INFORM : Jurnal Ilmiah Bidang Teknologi Informasi dan Komunikasi
Vol.3 No.2, Juli 2018, P-ISSN : 2502-3470, E-ISSN : 2581-0367

Security Management Implementation in Cloud Server

Awang Andhyka[1], Fawaidul Badri[2]

[1,2] *Program Studi Sistem Informasi Universitas Nahdlatul Ulama Sidoarjo*

[1] awang85.si@unusida.ac.id

[2] fawaid90.ti@unusida.ac.id

Abstract— The need of servers is currently growing rapidly. Every company or school needs a server to store electronic data properly. As for email and Information Systems with cloud servers, it is expected to be accessible to users from anywhere. But in building a server there are several security problems that often occured, such as the server being hacked, and causing the data to be lost. From these problems, a study was made to produce a discussion of security management in a cloud server with a minimum cost that can be applied to a company or campus or another. In scanning security on the cloud server, Android authentication can be used. Each root user will log in to the cloud server, then Android authentication will send a data. Apart from android authentication, security can use firewall ip tables in the cloud server and added with SSL (Secure Socket Layer), in every data from, and, to the encrypted server.
Keywords— Server, Security, Authentication, Cloud Server, Secure Socket Layer, Firewall.

Abstrak— Kebutuhan akan server saat ini berkembang pesat. Setiap perusahaan atau sekolah membutuhkan server untuk menyimpan data elektronik dengan baik. Seperti untuk email dan Sistem Informasi, dengan cloud server diharapkan dapat diakses pengguna dari manapun berada. Tetapi dalam membangun sebuah server ada beberapa masalah keamanan yang sering terjadi, seperti server dibobol, dan menyebabkan data server hilang. Dari permasalahan tersebut, dibuat suatu penelitian untuk menghasilkan pembahasan manajemen keamanan dalam cloud server dengan biaya minimum yang nanti dapat diterapkan pada suatu perusahaan atau kampus maupun yang lain. Dalam mengeloa keamanan pada cloud server dapat digunakan authentication android. Setiap user root yang akan login pada cloud server, kemudian authentication android akan mengirimkan sebuah data. Selain dari authentication android, pengamanan dapat menggunakan firewall ip tables di cloud server dan ditambahkan dengan SSL (Secure Socket Layer), di setiap data dari, dan, ke server yang dienskripsi.
Kata kunci— Server, Keamanan, Otentikasi, Server Cloud, SSL, Firewal.

I. PENDAHULUAN

Cloud Computing disebut juga sebagai layanan berjenis komputasi yang memiliki fokus pada proses bisnis dan layanan bidang Teknologi Informasi, sehingga proses bisnis yang dihasilkan dapat digunakan secara otomatis tanpa batas dalam penggunaan layanan Teknologi Informasi. Sebagai contoh teknologi komputasi adalah layanan berbasis arsitektur yang memiliki orientasi layanan (SOA) dan Layanan berbasis Web. SOA berfungsi memfasilitasi layanan teknologi informasi antara sistem terdistribusi untuk berkomunikasi dan bertukar data antar pengguna satu degnan yang lain [1]. sehingga menyediakan sarana yang seragam bagi pengguna layanan dan penyedia untuk menemukan dan menawarkan layanan masing-masing.

Hal demikian yang memunculkan berbagai penyedia layanan web yang berfungsi untuk bisnis yang dikelola secara mandiri dan beroperasi melalui Internet. Cloud computing menggunakan sumber daya sebagai komputasi dalam istilah ekonomi sehingga pengguna sumber daya harus membayar penyedia sumber daya untuk memanfaatkan sumber daya komputasi [2]. Oleh karena itu, cloud computing mampu memberikan manfaat, seperti menawarkan insentif bagi penyedia sumber daya untuk menyumbangkan sumber dayanya bagi orang lain untuk menggunakan dan mengambil untung darinya, mengatur pasokan dan permintaan sumber daya komputasi pada keseimbangan pasar, menawarkan insentif bagi pengguna sumber daya untuk mundur ketika diperlukan, menghilangkan kebutuhan untuk koordinator pusat (selama negosiasi antara pengguna dan penyedia untuk menetapkan kualitas harapan layanan dan harga layanan), dan memungkinkan baik pengguna dan penyedia untuk membuat keputusan independen untuk memaksimalkan utilitas dan laba masing-masing[3].

Cloud computing adalah solusi penyimpanan yang disediakan untuk pengguna dan perusahaan dengan berbagai fasilitas kemampuan untuk menyimpan serta memproses data mereka dalam lokasi yang dipusatkan dan dimiliki pihak ketiga [4]. Organisasi menggunakan Cloud dalam suatu variasi model layanan yang berbeda (SaaS, PaaS, dan IaaS) dan model penyebaran (Pribadi, Umum, Hibrida, dan Komunitas). Ada sejumlah keamanan kekhawatiran terkait cloud server[5].

Masalah-masalah dibagi dalam beberapa kategori besar sebagai keamanan yang dihadapi oleh penyedia cloud (organisasi menyediakan perangkat lunak, platform, atau infrastruktur sebagai layanan via cloud) dan masalah keamanan yang dihadapi oleh pelanggan mereka terdiri perusahaan serta organisasi pembuat aplikasi atau menyimpan data di cloud) [6]. Penyedia harus memastikan bahwa infrastruktur mereka aman dan aplikasi klien dilindungi, sementara pengguna harus mengambil tindakan untuk memperkuatnya pada login aplikasi dengan menggunakan kata sandi berdigit yang kuat dan langkah-langkah otentikasi harus digunakan [7].

DOI: 10.25139/inform.v3i2.1050

Ada banyak masalah keamanan untuk cloud komputasi karena mencakup banyak teknologi termasuk jaringan, basis data, operasi sistem, virtualisasi, penjadwalan sumber daya, manajemen transaksi, *load balancing*, konkurensi kontrol dan manajemen memori [8]. Oleh karena itu, masalah keamanan sangat dibutuhkan pada sistem dan teknologi berlaku untuk komputasi awan. Misalnya, jaringan itu interkoneksi sistem di awan harus aman.

Selanjutnya paradigma virtualisasi dalam hasil komputasi awan di beberapa keamanan mempunyai kekhawatiran. Misalnya, memetakan virtual mesin ke mesin fisik harus dilakukan dengan aman. Keamanan data melibatkan mengenkripsi data serta memastikan itu kebijakan yang tepat diberlakukan untuk data berbagi. Selain itu, alokasi yang digunakan sebagai sumber daya serta manajemen penggunaan algoritma pada memori harus aman[9].

VPN menggunakan enkripsi untuk memberikan kerahasiaan data. Sekali terhubung, VPN menggunakan *tunneling* mekanisme yang difungsikan untuk mengenkapsulasi data yang dienkripsi ke dalam terowongan yang aman, dengan header yang bisa dibaca secara terbuka menyeberangi jaringan publik. Paket melewati publik jaringan dengan cara ini tidak dapat dibaca tanpa benar kunci dekripsi, sehingga memastikan bahwa data tidak diungkapkan atau berubah dengan cara apa pun selama transmisi. VPN juga bisa memberikan pemeriksaan integritas data. Ini biasanya dilakukan menggunakan authentifikasi pesan untuk memberikan masukan bahwa data belum dirusak selama transmisi.

Secara default, VPN tidak memberikan atau menegakkan otentikasi pengguna yang kuat[10]. Pengguna dapat memasukkan data pengguna beserta kata sandi yang sederhana untuk digunakan akses ke jaringan pribadi internal dari rumah atau melalui yang lain jaringan yang tidak aman. Namun demikian, VPN tidak mendukung addon mekanisme otentikasi, seperti kartu pintar, token.

Dalam penelitian ini mengimplementasikan rancangan sistem keamanaan pada perpindahan data yang membahas masalah security dalam server dengan biaya minimum yang nanti dapat diterapkan pada suatu perusahan atau kampus maupun yang lain. Dalam memanagement security pada cloud server dapat digunakan authentication android, setiap user root yang akan login pada cloud server maka, *authentication android* akan mengirimkan sebuah data yang ada pada android sehingga dengan menghasilkan kode pada android yang digunakan oleh user.

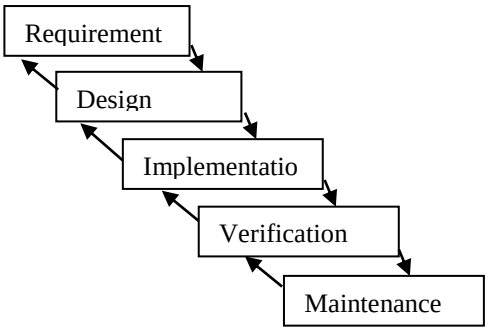
II. METODOLOGI PENELITIAN

Penelitian mempunyai beberapa tahapan dengan menggunakan metode waterfall yang sering digunakan, sehingga proses dan penggunaan dalam kebutuhan pada keamanan *cloud server* serta managemen mudah dipahami.

A. Requirement

Dalam penelitian ini, data inputan berupa *cloud serve*r yang digunakan sebagai server utama dan server data storage. Selain itu juga dibutuhkan android sebagai keamanan untuk menghasilkan kode agar sebelum user login, kode dapat digunakan.

Penggunaan enkripsi pada cloud juga dibutuhkan sebagai keamanan tambahan. Cloud server juga membutuhkan OS supaya dapat digunakan sebagai server dan Os yang paling mudah yaitu penginstalan OS linux versi Ubuntu.

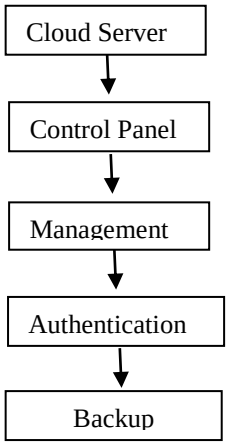


Gambar 1. Tahapan dan metode penelitian

Gambar 1. Merupakan tahapan dan metodelogi penelitian dari penelitian ini, berikut penjelasan dari masing-masing tahapan penelitian ini.

B. Design

Setelah *Cloud server* terdapat OS dan siap digunakan, maka untuk mempermudah dalam memanagement suatu cloud server dibutuhkan Kontrol panel. Berbagai macam Kontrol panel yang ada pada cloud server, dari yang berbayar sampai yang tidak berbayar, akan tetapi yang paling mudah digunakan dalam memanagement cloud server yaitu Kontrol panel berjenis plesk yang berbayar, hal tersebut dikarenakan plesk dapat berjalan pada versi windows dan linux, serta Kontrol panel virtualmin yang tidak berbayar. Kontrol panel plesk digunakan untuk memanagement pada cloud server utama, sedangkan Virtualmin digunakan pada *cloud server backup*. Agar mempermudah dalam pemahaman, berikut blok diagram desain pada penelitian ini seperti pada Gambar 2:



Gambar 2. Flowcart Design

DOI: 10.25139/inform.v3i2.1050

C. *Implementation*

Login root pada setiap cloud server sangat rawan terkena hack, karena akses user dan password dapat di duplikasi oleh pihak yang tidak bertanggung jawab.

Untuk melindungi hal tersebut maka di lakukan penginstallan security berupa authentication android pada root, sehingga pada saat user mengakses root akan diminta authentication android berupa sms, telepon ataupun menekan tombol pada android user yang memiliki akses ke *cloud server*.

Dengan adanya *authentication* android, setiap user yang tidak tersinkronisasi dengan cloud server dan tidak mempunyai authentication android tidak dapat mengakses login root pada cloud server.

D. Verification

Pada *management security* dilakukan firewall berupa ip tables yang meminimalkan ip address pada login root dibatasi. Hal selanjutnya yaitu merubah port dan menutup port untuk login pada root.

Selain itu juga menambah waktu pada proses pengambilan kode yang di hasilkan oleh android dengan waktu yang diberikan dan ditentukan seperti 30 detik, sehingga user tidak bisa berlama-lama dalam login user.

E. Maintenance

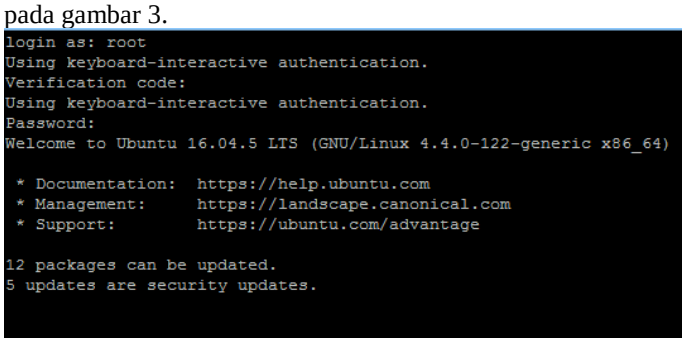
Untuk mendukung cloud server utama agar data tidak hilang jika terjadi hack, maka dilakukan penginstalan dan memanagement security pada cloud server kedua yang digunakan sebagai backup. Cloud Server ini juga digunakan sebagai data storage.

Setiap management security pada cloud server utama juga dilakukan pada cloud server kedua yaitu menggunakan authentication android.

Setelah cloud server utama dan cloud server backup siap digunakan dan telah di manage securitynya, maka dilakukan sinkronisasi pada kedua cloud server tersebut. Hari, tanggal, bulan serta jam digunakan sebagai ukuran dalam sinkronisasi data pada cloud server tersebut, sehingga pada saat terjadi backup data dapat dilihat beberapa hari sebelumnya.

III. HASIL DAN PEMBAHASAN

Hasil penelitian menurut metode waterfall dan block diagram diatas apabila diterapkan pada sebuah cloud server maka dapat digambarkan dengan login user yang terproteksi pada gambar 3.

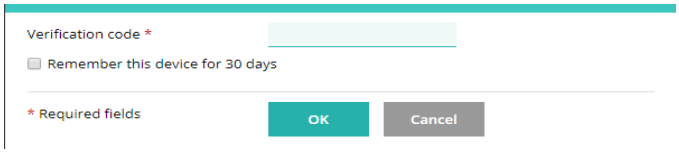


Gambar 3. Login root dengan authentication

Ketika setiap user pada saat login menginputkan nama maka akan muncul keamanan yang membutuhkan proteksi berupa sebuah kode yang diambil dari android. Kode tersebut digunakan untuk mengaktifkan siapa user yang akan mengakses tersebut.

Kode yang dihasilkan oleh android, dilakukan dan dibatasi dengan waktu 30 detik, apabila dengan waktu tersebut kode tidak dimasukan maka login user akan terputus dari server dan memulai kembali proses login seperti awal. Setelah kode dimasukan, maka dilanjutkan ke proses berikutnya yaitu memasukan *password*, yang nantinya apabila password sesuai akan muncul tampilan login seperti pada gambar 3.

Selain dari login dengan *root* apabila akan menggunakan Kontrol Panel Plesk, dapat juga digunakan android sebagai proteksi saat login seperti pada Gambar 4.



Gambar 4. Login kontrol panel plesk dengan authentication

Verifikasi yang dibutuhkan diambil pada android dengan sebuah kode yang mempunyai waktu yang sama pada server dan pada android, dengan kata lain apabila waktu berbeda maka kode yang dihasilkan pun akan berbeda yang mengakibatkan tidak dapat login.

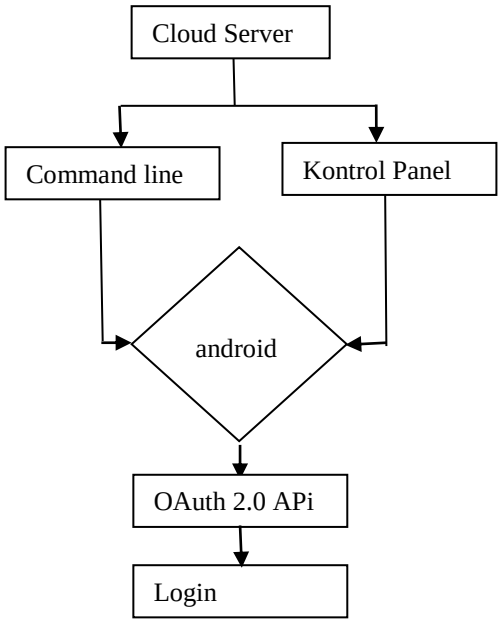
Keamanan yang sederhana tersebut sangat dibutuhkan dalam keamanan sebuah server, dimana sekarang ini sering terjadi kehilangan data, ataupun kerusakan data yang disebabkan dari berbagai macam kendala. Seperti di hack ataupun digunakan oleh orang lain. Verifikasi yang digunakan pun sangat mudah karena menggunakan google android authentification yang dapat diambil dari mana saja.

Penggunaan google android pun juga sudah umum, hanya saja penerapannya pada keamanan sebuah server yang sangat jarang diperhatikan pada umumnya. Kode yang dimasukan pun dapat disimpan dengan jangka waktu maksimal 30 hari, akan tetapi pilihan tersebut jarang digunakan karena apabila verifikasi disimpan, maka login pada kontrol panel plesk tidak membutuhkan authentication lagi, yang menyebabkan keamanan rentan untuk digunakan orang lain.

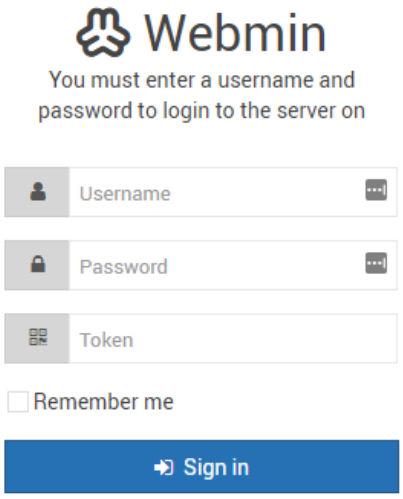
Pada dasarnya android menggunakan authentication yang dimiliki oleh google, dimana setiap data yang diakses berupa kode yang diminta dan diberikan melalui API (Application programming interface) pada google gambar 6.
Dalam kontrol panel webmin pun juga dapat digunakan authentication, seperti contoh pada gambar 6. Token menjelaskan bahwa untuk login, user juga membutuhkan password dan kode authentication yang diambil dari android. Kode tersebut digunakan berdasarkan API yang sudah disediakan oleh google. Selain itu pembuatan kode juga banyak tersedia yang bersifat open source sehingga dalam

DOI: 10.25139/inform.v3i2.1050

penggunaanya lebih mudah. Dari berbagai macam percobaan yang telah dilakukan dapat dikatakan bawah authentication memiliki fungsi yang penting sehingga memiliki beberapa perbedaan mendasar seperti pada tabel 1.



Gambar 5. Flowcart android API



Gambar 6. Login kontrol panel webmin dengan authentication

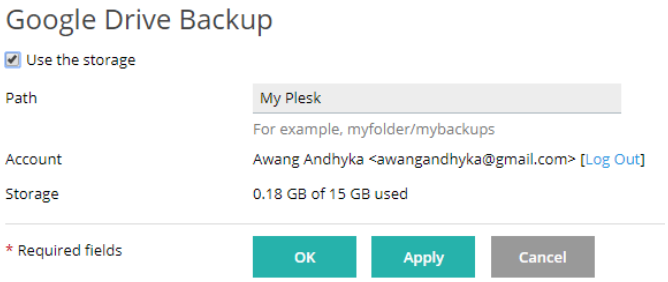
Tabel 1. Perbedaan authentication

Jenis	Authentication	Non authentication
Keamanan	Keamanan lebih terjaga	Lebih mudah di bobol
Waktu	30 detik harus login	Memudahkan untuk bruce force attack
User	Memiliki 3 step	Hanya dari password
Stabilitas	login token diambil dari android sendiri	Tidak memerlukan
Program	Lebih mudah pembuatan karena tersedia API	Tidak diperlukan

Tabel 1 menjelaskan bahwa authentication sangat dibutuhkan oleh setiap user dalam melakukan login. Selain dari itu, keamanan juga dapat ditingkatkan dengan adanya SSL (Security Socket Layer) sehingga setiap data yang akan, dan, ke alamat yang dituju telah dienskripsi. Apalagi google sekarang lebih ketat dalam menetapkan ada atau tidaknya sebuah server pada ssl. Penggunaan API juga dapat digunakan untuk backup sebuah server, user hanya membutuhkan sebuah program yang dapat dikoneksikan kedalam google drive melalui authentication API yang sudah disediakan.

Seperti pada gambar 7 menunjukan bahwa apabila setiap server tidak mempunyai ssl maka akan adanya warning dari web browser dan kurang aman dalam perpindahan data. Hal tersebut sangat dibutuhkan mengingat apabila backup data ke server lain akan membutuhkan biaya yang sangat besar dengan jumlah kapasitas seperti diatas 10000 gigabytes.

Gambar 7. Security Socket Layer



Gambar 8. Backup authentication google drive

Selain digunakan pada android authentication juga digunakan untuk backup server ke google drive seperti pada gambar 9. Penggunaanya menggunakan fungsi API yang telah disediakan, sehingga mempermudah dalam pembuatan koneksinya.

Tabel 2. Perbedaan authentication backup

Jenis	Google drive, dropbox	Server backup biasa
Keamanan	Keamanan lebih terjaga	Membutuhkan keamanan tambahan

DOI: 10.25139/inform.v3i2.1050

Jenis	Google drive, dropbox	Server backup biasa
Biaya	Murah, dan terjangkau dengan kapasitas 100000 Gigabytes	kapasitas hardisk besar yang mengakibatkan biaya bertambah
Maintenance	Sudah termasuk pada biaya	Membutuhkan user yang mengawasi
Stabilitas	Selalu online dan tidak error	Server mati, maka backup tidak berfungsi
Data	Tidak pernah error ataupun hilang	Server error, data rentan hilang

Perbedaan sederhana seperti tabel 2 yang menyebabkan backup dengan server sendiri membutuhkan biaya besar dan beresiko kehilangan data apabila server di restart ataupun mati.

IV. KESIMPULAN

Penelitian ini menghasilkan beberapa kesimpulan sederhana yang sering dilupakan oleh setiap user ataupun perusahaan yang menggunakan server. Beberapa hal yang sering dilupakan tersebut merupakan hal yang sangat penting, akan tetapi mudah dalam penggunaanya yaitu masalah keamanan dan *backup*. Secara sederhana keamanan dapat ditingkatkan dengan menggunakan *authentication* dari google yang dapat diunduh dengan mudah, selain itu penggunaan dalam authentication juga lebih mudah dalam pembuatan koneksinya karena sudah tersedianya API. Hal kedua yang sering dilupakan adalah masalah backup, dimana backup server sering kali menggunakan server tradisional, yang berakibat apabila server tersebut mati, maka server tidak dapat memberikan fungsi *backup*, dan juga kapasitas dalam backup server juga rawan dalam kehilangan, dikarenakan server hang ataupun *error*. Penyimpanan kapasitas data pun juga lebih besar dan dapat berlangsung lama apabila menggunakan authentication ke dalam backup server pada google drive, dropbox ataupun yang lain, dalam artian data akan tersimpan dalam jangka waktu yang sangat lama (lebih dari 10 tahun) tanpa takut kehilangan data ataupun rusak. Selain dari itu harga pun menjadi bahan pertimbangan, dengan adanya hal tersebut biaya menjadi lebih murah apabila dibandingkan menggunakan server *backup* tradisional ataupun server tunggal.

REFERENSI

[1] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, I. Brandic, "Cloud computing and emerging IT platforms: Vision hype and reality for delivering computing as the 5th utility", Future Generation Computer Systems, vol. 25, no. 6, pp. 599-616, 2009

[2] D. Abramson, R. Buyya, J. Giddy A computational economy for grid computing and its implementation in the Nimrod-G resource broker Future Generation Computer Systems, 18 (8) (2002), pp. 1061-1074

[3] International Journal of Information Security and Privacy, 4(2), 39-51, April-June 2010

[4] Jump up to:a b c d Haghighat, M., Zonouz, S., & AbdelMottaleb, M. (2015). CloudID: Trustworthy Cloud-based and Cross-Enterprise Biometric Identification. Expert Systems with Applications, 42(21), 7905–7916.

[5] Jump up to:a b Srinavasin, Madhan (2012). "'State-of-theart cloud computing security taxonomies: a classification of security challenges in the present cloud computing environment". ACM ICACCI'.

[6] Jump up^ "Swamp Computing a.k.a. Cloud Computing". Web Security Journal. 2009-12-28. Retrieved 2010-01-25

[7] Moretti, C., Steinhaeuser, K., Thainer, D., & Chawla, N. (2008). Scaling Up Classifiers to Cloud Computers. In Proceedings of the IEEE ICDM.

[8] Jones, M., & Hamlen, K. W. (2009). Enforcing IRM Security Policies: Two Case Studies. In Proceedings of the IEEE Intelligence and Security Informatics Conference (ISI)

[9] TS Chou, "Security threats on cloud computing vulnerabilities", International Journal of Computer Science & Information Technology, vol. 5, no. 3, pp. 79, Jun 2013.

[10] D. Abramson, R. Buyya, J. Giddy A computational economy for grid computing and its implementation in the Nimrod-G resource broker Future Generation Computer Systems, 18 (8) (2002), pp. 1061-1074.

DOI: 10.25139/inform.v3i2.1050