# Perkhidmatan Capaian Terkawal Jarak Jauh Untuk Aplikasi HRMIS

Razale Ibrahim
*Fakulti Teknologi Sains Maklumat*
*Universiti Kebangsaan Malaysia*
*Bandar Baru Bangi, Selangor*
*Email: razale.ibrahim@yahoo.com*

## Abstract

*Pangkalan Data Aplikasi HRMIS terletak di Pusat Data HRMIS, Parcel C, Pusat Pentadbiran Kerajaan Persekutuan Putrajaya. Semasa ini pengguna HRMIS hanya boleh mencapai ke aplikasi tersebut melalui 4 rangkaian persendirian sahaja iaitu melalui:*

*a) Putrajaya Campus Network (PCN)*

*b) EG*Net yang telah diintegrasikan dengan PCN*

*c) integrasi rangkaian antara EG*Net dengan State*Net*

*d) integrasi rangkaian antara EG*Net dengan Intranet Agensi*

*Justeru itu, pengguna dari rangkaian persendirian lain yang tidak mempunyai integrasi rangkaian dengan EG*Net atau tidak mempunyai talian EG*Net tidak boleh mencapai aplikasi HRMIS. Ini merupakan cabaran utama yang dihadapi oleh JPA dalam usaha memperluaskan capaian aplikasi HRMIS dengan selamat terutamanya bagi Pejabat Kerajaan di luar negara.*

*Perkhidmatan atau teknologi capaian yang digunakan adalah perlu mengambilkira tahap keselamatan dan juga melibatkan kos yang berpatutan sejajar dengan bilangan kakitangan dan pejabat kerajaan di luar negara.*

## 1. Pengenalan

1.1 Terdapat kira-kira 1 juta warga perkhidmatan awam di Malaysia. Ini termasuk yang berkhidmat dengan Kerajaan Persekutuan, Kerajaan Negeri, Kerajaan Tempatan, Perguruan, Polis dan Tentera. Pegurusan sumber manusia di agensi-agensi ini melibatkan Jabatan Perkhidmatan Awam (JPA) dan pelbagai suruhanjaya perkhidmatan seperti Suruhanjaya Perkhidmatan Awam, Suruhanjaya Perkhidmatan Negeri dan Suruhanjaya Perkhidmatan Pelajaran.

1.2 Setiap Suruhanjaya bertanggung-jawab terhadap pemilihan dan pengambilan kakitangan awam di dalam skim perkhidmatan masing-masing. JPA pula bertanggung-jawab membangunkan polisi-polisi perancangan, pembangunan dan pengurusan sumber manusia awam. Sementara pelaksanaan dilakukan oleh agensi-agensi Kerajaan.

1.3 Dalam melaksanakan pengurusan sumber manusia, setiap Agensi bergantung kepada Sistem Pengurusan Sumber Manusia berkomputer atau menggunakan kaedah manual. Semua sistem ini beroperasi dan diuruskan secara sendirian tanpa ada sebarang integrasi. Akibatnya maklumat inter dan intra Agensi mahupun antara Suruhanjaya Perkhidmatan tidak dapat disatukan dan dimanfaatkan untuk memperbaiki sistem pengurusan dan operasi pengurusan sumber manusia perkhidmatan awam seluruh negara.

1.4 Untuk mengatasi masalah ini Kerajaan telah membangunkan satu Sistem Pengurusan Sumber Manusia yang boleh digunapakai oleh semua Agensi dan Suruhanjaya Perkhidmatan yang dikenali sebagai Aplikasi HRMIS (Human Resource Management Information System).

1.5 Aplikasi HRMIS ialah salah satu Aplikasi Perdana EG yang dilaksanakan oleh Kerajaan yang berkonsepkan sistem terbuka dan fleksible. Ia dapat memperbaiki edaran maklumat dalam proses operasi dan pengurusan sumber manusia (HRM) Kerajaan.

1.6 Disamping itu HRMIS juga mempunyai matlamat-matlamat berikut:

Mencapai satu saiz perkhidmatan awam yang optimum melalui penggunaan maklumat HRM mengautomasi proses operasi HRM Mendapatkan maklumat HRM yang terkini dan tersatu supaya perancangan HRM di antara Agensi lebih efektif Memperbaiki komunikasi, integrasi melintang dan proses yang lebih kemas (streamlined processes) melalui satu persekitaran sistem kolaborasi antara Agensi supaya hanya ada satu sistem capaian ke atas transaksi HRM; dan ini dapat digunapakai oleh semua Agensi Memperbaiki kebolehan pengurusan sumber manusia tanpa-kertas antara Agensi seperti pengedaran elektronik manual polisi sumber manusia dan pekeliling

rbi
9 Ogos 2009

## 2. Keperluan

### 2.1. Keperluan Organisasi

2.1.1 JPA telah mensasarkan 2 kumpulan yang unik yang perlu menggunakan HRMIS pada tahun hadapan. Dua kumpulan tersebut adalah kakitangan Kerajaan di luar negara dan kakitangan sekolah yang mewakili lebihkurang 30

2.1.2 Kakitangan Kerajan di luar negara tidak boleh menggunakan aplikasi HRMIS kerana ketiadaan talian EG*Net.

Begitu juga dengan 300,000 warga guru yang tidak dapat mencapai ke aplikasi HRMIS kerana tiada integrasi rangkaian di antara EG*Net dan School*Net.

2.1.3 Disebabkan masalah ini HRMIS tidak dapat dicapai oleh kakitangan Kerajaan secara meluas. Ini menyebabkan perancangan JPA untuk memastikan aplikasi ini digunakan oleh semua kakitangan Kerajaan tidak dapat dicapai dalam tempoh terdekat.

2.1.4 Bagi kakitangan luar negara, salah satu cara untuk mereka mencapai aplikasi HRMIS ialah dengan menyediakan talian EG*Net Global. Walaupun penyelesaian ini adalah selamat namun ia melibatkan kos yang amat tinggi. Penyelesaian alternatifnya pula ialah capaian melalui rangkaian Internet. Ini dapat mengurangkan kos rangkaian. Bagaimanapun penggunaan rangkaian Internet pula mempunyai risiko keselamatan yang tinggi.

### 2.2. Keperluan Teknikal

2.2.1 Cadangan penyelesaian perlu memenuhi keperluan teknikal berikut:

(a) Aplikasi HRMIS dapat dicapai oleh kakitangan Kerajaan yang berkhidmat di luar negara. Ini termasuk 103 kedutaan dan konsular negara, pejabat Kementerian Industri dan Perdagangan Antarabangsa (MITI), dan pejabat-pejabat Kerajaan yang lain yang berada di luar negara.

(b) Aplikasi HRMIS dapat dicapai oleh kakitangan kerajaan yang berkhidmat di pusat-pusat pendidikan yang dihubungkan melalui SchoolNet.

(c) Aplikasi HRMIS boleh dicapai oleh kakitangan yang melata. Ini termasuk kakitangan yang sering bergerak (mobile user). Justeru itu, ia perlu memenuhi keperluan pengkomputeran melata (ubiquitos computing).

(d) Tiada kompromi dengan keselamatan ICT. Ini termasuk hanya kakitangan yang dibenarkan sahaja boleh mencapai apliksai HRMIS dan memastikan komputer yang mencapai aplikasi HRMIS memenuhi polisi keselamatan yang minimum seperti mempunyai perisian anti-virus.

(e) Kos yang efektif.

## 3. Cadangan Penyelesaian

**3.0.1. Objektif Cadangan Penyelesaian.** 3.1.1 Objektif cadangan penyelesaian ialah untuk menyediakan satu perkhidmatan capaian untuk membolehkan kakitangan Kerajaan di luar negara dan kakitangan sekolah mencapai ke aplikasi HRMIS tanpa mengkompromi keselamatan aplikasi HRMIS dengan kos yang berpatutan.

### 3.1. Skop Penyelesaian

3.2.1 Skop penyelesaian adalah seperti berikut:

(a) menyediakan satu perkhidmatan capaian untuk membolehkan kakitangan Kerajaan di luar negara dan kakitangan sekolah mencapai ke aplikasi HRMIS tanpa mengkompromi keselamatan sistem maklumat dan komunikasi.

(b) menyediakan perkhidmatan direktori yang diintegrasikan dengan perkhidmatan kawalan capaian yang dicadangkan dan HRMIS (jika diperlukan)

(c) melatih pegawai HRMIS menggunakan perkhidmatan capaian yang dicadangkan melalui kaedah melatih jurulatih utama (train the trainers). Melalui kaedah ini jurulatih utama HRMIS boleh melatih pengguna-pengguna HRMIS.

(d) Menyediakan perkhidmatan sokongan termasuk meja bantuan kepada pengguna-pengguna HRMIS, sistem perkhidmatan capaian, perkhidmatan direktori dan sistem integrasi direktori perkhidmatan capaian yang dicadangkan dengan direktori HRMIS (jika ada).

(e) Menyambungkan LAN dan WLAN sekolah ke SchoolNet.

### 3.2. Alternatif Penyelesaian Teknikal

3.3.1 Terdapat 4 penyelesaian alternatif untuk memenuhi keperluan MAMPU dan JPA dalam memastikan kakitangan Kerajaan dapat mencapai aplikasi HRMIS.

(a) Perkhidmatan EG*Net Global

(b) Perkhidmatan IP-Sec

(c) Perkhidmatan Kawalan Capaian dengan klien

(d) Perkhidmatan Kawalan Capaian tanpa klien atau SSL-VPN

3.3.2 Bagi setiap cadangan alternatif, kami membuat analisa dari 6 sudut iaitu:

i. Kos (cost) perbelanjaan harta modal dan kos pengurusan

ii. Pengkomputeran melata (ubiquitous computing) pengguna boleh mencapai aplikasi HRMIS dengan mudah, tidak kira di mana dia berada

iii.Prestasi capaian (access performance) adakah capaian ke aplikasi HRMIS pantas atau perlahan.

iv. Pengurusan kos dan masa pentadbir dalam menguruskan penyelesaian

v. Pengalaman pengguna (user experience) pengguna mudah untuk mencapai aplikasi HRMIS tanpa banyak kerenah atau kekangan.

vi. Keselamatan (security) risiko keselamatan apabila penyelesaian dilaksanakan

3.3.3 Perkhidmatan EG*Net Global

3.3.3.1 Asas perkhidmatan ini ialah sama seperti perkhidmatan IP-VPN EGNet. Perbezaannya ialah pejabat Kerajaan di luar negara dihubungkan melalui satu rangkaian IP-VPN antarabangsa dengan last mile litar suwa atau jalur lebar. Pejabat-pejabat Kerajaan di Madinah, London dan Tokyo dihubungkan ke satu rangkaian IP-VPN yang di kenali sebagai EG*Net Global. EG*Net Global pula dihubungkan ke EG*Net melalui gateway GITN di Cyberjaya.

3.3.3.2 Seperti rangkaian EG*Net tempatan, EG*Net Global adalah satu rangkaian IP-VPN persendirian (Intranet), bukan IP-VPN melalui rangkaian awam (Internet). Ia

diintegrasikan dengan EG*Net tempatan di gateway Cyberjaya. Memandangkan ia adalah satu rangkaian persendirian, kosnya amat tinggi. Namun begitu, di segi keselamatan, ia memberikan peace of mind kepada pentadbir yang rangkaiannya adalah selamat daripada penggodam luar dan serangan penjenayah siber.

3.3.3.3 Melalui integrasi ini pengguna di Madinah boleh mencapai aplikasi HRMIS seperti ia berada di dalam LANnya sendiri. Disegi prestasi ia lebih baik dari penggunaan Internet kerana dalam konsep rangkaian Intranet, trafik boleh dikawal jalan laluannya (route path). Lebih lagi, ia tidak berkongsi dengan trafik lain.

3.3.3.4 Pengkomputeran melata adalah terhad kerana ia hanya boleh digunakan ketika kakitangan Kerajaan berada di pejabat-pejabat yang disediakan dengan talian EG*Net Global.

3.3.4 Perkhidmatan IP-Sec

3.3.4.1 Terdapat 2 komponen utama dalam membentuk penyelesaian IP-Sec. Pertama, peralatan yang akan membuat terowong perhubungan di antara tempat capaian dengan gateway capaian. Sebagai contoh, dari Pejabat Pesuruhjaya di Madinah ke gateway EG*Net di Cyberjaya. Kebiasaannya peralatan yang digunakan ialah firewall. Kedua, rangkaian kawasan luas (wide area network).

3.3.4.2 Salah satu nilai cadangan utama (main value proposition) IP-Sec ialah ia lebih murah daripada penyelesaian rangkaian persendirian seperti EG*Net Global. Kos yang lebih murah hanya boleh dicapai dengan menggunakan rangkaian Internet. Tetapi kelemahan IP-Sec ialah di segi keselamatan dan pengurusan.

3.3.4.3 Oleh kerana IP-Sec menggunakan Internet, ia boleh digodam, dihidu (snif) dan dipasang telinga (eavesdropping) oleh penjenayah siber (cyber terrorists). Bagi organisasi yang mementingkan keselamatan, IP-Sec bukanlah pilihan utama mereka walaupun ia murah.

3.3.4.4 Konsep asas Internet ialah penggunaan bersama lebar jalur rangkaian (shared bandwidth). Bermakna, sesuatu paket data perlu mencari route yang paling sesuai untuk ia tiba ke sesuatu destinasi. Sekiranya ia bertembung dengan satu nod Internet yang sibuk dan sesak, ia akan mencari nod Internet lain. Sesuatu paket Internet tidak mementingkan tempoh yang diperlukan untuk tiba ke destinasi. Yang lebih penting baginya ialah ia telah tiba ke destinasi walaupun ia mengambil masa yang lama. Bagaimanapun, sekiranya masa yang diambil terlalu lama, paket tersebut akan hilang dalam perjalanan. Ini menyebabkan laman web yang dimuat turun tidak dapat dipaparkan di skrin komputer.

3.3.4.5 Terdapat 3 cabaran utama pengurusan penyelesaian IP-Sec ini. Pertama, setiap tempat mesti mempunyai firewall dan ini perlu di beli (harta modal), dikonfigurasikan, dipasang dan kemudian diselengarakan. Kos dan masa yang perlu digunakan untuk penyelesaian ini akan menyebabkan pentadbir IP-Sec berkerut dahi.

3.3.4.6 Kedua, Internet itu sendiri tidak boleh diuruskan kerana ia berkonsep terbuka dan bebas. Ini bermakna organisasi tidak boleh menentukan bagaimana paket data bergerak apabila ia berada di dalam rangkaian Internet. Paket tersebut akan menentukan arah perjalanannya sendiri. Justeru itu pentadbir IP-Sec tidak boleh memaksa paket IP-Sec bergerak dengan efisien. Kesannya, prestasi rangkaian akan menurun.

3.3.5 Perkhidmatan Kawalan Capaian dengan klien (IP-Sec VPN)

3.3.5.1 Teknologi kawalan capaian dengan klien atau juga dikenali sebagai IP-Sec VPN memerlukan komputer dipasang dengan klien. Klien ini akan bertindak sebagai rujukan dan kawalan komunikasi di antara komputer dengan perkakasan kawalan capaian di gateway. Sebagai contoh, perhubungan di antara komputer di London dengan gateway di Cyberjaya. Apabila perhubungan dan pengesahan di kedua-duanya tempat telah wujud, barulah pengguna boleh menggunakan pelayar untuk mencapai aplikasi HRMIS di Putrajaya.

3.3.5.2 Seperti teknologi IP-Sec, klien yang digunakan merupakan cabaran utama penyelesaian ini kerana klien tersebut perlu dibeli, dikonfigurasikan, dipasang dan seterusnya perlu diselenggrakan. Ianya lebih rumit untuk diuruskan kerana klien berada di dalam komputer dan bagi pengguna melata, pentadbir sukar menjejaki di manakah mereka berada supaya pengurusan klien dapat dijalankan dengan baik.

3.3.5.3 Seperti IP-Sec, penyelesaian ini biasanya digunakan melalui rangkaian Internet. Oleh itu, semua masalah yang dibincangkan mengenai IP-Sec juga tepakai dengan penyelesaian ini.

3.3.5.4 Masalah lain yang sering dihadapi oleh penyelesaian ini ialah keperluan konfigurasi antara rangkaian Internet dengan rangkaian persendirian. Ini termasuk Terjemahan Alamat Rangkaian (NAT  Network Address Translation) dan pembukaan port-port keselamatan. Ia akan menjadi lebih kompleks apabila oa melibatkan 2 rangkaian persendirian. Ini kerana trafik permulaan (source) dan trafik destinasi perlu membuat pengesahan (authenticate) supaya perhubungan dapat diwujudkan (established communication).

3.3.5.5 Sebagai contoh, jika klien berada di dalam rangkaian persendirian, rangkaian persendirian itu perlu membuka port tertentu dan juga memastikan NATing dibuat dengan betul. Apabila tiba di destinasi rangkaian persendirian, rangkaian tersebut perlu membuka port tertentu dan membuat NATing ke rangkaiannya pula.

3.3.6 Perkhidmatan Kawalan Capaian Tanpa Klien atau SSL-VPN

3.3.6.1 SSL-VPN adalah satu perkhidmatan kawalan capaian tanpa klien melalui jarak jauh. Secara konsepnya ia adalah sama seperti IP-Sec VPN. Perbezaannya ialah pada klien. Penyelesaian ini tidak memerlukan sebarang klien khas. Sebaliknya ia hanya menggunakan pelayar popular seperti Mozilla, Internet Explorer ataiu Safari. Dengan cara ini ia menyelesaikan masalah utama IP-Sec VPN iaitu memasang, mengkofugurasi dan menyelenggara klien IP-Sec

VPN di komputer. Inilah manfaat utama SSL-VPN tanpa mengkompromikan keselamatan capaian.

3.3.6.2 Peralatan SSL-VPN dipasang pada gateway Cyberjaya. Pengguna hanya perlu melancarkan pelayar Mozilla (sebagai contoh) untuk berhubung dengan peralatan SSL-VPN. Selepas mendapatkan pengesahan, pelayar tersebut boleh mencapai aplikasi HRMIS.

3.3.6.3 Dalam keadaan tanpa klien, bebanan pentadbiran untuk menyediakan kemudahan inter-operasi (interoperability) dengan aplikasi yang memerlukan penggunaan klien seperti SAP dapat diselesaikan. Justeru itu, capaian ke aplikasi seperti HRMIS dapat dibuat dengan menggunakan sebarang komputer yang mempunyai talian Internet.

3.3.6.4 Cabaran-cabaran lain seperti yang dibincangkan sebelum ini juga dapat diatasi kerana semua komunikasi menggunakan port-port http dan https. Ini adalah port-port yang dibenarkan oleh semua firewall.

3.3.6.5 Walaupun SSL-VPN dapat menyelesaikan masalah IP-SEC dan IP-Sec VPN, namun penggunaan Internet sebagai rangkaian perhubungan akan tetap mengundang masalah-masalah yang telah dibincangkan sebelum ini.

3.3.6.6 Justeru itu, pilihan terbaik ialah penyelesaian dengan menggunakan SSL-VPN yang melibatkan kos yang efektif dan memenuhi ciri-ciri keselamatan dan pengkomputeran melata.

## 4. SSL-VPN

4.1 SSL-VPN adalah satu perkhidmatan kawalan capaian tanpa klien melalui jarak jauh. Ia membolehkan pengguna, peralatan dan rangkaian dicapai dengan selamat. Penyelesaian ini tidak memerlukan sebarang klien khas.

4.2 Untuk mencapai ke aplikasi HRMIS, pengguna tidak memerlukan sebarang klien khas. Sebaliknya ia hanya menggunakan pelayar popular seperti Mozilla, Internet Explorer atau Safari untuk berhubung dengan peralatan SSL-VPN di Gateway GITN, Cyberjaya. Selepas mendapatkan pengesahan, pelayar tersebut akan dibenarkan untuk mencapai aplikasi HRMIS secara automatik mengikut polisi kawalan capaian (access control policy) yang ditentukan.

4.3 Dalam Model OSI, perkhidmatan SSL-VPN ini dicapai melalui Lapisan 3. SSL menyediakan perkhidmatan encryption di Lapisan 6. Semua trafik diencrypt dengan menggunakan port 443 untuk memastikan keterhubungan yang selamat.

4.4 SSL VPN akan mengawal capaian dengan mengumpul maklumat dan mengambil tindakan berikut:

Mengesan mengesan apakah yang beroperasi di peralatan end-point . Ini termasuk pelayar yang digunakan, perisian anti-virus, pangkalan data anti-virus yang telah dikemaskini, sijil digital atau peralatan yang sah sahaja.

Pertahanan mempertahan aplikasi yang dicapai dengan menggunakan kawalan capaian. Kawalan capaian akan mengikut pengenalan pengguna dan integriti peralatan yang digunakan. Melalui kawalan ini pengguna hanya akan dapat mencapai aplikasi yang dibenarkan sahaja.

Perhubungan menghubungkan pengguna secara selamat dan mudah ke aplikasi yang dibenarkan.

4.5 Salah satu masalah utama dengan penggunaan SSL-VPN ialah perkomputeran melata. Pengkomputeran melata bukan sahaja bermaksud pengguna-pengguna boleh mencapai aplikasi HRMIS di mana-mana, tetapi mereka boleh menggunakan apa saja komputer. Apabila menggunakan sebarang komputer, komputer yang digunakan tidak semestinya selamat. Mungkin komputer tersebut merupakan tapak pelancaran malware. Ini adalah risiko yang terpaksa diambil apabila menggunakan penyelesaian ini.

4.6 SSL-VPN mengurangkan masalah ini dengan menguatkuasakan polisi keselamatan. Ia boleh mengesan komputer yang tidak mempunyai anti-virus dan menghalang komputer tersebut daripada mencapai aplikasi HRMIS. Ini merupakan pertahanan pertama untuk mengurangkan serangan malware atau penggodam ke atas aplikasi HRMIS.

4.7 Masalah lain yang dibawa oleh pengkomputeran melata ialah maklumat transaksi selalunya tertinggal di ingatan cache pelayar. Seseorang yang mahir boleh mencari fail-fail sementara itu dan mungkin meyalahgunakan maklumat-maklumat tersebut untuk kepentingan diri.

4.8 Untuk memastikan maklumat-maklumat di ingatan cache pelayar tidak disalahgunakan, teknologi SSL-VPN boleh menghapuskan ingatan cache, sejarah, cookies dan kata laluan apabila pengguna mematikan pelayarnya dan melog keluar.

## 5. Kesimpulan

Perkhidmatan Capaian Terkawal Jarak Jauh untuk apliksi HRMIS dengan menggunakan SSL-VPN diharapkan dapat meningkatkan penggunaan dan pengemaskinian data oleh kakitangan kerajaan di luar negara dan kakitangan perkhidmatan perguruan dengan menggunakan kemudahan internet sedia ada.

## Penghargaan

Terima kasih diucapkan kepada Encik Asmadi Md Saleh (Ketua, Perancangan Perundingan, StrICT) dan Adzril Adnan (Eksekutif, Perancangan Perundingan, StrICT) dari Syarikat GITN Sdn. Bhd. kerana membekalkan maklumat-maklumat yang diperlukan dalam penulisan ini.