**Penerapan Fitur Kamera CCTV Untuk *Access Control System* (ACS) Menggunakan System Onguard 2013**

**(Studi Kasus: PT. Chevron Pasific Indonesia)**

**Sutoyo 1, Triyono2 , Saepudin3**

Dosen Jurusan Teknik Elektro UIN SUSKA RIAU**1**

Mahasiswa Jurusan Teknik Elektro UIN SUSKA RIAU**2**

PT Chevron Pasific Indonesia**3**

Jl HR Soebrantas KM 15 Panam Pekanbaru

e-mail : sutoyo@uin-suska.ac.id

***Abstrak***

*Access Control System* (ACS) merupakan suatu perangkat kontrol yang terpasang pada pintu ruangan berguna untuk membatasi akses pengunjung dalam memasuki ruangan. Ada banyak *Access* ACS yang digunakan untuk mendukung system keamanan, salah satunya adalah OnGuard 2013. Akan tetapi dengan system ini masih banyak ditemukan para pengguna yang memasuki ruangan menggunakan identitas orang lain. Untuk itu, diterapkan fitur kamera CCTV untuk menunjang ACS menggunakan sistem OnGuard 2013. CCTV memiliki kemampuan merekam dan mengamati suatu objek setiap waktu sehingga sangat berguna untuk keamanan didalam suatu gedung. Penambahan fitur CCTV pada *ACS* dapat mengidentifikasi pihak-pihak yang dikenal maupun tidak dikenal sehingga dapat diteliti dan dijadikan informasi untuk kebutuhan data dilapangan. Pada penelitian ini merancang dan mensimulasikan penerapan fitur kamera CCTV untuk *ACS* menggunakan sistem OnGuard 2013. Data yang berupa gambar dan identitas para pengunjung dapat direkam dengan menggunakan kamera CCTV pada saat masuk ruangan dengan menggunakan *Card* ID / *Proxymity Card*. Pengunjung yang sah pada saat hendak memasuki ruangan dapat dibandingkan dengan identitas penggunanya agar pintu yang terpasang *ACS* dapat terbuka. Berdasarkan data pegujian menunjukan hasilnya mencapai 100%, *“Granted No entry”* 0%. Kemudian dengan menggunakan metode antipussback pengunjung ruangan dapat dengan mudah dikenali siapa saja yang masih berada didalam ruangan dan ditampilkan pada sistem OnGuard.

***Kata kunci:*** *Access Control Sistem* (ACS), Antipussback, CCTV, Sistem OnGuard*.*

1. **Pendahuluan**

 Seiring dengan perkembangan teknologi yang berkembang pesat, berkembang pula teknologi untuk *system* pengawasan keamanan. Perkembangan ini sangat membantu petugas keamanan dalam melaksanakan pengawasan yang diterapkan pada gedung-gedung, perkantoran, instansi maupun perusahaan. Ada beberapa teknologi dalam melakukan pengawasan keamanan yang banyak digunakan antara lain *Closed Citcuit Television* (CCTV) dan *Access Control System* (ACS). CCTV memiliki kemampuan untuk merekam dan mengamati suatu objek secara continue setiap waktu sehingga sangat berguna untuk keamanan didalam suatu gedung yang dipantau oleh petugas keamanan.

*Access Control System* (ACS) merupakan suatu perangkat kontrol yang terpasang pada pintu ruangan berguna untuk membatasi akses pengunjung dalam memasuki ruangan. Kehadiran *Access Control System* (ACS) sangat membantu petugas keamanan misalnya pada suatu perusahaan dalam melakukan pengawasan keamanan ruangan, dimana *Access Control System* (ACS) ini dapat mengidentifikasi setiap pengunjung yang memasuki suatu ruangan di dalam gedung. *Access Control System* (ACS) merupakan tingkat keamanan ruangan yang mana setiap ruangan harus dapat mengidentifikasi semua pengunjung yang telah masuk ataupun keluar dari ruangan[1].

Penelitian terkait yang sudah dilakukan tentang pengawasan gedung menggunakan fitur CCTV yaitu dengan judul “Perancangan *Active Survailance camera* Dalam Otomasi Pengawasan Gedung” pada penelitian ini menjelaskan bahwa pengamatan dalam merekam kejadian dapat dibuat lebih efisien dengan mengaktifkan fungsi rekam saat objek terdeteksi saja, dan yang terakhir adalah fungsi alarm mampu memberi peringatan secara *audio* pada petugas keamanan saat objek terdeteksi [2].

 Penelitian selanjutnya membahas tentang *Access* 3 *Control System* (ACS) dengan judul “Rancang Bangun Akses Kontrol Pintu Sebagai Identifikasi Pengunjung Untuk Menunjang Keamanan Ruangan”. Penelitian ini memiliki tujuan untuk membuat sebuah akses untuk keamanan yang dapat mengidentifikasi pengunjung ruangan menggunakan *Card* ID/*Proxymity Card* yang terdaftar dengan mendekatkan RFID *Reader* dan dapat mengunci ruangan dari jarak jauh [1]. Dengan melihat keunggulan yang dimiliki oleh *Closed Citcuit Television* (CCTV) dan *Access Control System* (ACS), telah banyak perusahaan yang menerapkan teknologi dari *Closed Citcuit Television* (CCTV) dan *Access Control System* (ACS), salah satunya adalah PT. Chevron Pasific Indonesia. PT. Chevron Pasific.

Pada penelitian ini mengidentifikasi bahwa penggunaan *system* pengawasan misalnya *Closed Citcuit Television* (CCTV) dan *Access Control System* (ACS) digunakan secara terpisah seperti halnya pada PT. Chevron Pasific Indonesia yang berlokasi di daerah Rumbai-Pekanbaru. Berdasarkan hasil survei yang dilakukan penulis, bahwa penggunaan *system* masih terpisah, *Closed Citcuit Television* (CCTV) menggunakan *system* Milestone dan *Access Control System* (ACS) menggunakan *system* Lenel OnGuard sehingga didalam memonitoring pengunjung yang masuk atau keluar menggunakan *Access Control System* (ACS) dari suatu ruangan didalam gedung atau kantor pada PT. Chevron Pasific Indonesia masih belum terindentifikasi secara objektif identitas pengunjungnya. Karena kerja dari *Access Control System* (ACS) hanya menggunakan *smartbadge* sebagai akses keluar masuk ruangan. Masalah yang terjadi yaitu pengunjung yang keluar masuk menggunakan *Card* ID/*Proxymity Card* belum tentu pemilik *smart badge* nya. Untuk mengatasi masalah ini diperlukan penerapan *Closed Citcuit Television* (CCTV) pada *system Access Control System* (ACS).

1. **Metodologi Penelitian**

Metodologi penelitian merupakan langkah-langkah kegiatan dalam mendapatkan hasil penerapan fitur kamera CCTV untuk *Access Control System* (ACS) menggunakan sistem OnGuard 2013 (Studi Kasus : PT. Chevron Pasific Indonesia) dengan tujuan agar meningkatkan kinerja keamanan pada sistem *Access Control System* (ACS) dan dapat mencegah akses ilegal bagi pengunjung ruangan.. Adapun tahapam penelitian secara rinci seperti gambar 1 dibawah ini :

Gambar 1. Tahapan Penelitian

**2.1 Perancangan *Access Control System* (ACS dan CCTV)**

Perancangan sistem dapat diidentifikasikan sebagai penggambaran, perancangan dan pembuatan sketsa atau pengaturan dari beberapa elemen terpisah kedalam satu kesatuan yang utuh dan berfungsi. Tujuan dari perancangan sistem adalah untuk memenuhi kebutuhan kepada pemakai sistem dan untuk memberikan gambaran secara jelas, rancang bangun yang lengkap kepada program komputer dan ahli teknik-teknik lainnya. Pada penelitian ini, merancang pada ACS untuk memudahkan dalam investigasi dalam satu ruangan.

* + 1. **Topologi *Access Control System (ACS)***

Pengertian topologi Jaringan adalah susunan lintasan aliran data didalam jaringan yang secara fisik menghubungkan simpul yang satu dengan simpul lainnya (Anis Yuswo Maslahan. 2011). Berikut ini adalah tampilan struktur *Access Control System* (ACS) untuk memudahkan dalam invertigasi dalam suatu ruangan.



Gambar 2 Topologi Lenel

(Sumber: PT. Chevron Pasific Indonesia)

Agar *user* dapat masuk ruangan yang terpasang *Access Control System* (ACS) maka harus menempelkan kartu atau *Card* ID/*Proxymity Card*ke *Reader* yang sudah di *grant* ke sistem dari *server*, *Reader* akan mengirimkan data ke Lenel dan data tersebut akan di kirim kembali ke *server* melalui jaringan *internet* atau *intranet* yang digunakan oleh PT. Chevron Pasific Indonesia. Data tersebut akan di *check* di *database* jika data tersebut sudah sesuai maka pintu dapat terbuka dan apabila data tersebut tersebut tidak sesuai, masa aktif *Card* ID / *Proxymity Card* sudah berakhir maka pintu tersebut akan tetap terkunci.

*Inteligent System Control* adalah tempat penyimpanan yang berada di *database* sehingga jika ada pencarian *Card* ID/*Proxymity Card*user yang masuk. *Dual reader interface module* digunakan untuk sistem Lenel 1320 maka dalam integrasi Lenel ke sistem menggunakan *dual reader interface module*. Maximum jarak antara Lenel ke *device* yaitu 500 *feet*/152.4 m sehingga untuk memasang *device* harus dekat dengan Lenel agar *tranfer* data dari *Reader* ke Lenel atau sebaliknya lebih cepat.

* + 1. **Perancangan Penempatan CCTV**

Perancangan penempatan kamera CCTV dipasang diatas dan atau mendekati pintu masuk sehingga para pengunjung ruangan yang hendak masuk dapat di identifikasi wajah pengguna dengan identitas yang sedang dipakai. Kamera akan merekan semua pengunjung yang hendak memasuki ruangan dan akan disimpan diserver yang sudah terhubung dengan sistem OnGuard 2013, hasil rekaman dapat dijadikan bukti bagi semua pengunjung ruangan. Berikut gambar dari perancangan kamera CCTV yang terhubung dengan sistem OnGurd 2013.



Gambar 3. Perancangan kamera CCTV

* + 1. **IP *Address***

Pada tahap ini melakukan langkah perancangan untuk menentukan IP *Address* yang akan digunakan dalam sistem OnGuard 2013 yaitu:

1. IP *AddressAccess Control System* (ACS)

*Access Control System* (ACS) memerlukan IP *Address* dan IP yang digunakan dalam penelitian ini menggunakan kelas C dengan IP *Address* xxx.xxx.xxx.

1. IP *Address* CCTV

Kamera CCTV diperlukan IP *Address* agar bisa untuk komunikasi antara kamera dengan sistem OnGuard 2013 dan IP yang digunakan dalam penelitian ini menggunakan kelas C dengan IP *Address* xxx.xxx.xxx.

* + 1. **Jaringan *Access Control System* (ACS) Yang Sudah Berjalan**

Jaringan *Access Control System* (ACS**)** yang sudah berjalan di PT. Chevron Pasifik Indonesia saat ini terlihat pada gambar berikut ini:



Gambar 4. *Access Control System* (ACS) Di PT. Chevron Pacific Indonesia

(Sumber: PT. Chevron Pafic Indonesia)

Pada gambar diatas menggunakan satu *server* untuk *accsess control system* (ACS) yaitu yang berada di rumbai. Di setiap IT *Norht*, IT *South* dan Kalimantan diberikan *access* untuk *client* agar bisa *login* ke OnGuard 2013 sehingga dapat membantu *admin* dalam melakukan *monitoring* akan tetapi untuk *client user* juga diberikan *access* terbatas sehingga tidak bisa merubah data yang berada di *server*.

* + 1. **Jaringan *Access Conrtrol System* (ACS) Yang Akan Dibangun**

Pada penelitian ini *Access Control System* (ACS) akan ditambahkan dengan menggunakan kamera CCTV. Penelitian ini diaplikasikan langsung dilapangan dengan adanya *Access Control System* (ACS) ditambahkan fitur kamera CCTV, dengan asumsi bagi pengunjung yang masuk pada saat mendekatkan *Card* ID/*Proxymity Card*ke *Reader* maka pintu akan terbuka dan kamera CCTV akan melaporkan pengunjung tersebut sehingga dalam proses identifikasi antara pengunjung dengan pemilik *Card* ID/*Proxymity Card*dapat disesuaikan. Perancangan tersebut dapat dilihat pada gambar dibawah ini.



Gambar 5. Integrasi CCTV pada *Access Control System (*ACS*)*

* 1. **Implementasi**

Implementasi dilakukan mulai dari pemasangan *hardware* maupun *software* untuk pendukung pada sistem OnGuard 2013 padasaat dilapangan.

* + 1. ***Hardware* dan *Software* Pendukung**

Tahapan selanjutnya untuk menambahkan fitur kamera CCTV kedalam *Access Control System* (ACS) adalah mempersiapkan perangkat yang mendukung baik *hardware* (perangkat keras) maupun *software* (perangkat lunak).

* + - 1. **Hardware**

Berdasarkan fungsi dan penerapannya *hardware* yang digunakan pada penelitian ini terbagi menjadi beberapa bagian yaitu sebagai berikut.

* + - * 1. ***Hardware* yang digunakan dalam Implementasi yaitu :**
1. Dekstop PC Intel (R) Cord(TM) i3-2330M CPU @ 2.20GHz 2.20GHz RAM 2.00 GB system tipe 32-bit Operating System
2. Monitor LCD 19 inc , Keyboard, dan Mouse optic
	* + - 1. ***Hardware* Lain yang digunakan proses penambahan fitur pada *Access Control System* (ACS) yaitu :**
				2. Kamera CCTV Axis M1114

 Kamera yang akan digunakan adalah sebagai pengambilan gambar dari setiap pengunjung yang hendak masuk ke dalam ruangan.

* + - * 1. ***Hardware* yang Digunakan Dalam proses identifikasi pengunjung antara lain :**
1. *Card* ID/*Proxymity Card*

*Card* ID/*Proxymity Card*yaitu digunakan sebagai alat penyimpan data berupa ID untuk akses identifikasi *Access Control System (*ACS)

1. Lenel 2210

Lenel 2210 adalah *controller* yang digunakan untuk menghubungkan antara sistem OnGuard 2013 dengan *device*-*device* untuk menjalankan *Access Control System* (ACS) seperti *reader, sirine, door contact, maglock, breakglass,* dan *push button*.

1. *Reader*

*Reade* yaitu berfungsi sebagai alat untuk membaca pada *Card* ID/*Proxymity Card.*

1. *Sirine*

*Sirine* yaitu berfungsi sebagai alat untuk membirikan tanda-tanda ketika sedang terjadi masalah

1. *Magnetick Lock*

*Magnetick Lock* yaitu berfungsi sebagai pengunci pada pintu

1. *Pushbutton*

*Push button* yaitu berfungsi sebagai pembuka pada pintu dengan cara cara ditekan.

1. *Breakglass*

*Break glass* yaitu berfungsi sebagai pemutus arus dari Lenel 2210 ke *magnetic Lock* pada saat terjadi *emergency*.

1. *Door contact*

*Doorcontact* adalah sebagai *sensor* dalam pembacaan pada saat pintu tertutup secara otomatis maka *magnetic lock* akan langsung mengunci.

* + - 1. ***Software***

Selanjutnya berdasarkan fungsi dan penerapannya *software* yang digunakan pada penelitian ini terbagi menjadi beberapa bagian yaitu sebagai berikut**.**

* + - * 1. **OnGuard 2013**

*Software* OnGuard 2013 yang digunakan adalah sebagai sistem untuk mengontrol atau memonitoring akses pada setiap pengunjung ketika hendak masuk kedalam ruangan. *Software* tersebut sudah dilengkapi untuk kamera CCTV namun tanpa adanya *aplikasi* pendukung seperti *Lenel Network Video Suite*(LNVR) maka kamera tersebut tidak bisa diintegrasikan kedalam Sistem OnGuard 2013.

* + - * 1. **Lenel Network Video Suite**

*AplikasiLenel Network Video Suite* (LNVR) digunakan sebagai penghubung antara kamera CCTV kedalam Sistem OnGuard 2013 agar bisa berjalan sesuai yang diharapkan.

* + 1. **Konfigurasi *Access Control System* (ACS)**

Konfigurasi *Access Control System* (ACS) dilakukan agar semua *device-device* yang terpasang dapat terkoneksi kedalam sistem OnGuard 2013.

* + 1. **Konfigurasi Kamera CCTV**

Pada tahapan ini kamera CCTV dilakukan dengan cara konnfigurasi pada IP *address* sehingga agar dapat terdeteksi pada sistem OnGuard 2013.

* + 1. **Konfigurasi *Access Control System* (ACS) dan CCTV Pada OnGuard2013**

Setelah pemasangan pada *deviceAccess Control System* (ACS) maka dilakukanlah integrasi *Access Control System* (ACS) tersebut ke Sistem OnGuard 2013 agar dapat berjalan sesuai yangdiharapkan. Konfigurasi ini dilakukan adalah bertujuan untuk menjalankan semua *device* yang terpasang.

* 1. **Pengujian**

Pengujian ini dilakukan agar dapat mengetahui apakah semua *Access Control System* (ACS)sudah berfungsi dengan benar sesuai dengan yang diharapkan. Pada tahapan pengujian adalah sebagai berikut:

* + 1. **Pengujian Menggunakan *Card* ID/*Proxymity Card***

Dalam tahap pengujian ini diperlukan pengujian menggunakan *Card* ID/*Proxymity Card*, sehingga pengguna *Card* ID/*Proxymity Card*ketika memasuki ruangan dapat teridentifikasi sesuai identitas penggunanya.

* + 1. **Pengujian Anti *Pussback***

Pengujian ini dilakukan agar dapat di identifikasi ketika pengunjung yang telah masuk ruangan yang sedang berada di dalam ruangan sehingga jika terjadi insiden maka akan mudah di kenali.

* + 1. **Pengujian *Card* ID/*Proxymity Card* Yang Tidak Terbaca di Sistem.**

*Card* ID/*Proxymity Card* yang telah di bawa oleh *user* belum tentu semuanya bisa terbaca pada sistem OnGuard 2013 hal ini sering terjadi dilapangan. sehingga Pengujian ini perlu dilakukan agar *user* yang membawa *Card* ID/*Proxymity Card*dapat terbaca pada sistem.

1. **Hasil Pengujian dan Analisa**

Pada bagian ini akan diuraikan tentang hasil pengujian dan analisis dari penerapan fitur kamera CCTV untuk *Access Control System* (ACS) menggunakan sistem OnGuard 2013. Analisis meliputi implementasi dan konfigurasi CCTV dan *Access Control System* (ACS) pada OnGuard 2013. Untuk mengetahui apakah penerapan fitur CCTV pada *Access Control System* (ACS) telah berjalan dengan baik, maka akan dilakukan beberapa pengujian terhadap simulasi jaringan yang dibangun, seperti pengujian pada sistem dan pengguna *Card* ID/*Proxymity Card.*

* 1. **Uji konesi CCTV dan *Access Control System* (ACS)**
		1. **Uji Koneksi CCTV**

 Tahap pengujian ini dilakukan dari *server* agar koneksi antara kamera CCTV dengan *server* bisa terhubung sehingga harus dilakukan uji coba menggunakan program *ping (packet internet gopher).Ping* adalah sebuah program utilitas yang digunakan untuk memeriksa dan mengetahui konektifitas jaringan berbasis teknologi *TCP/IP (Transmission Control Protocol/Internet Protocol)*, dengan ini dapat di uji apakah *Device* dapat terhubung ke *Server*. *Ping* akan mengirimkan sebuah paket kepada alamat *IP* tujuan, sehingga didapat nilai *Packet Loss* dan *Round Trip Time* dari paket yang dikirim untuk menentukan kualitas dari konektifitas *Device* yang terpasang. *Packet Loss* merupakan suatu parameter yang menggambarkan suatu kondisi yang menunjukkan jumlah total paket yang hilang. Sedangkan *Round Trip Time* merupakan pengukuran terhadap waktu yang dibutuhkan untuk mengirimkan sebuah paket dari suatu sumber ke alamat tujuannya lalu kembali lagi ke sumber tersebut.

Uji koneksi antara kamera CCTV sebagai perangkat yang akan digunakan sebagai fiture tambahan pada *Access Control System* (ACS) atau *Access Point* dengan *IPAddress* kelas C dengan IP *adderess* xxx.xxx.xxx.xxx kamera CCTV yang sebagai *client* dan *server* dengan *IPAddress*xxx.xxx.xxx.xxx. Tahapan uji coba dapat dilihat pada Gambar 6 sebagai berikut ini.



Gambar 6. Uji koneksi kamera CCTV

* 1. **Hasil Perbandingan tanpa Kamera CCTV dan menggunakan Kamera CCTV pada *Access Control System*( ACS)**

Dengan adanya penambahan fitur kamera CCTV pada *Access Control system* (ACS) untuk lebih mudah dalam mendapatkan hasil verifikasi.Verifikasidihasilkan melalui Proses dalam penambahan fitur kamera CCTV pada *Access Control system* (ACS) dengan menggunakan sistem OnGuard 2013 dengan cara membanding pemilik *Card* ID/*Proxymity Card* dengan penggunanya. Kemudian untuk mengetahui pengguna *Card* ID/*Proxymity Card*yang sah dan tidak sah menggunakan kamera CCTV dan tanpa menggunakan kamera CCTV perlu dilakukan perbandingan. Berikut ini adalah hasil dari perbandingan tanpa menggunakan kamera CCTV dan menggunakan kamera CCTV pada *Access Control system* (ACS).

Table 1. hasil perbandingan pada *Access Control system* (ACS)

|  |  |  |  |
| --- | --- | --- | --- |
| No | Perbandingan | Tanpa Menggunakan Fitur Kamera CCTV | Menggunakan Fitur Kamera CCTV |
| 1 | Pengunjung pada saat masuk ruangan (*tapCard* ID/*Proxymity Card*ke *reader*). | *Granted Access.* | Granted Access. |
| 2 | Tampilan pada monitor pihak*security*. | Terlampir identitas pengunjung. | Terlampir identitas pengunjung beserta rekaman *Video*. |
| 3 | Identifikasi pengunjung dari pihak *security*. | Masih kesulitan dalam identifikasi dari pengunjung dengan pengguna *Card* ID/*Proxymity Card*yang sah. | Mudah diidentifikasi hasil dari pengunjung yang telah masuk ruangan dengan adanya rekaman *Video*. |



(b)

Gambar 7. Perbandingan pengguna *Card* ID/*Proxymity Card* pada sistem OnGuard 2013.

Berdasarkan data hasil perbandingan penambahan fitur kamera CCTV pada *Access Control System* (ACS) diatas diketahui dari tampilan Alarm Monitoring menampilkan semua identitas bagi pemilik*Card* ID/*Proxymity Card*d dan yang menggunakannya. Penambahan fitur kamera CCTV pada *Access Control System* (ACS) jauh lebih baik dibandingkan tanpa menggunakan kamera CCTVseperti pada saat penggunjung masuk ruangan teridentifikasi langsung bagi yang menggunakan *Card* ID/*Proxymity Card* sesuai dengan pemiliknya, dapat dijadikan bukti dari hasil pengunjung ruangan dengan adanya *Video* rekaman yang dapat dikonversi kedalam .*asf* sehingga dapat dibuka hasil rekamannnya tanpa harus masuk ke Sistem OnGuard 2013.

**4. KESIMPULAN**

Dari hasil penelitian ini diperoleh beberapa kesimpulan berdasarkan hasil penerapan fitur kamera CCTV untuk *Access Control System* (ACS) menggunakan sistem OnGuard 2013 (Studi Kasus : PT. Chevron Pasific Indonesia) antara lain :

1. Pengguna *Card* ID/*Proxymity Card* bagi pengunjung yang sah dan tidak sah dapat di identifikasi sesuai gambar dari pemilik *Card* ID/*Proxymity Card*. Telah dilakukan pengujian dan hasilnya mencapai 100 % sehingga pada saat terjadi kerusakan atau hal-hal yang telah merugikan bagi Perusahaan dapat dibuktikan dengan adanya *video* bagi pengunjung.
2. Pengujian dengan menggunakan anti *pushback* sangat membantu dalam pengawasan atau investigasi. Pada saat terjadi hal-hal yang tidak diinginkan pengunjung ruangan dapat langsung dikenali siapa saja yang sedang berada diruangan.
3. *Card* ID/*Proxymity Card* menggunakan *enkripsi* *Card* ID/*Proxymity Card* dapat terbaca pada sistem yaitu dengan cara indentifikasi dari jumlah bilangan yang terdapat pada *Card* ID/*Proxymity Card*, karena semua jenis *Card* ID/*Proxymity Card* mempunyai nilai yang berbeda-beda. Sistem OnGuard 2013 menggunakan bilangan enkripsi maka jumlah enkripsi pada *Card* ID/*Proxymity Card* harus ditambahkan pada sistem OnGuard 2013.

**REFERENSI**

1. Choirul Huda dkk. *Rancang Bangun Akses Kontrol Pintu Sebagai Identifikasi Pengunjung Untuk Menunjang Keamanan Ruangan.* Jurnal Informatika, Program Teknologi Informasi Dan Ilmu Komputer,Universitas Brawijaya. 2013
2. Neo Orta Negara dkk. *Perancangan Active Surveillance Camera Dalam Otomasi Pengawasan Gedung.* Jurnal, Jurusan Teknik Industri Institut Teknologi Sepuluh Nopember (ITS) Surabaya Kampus ITS Sukolilo Surabaya 60111. 2011.
3. Belhekar Vipul Krushna1 dkk. *Multi-Clouds Security: Using Access Control*. International Journal of Advance Research inComputer Science and Management Studies. 2014
4. dhaka. *Development of Low Cost Private Office Access Control System(OACS).* International Journal of Embedded Systems and Applications. . 2012
5. Eric Priyo Tranggono dkk.. *Rancang Bangun Sistem Informasi Kontrol Kondisi Lalu Lintas Dengan Kamera Pemantau CCTV Berbasis gis.*Jurnal, Jurusan Sistem Informasi. Sekolah Tinggi Manajemen Informatika & Teknik Komputer Surabaya. 2012
6. Eric Priyo Tranggono dkk. *Monitoring Dan Analisis Kualitas Layanan Trafik Kamera Cctv Pada Jaringan Wireless (Studi Kasus : PT. Bukit Asam (Persero) Tbk Tanjung Enim).*Skripsi, Rahayu. JurusanKomputer. Universitasbinadarma. 2013.
7. Eric Priyo Tranggonodkk. *Internet Protocol Virtual Private Network (IP VPN) dan Network Management untuk Efisiensi Koneksi Internet dengan Sistem Intranet (Studi Kasus : 4 Warung Internet di Desa Pujud Rokan Hilir Riau).*Skripsi, Ramadani.JurusanTelekomunikasi. Universitas Islam Negeri Sultan Syarif kasim. . 2013
8. Ega Albert dkk..*Sistem Otomatisasi Perekaman Video Dengan Kamera Cmos 12 Led Berbasis Mikrokontroler At89s51 Menggunakan Sensor Pir (Passive Infrared).*Jurnal, Jurusan Fisika FMIPA UniversitasAndalas. 2013
9. Gintorodkk..*Sistem Smart Class Room Berbasis Smart Card* DanBahasaPemrograman *C++.*Seminar Nasional Aplikasi Teknologi Informasi. 2010