ISSN (Printed) : 2579-7271
ISSN (Online) : 2579-5406

Penerapan Fitur Kamera CCTV Untuk *Access Control System* (ACS) Menggunakan System Onguard 2013 (Studi Kasus: PT. Chevron Pasific Indonesia)

Sutoyo [1], Triyono[2] , Saepudin[3]
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 Closed Citcuit Television (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 seperti pada PT Chevron Pasific Indonesia. 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 hasil pengujian 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 sistem 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.

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

Penelitian terkait tentang system keamanan antara lain yang sudah dilakukan tentang perancangan sistem keamanan menggunakan RFID [2,3,4], kemudian system keamanan menggunakan fitur camera [5,6,7,8].

Dengan melihat keunggulan yang dimiliki oleh CCTV dan ACS, telah banyak perusahaan yang menerapkan teknologi ini baik *Closed Citcuit Television* (CCTV) maupun *Access Control System* (ACS) sebagai bentuk sistem keamanan salah satunya berada pada PT. Chevron Pasific Indonesia.

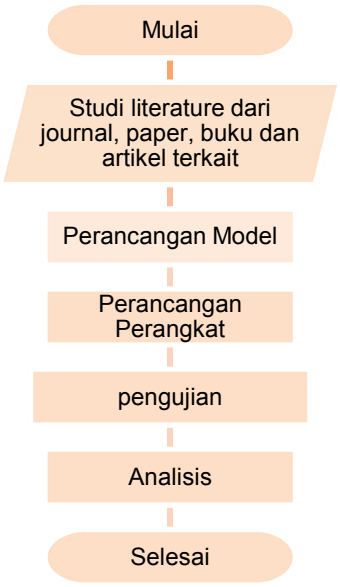
Pada penelitian ini mengidentifikasi bahwa penggunaan sistem pengawasan misalnya *Closed Citcuit Television* (CCTV) dan *Access Control System* (ACS) digunakan secara terpisah pada PT. Chevron Pasific Indonesia yang berlokasi di daerah Rumbai-Pekanbaru. Hasil

ISSN (Printed) : 2579-7271
ISSN (Online) : 2579-5406

idenfikasi menunjukkan bahwa *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) di embededkan ke *system Access Control System* (ACS)dalam meningkatkan fungsi keamanan di PT. Chevron Pasific Indonesia.

2. 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 tahapan penelitian secara rinci seperti gambar 1 dibawah ini :



Gambar 1. Tahapan Penelitian

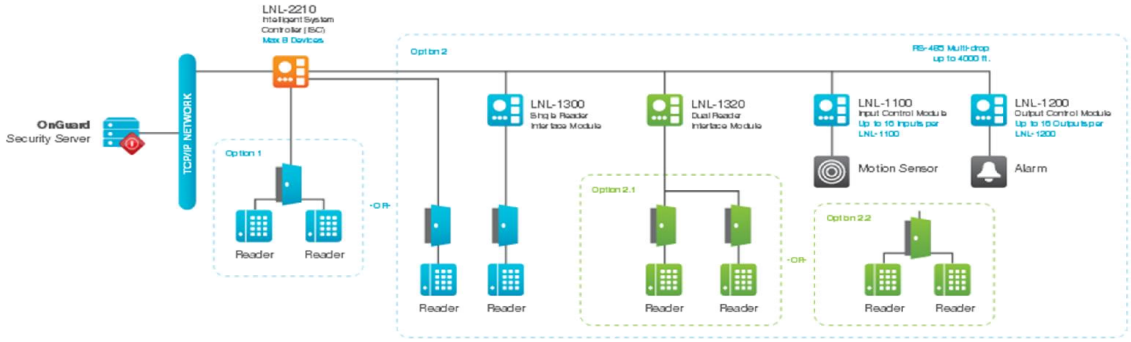
2.1 Perancangan *Access Control System* (ACS dan CCTV)

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.

2.1.1 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.

ISSN (Printed) : 2579-7271
ISSN (Online) : 2579-5406



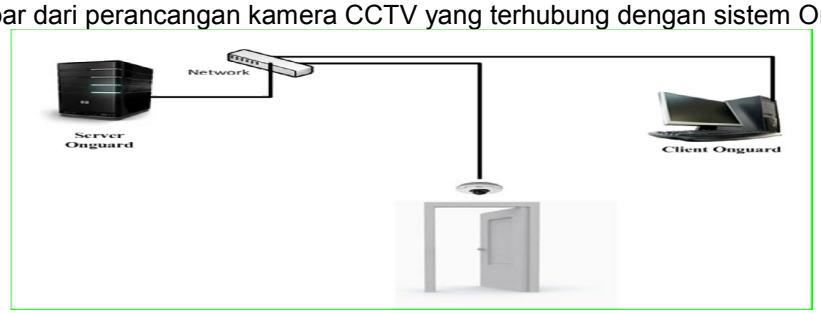
Gambar 2. Topologi Lenel
(Sumber: PT. Chevron Pasific Indonesia)

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.

2.1.2 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

2.1.3 IP *Address*

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

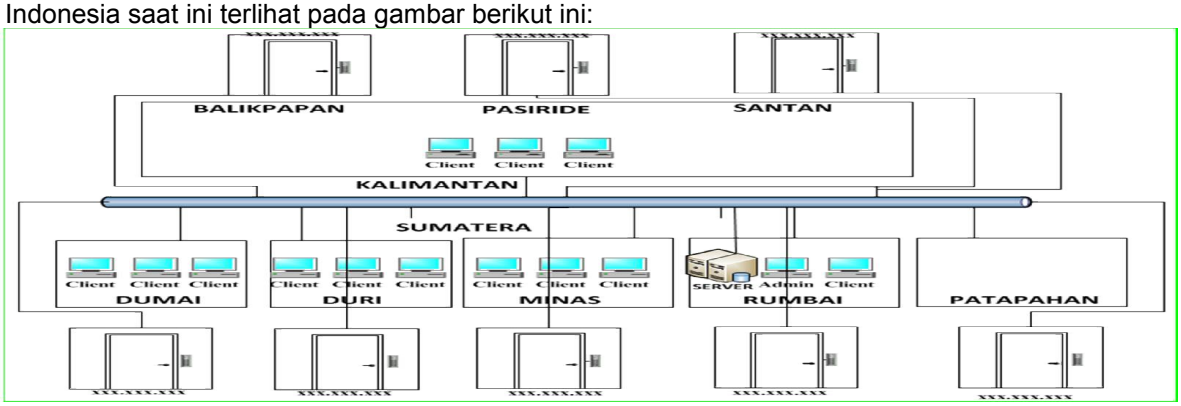
1. IP *AddressAccess Control System* (ACS)
   Access Control System (ACS) memerlukan IP *Address* dan IP yang digunakan dalam penelitian ini menggunakan kelas C dengan IP *Address* xxx.xxx.xxx.
2. IP *Address* CCTV

ISSN (Printed) : 2579-7271
ISSN (Online) : 2579-5406

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.

2.1.4 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:

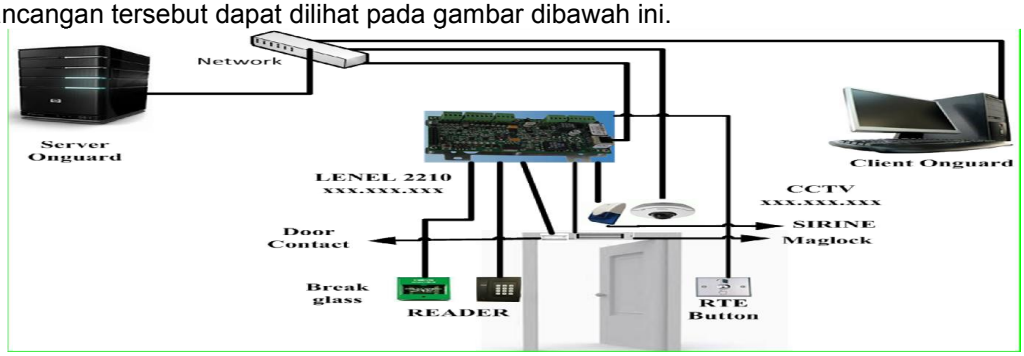


Gambar 4. *Access Control System* (ACS) Di PT. Chevron Pacific Indonesia
(Sumber: PT. Chevron Pafic Indonesia)

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*.

2.1.5 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*)*

2.2 Implementasi

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

2.2.1 *Hardware* dan *Software* Pendukung

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

2.2.1.1 Hardware

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

2.2.1.1.1 *Hardware* yang digunakan dalam Implementasi yaitu :

a. Dekstop PC Intel (R) Cord(TM) i3-2330M CPU @ 2.20GHz 2.20GHz RAM 2.00 GB system tipe 32-bit Operating System
b. Monitor LCD 19 inc , Keyboard, dan Mouse optic

2.2.1.1.2 *Hardware* Lain yang digunakan proses penambahan fitur pada ACS yaitu :

a. Kamera CCTV Axis M1114
   Kamera yang akan digunakan adalah sebagai pengambilan gambar dari setiap pengunjung yang hendak masuk ke dalam ruangan.

2.2.1.1.3 *Hardware* yang Digunakan Dalam proses identifikasi pengunjung antara lain :

Adapun hardware yang digunakan dalam proses identifikasi antara lain Card ID/*Proxymity Card*, Lenel 2210, *Reader*, *Sirine*, *Magnetick Lock*, *Pushbutton*, *Breakglass* dan *Door contact*

2.2.1.2 *Software*

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

2.2.1.2.1 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.

2.2.1.2.2 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.

2.2.2 Konfigurasi *Access Control System* (ACS)

Konfigurasi ACS dilakukan agar semua *device-device* yang terpasang dapat terkoneksi kedalam sistem OnGuard 2013.

2.2.3 Konfigurasi Kamera CCTV

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

2.2.4 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.

2.3 Pengujian

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

2.3.1 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.

2.3.2 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.

2.3.3 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.

3. Hasil Pengujian dan Analisa

Pada bagian ini akan diuraikan tentang hasil pengujian dan analisis dari penerapan fitur kamera CCTV untuk ACS menggunakan sistem OnGuard 2013. Analisis meliputi implementasi dan konfigurasi CCTV dan ACS pada OnGuard 2013. Untuk mengetahui apakah penerapan fitur CCTV pada 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.*

3.1 Uji konesi CCTV dan *Access Control System* (ACS)

3.1.1 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 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

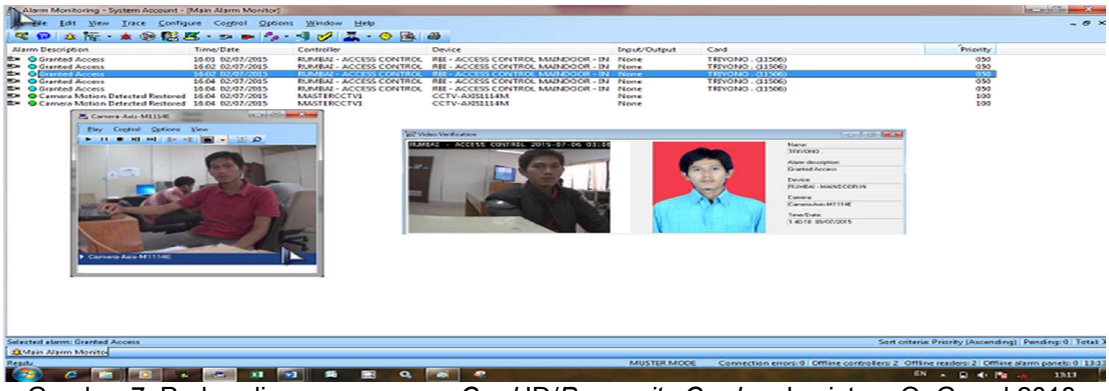
3.2 Hasil Perbandingan tanpa Kamera CCTV dan menggunakan Kamera CCTV pada *Access Control System*(ACS)

Dengan adanya penambahan fitur kamera CCTV pada ACS untuk lebih mudah dalam melakukan verifikasi menggunakan sistem OnGuard 2013 dengan cara membanding pemilik *Card* ID/*Proxymity Card* dengan penggunanya. Fitur CCTV di embed kan ke sistem ACS sehingga akan ada pemrosesan gambar terhadap hasil rekaman CCTV kemudian disesuaikan dengan database kartu dan system ACS akan melakukan verifikasi. Kemudian dilakukan perbandingan untuk mengetahui pengguna *Card* ID/*Proxymity Card* yang sah maupun yang tidak sah antara menggunakan kamera CCTV dan tanpa menggunakan kamera CCTV pada sistem ACS seprti pada hasil tabel 1 dibawah ini.

ISSN (Printed) : 2579-7271
ISSN (Online) : 2579-5406

Table 1. Hasil perbandingan pada *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*.



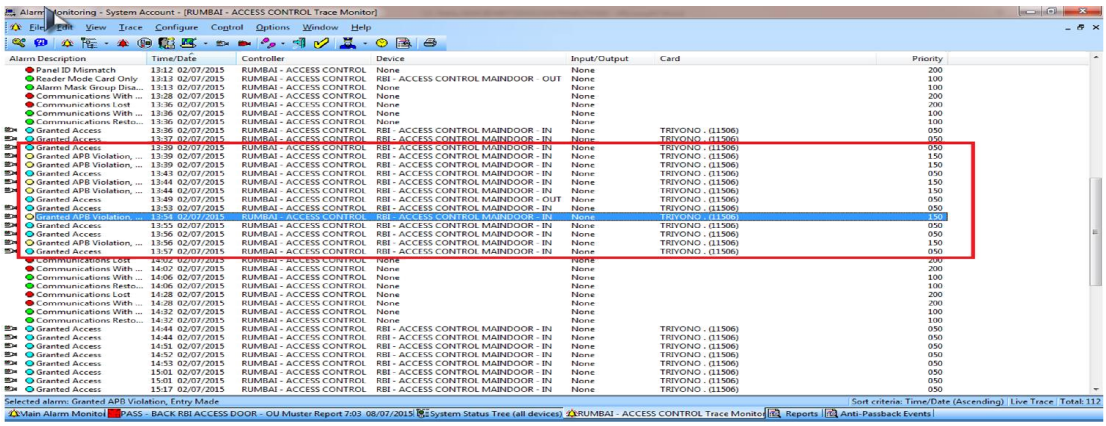
Gambar 7. Perbandingan pengguna *Card* ID/*Proxymity Card* pada sistem OnGuard 2013.

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* dan yang menggunakannya. Penambahan fitur kamera CCTV pada *Access Control System* (ACS) jauh lebih baik dibandingkan tanpa menggunakan kamera CCTV seperti 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. Untuk menjalankan kamera CCTV menggunakan aplikasi *Lenel Network Video Suite* 7.1. *Lenel Network Video Rekorder* (LNVR) merupakan aplikasi yang dirancang dengan memanfaatkan teknologi jaringan IP *Address* yang memungkinkan melakukan perekaman berupa *video* yang dapat diakses dan *diremote* dari jarak jauh. Sehingga dengan adanya aplikasi LNVR ini, dapat berguna untuk *Access Control System* (ACS) pada sistem OnGuard 2013.

3.3 Hasil Pengujian dengan menggunakan Anti *Pussback*

Anti *pussback* digunakan untuk pengunjung yang telah masuk dengan cara menempelkan *Card* ID/*Proxymity Card* ke *reader* yang berada di pintu masuk harus di menempelkan ke *reader* yang berada dipintu keluar agar saat pengunjung hendak masuk kedalam ruangan tersebut dapat diijinkan masuk. Hal ini bertujuan untuk memastikan pada saat terjadi hal-hal yang tidak diinginkan dan dapat di identifikasi siapa saja yang masih berada didalam ruangan seperti pada gambar 8.

ISSN (Printed) : 2579-7271
ISSN (Online) : 2579-5406



Gambar 8. Pengujian dengan menggunakan Anti PussBack.

4. Kesimpulan

Dari hasil penelitian ini diperoleh beberapa kesimpulan 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*. Hasil pengujian menunjukkan hasilmencapai 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.

Daftar Pustaka

[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] K.Srinivasa Ravi dkk.. RFID *Based Security System.International Journal of Innovative Technology and Exploring Engineering* (IJITEE). 2(5) 2013.

[3] Jagdish Lal Raheja dkk.. *Rfid Based Networked Gate Entry ControlSystem (GECS).International Journal of Computer Networks & Communications.* 1(3). 2009

[4] Puguh gambiri, dkk.. *Perancangan Sistem Keamanan Hak Akses Pintu AkpolSemarang Menggunakan Rfid*.Jurnal, Jurusan Teknik Elektro, Universitas Diponegoro SemarangJl. Prof Sudharto, SH, Kampus UNDIP Tembalang, Semarang 50275, Indonesia. 3(3). 2014

[5] 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.

[6] 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

[7] 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

[8] 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.