem, tinta ultra violet yang berkualitas tinggi dan gambah yang tersamarkan yang merupakan foto kedua dari pemegang yang dapat diletakkan pada tempat lain dalam kartu dan hologram yang berlapis-lapis dan dapat juga menggunakan gambar tiga dimensi.

Jika kartu dirancang dan diimplementasikan dengan tepat, smart card hampir tidak mungkin di aplikasikan atau dipalsukan, dan data yang tersimpan didalam chip tidak akan dapat dimodifikasi tanpa otorisasi yang jelas biasanya menggunakan password, otentifikasi biometric, atau kunci akses menggunakan cryptograpi.

Selama sistem yang diimplementasikan memiliki kebijakan keamanan yang efektif dan diikuti dengan layanan keamanan yang penting yang disediakan oleh smart card, organisasi dan pemegang kartu dapat memiliki tingkat kepercayaan yang tinggi dalam hal integritas kartu identitasnya dan keamanan dalam penggunaannya.

5.2 Proteksi Data

Satu hal yang menjadi alasan utama menggunakan smart card sistem sebagai sistem pengendali akses fisik kemampuan untuk menggunakan pengacakan data atau teknik cryptography untuk melindungi informasi yang ada dalam chip atau pada saat transmisi data. Informasi yang aman dan dapat dipercaya sangat diperlukan untuk melakukan identifikasi seseorang dan hak serta kewenangannya sebagai

kunci sukses dalam sistem pengendalian akses fisik.

Smartcard dapat mengggunakan symmetric cryptography algoritm seperti DES, Triple DES, IDEA, AES dan MIFARE , yang menjamin perlindungan mendasar dan waktu pemrosesan yang sempurna. Symmetric key cryptography merupakan sistem cryptography yang digunakan secara luas dalam pengendalian akses fisik dan penggunaan kunci yang sama untuk enkripsi dan deskripsinya membuat sistem ini menjadi sangat cepat dan dapat dipercaya. Jika pengendalian akses ini termasuk pengendalian logical akses dan kewenangan PKI dan jika waktu pemrosesan bukanlah sebagai hal yang diutamakan asymetric cryptographic algoritm seperti RSA, ECC dan DSA dapat digunakan.

Kunci yang bermacam-macam dapat disimpan dalam satu chip untuk meningkatkan persyaratan keamanan dengan menggunakan aplikasi yang beragam, jadi smart card mampu menyediakan pengamanan yang lebih baik untuk peningkatan kompleksitas sistem.

5.3 Otentifikasi Kartu dan Data

Sistem pengendalian akses fisik yang aman harus dapat menjamin bahwa data yang di tertera dalam kartu identitas dan isi dari kartu identitas tersebut sama. Dalam beberapa kasus, sangatlah penting untuk melakukan verivikasi bahwa mesin pembaca kartu juga otentik untuk menjamin bahwa tidak ada terminal yang palsu yang digunakan untuk proses ekstraksi data.

Pemisahan dari penggunaan PIN dan atau sistem biometric yang tidak mengunci kartu atau otentifikasi orang tersebut, smart card memiliki kemampuan yang unik dengan menawarkan keunggulan otentifikasi berbasis internal chip yang memanfaatkan symmetric atau asymetryc cryptographic mechanism yang menawarkan solusi yang dapat dipercaya untuk pembuktian keaslian kartu dan datanya. Untuk keamanan otentifikasi kartu smart card dapat secara unik menggunakan teknik cryptography yang aktif untuk merespon mesin pembaca kartu dan membuktikan bahwa pemrosesan kartu bersifat rahasia dan otentifikasi kartu tersebut valid.

5.4 Komunikasi Antara Kartu dan Mesin Pembaca Kartu

Karena seluruh proses melibatkan sinyal elektronik, data yang ditransmisikan diantara seluruh peralatan dapat dimonitor. Kemungkinan ini harus menjadi pertimbangan yang serius dalam perancangan sistem keamanan, sebagai contoh dalam suatu area seseorang dapat melakukan pengawasan secara tidak sah atau seseorang dapat memasukkan peralatan lain atau menempatkan peralatan

untuk memonitor komunikais diantara jangkauan sinyal komunikasi, serta bentuk-bentuk penyerangan lainnya.

Tergantung dari lingkungan dan profil resiko, suatu organisasi mungkin sangat konsern terhadap proses pengiriman data dari contact atau contactless card ke mesin pembaca kartu yang dapat dimonitor, sehingga menyebabkan kemungkinan masuknya seseorang secara illegal jika ada kartu atau peralatan yang dapat menyadap dan menduplikasikan data. Smart card mendukung standard enkripsi yang diperlukan industri dan teknik pengamanan yang menjamin keamanan komunikasi antara kartu dan mesinpem bacanya dan memungkinkan kartu dan mesin pembaca kartu saling melakukan proses otentifikasi satu sama lainnya. Enkripsi dan otentifikasi merupakan kunci utama sistem pengamanan yang menjaga keamanan dari kartu dan mesin pembaca kartu dan hal ini sangat sulit untuk diserang.

Dalam suatu lokasi akses poin yang tidak diawasi atau tidak memiliki sistem pengamanan secara fisik, organisasi harus menyadari bahwa ada kemungkina seseorang yang tidak diharapkan dapat mengambil satu mesin pembaca dari tempat mesin tersebut diletakkan dan membaca aliran data yang dikirimkan ke kontrol panel atau menempatkan sebuah personal komputer atau peralatan lainnya didalam lokasi tersebut dan merekam pemasukan data dari kartu untuk memperoleh otorisasi.

Hampir seluruh mesin pembaca mengirimkan data ke kontrol panel menggunakan satu atau dua bentuk yaitu wiegabt atau pita magnetic. Format wiegand menggunakan dua signal D0 untuk mentransmisikan pulsa “zero” dan D1 untuk mentransmisikan data pula “satu”. Format pita magnetic juga menggunakan dua bentuk signal, satu untuk data dan satu lagi untuk clok. Bentuk data ini kurang aman.*Physical Access Control System Berbasis Smart-card*

Suatu sistem pengaturan terhadap akses secara fisik yang baik adalah suatu jaringan yang terkoordinir antara kartu identitas, mesin pembaca elektronis, databases khusus, software dan jaringan komputer yang digunakan untuk memonitor dan mengontrol “lalu lintas” melalui akses poin.

Kartu identitas diberikan kepada setiap pegawai, yang berisi tentang informasi tentang diri dan keterangan tentang kemungkinan penggunaan kartu tersebut secara tidak sah dan identitas yang menunjukkan hak-hak pemegang kartu identitas tersebut, yang semuanya dalam keadaan tercetak. Disetiap kartu disertai foto pemegang kartu tersebut. Setiap kartu berisi informasi rahasia

tentang pemilik kartu tersebut dan kewenangan yang dimilikinya.

Jika seseorang terlibat dalam kelembagaan tersebut dia akan menerima kartu identitas yang berarti kewenangan yang telah tertulis secara akurat dan aman serta telah disosialisasikan melalui sistem (jika beberapa kewenangannya berubah, informasi yang baru tersebut dapat segera di ubah secara aman melalui jaringan tersebut). Ketika kartu tersebut diletakkan didalam atau dekat dengan pembaca elektronis, ada dua kemungkinan terhadap pemegang kartu tersebut yaitu, kewenangan akses yang ditunjukkan secara akurat dan aman atau penolakan terhadap akses untuk tempat-tempat tertentu (sebuah areal parkir, bangunan tertentu, kantor atau jaringan komputer tertentu). Ketika orang tersebut keluar dari areal kewenangan, maka semua kewenangan aksesnya akan dihapus. Segala usaha yang dilakukan oleh orang yang sudah keluar tersebut dimasa yang akan datang untuk memasuki asset kelembagaan menggunakan kartu yang sudah kadaluwarsa atau sudah dihapus akan ditolak dan dicatat secara otomatis.

5.5 Sistem Pengendalian Akses Fisik

Bagi pengguna, suatu sistem pengendalian akses terdiri dari tiga alemen yaitu :

1. Sebuah kartu atau tanda (identitas yang valid) yang ditunjukkan pada mesin pembaca di pintu.
2. Sebuah mesin pembaca di pintu masuk, yang akan menunjukkan bahwa kartu tersebut valid dan pemegangnya berwenang memasuki areal tersebut.
3. Sebuah pintu atau gerbang yang secara otomatis akan terbuka ketika akses tersebut diijinkan (valid)

Dibalik semua itu terdapat suatu jaringan yang kompleks yang terdiri dari data, komputer-komputer, dan software yang mendukung proses pengamanan.

5.6 Proses Access Control

Proses pengontrolan akses dimulai ketika seorang pengguna menunjukkan kartu identitasnya (biasanya berupa kartu pegawai yang berupa smart card, badge atau kartu identitas) ke mesin pembaca, yang biasanya terletak sebelum pintu masuk. Mesin pembaca akan melakukan ekstraksi data dari kartu, memprosesnya dan mengirimkan ke kontrol panel.

Mula-mula kontrol panel akan melakukan validasi untuk mesin pembaca kartu tersebut kemudian baru menerima data yang dikirimkan oleh mesin pembaca kartu.

Kontrol panel akan meneruskan data kepada server pengendali akses. Server pengendali akses akan membandingkan data yang diterima dari kartu dengan informasi tentang pengguna kartu yang tersimpan dalam database. Software pengendali akses akan membaca dan menunjukkan kewenangan akses dan

melakukan otorisasi bagi pengguna kartu, waktu, tanggal pintu masuk yang digunakan dan informasi lainnya yang diperlukan oleh kepegawaian atau bagian yang berhak untuk menjamin keamanan. Jika pengguna kartu ternyata memiliki akses, maka server pengendali akses akan memberikan tanda kepada kontrol panel untuk membuka pintu. Kontrol panel kemudian mengirimkan dua sinyal, satu untuk pintu yang harus dibuka dan yang satunya kepada pintu pembaca kartu yang berupa sinyal atau suara yang menandakan pengguna kartu tersebut boleh masuk.

Atau dapat dibuat kontrol panel adalah pengambil keputusan apakah pemegang kartu tersebut diperbolehkan masuk atau tidak. Secara periodic server pengendali akses menyediakan data kepada kontrol panel untuk dapat digunakan oleh software yang berada di kontrol panel mangambil keputusan apakah pengguna tersebut diijinkan untuk mengakses tempat tersebut. Kemudian kontrol panel melakukan seluruh tugas yang dilakukan oleh server seperti tersebut diatas (membuka pintu dan memberi sinyal/tanda). Keuntungan dari sistem terdistribusi ini adalah berkurangnya waktu untuk komunikasi antara kontrol panel dan server pengendali serta pusat data, sehingga performa dari sistem meningkat.

Dalam sistem tersebut dapat disertakan security biometric atau PIN dalam sistem tersebut, mesin pembaca biasanya melakukan autentifikasi terhadap data ini. Validasi dapat dilakukan oleh mesin pembaca atau didalam kartu identitas tersebut dengan membandingkan data dengan template biometric atau PIN yang tersimpan dalam kartu(data biometric akan dikirimkan ke kontrol panel untuk dilakukan pemrosesan). Jika informasi tambahan tadi valid, maka mesin pembaca mengirimkan nomer kartu identitas tersebut kepada kontrol panel, tetapi jika identifikasi tadi tidak valid, kemudian mesin pembaca kartu juga mengidentifikasikannya, maka akses tersebut akan ditolak.

Respon untuk kartu yang invalid harus didefinisikan terlebih dahulu dalam kebijakan dan prosedur pengamanan kelembagaan. Server pengendali dapat mengabaikan data dan tidak mengirimkan kode pembukaan pintu kepada kontroler atau pintu yang tertutup.

Hal ini dapat dilakukan dengan mengirimkan tanda kepada mesin pembaca untuk mengeluarkan suara yang berbeda, sebagai suatu tanda bahwa akses tersebut tidak dibenarkan. Hal ini juga dapat dilakukan dengan peralatan security tambahan seperti closet circuit TV dan alarm, yang dapat mengindikasikan bahwa kartu yang tidak sah sedang dicoba digunakan untuk membuka sistem

6. PERUMUSAN HIPOTESA EKSPERIMEN

Dari masalah-masalah dan kajian-kajian serta kerangka berfikir yang telah diuraikan dengan kemampuan proses data dengan bantuan Card yang akan digunakan oleh berbagai kalangan masyarakat maka dirumuskan sebagai berikut :

6.1 Hipotesis Pertama

Secara keseluruhan dari perumusan yang didapat tentang bagaimana identitas seseorang dapat diakses dengan menggunakan Card yaitu ID CARD yang sangat berguna sekali

6.2 Hipotesis Kedua

Terdapat interaksi antara proses data dengan media Card dan sebagai alat bantu yang dapat diandalkan.

7. KESIMPULAN

Dari hasil pembahasan dalam makalah yang berjudul ***PENGEMBANGAN TEKNOLOGI INFORMASI BERBASIS ACCES ID CARD*** dapat disimpulan bahwa id card atau smart card adalah sebuah kartu yang memiliki sistem pengendali akses fisik yang berkemampuan untuk menggunakan pengacakan data atau teknik cryptography untuk melindungi informasi yang ada dalam chip atau pada saat transmisi data. Contoh smart card adalah SIM, kartu perpustakaan, ATM dan kartu pegawai. Informasi yang aman dan dapat dipercaya sangat diperlukan untuk dapat melakukan identifikasi seseorang dan hak serta kewenangannya sebagai kunci sukses dalam system penendalian akses fisik.

8. SARAN – SARAN

Kami menyadari bahwa dalam penulisan makalah yang berjudul **PENGEMBANGAN TEKNOLOGI INFORMASI BERBASIS ACCES ID CARD** jauh dari sempurna oleh karena itu, kami sangat mengharapkan kritik dan saran dari semua pihak agar makalah ini dapat berguna dimasa yang akan datang.

Bagi kalangan masyarakat yang belum menerapkan sistem Card ini sebaiknya secepatnya menerapakan sistem teknologi Access ID Card karena banyak sekali kegunaannya diantaranya adalah proses data terjamin aman, tidak perlu harus memakan waktu yang lama karena dengan menempelkan Card tersebut dengan sebuah alat pembaca data maka proses akan dengan cepat dihasilkan.

Akhir kata kami berharap semoga penulisan makalah ini dapat menambah pengetahuan dalam bidang teknologi informasi dengan alat Bantu media Card.

REFERENSI

[1] Frans.K (1996) "***Privacy and Secure Identification System : The Role of Smart Card as a Privacy-Enabling Technology"***,New York

[2]Jemmy,Eric.P, (2002). "***Contactless Technology for Secure Physycal Access : Technologi and Standard Choices***", Jakarta

[3] Johan,et al , (2002). "***Contactless Smart Card Technology for Physical Access Control"***, Jakarat

[4] Jemmy. (2003) ***Using Smart cart for Secure Physical Access***", a Smart Card Alliance White Paper, Jakarta