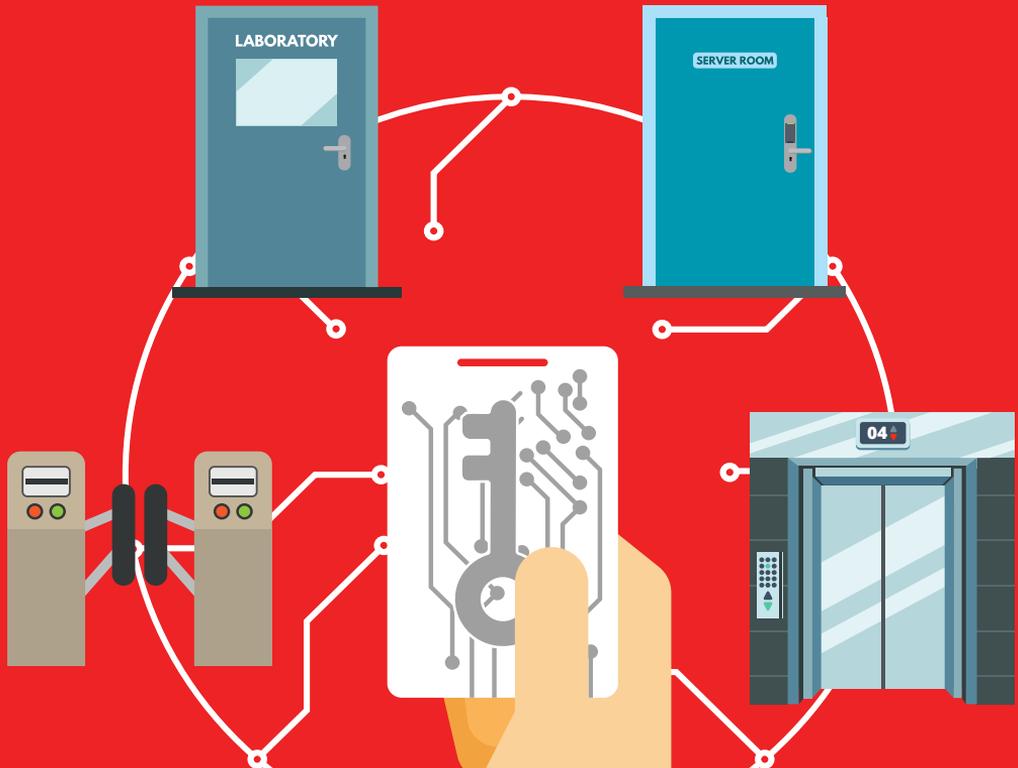


AUTO-ID

UNTUK KALANGAN SENDIRI



SINGLE ID MANAGEMENT FOR ENTERPRISE ACCESS CONTROL

TEKNOLOGI FACIAL
RECOGNITION UNTUK
ACCESS CONTROL

Tips Info tentang
FIDO
(Fast Identity Online)



MEDIA KOMUNIKASI
PELANGGAN

ACS GROUP

PT. AUTOJAYA IDETECH
PT. SOLUSI PERIFERAL
www.acsgroup.co.id

EDITORIAL

Para pembaca setia salam jumpa kembali dalam edisi yang ke 48, kami sangat menghargai dan bangga karena dapat selalu memberikan update-update solusi yang baru yang sekiranya memungkinkan menjadi solusi yang tepat dan berguna bagi perusahaan Anda kedepan.

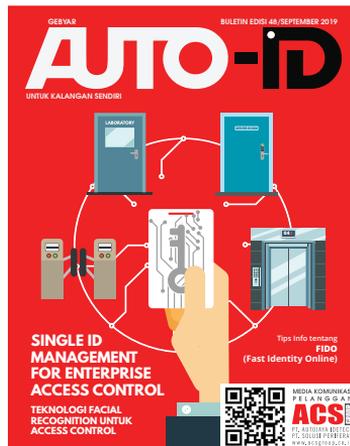
Para pembaca yang budiman mungkin Anda pernah mengetahui kata Single sign-on, istilah ini secara singkat dapat dijabarkan sebagai user/pengguna yang memperoleh akses masuk ke beberapa aplikasi atau sumber daya hanya dengan menggunakan satu akun atau sekali login saja.

Saat ini dalam dunia access control hal tersebut dapat juga diimplementasikan dimana pengguna dapat masuk ke beberapa ruangan atau area hanya dengan menggunakan satu kartu akses.

Solusi Access Control dengan kartu akses tunggal atau satu kartu akses untuk semua akan kami kupas secara detail pada edisi ke 48 ini mulai dari komponen akses control, kegunaan dari kartu akses tunggal/single ID dan kelebihanannya, cara kerjanya, tata kelola (manageability) sampai pada topologinya. Di samping itu kami juga sedikit menyinggung perkembangan dari teknologi pengenalan wajah atau Facial Recognition, Implementasi jaringan WLAN di area pelabuhan, serta rubrik menarik lainnya, pembaca juga disuguhkan dengan info update produk dan seputar kegiatan ACS Group.



Salam,
Taufiq Rahman
Professional Services
Director



PEMIMPIN REDAKSI

Andre S.Kouanak

SEKRETARIS REDAKSI

Listya Kartikasari (Jakarta)
Indah Widiyanti (Cikarang)
Luh Wayan Sumariani (Denpasar)
Herdina Septiyaningrum (Semarang)
Sari Wilujeng (Surabaya)

EDITOR

Chandra Tjahjadi

DESAINER

Oscar Budi Trianto

KONTRIBUTOR (PENULIS)

Taufiq Rahman
Irvan Kurniawan

ALAMAT REDAKSI

Jakarta (HO)

Perkantoran Gunung Sahari Permai
#C03-05, Jl. Gunung Sahari Raya
No 60-63 Jakarta 10610.
Telp : +6221-4208221(H), 4205187(H)
Fax : +6221-4207903, 4207904, 4205853

CONTENT

- 2 Editorial - **Taufiq Rahman**
- 3 Single ID Management for Enterprise Access Control
- 9 Teknologi Facial Recognition Untuk Access Control
- 12 Implementasi
- 13 News & Event
- 16 Product Highlight
- 18 Corporate & Principal Info
- 22 Tips Info tentang : Beacon Tag

SINGLE ID MANAGEMENT FOR ENTERPRISE ACCESS CONTROL



Dalam bulletin edisi ini, pembahasan Single ID Management ini dibatasi penerapan pada Access Control System dalam cakupan Sistem Keamanan Fisik, bukan sistem keamanan digital.

Dalam dunia keamanan fisik, Access Control System pada umumnya adalah bagian dari suatu sistem keamanan yang fungsi utamanya adalah mengontrol akses masuk suatu gedung, ruangan atau tempat. Dengan objektif, hanya orang-orang tertentu yang memiliki hak untuk mengakses, gedung, ruangan atau tempat tersebut, diwaktu-waktu tertentu. Secara umum parameter kontrolnya adalah:

- a. Siapa
- b. Dimana
- c. Kapan

Komponen teknologi dari Access Control System:

- a. Electric door lock (termasuk: tripod-turnstile, full-height-turnstile, dan lain-lain)
- b. Access Reader:
 - 1) Magnetic Stripe Reader (MSR)
 - 2) Proximity Card Reader
 - 3) Biometric (finger-scan, palm-scan, face-recognition, dan lain-lain)
 - 4) Numeric-Keypad
 - 5) Dan lain-lain
- c. Panel Control
- d. Integrated Access Control Software

Access Control System dipakai untuk manajemen sistem keamanan dalam mengatur dan membatasi kewenangan setiap orang sesuai dengan peran, kepentingan dan waktu yang disepakati. Selain itu, setiap kali kewenangan/credential access digunakan, hal tersebut akan dicatat access control software. Informasi tersebut dapat digunakan untuk membuat laporan dan informasi

pendukung pihak manajemen untuk keselamatan dan kesehatan kerja (departemen K3/ HSE) yang berwenang.



Dari waktu ke waktu perkembangan teknologi semakin mempermudah banyak aspek kehidupan, termasuk juga dalam Access Control System. Dahulu Access Control System yang diterapkan dalam suatu organisasi yang memiliki banyak gedung, banyak ruangan dan tidak dalam satu lokasi (beda area/beda kota), mengharuskan user menggunakan beberapa kartu akses (ID Card). Atau bagi yang akan berkunjung ke kantor cabang, maka data base yang bersangkutan harus diregister terlebih dahulu beberapa hari sebelumnya, dan hal ini tentunya sangat merepotkan pengelola sistem keamanan dan Access Control System itu sendiri.

Saat ini, dimana konektivitas sudah dimudahkan dengan adanya koneksi internet, maka dimungkinkan suatu Access Control System yang terintegrasi (terpadu) dan menerapkan sistem 'satu-identitas-akses' untuk semua, atau dalam dunia keamanan fisik, biasa disebut Single-ID-Management. Dengan satu-kartu-akses, atau satu-identitas pengguna dapat mengakses tempat atau fasilitas fisik yang ditangani sistem Access Control yang terintegrasi tersebut, sesuai dengan hak dan otoritas dari si pemegang identitas berikut dengan credential nya.



Kelebihan Single ID Management dalam sistem Access Control:

Memudahkan manajemen sistem keamanan dalam mengontrol dan melakukan pengaturan akses, berdasarkan hak (otoritas), tempat, dan waktu nya secara terpusat dan terpadu.

Hal tersebut memberikan keuntungan, diantaranya:

- a. Menekan kasus pemalsuan identitas
- b. Menekan kasus penyusupan
- c. Efisiensi dan efektivitas manajemen sistem keamanan meningkat
- d. Meningkatkan keselamatan kerja

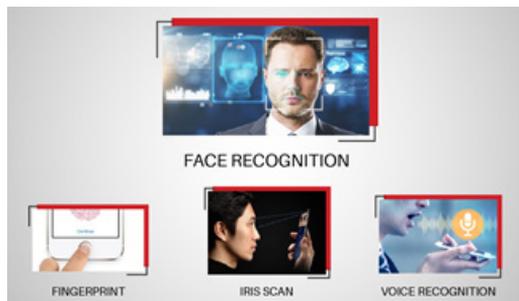
Teknologi ini dapat diterapkan untuk semua organisasi bisnis dari SOHO sampai Big-Enterprise, untuk gedung perkantoran, apartemen, sekolah, rumah sakit, pabrik, pelabuhan laut, pelabuhan udara, area industri dan sebagainya.

Dapat dibayangkan bila tanpa teknologi ini, maka akan terjadi banyak kerepotan dan ketidakefisienan. user akan merasa frustrasi karena harus membawa beberapa kartu identitas untuk mengakses suatu ruangan tertentu, atau mengalami kesulitan akses karena identitasnya tidak dikenali oleh sistem. Dengan sistem terpadu yang berbasis 'Single-ID-Management' hal tersebut tentunya dapat dihindari dengan efektif dan efisien.

Single-ID merujuk kepada proses otentikasi user yang memungkinkan user mengakses multi area atau ruangan yang dikelola dengan sistem keamanan tingkat tinggi, menggunakan Singel-ID yang dapat berupa

kartu-akses (ID-Card, Access-Badge), atau credential berupa identitas biometric dari user seperti, sidik jari, telapak tangan, facial-recognition, retina scan, dan lain sebagainya, dapat digunakan sebagai Singel-ID dari user.

Untuk memberikan wawasan lain dan pemahaman lebih, Single ID dalam dunia Digital dikenal dengan Single Sign On/SSO yang dengan SSO user hanya butuh satu user-name dan password untuk bisa mengakses beberapa aplikasi. Dengan teknologi SSO, user sudah terotorisasi secara sesi aplikasi dan teridentifikasi untuk sinkron dengan beberapa profil aplikasi yang akan dibuka oleh user.



Kembali kepada pembahasan Single ID dalam dunia sistem keamanan fisik dimana teknologi ini dimungkinkan karena fitur controller dan software di belakang reader yang dapat melakukan proses verifikasi secara terpusat dan cepat agar user mendapatkan hak atau tidak saat akan mengakses tempat tertentu. Agar terjadi hal di atas, sistem Access Control harus terintegrasi dengan jaringan data atau sistem informasi yang berbasis IP tentunya.

Agar lebih jauh dapat memahami konsep sistem keamanan fisik berbasis Single-ID-Management maka sebaiknya kita pahami dulu bisnis proses atau sistem yang ingin diatur untuk otorisasi user, karena boleh jadi ada ketentuan tertentu yang secara kebijakan (policy) dalam satu perusahaan berbeda dengan perusahaan lainnya. Untuk mencapai objektif tersebut harus dirancang dahulu skenario bagi masing-masing user yang akan diberikan hak akses dan yang tidak diberikan hak akses. Termasuk regulasi dan algoritma seperti, user tidak dapat hak untuk keluar ruangan jika user tidak masuk ke ruangan tersebut sebelumnya. Aturan dan algoritma tersebut dapat di-setting sesuai dengan logika-logika yang akan diterapkan. Selain itu hal lain yang dapat dicapai dengan sistem Single ID, semua user dapat dilacak dan diketahui lebih tepat dimana keberadaannya.

Hal lainnya, Single ID juga dapat diintegrasikan dengan LDAP (Lightweight Directory Access Protocol) di dunia digital, dimana hanya user yang sudah masuk ke dalam suatu ruang tertentu, secara otomatis mendapatkan hak mengakses jaringan data (Data/IT Network) yang disediakan untuk user tersebut.

Penerapan Single ID dan pengembangan fiturnya dapat secara kreatif dikembangkan oleh manajemen sistem keamanan fisik maupun digital (cyber security) untuk kepentingan keamanan dalam suatu perusahaan secara menyeluruh dan terpadu. Dengan sistem Single ID, akan sangat memberikan dampak kemudahan, sistem pengaturan dan monitoring terpusat (sentralisasi) dan yang akhirnya dapat mencapai aspek keamanan, keselamatan dan kenyamanan untuk user itu sendiri.

Model autentikasi tunggal yang dalam bahasa digitalnya adalah Single Sign On (SSO) yang mana hal ini juga kurang lebih sama dengan Single ID bahkan lebih luas lagi penerapannya karena dapat menawarkan layanan lain yang mungkin mengharuskan pengguna untuk membuat pilihan saat masuk ke sumber daya aplikasi, tetapi dapat dikonfigurasi untuk akses masuk secara SSO diaktifkan atau dinonaktifkan sehingga kewenangan user bisa ditetapkan dalam SSO ini, oleh sebab itu dalam single ID hal tersebut kewenangannya berada pada administrator bukan pada user pada saat user ingin memilih masuk ke area atau ruangan tertentu.

Cara kerja Single ID

Penjabaran cara kerja Single ID disini credential user adalah berupa Kartu-Akses (ID Card/ Access Badge). Berikut penjabarannya:

Saat user melakukan 'tapping' ID card ke Card Reader maka Chip yang ada pada ID Card tersebut mengirimkan nomor ID atau data lain ke koil antena yang mentransmisikannya melalui signal frekuensi radio kembali ke unit pembaca lalu card reader memeriksa apakah nomor ID dari kartu sudah benar. Jika sudah benar maka data tersebut dikirim ke sentral untuk dilakukan otorisasi hak akses dan dilakukan verifikasi. Jika terverifikasi maka Host/Server akan memberitahukan ke controller dan melanjutkan ke pintu agar aksesnya diperbolehkan. Tetapi sebaliknya pintu akan tetap terkunci selama proses autentikasi dan verifikasi di Host tidak membolehkan pintu untuk dibuka, dan jangan lupa semua proses tersebut akan direkam jejaknya walaupun hak aksesnya berbeda.

Untuk melakukan hal di atas secara sistem mutlak harus

terintegrasi dan terhubung secara on-line karena tanpa hal tersebut, sistem Single ID tidak akan bisa diterapkan. Jadi sistem Access Control yang bersifat stand-alone tidak dapat menjalankan sistem Single-ID ini.



Konsep sentralisasi dalam akses control diperlukan untuk melakukan hal-hal di bawah ini sebagai bentuk menggabungkan identitas kartu dalam satu wadah di Host atau server yang nantinya identitas tersebut dapat digunakan oleh controller lainnya untuk memberikan layanan kepada pengguna ID atau user.

Hal-hal yang dilakukan dalam Host yang tersentralisasi adalah sebagai berikut:

- Autentikasi
- Otorisasi
- Data base User Profile
- Algoritma dan Logic User ID management

Aspek autentikasi ini dilakukan berkaitan dengan proses validasi pengenalan dari pengguna dan menetapkan identitas pengguna apakah sebagai staff/anggota yang terdaftar atau sebagai penyusup/orang luar.

Sedangkan otorisasi adalah untuk memastikan pengguna kartu tersebut diperbolehkan atau ditolak oleh system.

Aspek atribut/user profile berhubungan dengan berbagai data si pengguna, misalkan tingkatan hirarki hak akses atau identitas pengguna hal tersebut diperlukan untuk mencegah duplikasi data dengan atribut/user profile terkait.



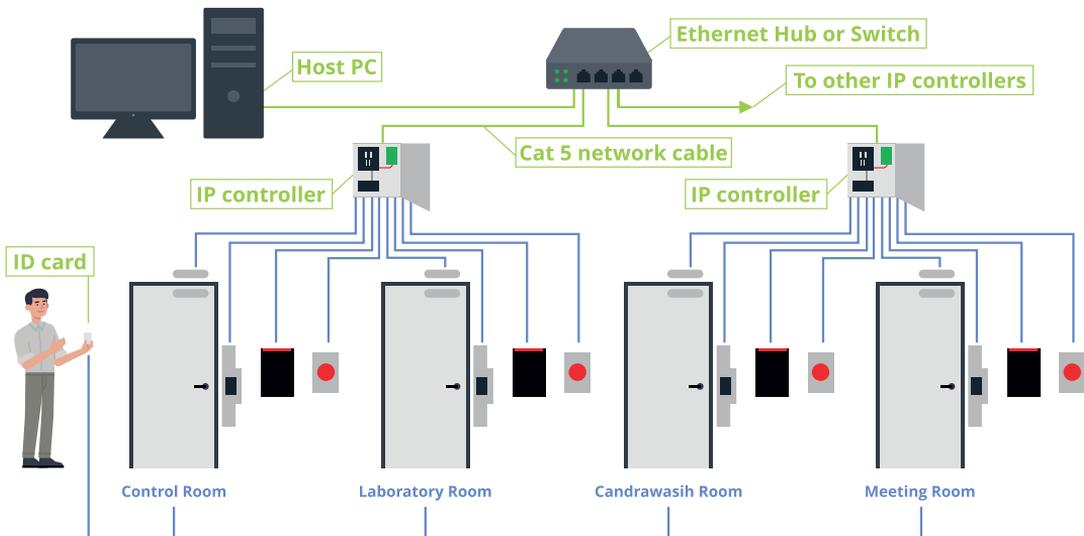
Yang terakhir adalah user management, hal ini terkait dengan aspek administrasi (pembuatan, penghapusan, pembaruan) akun pengguna. Sistem akses control yang terpusat biasanya menyediakan sarana bagi administrator (atau pengguna) untuk menangani akun di seluruh domain atau subsistemnya hal itu diperlukan untuk menetapkan identitas pengguna dan kemudian berbagi informasi dengan setiap subsistem yang membutuhkan data.

Mengapa Single ID sangat terkait dengan otentikasi identitas karena salah satunya adalah untuk menetapkan identitas pengguna /user dan kemudian berbagi informasi itu dengan setiap subsistem yang membutuhkan data dari Host/Server, bahkan hal ini juga dapat digunakan untuk membuka akses internet dan menjalankan aplikasi yang diatur oleh perusahaan.

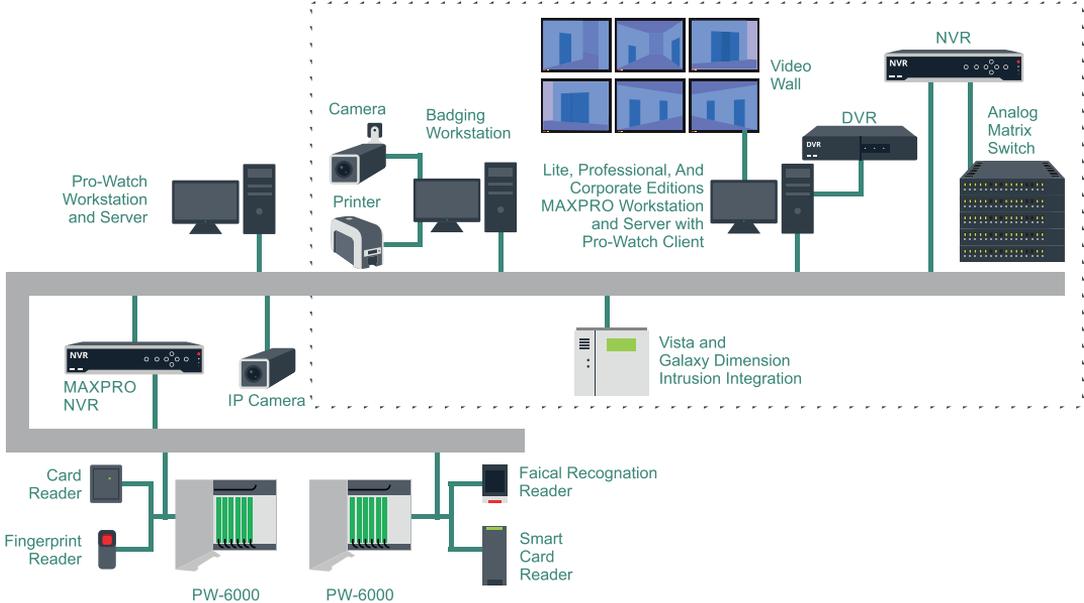
Perlu kita ketahui bahwa Single ID dibangun sebagai landasan kepercayaan system terhadap user dalam mengakses tempat, ruangan dan atau aplikasi, karena saat sistem mempercayakan user masuk ke dalam satu sistem, maka selanjutnya hak sepenuhnya ada pada user yang secara bijak dapat mengakses apapun setelah user tersebut masuk ke dalam suatu ruangan atau aplikasi dan user tersebut juga harus bertanggung jawab penuh atas hak yang diberikan oleh sistem karena user memiliki kekuatan dan pilihan untuk menentukan, menyaring dan menggunakan hak akses ruangan atau aplikasi sesuai dengan profil dan atributnya.

Solusi Single ID

Dalam dunia keamanan secara fisik, solusi Access Control System yang tersedia di pasar tidak banyak yang mampu dan memiliki kapabilitas teknologi Single ID Management seperti ini. Karena teknologi ini bukan hanya sentralisasi sistem Access Control saja, tetapi teknologi yang harus didukung oleh sistem software dengan kemampuan/kecerdasan yang tinggi, memiliki fleksibilitas, skalabilitas dan ketangguhan yang teruji. Hal ini mutlak diperlukan agar sistem dapat bekerja sesuai dengan ekspektasi, dan dapat memproteksi investasi dari customer secara jangka panjang dan menjamin kesinambungan suatu sistem yang kompleks dengan minimum masalah kompatibilitas.



Integrations available using Pro-Watch



Sistem juga harus memiliki standar internasional (compliance aspect), agar dapat mudah terjadi proses implementasi dan penerapan sistem Single ID Management yang baru, terhadap suatu sistem lama yang stand-alone dimana sudah ada berbagai teknologi atau brand access control yang eksis. Hanya dengan solusi yang memiliki fitur dan diciptakan untuk big-enterprise saja permasalahan integrasi dapat dilaksanakan dengan baik, sukses, dan berkesinambungan.

Benefit Single-ID-Management:

Keuntungan yang diperoleh management dengan adanya Single ID yang tersentralisasi ini management dapat dengan mudah memonitor kapan, dimana, siapa dan aplikasi apa yang digunakan oleh user karena saat ini dengan meningkatnya jumlah aplikasi yang digunakan dalam pengaturan bisnis, serta penambahan layanan cloud, mengelola pengguna seringkali merupakan tugas yang sulit dan rumit. Jadi dengan menerapkan Single ID ini perusahaan dan management dapat mengontrol akses dan otentikasi pengguna secara terpusat dan dengan lebih baik dan lebih cepat. Beberapa keuntungan dengan menerapkan teknologi Single ID ini yaitu:

- Mengurangi jumlah ID card oleh satu user, sehingga

user tidak perlu lagi mengingat ID Card tertentu untuk mengakses ruangan tertentu.

- Dengan Single ID akan menghemat waktu dan resources bila diintegrasikan dengan sistem akses ke jaringan (Networks Access Control) dan sistem aplikasi yang relevan yang akan diakses oleh user yang sama.
- Memungkinkan user dapat mengakses ruangan dimana saja dan kapan saja selama dalam satu "domain" tanpa harus mengganti atau mendaftarkan identitas baru atau kartu-akses baru, sehingga terjadi efisiensi.
- Sistem keamanan akan lebih sulit disusupi atau diretas, karena duplikasi identitas atau kartu-akses akan sulit dilakukan. Bila ada duplikasi identitas akan terdeteksi oleh sistem.
- Terjadi efisiensi karena hanya menggunakan 1 (satu) identitas untuk mengakses multi area.

Ada hal lain yang perlu dilakukan sebelum menerapkan Single ID ini adalah :

- Mengevaluasi dan merencanakan secara cermat dan matang rule of the gamenya terhadap user/pengguna

TOPIK

ID tersebut yang diawali dengan menginventarisir jumlah user,

- Grouping user berdasarkan departemen atau divisi
- Skenario dalam mengakses ruangan untuk user tertentu, memetakan user sesuai dengan level dan otorisasinya kemudian menerapkan dalam implementasi di lapangan,
- Mencoba scenario rule of the gamenya agar sesuai dengan objective yang ingin dicapai.

Teknologi Access Control di masa mendatang

Saat ini yang banyak diterapkan dalam single ID masih berbasis fisik kartu yang dibawa oleh user untuk membuka akses, tetapi kedepannya dengan melihat perkembangan teknologi maka sudah mulai diterapkan

penggunaan teknologi biometric selain finger-scan, yaitu penerapan Face-Recognition untuk sistem Access Control. Face-Recognition kedepan akan terus meningkat kebutuhannya, dengan pertimbangan-pertimbangan antara lain:

1. Wajah manusia itu unik
2. Teknologi yang mendukung sudah banyak dan semakin pintar. Digabung dengan Artificial-Intelligent (AI), teknologi ini semakin aman untuk diterapkan.

Namun teknologi Access Control masing-masing memiliki keunikan, kelebihan dan kekurangan maka tergantung kepada bisnis proses dan budget yang dimiliki oleh perusahaan yang ingin menerapkan solusi tersebut.

*/ Penulis : Taufiq Rahman (taufiq.rahman@acsgroup.co.id)

ACS PT. AUTOJAYA IDETECH
PT. SOLUSI PERIFERAL
www.acsgroup.co.id

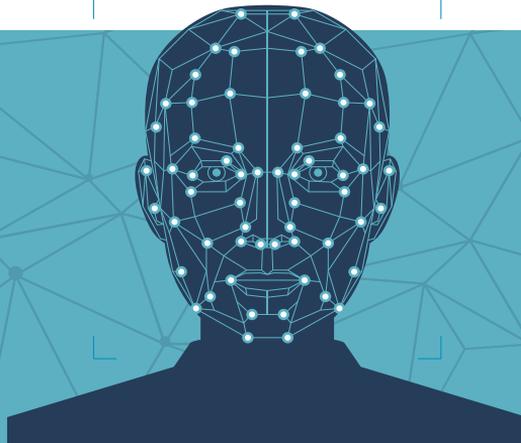
Seluruh Staff dan Management
ACS Group mengucapkan

Selamat Tahun Baru Islam

**1 Muharram
1441 Hijriyah**



TEKNOLOGI FACIAL RECOGNITION UNTUK ACCESS CONTROL



Sistem pengenalan wajah atau lebih dikenal Facial Recognition adalah teknologi komputer yang memungkinkan kita untuk mengidentifikasi atau memverifikasi wajah seseorang melalui sebuah gambar digital. Caranya ialah dengan mencocokkan tekstur lekuk wajah kita dengan data wajah yang tersimpan di database.

Hal ini juga digambarkan sebagai aplikasi berbasis kecerdasan buatan biometrik (Artificial Intelligent Biometric) yang dapat secara unik mengidentifikasi seseorang dengan menganalisis pola berdasarkan tekstur dan bentuk wajah seseorang.

Saat ini penggunaan atau penerapan sistem pengenalan wajah luas merambah ke berbagai sistem keamanan, dan yang paling banyak adalah untuk Access Control pada sistem keamanan fisik. Meskipun keakuratan sistem pengenalan wajah sebagai teknologi biometrik masih berada di bawah sistem pengenalan iris atau retina mata dan pengenalan sidik jari, tetapi sistem ini diadopsi secara luas karena prosesnya yang tanpa kontak dan non-invasive. (Catatan: sudah menjadi tren Facial Recognition digunakan juga untuk access control dunia digital, seperti akses masuk ('Login') ke Smart-Phone, PC, Note-Book dan sebagainya)

Cara kerja Facial Recognition

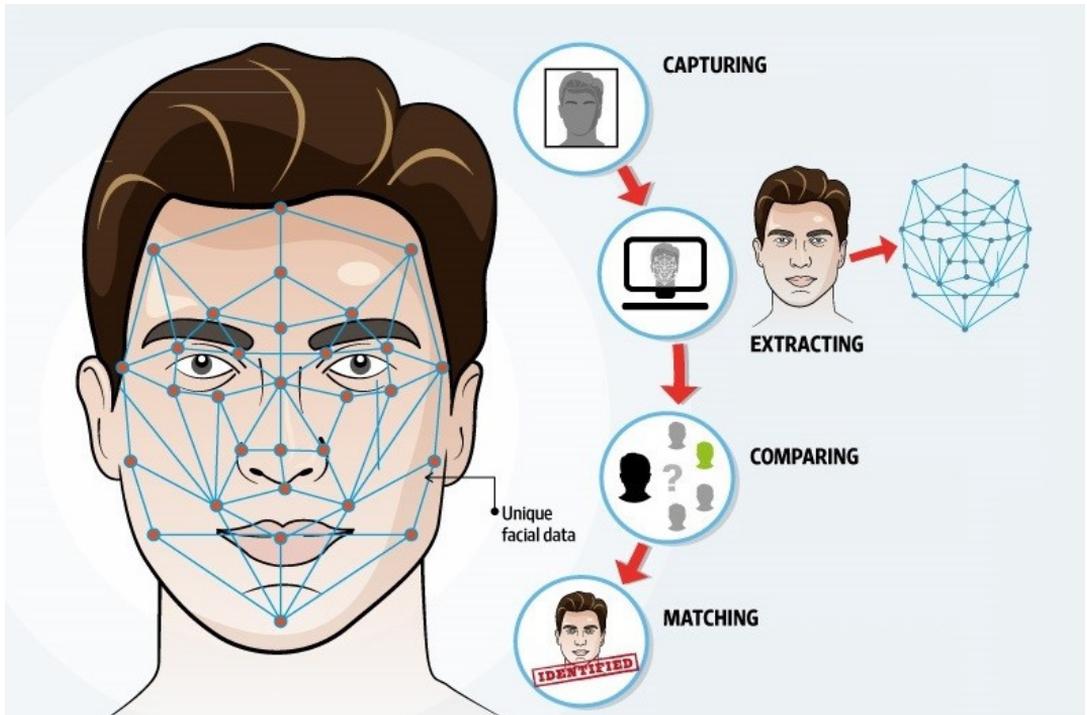
Anda mungkin pandai mengenali wajah seseorang, anda juga mungkin menemukan hal itu dengan mudah untuk mengidentifikasi wajah anggota keluarga, teman, atau kenalan. Anda terbiasa dengan wajah mereka - mata, hidung, mulut - dan sebagainya. Tetapi menurut penelitian bahwa rata-rata manusia dapat mengenal

dengan cepat dan membedakan wajah seseorang dalam hitungan ratusan sampai ribuan wajah saja, tetapi dengan aplikasi pengenalan wajah hal tersebut akan menjadi lebih banyak dan lebih cepat tetapi dalam skala besar dalam jumlah jutaan wajah dengan cara algoritmik yang mana data itu dapat disimpan dan diakses. Sebagai contoh, setengah dari semua orang dewasa Amerika memiliki gambar mereka disimpan dalam satu atau lebih database pengenalan wajah yang dapat dicari oleh lembaga penegak hukum.

Pengenalan wajah adalah cara mengenali wajah manusia melalui teknologi AI atau Artificial Intelligent, Sistem pengenalan wajah menggunakan biometrik untuk memetakan texture wajah dari foto atau video dan membandingkan informasi dengan database wajah yang dikenal untuk menemukan kecocokan.

Teknologi pengenalan wajah sebetulnya bermacam macam akan tetapi secara umum inilah cara kerja dan langkah langkahnya:

1. Gambar wajah anda diidentifikasi oleh kamera dari foto atau video.
2. Proses mengubah informasi analog (wajah) menjadi satu set informasi digital (data) berdasarkan fitur wajah seseorang dengan bantuan perangkat lunak pengenalan wajah untuk membaca geometri wajah anda termasuk jarak antara mata anda dan jarak dari dahi ke dagu, perangkat lunak ini juga mengidentifikasi beberapa titik unik wajah yang merupakan kunci untuk membedakan wajah anda dan hasilnya menjadi identity yang unik untuk setiap wajah seseorang.
3. Identity wajah yang unik tersebut secara matematis



dibandingkan dengan database yang sudah simpan dalam database wajah atau dengan kata lain proses memverifikasi jika ada lebih dari dua wajah milik orang yang sama.

4. Penentuan wajah seseorang yang cocok dengan gambar yang ada dalam database sistem pengenalan wajah.



Solusi Facial Recognition

Sudah ada beberapa institusi dan perusahaan yang mulai menerapkan system pengenalan wajah untuk kebutuhan identifikasi dan akses control, beberapa contoh sebagai berikut:

- **Pintu masuk ke area bisnis atau area terbatas sebagai Access Control** : Implementasi akses control yang biasanya menggunakan kartu atau sidik jari dapat diganti dengan alat pengenalan wajah di sisi readernya.
- **Bandara** : Dengan penerapan sistem pengenalan wajah dapat memonitor orang yang datang dan pergi di bandara. Hal ini dapat dilakukan oleh Departemen atau Lembaga Negara untuk menggunakan teknologi dalam rangka mengidentifikasi orang-orang yang telah memperpanjang masa berlaku visa mereka atau mungkin sedang dalam penyelidikan kriminal.
- **Gerbang keberangkatan untuk Maskapai penerbangan** : Cara biasa yang mungkin terjadi saat ini adalah maskapai meminta petugas memeriksa boarding pass secara manual di gerbang sebelum

para penumpang naik ke pesawat, jika pemindai ini diterapkan maka pemeriksaan secara manual tidak akan dilakukan lagi namun cukup hanya dengan memindai penumpang menggunakan kamera.

- **Toko Retail** : Toko Retail dapat menggabungkan kamera dan pengenalan wajah untuk memindai wajah pembeli dengan tujuan yaitu mengidentifikasi pelanggan tetap/member atau mengidentifikasi karakter orang yang mencurigakan dan pengutil barang potensial yang sudah dalam pantauan.



- **Sosial Media** : Sebetulnya Facebook sudah menggunakan algoritma untuk melihat wajah ketika kita mengunggah foto ke platformnya, dan media sosial sebelumnya selalu tersebut bertanya apakah anda ingin memberi tag orang di foto anda ? Jika anda menjawab ya, maka hal itu akan membuat tautan ke profil mereka, dan Facebook dapat mengenali wajah dengan akurasi 98%.
- **Telepon Genggam** : Apple adalah salah satu yang pertama mengimplementasikan pengenalan wajah untuk unlock iPhone X, dan kini banyak telepon genggam lainnya yang juga punya fitur yang kurang lebih sama.

Keuntungan:

Dengan penggunaan pengenalan wajah berikut sejumlah benefit yang dapat dirangkum:

- Tidak perlu secara fisik bersentuhan dengan perangkat untuk otentikasi coba bandingkan dengan teknik otentikasi biometrik berbasis kontak lainnya seperti pemindai sidik jari, yang mungkin tidak berfungsi dengan baik jika tangan seseorang tidak bersih saat otentikasi.
- Membutuhkan lebih sedikit pemrosesan dibandingkan dengan teknik otentikasi biometrik lainnya.

- Mudah diintegrasikan dengan fitur keamanan yang ada.
- Akurasi bacaan telah meningkat dari waktu ke waktu.
- Dapat digunakan untuk membantu mengotomatiskan otentikasi.

Kesimpulannya Teknologi pengenalan wajah secara global sudah mulai dapat digunakan sesuai dengan kebutuhan dan teknologi ini terus dikembangkan untuk kecepatan dan keakuratan dengan tetap menjaga tingkat keamanan, privasi, dan kenyamanan tertinggi. Sistem pengenalan wajah juga sangat dengan mudah diintegrasikan dengan berbagai sistem akses control, dimana wajah kita menjadi 'tanda pengenal' atau 'credentials' kita untuk mendapatkan hak atau tidaknya dalam sistem keamanan.

Kelemahan:

Harus disadari semua teknologi tidak ada yang sempurna, ada titik-titik tertentu yang harus di-improve atau berimbas kepada masalah sosial dan privasi apalagi teknologi pengenalan wajah menjadikan wajah sebagai "data" yang bisa saja dapat digunakan secara tidak bertanggung jawab oleh pihak tertentu.

Berikut kelemahan teknologi pengenalan wajah:

1. Ketersediaan data gambar

Sulitnya untuk mendapatkan gambar wajah dengan berbagai macam pose seseorang pada usia yang berbeda-beda.

2. Waktu proses

Untuk mendapatkan tingkat akurasi yang tinggi dalam melakukan proses pengenalan wajah, diperlukan algoritma yang cukup kompleks sehingga diperlukan pengolahan menggunakan komputer khusus (super computer).

3. Proses penuaan

Terlalu banyak variasi wajah pada orang-orang di tingkatan usianya.

4. Usia

Dalam beberapa penelitian menuliskan jika tingkat akurasi pengenalan sangat bergantung pada usia subyek tersebut.

*/ Penulis : Taufiq Rahman (taufiq.rahman@acsgroup.co.id)

Implementasi jaringan Wireless LAN Outdoor di Pelabuhan Laut.

Indonesia merupakan negara maritim dan termasuk sebagai negara dengan laut terluas di dunia. Memasuki era industri 4.0, digitalisasi adalah keniscayaan yang harus hadir di setiap lini, termasuk industri pelabuhan guna mendorong peningkatan produktivitas dan daya saing berskala Internasional. Untuk mendukung hal tersebut pelabuhan laut di Indonesia telah mengembangkan infrastruktur Teknologi Informatika dengan mengimplementasikan jaringan Wireless LAN (WLAN). ACS Group turut serta dalam Project Infrastruktur Sistem Informasi di beberapa pelabuhan laut Nusantara, dimana dengan mengimplementasi jaringan Wireless LAN (WLAN) di outdoor atau lingkungan di luar ruangan dalam hal ini di daerah pantai dan di atas laut, tentunya perlu diperhatikan bahwa perangkat yang dipasang harus memiliki ketahanan suhu, hujan, korosi atau karat, kecepatan angin, kelembaban udara, debu dan sebagainya. Perangkat Extreme Network yang diimplementasikan pada proyek ini terbukti dan teruji menjawab tantangan di lingkungan luar ruangan dan berjalan dengan sangat baik dan handal untuk kecepatan data, jaringan stabil dan tahan gangguan. Perangkat Wireless LAN outdoor **Extreme Networks AP7562 access point 802.11ac** menjawab semua kebutuhan dan tantangan tersebut dalam mengamankan operasional pelabuhan dan menunjang efektivitas operasional dengan memberikan pengalaman mobilitas yang luar biasa bagi penggunaannya sehingga produktivitas bisnis di pelabuhan semakin meningkat.



Solution Day Industry 4.0

Step A Head for Industrial Automation System



Bertempat di Hotel Sahid Jaya Lippo Cikarang tanggal 10 Juli 2019, ACS Group menggelar Solution Day Industry 4.0 dengan tema “Step A Head for Industrial Automation System”. Bersama **KOMITKABE (Komunitas IT Karawang Bekasi)** acara ini tentunya sangat mendukung program pemerintah dalam melakukan revitalisasi industri di bidang manufaktur untuk mengimplementasi Industri 4.0 sebagai langkah strategis mencapai target menjadi 10 negara dengan perekonomian terbesar di dunia pada tahun 2030.

Pada acara ini ACS berbagi informasi mengenai Solusi teknologi RFID dan peranannya dalam aspek supply chain management khususnya pada perusahaan manufaktur. Kemudian produk Roambee sebagai solusi smart supply chain yang memanfaatkan teknologi internet of things (IoT). Solusi cerdas yang diintegrasikan ke dalam sistem keseluruhan dalam memberikan gambaran detail setiap proses yang dijalankan (visibility), otomatisasi melalui pemanfaatan teknologi IoT (automation), serta memberikan dukungan terhadap kontrol finansial melalui konsep pay-as-you-go (on-demand). Mulai

dari manajemen gudang secara real-time, akurat dan teroptimasi, hingga pengiriman barang yang lebih tepat waktu dengan mengetahui estimasi jalur perjalanan yang akan dilalui, penentuan berangkat dan tiba juga secara real-time. Secara detail solusi **Roambee** sudah dibahas pada Edisi 47 yang terbit bulan Juni lalu. Solusi produk lainnya yaitu **Zebra MotionWorks Asset** yang memberikan kemudahan untuk mengelola semua aset penting dalam bisnis Anda dan membuat keputusan bisnis yang hasilnya menjadi lebih baik. Dengan solusi ini proses manual dan downtime dapat dikurangi secara dramatis, sehingga dapat menghemat dana dan waktu. Solusi MotionWorks Material memungkinkan Anda mengelola penambahan material dan meningkatkan efisiensi penanganan material Anda berkat akuntabilitas, kemampuan pengukuran, dan komunikasi yang dapat diandalkan. Dan pada acara ini juga dipaparkan solusi **Nutanix** yang merupakan solusi cloud computing yang membawa enterprise cloud platform yang simple untuk membangun suatu data center sehingga IT bisa lebih fokus dalam memberikan masukan pada core bisnis dari suatu perusahaan.



Joint Event

National Hotel Information Technology Conferences 2019

HITA (Hotel Information Technology Association) Indonesia menggelar acara rutin 2 (dua) tahunan yang mengusung tema “National Hotel Information Technology Conferences 2019”. Acara yang digelar pada tanggal 13 Juli 2019 di Double Tree by HILTON, Cikini - Jakarta Pusat ini bertujuan untuk meningkatkan pengetahuan dan perkembangan Information Technology (IT) yang semakin penting terhadap industri perhotelan Indonesia di era Revolusi Industri 4.0. Persaingan bisnis antar hotel dewasa ini semakin ketat di Indonesia, bukan hanya dalam hal harga dan pelanggan/konsumen saja tetapi tentunya fasilitas teknologi yang kian dituntut untuk menunjang operasional hotel, kemudahan pelanggan membooking hotel secara online serta jaminan keamanan dan kenyamanan dalam mengakses WiFi saat mereka berada di Hotel tersebut.

ACS Group bersama **Aruba HPE** turut serta bergabung pada acara ini sebagai sponsor utama sekaligus mempresentasikan tentang “Mobile First for Hospitality, New Blueprint for Hotels”, teknologi Aruba yang menawarkan beragam solusi salah satunya adalah solusi



“Hotel Pintar” yang memungkinkan pelanggan hotel untuk check-in dan langsung menuju pintu kamarnya tanpa harus antri di resepsionis hotel. Dan fitur penunjuk jalan atau GPS dalam ruang memungkinkan pelanggan hotel menuju spot-spot yang ingin dituju dalam area hotel karena terhubung dan mengetahui lokasi dimana mereka berada, serta memungkinkan juga bagi para tenant untuk broadcast fitur advertising guna memberikan penawaran-penawaran yang menarik bagi para tamu hotel dan segala informasi mengenai produk yang ada di toko tersedia selalu 24 jam dan detail dengan kemudahan akses dari perangkat mobile pintar yang dimiliki oleh para tamu hotel.

KOLOM KETAWA

Suatu hari saat cuaca mendung, ada nenek seorang diri pergi ke pasar untuk membeli kebutuhan sehari-hari, lalu hujan pun mulai turun, nenek yang mau pulang pun kebingungan, hingga ada tukang ojek menawarkan diri.

Tukang ojek : nek mau kemana nek ujan gini ngojek aja.

Nenek : iya boleh.

Tukang ojek : mau anterin kemana.

Nenek : anterin sampai rumah ya, deket ini di belakang pasar.

Tukang ojek : iya nek.

Didalam perjalanan pun nenek Nenek sempet dibikin kesel tukang ojeknya.

NENEK NAIK OJEK

Nenek : jangan ngebut-engebut dong

Tukang ojek : iya nek ini juga pelan gak ngebut

Nenek : kok masih ngebut, pelanin lagi donk

Tukang ojek : nenek lama lama bawel, saya ngebut juga gak mungkin sekenceng motor

Nenek : kenapa emang

Tukang ojek : saya kan tukang ojek payung

Nenek : hehe





Solution Day Industry 4.0

Digital Transformation in Palm Plantation

Dalam rangka percepatan implementasi Industri 4.0, Indonesia telah menyusun peta jalan (road-map) industri 4.0 dengan menetapkan lima sektor manufaktur yang akan menjadi prioritas utama dalam pengembangannya, salah satu prioritasnya yaitu pada industri makanan dan minuman.

Industri kelapa sawit, memiliki pangsa pasar besar dan menjadi salah satu penyumbang devisa terbesar dari sektor non-migas. Keberhasilan ini harus terus ditunjang oleh teknologi digital yang mumpuni antara lain penerapan Internet of Things (IoT), Artificial Intelligence (AI) dan Digitalized Infrastructure (DI) dan teknologi digital lainnya.

Melihat perkembangan tersebut ACS Group menyelenggarakan acara Solution Day - Industry 4.0 dengan tema "Digital Transformation in Palm Plantation" bertempat di Hotel Mercure Jakarta, pada tanggal 7 Agustus 2019. produk solusi yang disampaikan pada acara ini antara lain:

ABS sebagai solusi aplikasi yang komprehensif untuk direct performance management yang memasukkan unsur-unsur operasional, keuangan, dan agronomi. ABS memiliki software aplikasi seperti Program Mikro Makro Perkebunan (PMMP) dan Program Mikro Makro Pabrik (MMMP) untuk membantu perusahaan Minyak Sawit dalam mengejar pertumbuhan yang berkelanjutan. Aplikasi ini berbasis seluler yang mencakup integrasi GPS, geo-mapping, dan fitur-fitur canggih lainnya yang memberikan pemantauan secara real-time atas kinerja perkebunan. Sistem ini membantu menyederhanakan kegiatan manajemen sehingga mampu meningkatkan produktivitas.

Helios Mobility Suites (HMS) adalah sebuah solusi mobilitas untuk kebutuhan perusahaan yang dirancang dan dikembangkan berdasarkan dari hambatan yang dialami oleh klien kami dalam adopsi enterprise mobility. Solusi HMS dapat membantu mengatasi permasalahan

perusahaan dalam hal keamanan dan manajemen perangkat, serta meningkatkan produktivitas para pekerja di lapangan. HMS menyediakan solusi end to end, mulai dari solusi yang dapat mendukung produktivitas, manajemen hingga keamanan dari perangkat mobile anda. HMS juga dapat dengan mudah di integrasikan dengan aplikasi mobile anda. Dengan Helios Mobility Suites, anda dapat terus berinovasi dan mempercepat bisnis proses yang ada di perusahaan melalui solusi mobilitas yang ada di tangan anda.

Solusi **Sangfor** mencakup tiga perangkat solusi yaitu Internet Access Management yang digunakan untuk memberikan pengaturan yang efisien terhadap aktivitas akses internet. Solusi ini dibutuhkan mengingat saat ini hampir semua korporasi sudah terhubung dengan internet. Dengan semakin banyaknya aplikasi atau content di internet, maka pengaturan sangat diperlukan agar penggunaan akses internet sesuai dengan kebutuhan perusahaan.

Solusi ke dua yaitu WAN Optimization terkait dengan peningkatan performansi aplikasi. Hal ini biasanya terkait dengan kondisi dimana user-user yang ada di cabang mengakses aplikasi atau server yang terletak di data center melalui jaringan WAN. Komponen seperti latency dan bandwidth yang kecil biasanya menyebabkan akses menuju aplikasi akan terasa lambat. Dengan menggunakan solusi WAN Optimization maka akses aplikasi akan menjadi lebih cepat. Sedangkan SSL VPN adalah solusi untuk remote akses. Saat ini seiring dengan berkembangnya trend BYOD (Bring Your Own Device), kita dapat bekerja kapan saja dan dari mana saja. Biasanya pekerja yang bekerja secara mobile akan melakukan akses ke network perusahaan dengan metode remote akses. Dengan SSL VPN memungkinkan pekerja mobile mengakses resource perusahaan secara remote dengan aman, karena dilengkapi dengan beberapa fitur keamanan akses seperti autentikasi, host checker dan lainnya.



Honeywell Security

Prowatch System® Security Management Suite

Solusi untuk sektor industri : Kampus, Perkantoran, Healthcare, Manufaktur, Apartemen, Hotel, dll

Pro-Watch® Honeywell adalah software platform security untuk skala enterprise dan infrastruktur yang kritis. Sangat memungkinkan jika diintegrasikan dengan Video System dari Honeywell dan manufaktur lain dari pihak ketiga, untuk mendapatkan harga dan biaya yang lebih murah, juga kemudahan instalasi. Dengan client berbasis Web Pro-Watch, pelanggan dapat menggunakan infrastruktur jaringan yang ada untuk menyediakan manajemen keamanan jarak jauh untuk badging, pelaporan, alarm dan pemantauan kejadian. Pro-Watch mampu menyediakan opsi komprehensif untuk audit dan pelaporan dalam mengatasi kebutuhan forensik, dan kepatuhan. Aplikasi Pelaporannya mencakup template laporan dasar dan kemampuan untuk menghasilkan laporan khusus. File laporan bisa dalam format XLS, CSV, dan PDF.



Honeywell Security

LobbyWorks® Visitor Management Suite

Solusi untuk sektor industri : Kampus, Perkantoran, Healthcare, Manufaktur, Apartemen, Hotel, dll

LobbyWorks adalah System atau Software Visitor Management yang akan meningkatkan investasi system keamanan dan Access Control dengan menyediakan cara yang sederhana dan efektif untuk mendaftarkan karyawan baru, membuat kartu tamu, dan melacak pergerakan tamu. System ini mempunyai kemampuan untuk menghasilkan laporan pergerakan karyawan, tamu, secara detail. System ini juga digunakan untuk menegakkan aturan atau kebijakan keamanan tamu / kontraktor. Kehandalan dan fleksibilitas membuat LobbyWorks cocok untuk penggunaan skala kecil dengan menggunakan versi Express Edition atau skala besar berbasis WAN dengan menggunakan versi Premier Edition.



HPE Aruba

Aruba Instant On

Solusi untuk sektor industri : Semua sektor industri.

Dengan teknologi 802.11ac Wave 2 dari Aruba Instant On menghadirkan teknologi Wi-Fi yang mudah diimplementasikan dan fleksibilitas sehingga bisa terus ditingkatkan skalabilitasnya sesuai dengan kebutuhan dan perkembangan bisnis. Beberapa fitur yang menarik Aruba Instant On antara lain:

- Aplikasi mobile untuk kemudahan dalam instalasi tersedia di AppStore dan Google Play.
- Easy to use, pengelolaan dapat melalui aplikasi Mobile app atau portal web berbasis cloud (web-based management).
- Tingkat keamanan terbaik di kelasnya, telah mendukung protokol otentikasi terbaru seperti WPA2/WPA3
- Teknologi Smart Mesh untuk perluasan jaringan ke area yang sulit dijangkau dengan jaringan kabel
- Fleksibilitas dalam pemasangan, baik di plafon, di dinding, atau di atas meja, yang dapat disesuaikan dengan lingkungan bisnis perusahaan skala kecil dan menengah yang beragam.



Zebra Technologies
ZC300 Card Printer

Solusi untuk sektor industri : Ritel, Education, Hospitality & Banking.

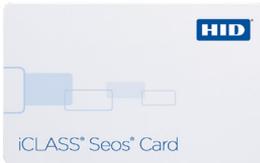
Printer ID Card Zebra ZC300 dengan bentuk slim yang mampu mencetak dua sisi dengan pita warna YMCKO untuk 200 kartu PVC secara cepat. Printer yang dilengkapi dengan layar LCD serta interface USB, Ethernet dan optional WiFi agar mudah digunakan bahkan kemudahan dalam penggantian pita karena didesain secara pas dan dengan smartchip yang sudah tertanam, Anda akan selalu tahu kapan harus mengganti pita.



Honeywell
Mobile Computer CK65

Solusi untuk sektor industri : Warehouse & Distribution.

Mobile Compter CK65 mampu mempercepat kinerja dan meminimalisasi kesalahan kerja di pusat-pusat distribusi dan gudang. Produk yang bermigrasi dari OS Windows® ke Android™ hadir dengan display 4" yang 2-3 kali lebih high resolution untuk mempermudah pembacaan dan lebih efisien. Memiliki battery 7000 mAh serta IP rating IP64, tahan terhadap debu, cipratan air dan benturan di atas beton sampai jarak 2,4 m.



HID
iCLASS® Seos™ Card

Solusi untuk sektor industri : Kampus, Perkantoran, Healthcare & Manufaktur.

HID iCLASS® Seos™ 13.56 MHz Smart Credentials hadir sebagai teknologi kartu pintar nirkontak(contactless) yang merupakan bagian dari platform iCLASS SE®, yang dirancang untuk menawarkan solusi "satu kartu" sejati untuk aplikasi kontrol akses fisik dan logical. Credentials dapat diprogram untuk akses membuka pintu dan mengakses sumber daya TI yang memang disediakan untuk mendukung aplikasi lain, termasuk One-Time Password Authentication (OTP) untuk login jaringan.



HID
HID® iCLASS SE® R10

Solusi untuk sektor industri : Kampus, Perkantoran, Healthcare & Manufaktur.

HID® iCLASS SE® R10 adalah network access control reader yang dapat digunakan untuk membaca kartu iClass (Smart Card) seperti membuka pintu. Reader ini didesain ramping dan minimalis serta mudah diintegrasikan dengan berbagai jenis network access controller. Disamping itu, iClass Reader juga menggunakan enkripsi untuk memberikan proteksi keamanan yang lebih baik dibandingkan dengan standar EM Card.

Reader iCLASS SE platform memiliki intelligent power management yang sudah ada di dalamnya sehingga mampu mengurangi konsumsi daya sebesar 59%.

Untuk penjelasan lebih detail lagi anda dapat menghubungi fitur chat kami di www.acsgroup.co.id.



ACS Group memperoleh Arward dari SAMSUNG & INGRAM

Pada bulan Agustus 2019 ini ACS Group memperoleh 2 Award sekaligus dari principal diantaranya dari SAMSUNG sebagai “Top Gold Partner 1st Half 2019 - Award ini diberikan pada acara tahunan “Samsung Partner Gathering 2019” yang berlangsung di Scenic 180” Resto & Lounge - Sahid Sudirman Centre.

Kemudian Award lainnya diperoleh dari principal INGRAM sebagai “Top IoT Partner 2018”. Penghargaan yang kami peroleh ini merupakan implikasi sebuah pengakuan tertinggi dari principal terhadap ACS Group. Penghargaan ini sekaligus menjadi cambuk bagi kami untuk lebih inovatif lagi dalam menghadirkan berbagai pelayanan yang berkualitas, terutama dalam menghadapi berbagai tantangan di masa depan.

ACS Group Representatif di Banten & Yogyakarta



Sejalan dengan perkembangan industri yang terus semakin bergerak maju, tentunya teknologi informasi akan sangat berpengaruh di era industri 4.0 untuk kelancaran dalam memproduksi barang, mengolah data dan menyebarkan informasi. Dalam perkembangan ini ACS Group di tahun 2019 ini mengembangkan sayap dengan membuka representatif untuk wilayah Banten dan Yogyakarta. Secara ekonomi wilayah Banten memiliki beberapa kawasan industri serta tersedianya pelabuhan laut untuk menunjang logistik & distribusi barang yang diproduksi oleh industri tersebut disamping itu adanya industri hospitality yang berkembang di propinsi ini. Yogyakarta juga merupakan kota pelajar dan juga terkenal dengan industri pariwisatanya, pertumbuhan fasilitas sekolah dan hospitality bertumbuh seiring dengan berkembangnya industri ini. Berharap ACS Group dapat berkontribusi melalui solusi empat pilar yang selama ini dapat berjalan sukses menjadi solusi tepat guna dalam peningkatan kinerja, efektivitas dan efisiensi .

Training Honeywell Security



Untuk menambah pengetahuan tentang produk Honewell Security beberapa sales dan enginner ACS Group tergabung dengan beberapa vendor mendapatkan training update produk - kali ini mereka memperoleh pengetahuan tentang controller PRO3000 IP-enabled. Produk ini merupakan panel accesss control canggih dengan arsitektur CPU 32-bit dan didukung oleh memori flash untuk firmware, protokol TCP / IP dan local cardholder database dengan kapasitas 55.000 dan transaction storage database sebesar 45.000 sehingga mampu memberikan solusi untuk aplikasi menengah hingga aplikasi besar. Kegiatan training ini mengambil tempat di Harrisma Informatika Jaya office - Jakarta.

RSA Conference 2019 Asia Pasific and Japan

RSA Conference 2019 Asia Pasific and Japan, adalah acara konferensi global dan eksposisi keamanan sistem informasi yang setiap tahunnya dihadiri puluhan ribu pengunjung yang terdiri dari para pemimpin, pakar dan industri dalam bidang keamanan sistem informasi. Tahun 2019 ini merupakan acara regional ke 7 di Singapura yang berlangsung pada tanggal 16-18 Juli 2019 untuk kawasan Asia Pasifik dan Jepang (APJ).

Selama tiga hari konferensi, menghadirkan 16 keynote speaker dan panelis serta 110 orang pembicara yang merupakan pakar keamanan sistem informasi, berfokus pada tema-tema seperti data governance and privacy, critical national infrastructure, artificial intelligence and blockchain, yang memberikan dampak pengaruh terhadap regional security landscape saat ini. Team Engineer ACS Group berkesempatan mengikuti event ini dan bergabung dalam industri cybersecurity ini guna memberdayakan industri cybersecurity secara kolektif untuk menghadapi dan mengatasi ancaman cyber di seluruh dunia dengan edukasi latest technologies dan hands-on educational sehingga dapat membantu para professional dan enterprise di Indonesia dalam mengamankan sistem informasi di perusahaannya.



Kick Off Meeting Untuk Proyek AMTS

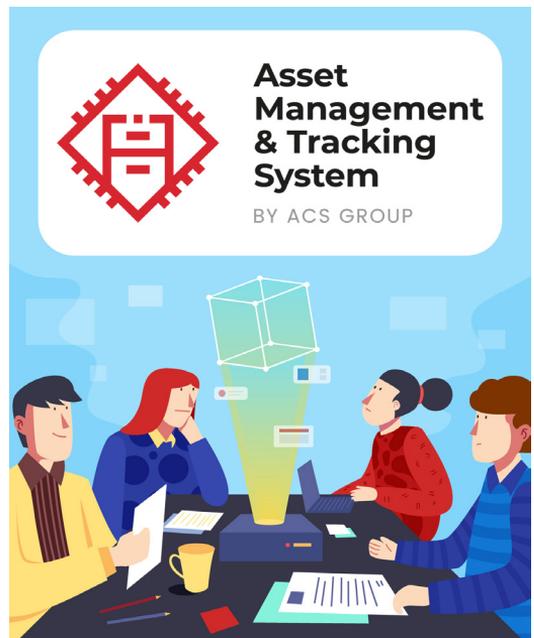
ACSGROUP melakukan kick-off meeting bersama tim pelaksana pengelola asset di salah satu perusahaan distribusi farmasi terbesar di Indonesia, dalam rangka penerapan software Asset Management and Tracking System.

Pada pertemuan ini membahas mengenai persiapan dan tahapan sehubungan pelaksanaan pengelolaan asset menggunakan aplikasi AMTS hasil pengembangan team engineer ACS Group sendiri.

AMTS merupakan aplikasi yang mudah diakses, bisa menggunakan banyak browser yang umum digunakan seperti Google Chrome, Mozilla Firefox, Internet Explorer, dan lain-lain.

Ada puluhan unit Zebra TC20 yang digunakan untuk mengakses AMTS versi Mobile, TC20 memiliki kecepatan scanning barcode dan pengolahan data yang baik, daya tahan baterai yang lama, tahan terhadap benturan dan percikan air maupun debu, menjadi pilihan device yang sangat optimal digunakan dalam proses pengelolaan aset di lapangan, seperti stock-opname atau audit asset.

Penggunaan Printer label Zebra GC420 dengan supplies Label Vinyl Yupo dan Ribbon Full-resin, juga merupakan pilihan yang tepat dan efektif untuk proses labeling asset.



CORPORATE & PRINCIPAL INFO

Hewlett Packard Enterprise(HPE) dan Nutanix(NTNX) Mengumumkan Kemitraan Global



Hewlett Packard Enterprise (HPE) dan Nutanix (NTNX) telah mengumumkan mengenai kemitraan global diantara mereka untuk menghadirkan solusi layanan cloud hybrid yang terintegrasi.

Hal ini memberi manfaat pada pelanggan dengan perangkat lunak Enterprise Cloud OS –nya Nutanix yang mana sudah termasuk didalamnya atau built-in, AHV hypervisor secara gratis, pada perangkat HPE GreenLake untuk solusi cloud hybrid yang dapat dikelola sepenuhnya, yang secara signifikan menurunkan total biaya kepemilikan dan mempercepat waktu proses serta memberikan nilai tambah.

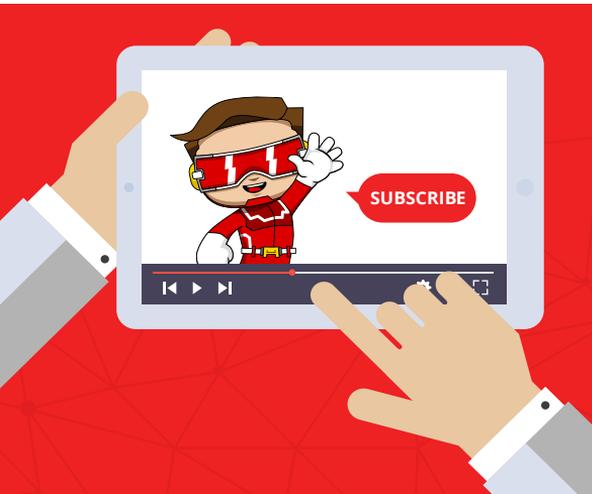
Dengan kerjasama ini maka server HPE dapat dikombinasi dengan Nutanix’s Enterprise Cloud OS software yang pembelannya sudah dalam satu integrated appliance.

Ingram Micro ONE APAC



Terletak di jantung pusat kota, di lantai 4 Raffles City Shopping Centre, Raffles City Convention Center, Ingram Micro mengadakan konferensi yang dihadiri oleh seluruh partner bisnisnya yang ada di Asia Pacific.

Tujuan dari konferensi ini adalah untuk memberikan pengetahuan dan wawasan tentang lanskap teknologi yang selalu berubah dan sangat dinamis, menampilkan solusi kolaboratif dan penawaran layanan kepada lebih dari 900 mitra strategis yang hadir dari seluruh wilayah APAC. Para peserta yang hadir dapat menyelami lebih dalam tentang tren Cyber Security, Cloud, Data Centre Transformation, Collaboration and Artificial Intelligence & Internet of Things sebagai kuncinya. ACS Group sebagai patner dari Indonesia turut hadir dalam acara akbar yang diisi oleh 8 keynote speaker.



SUBSCRIBE

ACS Group Youtube Channel

▶ PT Autojaya Idetech & PT Solusi Periferal (ACS Group)

Things that will you discover.

- Case Study
- Product Highlight
- Unboxing & Tutorial ... etc.



Scan this Qrcode



BEING **CERTIFIED** MEANS WE ARE **QUALIFIED** TO RUN HIGHER QUALITY JOB FOR YOU AS OUR VALUED CUSTOMER.



- Aruba Certified Design Professional (ACDP) V1
- Aruba Certified Mobility Professional (ACMP) V8
- Aruba Certified Switching Professional (ACSP) V1
- Cambium Networks ePMP Certified
- Cisco Certified CCNA
- CWNA Certified
- Extreme Network Certified
- Fortinet NSE Certified
- Hikvision HCSA Certified
- Honeywell Certified
- Microsoft Certified Professional (MCP)
- NCP Nutanix Certified Professional
- Nutanix Certified Systems Engineer: Level 1
- NCSR Nutanix Certified Sales Representative
- Samsung Knox Certified
- Zebra Technologies Certified
- Etc.

FIDO (Fast Identity Online)

FIDO adalah serangkaian spesifikasi dari keamanan sistem informasi untuk proses autentikasi yang kuat dan merupakan suatu teknologi agnostik yang memiliki kemampuan inter-operasi pada berbagai sistem. FIDO dikembangkan oleh FIDO Alliance, sebuah organisasi nirlaba yang mengupayakan standarisasi proses autentikasi pada client dan protocol layers.

Spesifikasi FIDO mendukung multifactor authentication (MFA) dan public key cryptography. Tidak seperti password database, FIDO menyimpan Personally Identifying Information (PII) atau informasi pengenalan pribadi, seperti data autentikasi biometrik, yang terletak secara lokal di perangkat pengguna untuk melindunginya. Biometrik FIDO dan identifikasi pribadi lainnya tersimpan secara local dimaksudkan untuk menjawab kekhawatiran pengguna tentang data pribadi yang disimpan di server eksternal di cloud.

Pemindai biometrik adalah alat yang menggunakan data biometrik untuk mengidentifikasi individu berdasarkan pengukuran karakteristik fisiologisnya. Karakteristik fisiologis ini memberikan kemampuan untuk mengontrol dan melindungi integritas data sensitif yang tersimpan dalam sistem informasi. Biometrik merupakan suatu metode komputerisasi yang menggunakan aspek-aspek biologi terutama karakteristik unik yang dimiliki oleh manusia.

Data biometrik yang mungkin digunakan antara lain sidik jari (fingerprint), retina, iris recognition, face recognition, DNA, palm print, hand geometry hingga pembuluh nadi (palm veins).

Dengan mengabstraksi implementasi protokol dengan Application Programming Interfaces (API), FIDO juga mengurangi beban pekerjaan yang diharuskan pada pengembang aplikasi untuk membuat login yang aman untuk mobile client yang berjalan dengan sistem operasi (OS) yang berbeda-beda pada berbagai jenis perangkat keras.

FIDO mendukung protokol Universal Authentication



Framework (UAF) dan protokol Universal Second Factor (U2F).

Pada protokol UAF, perangkat client akan membuat suatu key pair (pasangan kunci) yang baru selama pendaftaran dengan layanan online dan mempertahankan private key (kunci pribadi); sedangkan public key (kunci publik) sudah terdaftar dengan layanan online. Selama proses autentikasi berlangsung, maka perangkat klien harus membuktikan kepemilikan private key -nya ke layanan dengan beberapa cara, yang tentunya user-friendly action seperti memberikan sidik jari, memasukkan PIN, mengambil selfie, atau berbicara ke mikrofon.

Pada protokol U2F, proses autentikasi memerlukan faktor kedua yang kuat seperti menghubungkan Near Field Communication (NFC) atau dengan token keamanan USB (USB security token). Pengguna diminta untuk memasukkan dan menyentuh perangkat protokol U2F pribadi mereka selama proses login. Perangkat pengguna yang berkemampuan FIDO membuat key pair (pasangan kunci) yang baru, dan public key di-share dengan layanan online dan berkaitan dengan akun pengguna. Layanan kemudian dapat melakukan proses autentikasi pengguna dengan meminta agar perangkat yang terdaftar melakukan sign a challenge dengan private key.



*/ Penulis : Irvan Kurniawan(irvan@acsgroup.co.id)

8 TRENDS SHAPING IT INFRASTRUCTURE TODAY

The datacenter is no stranger to transformation. From storage to servers to software, IT infrastructure is a different beast now than it was years ago. Here's what's trending in infrastructure today.



01 FLASH STORAGE



IS FAST, DURABLE, RELIABLE, AND IT'S GETTING MORE AFFORDABLE

02 SOFTWARE

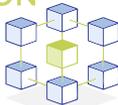
DEFINED DATACENTERS (SDDCs) ARE RISING, DELIVERING BETTER FLEXIBILITY WITH REDUCED COSTS



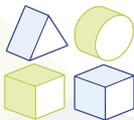
OF BUSINESSES SAY IMPLEMENTING AN SDCC STRATEGY IS AMONG THEIR TOP 3 INVESTMENT PRIORITIES

03 HARDWARE COMMODITIZATION

TODAY'S MOST POWERFUL STORAGE AND NETWORKING COMPANIES ARE ACTUALLY SOFTWARE COMPANIES



04 HYPERVISOR COMMODITIZATION



FEATURE-RICH HYPERVISORS ARE NOW A COMMODITY FOR MANY ORGANIZATIONS. SINCE THE GUARANTEED FEATURES ARE THERE, SWITCHING IS FAR MORE FEASIBLE

05 THE HYPERCONVERGED REVOLUTION

BRINGING CLOUD-LIKE POWER ON-PREMISES, HCI SIMPLIFIES DATACENTER ADMINISTRATION, DECREASES COSTS, AND INCREASES END-USER SATISFACTION



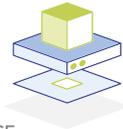
OF ORGANIZATIONS HAVE ADOPTED OR ARE CONSIDERING ADOPTING HCI

OF ORGANIZATIONS CITE HCI AS THEIR #1 INVESTMENT PRIORITY FOR 2019



06 MODERN APPLICATION ARCHITECTURES

BIMODAL IT MEANS CONFLICTING PRIORITIES, WITH MODE 1 RUNNING LEGACY APPLICATIONS AND MODE 2 RUNNING NEXT-GEN APPLICATIONS, IT MUST STRIKE A BALANCE



07 SECURITY EVOLUTION

ATTACKERS HAVE BECOME SMARTER, SNEAKIER, AND BOLDER, AND MICRO-SEGMENTATION IS EMERGING AS A VIABLE LINE OF DEFENSE

\$4M IS THE AVERAGE COST OF DATA BREACH

08 ADOPTION OF MULTI-CLOUD

WHILE MULTIPLE CLOUDS CAN ADDRESS MULTIPLE USE CASES, THEY CAN ALSO LIMIT VISIBILITY AND INCREASE COSTS

BY **2025** MULTI-CLOUD WILL BE THE NORM

4 PILLARS BUSINESS SOLUTIONS

ACS GROUP
PT. AUTOJAYA IDETECH
PT. SOLUSI PERIFERAL
www.acsgroup.co.id

Automatic Identification & Data Capture (AIDC)

- Barcode Scanner
- Enterprise Mobile Terminals / Computers
- Barcode Printers & Media
- Radio Frequency Identification (RFID)

IT Infrastructure

- Wired and Wireless Network
- Switches
- Aruba Clearpass - Network Access Control
- Unified Treat Management
- Hyper - Converge Infrastructure



Enterprise Security System

- Access Control
- Alarm System
- IP CCTV

Enterprise Business Solution

- Asset Management and Tracking System (AMTS)
- Document Asset and Tracking System (DATS)
- Mobile Meter Reading Solution (MMR)
- Agro Data Integration System (ADIS)
- Stability Program System (Stab-Pro)
- Gate Access System - Vehicle(GAS-V)
- STOCK KEEPER
- Chold Chain Monitoring System (CCMS)
- Laundry Tracking System (LTS)
- ABB Ability™ Ellipse®

BUSINESS PARTNERS



Jakarta (HO)

Perkantoran Gunung Sahari Permai #C03-05
Jl. Gunung Sahari Raya No 60-63 Jakarta 10610
Telp : +6221-4208221(H), 4205187(H)
Fax : +6221-4207903, 4207904, 4205853

Cikarang

Cikarang Square Blok E No 62, Jl. Raya Cikarang,
Cibarusah Km 40, Cikarang Barat, Bekasi
Telp : +6221.29612366, 29612367
Fax : +6221.29612368

Semarang

Grand Ngaliyan Square Blok B No.18,
Ngaliyan 50181, Semarang
Telp : +6224.76638092, 76638093
Fax : +6224.76638096

Surabaya

Komplek Ruko Gateway Blok D-27
Jl. Raya Waru, Sidoarjo 61254
Telp : +6231-8556277(H); 8556278
Fax : +6231-8556279

Denpasar

Ruko Grand Sudirman Agung Blok B No.29,
Jl. PB Sudirman, Dauh Puri Kelod,
Denpasar Barat, Denpasar - Bali 80114
Telp : +62361-4457859
Fax : +62361-4746526