ANALIIS DAN IMPLEMANTASI IDENTITY MANAGEMENT DENGAN METODE ROLE BASED ACCESS CONTROL UNTUK WEB SERVICE

Yhudha Juwono[1], Maman Abdurrahman[2], Kemas Rahmat Saleh Wiharja[3]

[1]Teknik Informatika, Fakultas Teknik Informatika, Universitas Telkom

Abstrak

Teknologi informasi sudah menjadi bagian hidup manusia modern, posisinya bahkan sudah berubah menjadi kebutuhan pokok tiap individu. Ini ditandai dengan semakin banyaknya konten yang tersedia di internet dan perangkat yang digunakan untuk mengakses layanan pada internet.

Hadirnya teknologi informasi yang semakin banyak juga menimbulkan tantangan tersendiri bagi penyedia layanan. Salah satunya yang dibahas pada tugas akhir ini adalah pengelolaan identitas penggunanya didalam sistem / layanan internet. Pada tugas akhir ini dicoba untuk mempersempit lagi scope sistemnya, yaitu pengelolaan identitas yang dimiliki oleh organisasi / perusahaan / kelompok yang lebih kecil.

Organisasi memiliki anggota sesuai dengan jabatan atau fungsionalitas didalam organisasinya. Hal ini akan sangat membatu untuk mendefinisikan hak dan batasan identitas tadi menyesuaikan dengan role didalam organisasi. Dengan adanya atribut role yang diberikan pada user, maka sistem akan lebih mudah memberikan hak dan batasan terhadap aktifitas user dengan harapan mampu memberikan layanan sesuai dengan fungsinya pada organisasi dan membatasi pada hal-hal yang tidak seharusnya ditangani oleh anggota organisasi yang tidak berhak.

Berdasarkan implementasi sistem identity management dengan menerapkan metode Role Based Access Control untuk pengaksesan web service didapatkan hasil bahwa performansi pengelolaan data Identitas dalam hal manajemen lifecycle dapat tercapai dan dengan tingkat pengamanan yang lebih baik.

Kata Kunci : Role, Akses kontrol, Manajemen Identitas, Hak Akses, Web Service, lifecycle.

Abstract

Information technology has become a part of modern human's life, his position even been turned into a basic need of each individual. This is indicated by the increasing number of content available on the internet and the devices used to access services on the internet.

The presence of a growing number of information technology also poses a challenge for service providers. One of them is discussed in this thesis is the management of user identities within the system / internet services. In this final again attempted to narrow the scope of the system, the management of the identity of the organization / company / group smaller.

Organization has members in accordance with the position or functionality within the organization. It would be petrified to define the rights and restrictions had to adjust to the role of identity in the organization. With the attributes of a given user role, then the system will be easier to provide rights and restrictions on user activity in the hope of providing services in accordance with the organization's functions and limits on things that should not be handled by members of the organization are not eligible.

Based on the implementation of identity management systems by implementing Role Based Access Control method for accessing web services showed that the performance in terms of data management identity management lifecycle can be achieved and the level of security become better.

Keywords : Role, Access Control, Identity Management, Permission, Web Service, lifecycle.

1. Pendahuluan

1.1 Latar belakang masalah

Hadirnya sistem teknologi informasi menjadi kebutuhan yang menunjang bagi organisasi atau perusahaan dalam membantu proses bisnis yang terjadi didalamnya. Sistem atau aplikasi tadi tentu memiliki pengguna atau biasa disebut *user* yang memiliki identitas, Identitas yang dimaksud adalah data biografi unik dari seperti nama, tanggal & tempat lahir, alamat dan lain sebagainya. Lalu data user ini perlu dikelola dengan baik agar mudah jika kemudian dilakukan penambahan, perubahan, dan pengurangan user.

Selain dari sisi identitas, pengembangan *identity management* juga harus memperhatikan skalabilitas dalam sistem. Berkembangnya organisasi atau perusahaan biasanya diikuti pula dengan berkembangnya sistem teknologi informasi yang dikelola, misalnya penambahan sistem keuangan, sistem pengukuran kinerja pegawai, atau sistem absensi yang mengakibatkan model pengelolaan harus mampu mendukung integrasi pada semua sistem.

Selanjutnya, pada sebuah organisasi tentu dijumpai pembagian tugas dan peran kepada individu yang merupakan bagian dari organisasi. Misalnya saja seorang individu berperan sebagai bendahara maka bendahara hanya akan memiliki akses untuk aplikasi yang menunjang perannya. Jadi definisi Role Based Access Control mengacu pada pemberian akses kepada individu yang memiliki bagian peran pada organisasi sesuai dengan peran dalam organisasi. Dengan pendekatan seperti ini maka mekanisme pemberian hak akses menjadi lebih aman, mudah, dan terkelola dengan lebih baik.

Dalam perjalanannya, organisasi atau perusahaan mengembangkan layanan atau service lain sehingga dapat dikatakan ekosistem aplikasi terus tumbuh seiring tumbuhnya organiasasi atau perusahaan. Oleh karena itu mekanisme manajemen identitas harus mampu mendukung berbagai macam platform yang digunakan organisasi. Hal ini dapat dijawab dengan menggunakan mekanisme *web service*. *Web service* mengakomodir layanan pada aplikasi karena menggunakan sistem komunikasi yang dapat diakses oleh semua *platform* aplikasi melalui media jaringan komunikasi yang ada[2][10]. Oleh karena itu, pada tugas akhir ini diharapkan dapat menjawab kebutuhan tersebut dalam menghadirkan solusi yang tepat.

1.2 Perumusan masalah

Berdasarkan latar belakang permasalahan di atas, ada beberapa masalah yang bisa dirumuskan, yaitu :

1. Bagaimana mengimplementasikan metode Role Based Access Control dalam pembuatan Identity Manajemen.
2. Bagaimana mengevaluasi aspek validasi dan verifikasi pemberian hak akses pada *user*.
3. Bagaimana mengevaluasi aspek keamanan pada proses komunikasi antar *service*.

1.3 Tujuan

Berdasarkan pemaparan latar belakang, maka tujuan tugas akhir ini adalah:

1. Mengimpelemtasikan metode Role Based Access Control dalam pengembangan Identity Manajemen.
2. Mengevaluasi aspek validasi dan verifikasi pemberian hak akses pada user.
3. Mengevaluasi aspek keamanan pada proses komunikasi antara service.

1.4 Hipotesa

Hipotesa awal pada tugas akhir ini penggunaan metode RBAC dapat meningkatkan performansi pengelolaan data Identitas dalam hal manajemen lifecycle dan usability dalam pembuatan aplikasi.

1.5 Metodologi Penyelesaian Masalah

Dalam penyusunan Tugas Akhir ini digunakan metodologi sebagai berikut:

1. Studi Literatur

Tahap ini dilakukan dengan cara mempelajari literatur-literatur baik yang berupa buku (*textbook*), jurnal dan artikel ilmiah, maupun *website* yang berhubungan dengan manajemen identitas, manajemen akses, R*ole Based Access Control*(RBAC), *Oauth versi 2*, Restful w*eb service*.

2. Analisis Penyelesaian Masalah

Analisis penyelesaian masalah dilakukan untuk menemukan solusi dalam penerapan *Role Based Access Control* pada *Identity Manajemen*. Menemukan mekanisme pengaman pada web service yang sesuai dengan kebutuhan sistem juga menjadi perhatian besar mengingat pentingnya data dan menjaga keamanan sistem secara keseluruhan.

3. Implementasi dan Pengujian Algoritma

Tahap implementasi dikerjakan berdasarkan rancangan mekanisme sistem yang akan dibuat. Dari hasil perancangan yang dihasilkan mengenai *identity lifecycle*, role based access control, dan pengamanan web service maka langkah selanjutnya adalah mengimplemetasikan hal diatas pada sistem. Setelah impelemetasi dilakukan selanjutnya adalah pengujian algoritma, pengujian yang dilakukan mengenai penerapan role based access control yang sesuai, identity lifecycle, dan pengujian kemanan pada web service.

4. Analisis Hasil dan Penarikan Kesimpulan

Analisis hasil dilakukan untuk memastikan kinerja Role Based Access Control dapat berjalan dengan baik, proses validasi dan verifikasi akses yang sesuai, dan aspek keamanan pada tiap service.

1.6 Jadwal kegiatan

Berikut jadwal yang direncanakan dalam pengerjaan tugas akhir ini.

Tabel 1-1 Jadwal Pengerjaan

Kegiatan	Bulan 1	Bulan 2	Bulan 3	Bulan 4	Bulan 5
Studi Literatur					
Perancangan Sistem					
Implementasi					
Analisis dan Testing					
Dokumentasi Peneleitian					

5. Penutup

5.1 Kesimpulan

Setelah dilakukan pengujian terhadap implementasi RBAC maka dapat diambil kesimpulan:

1. Dengan mengimplementasikan RBAC diperoleh performansi penggunaan dan pendefinisian lebih baik karena dapat di skemakan dengan leluasa oleh organisasi yang mengadopsi penggunaan role untuk akses ke aplikasi.
2. Proses role engineering yang dilakukan haruslah tepat dan perlu adanya mekanisme untuk verifikasi dan validasi yang membantu memastikan aplikasi atau sistem yang dibangun memenuhi parameter- perameter kebutuhan.
3. Mekanisme authentikasi menggunakan oauth dikhawatirkan mengancam aspek kamanan sistem apabila proses komunikasi tidak diamankan dengan enkripsi, metode enkripsi yang dilakukan yaitu dengan mengimplementasikan Secure Socket Layer (SSL) pada protokol komunikasi yang digunakan. – tambahkan analisis (sesuai draft rfc oauth).

5.2 Saran

Untuk pengembangan kedepan, Mekanisme RBAC dapat dipilih sebagai salahsatu metode yang baik untuk membangun sistem dengan akses kontrol yang lebih komplek. Hal ini dapat dicapat dengan memperhatikan Model RBAC yang sudah ada.

1. Impelementasi model hirarki pada RBAC dapat mempermudah dalam manajemen akses kontrol pada role yang memiliki sistem hirarki seperti organisasi. Model penerapan yang sederhana dapat dilakukan dengan mengadopsi sistem hirarki keorganisasiannya.
2. Salah satu tujuan dari membangun sistem Identity Provider adalah untuk menjaga data user agar tidak tercecer dan tetap dikelola oleh satu pihak yang dianggap terpercaya. Oleh sebab itu, service provider harus menjamin agar data user tidak dieksploitasi untuk kepentingan yang tidak disepakati. Disana Identity provider bertindak sebagai pemegang kendali terhadap siapa saja dan sejauh mana data user digunakan.
3. Untuk mempermudah service provider mengakses web service, ada baiknya Identity Provider menyediakan API dan dokumentasi yang jelas tentang bagaimana service dapat dimanfaatkan secara maksimal.

Daftar Pustaka

[1] Benantar, Messaoud. Access Control System: Security, Identity Management, dan Trust Model. Springer. Austin,TX,USA.2006.

[2] Fei, Zhu. Hongjun, Diao. Single Sign-On Assistant: An Authentication Broker for Web Applications. 2010 Third International Conference on Knowledge Discovery and Data Mining. IEEE.2010

[3] Fielding, Thomas Roy. Architectural Styles and the Design of Network-based Software Architectures. University of California. 2000

[4] Guerin, Trey. Lord, Richard. How role based access control can provide security and business benefits. Computer World. http://www.computerworld.com/s/article/86699/How_role_based_access_control_can_provide_security_and_business_benefits (10 Oktober 2011)

[5] Hada, Satoshi. Maruyama, Hiroshi. Session Authentication Protocol for Web services. Proceedings of the 2002 Symposium on Applications and the Internet. IEEE.2002

[6] Hyangjin, Lee. Inkyoung, Jeun. Hyuncheol,Jung. Criteria for evaluating the privacy protection level of Identity Management Services. Third International Conference on Emerging Security Information, Systems and Technologies.2009

[7] Jin,Wang. Daxing, Li. Qiang, Li. Bai, Xi. Constructing Role-Based Access Control and Delegation Based on Hierarchical IBS. IFIP International Conference on Network and Parallel Computing – Workshops. 2007.

[8] Lukawiecki, Rafal. Identity Life Cycle Management. Microsoft Corp & Project Botticelli Ltd. E&OE. 2006

[9] Sejong, Oh. Seog, Park. Enterprise Model as a Basis of Administration on Role-Based Access Control. Dept. of Computer Science, Sogang University, Seoul, Korea. 2001.

[10] Shandu, Ravi S. Coyne, Edward J. Feinstein, Hal L. Youman, Charles E. Roled Based Access Control Models. IEEE Computer. 1996(p38-47)

[11] Silva, Flavio. Pachecho, J AA. Rosa, Pedro F. A Web Service Authentication Control System Based on SRP and SAML. Proceedings of the IEEE International Conference on Web Services.2005

[12] Stamos, Alex. Stender, Scott. Web Service Security Scenarios, Patterns, and implementastion Guidance for Web Services Enhancements(WSE) 3.0.2005

[13] Ranganathan, Aravindan. Sum, Marina. Securing Applications With Identity Services. 2005. http://developers.sun.com/identity/reference/techart/id-svcs.html

[14] Shandu, Ravi. Ferrailo, David. Kuhn, Richard. The NIST Model for Role Based Access Control Towards A Unified Standard.