KONTROL AKSES DAN KEAMANAN DATA BAGI PENDUDUK MISKIN

Asrianda
Teknik Informatika, Teknik, Universitas Malikussaleh
Kampus Bukit Indah Jln. Batam Kecamatan Muara Satu
Email: 4srianda@gmail.com

ABSTRAK

Menetapkan role bagi pengguna yang melakukan pendataan atau pengguna tersebut seorang RT di gampong dan pengguna itu termasuk dalam kategori miskin, oleh sistem pengguna tersebut ditolak karena SSD hanya memperbolehkan satu role dimiliki oleh satu pengguna. Dengan menggunakan DSD dapat menyelesaikan permasalahan, tetapi hal tersebut akan mengalami kendala yang diakibatkan rawan terjadinya manipulasi. SOD digunakan untuk membatasi pengguna melakukan tugas-tugas tertentu sesuai ketentuan serta batasan yang diberikan oleh organisasi. SOD diimplementasikan pengguna melakukan tugas sesuai wewenang yang diberikan.

***Kata Kunci**:* SSD, SOD, pengguna, *role*, membatasi, manipulasi

ABSTRACT

Assign roles for users to collect data on the user or a user households in the village and it was included in the category of the poor, by the user's system was rejected because SSD allowing only one owned by one user role. By using DSD can solve the problems, but it will run into obstacles caused prone to manipulation. SOD is used to restrict users to perform certain tasks according to the provisions and restrictions provided by the organization. SOD is implemented users perform tasks according to the authority given.

***Keywords**:* SSD, SOD, user, role, limiting, manipulation

1 PENDAHULUAN

Pengontrolan terhadap hak akses berguna untuk membatasi pengguna yang akan mengakses informasi dan menjaga keamanan atas informasi yang dianggap rahasia, sehingga informasi tersebut tidak dapat diakses oleh pengguna yang tidak diinginkan. Informasi hanya dapat diberikan kepada pengguna yang telah diberikan otoritas akses terhadap sistem tersebut. Oleh sebab itu sangat diperlukan kontrol akses guna membatasi hak-hak apa saja dapat diakses oleh pengguna. Sehingga keamanan atas informasi dapat terjaga dari pihak-pihak yang tidak diinginkan. Kontrol akses mendukung kerahasian dan integritas keamanan dalam sebuah sistem sehingga pengguna a dibatasi hak yang boleh dilakukan dalam mengakses sistem.

Kontrol akses merupakan cara mencegah ancaman keamanan internal. *Role Based Access Control* (RBAC) merupakan mekanisme pengelolaan sejumlah besar hak akses pada basis data berukuran besar yang fleksibel. Dibandingkan model kontrol akses tradisional yaitu *Mandatory Access Control* (MAC) dan *Discretionary Access Control* (DAC) [1].

Mencegah terjadinya manipulasi data yang telah di data sebelumnya, harus dibuat suatu pengaturan data yang ketat sehingga data dapat dijaga keamanannya dari pihak yang tidak diinginkan. Membuat sistem menjadi lebih aman menerapakan *static separation of duty* (SSD) dalam RBAC menetapkan bahwa *mutual exclusive roles* atau hak akses tidak harus ditugaskan kepada subjek yang sama di waktu yang bersamaan [2].

Akses dibatasi berdasarkan otorisasi yang diberikan pada pengguna. Hal ini berarti bahwa subjek diizinkan untuk menentukan tipe akses apa yang dapat terjadi pada objek yang mereka miliki.

Kontrol akses dalam mengambil keputusan ditentukan oleh *role*, sehingga pengguna sebagai bagian dari sebuah organisasi akan mendapatkan hak akses sesuai dengan role yang didapatkannya. Membatasi pengguna dengan cara memberikan keistimewaan hak kepada mereka. Pelaksanaan suatu pekerjaan bukan hak yang telah diberikan kepada mereka sehingga akan ditolak

karena itu hal tersebut bukan tugas yang diberikan kepada pengguna.

Menetapkan *role* bagi pengguna yang melakukan pendataan atau pengguna tersebut seorang RT di gampong dan pengguna itu termasuk dalam kategori miskin, oleh sistem pengguna tersebut ditolak karena SSD hanya memperbolehkan satu *role* dimiliki oleh satu pengguna. Dengan menggunakan DSD dapat menyelesaikan permasalahan di atas, tetapi hal tersebut akan mengalami kendala yang diakibatkan rawan terjadinya manipulasi, misalnya pegawai negeri sipil (PNS) tidak termasuk dalam kategori miskin tetapi jika ada bantuan PNS tersebut akan dimasukkan sebagai penerima bantuan.

Hal ini disebabkan DSD dapat mengaktifkan banyak *role*, walaupun dalam waktu yang berbeda sehingga rawan terjadinya manipulasi data yang disimpan ke dalam database.

2 MODEL, ANALISIS, DESAIN, DAN IMPLEMENTASI

2.1 Kontrol Akses

Kontrol akses adalah pusat keamanan dalam sebuah komputer dengan cara membatasi pengguna untuk mengakses sumber daya, dan dimotivasi oleh kebutuhan untuk membocorkan akses dalam memperoleh informasi yang tersedia di sumber daya.

Pencegahan juga dilakukan untuk mencegah pengguna yang cerdik dengan cara berkoloborasi dengan pengguna yang memiliki wewenang untuk mengakses informasi tersebut [3]. Penggunaan kontrol akses dilakukan untuk memastikan bahwa orang berhak yang dapat mengakses informasi, dan memberikan kemampuan untuk mendikte informasi mana saja boleh dilihat ataupun dimodifikasi pengguna.

Kebijakan kontrol akses adalah mengijinkan hanya subyek yang mempunyai otorisasi yang bisa mengakses obyek yang sudah diijinkan untuk diakses. Obyek dari akses merupakan bagian yang pasif dari akses karena subyek melakukan aksi terhadap obyek. Kontrol akses mendukung kerahasian dan integritas sebuah sistem supaya sistem aman, serta melindungi kerahasian informasi dari orang yang tidak berhak untuk mendapatkan informasi.

2.2 *Role Based Access Control* (RBAC)

RBAC tidak menerapkan hak akses pelaku atau subjek, sebaliknya memberikan hak akses untuk *roles*. RBAC memberikan tugas keamanan pada kontrol akses sebagai prioritas tertinggi untuk mengontrol akses ke sumber daya.

RBAC menerapkan hak akses kepada pengguna membutuhkan waktu yang singkat, dengan cara menghubungkan subjek dengan *role*, sehingga memerlukan penunggasan hak akses untuk *role* pada setiap subjek [4].

Hak akses akan ditugaskan ke roles bukan langsung kepada pengguna, dan *roles* akan digunakan oleh pengguna, kemudian pengguna membuat sebuah *session*, dan *session* akan mendapatkan izin (*permission*) dari *role* yang didapatkan oleh pengguna kemudian akan mengaktifkan perannya (*roles*).

Pendefinisian *role* menjadi perdebatan sehingga perlu menjelasan konsep *role* tersendiri, sehingga untuk melakukan koloborasi dengan kontrol akses masih disesuaikan dengan kebutuhan. Dalam ilmu prilaku, *role* didefinisikan sebagai pola yang ditentukan sesuai prilaku seseorang dalam situasi tertentu berdasarkan posisi orang [6].

Permission merupakan wewenang diberikan kepada pengguna atau subjek melakukan beberapa operasi atau tindakan yang dilakukan kepada objek [7]. *Permission* adalah suatu keistimewaan diperoleh oleh pengguna, jika pengguna tersebut masuk ke dalam sistem maka operasi dilakukan terhadap objek tertentu dan dapat dilakukan karena pengguna telah mendapatkan *permission* [1].

Objek dalam kontek kontrol akses dianggap sebagai sumber daya pengguna dapat melakukan beberapa kegiatan [7]. Objek dapat berupa file, folder, *directory*, *record*, atau *table* dan lain-lain. Tipe objek tergantung dengan sifat pada sistem yang dibuat. Suatu objek bisa menjadi *entity* pasif yang hanya berisi informasi ataupun bisa menjadi sebuah entity aktif berupa printer atau program komputer yang pernah dibahas oleh *Department of Defense in an orange book* [8].

2.3 Aspek Kebijakan Keamanan

Penanganan keamanan dalam organisasi baik itu pemerintahan maupun perusahaan bisnis sangat tergantung pada informasi pengolahan data dalam melakukan sebuah operasional bisnis yang dijalankannya, baik bidang keuangan maupun informasi teknologi lainnya.

Integritas dan ketersedian atas kerahasian kunci keamanan dalam sistem perangkat lunak, database dan jaringan keamanan data telah menjadi kekhawatiran yang sangat besar di dalam segala sektor. Masalah korupsi atau pengungkapan data yang dilakukan dengan cara tidak sah atau pencurian sumber daya perusahaan dapat mengganggu sebuah organisasi yang dimiliki oleh perusahaan. Hal ini berdampak secara hukum sehingga kepercayaan publik akan berkurang [5].

2.4 Entitas dalam RBAC

Subjek merupakan proses dilakukan atas nama pengguna. Di dalam praktek sebenarnya proses

atau program komputer menjalankan tugas atau aktivitas atas nama pengguna, kemungkinan besar tugas dilakukan memerlukan keterlibatan beberapa subjek yang aktif serta berguna untuk menjalankan tugas tertentu. Jalur akses akan dilakukan oleh subjek pada setiap proses dalam menemukan apakah proses tersebut dipanggil oleh pengguna yang resmi atau tidak. Hal ini dilakukan pengguna dengan memasukkan identitasnya dalam melakukan *login* ke *website* bank pada sistem perbankan *online*. Program utama yang beroperasi atas nama pengguna untuk *login* didefinisikan sebagai subjek [7].

Operation bisa berupa *write, read, execute, delete, update* dan sebagainya. Jenis Operation tergantung pada jenis objek yang dijalankan. Misalnya pengguna pada *online banking* memasukkan informasi yang dibutuhkan untuk dapat *login* ke sistem. Hal tersebut menyatakan bahwa program utama akan bertindak sebagai subjek mewakili pengguna untuk menjalankan operasi yang ada pada sistem seperti pengecekan saldo, mentransfer uang, melihat informasi pribadi ataupun mengubah sandi dan lain- lain.

Dalam praktek sebenarnya pengguna akan terikat untuk memiliki satu *session* pada waktu yang bersamaan atau waktu yang berbeda. Pengguna akan ditetapkan untuk dapat memiliki salah satu *role* aktif per *session* atau pengguna dapat mengaktifkan beberapa *role* per *session* [1].

2.5 *Separation of Duty* (SOD)

SOD digunakan untuk membatasi pengguna melakukan tugas-tugas tertentu sesuai ketentuan serta batasan yang diberikan oleh organisasi. SOD diimplementasikan pengguna melakukan tugas sesuai wewenang yang diberikan oleh organisasi.

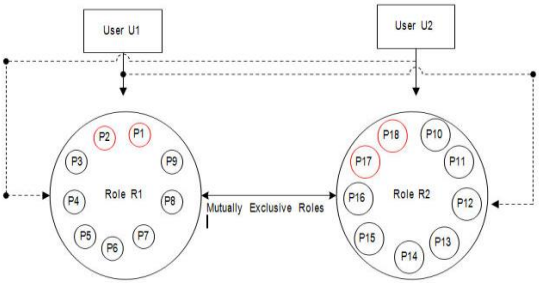
Tugas tersebut dilakukan dengan cara melibatkan lebih dari satu pengguna dibandingkan hanya menggunakan satu pengguna, sehingga keamanan untuk mengakses sistem dapat terjamin. Konsep SOD diterapkan menimbulkan masalah, pengguna sistem dapat memilih untuk tidak menggunakannya atau menerapkan konsep tersebut.

2.6 Mutual Exclusion (ME)

Mutually exclusive merupakan situasi diterimanya salah satu alternatif secara otomatis dengan cara tidak memasukkan alternatif lain. ME merupakan konsep dasar dari Separation of Duty (SOD). Dalam praktek SOD diterapkan dengan mengimplementasikan bantuan dari *Mutually exclusive*.

2.7 Penurunan Ke wenangan Pengguna RBAC

RBAC *role* menjadi perhatian utama dan memiliki posisi strategis, sehingga administrator keamanan membuat *role* sesuai dengan kebutuhan struktur organisasi. Umumnya *role* terdiri dari dua bagian yang salah satunya hak akses yang saling bertentangan dan menciptakan konflik kepentingan dengan hak akses *role* lainnya. Bagian lainnya terdiri dari hak akses yang tidak menciptakan hambatan dengan hak akses dari *role* lainnya. Hak akses yang saling bertentangan dikatakan sebagai *mutually exclusive permissions* dalam mengimplementasikan DSD. Ini berarti bahwa *role* hanya dapat memiliki dua jenis hak akses [1].

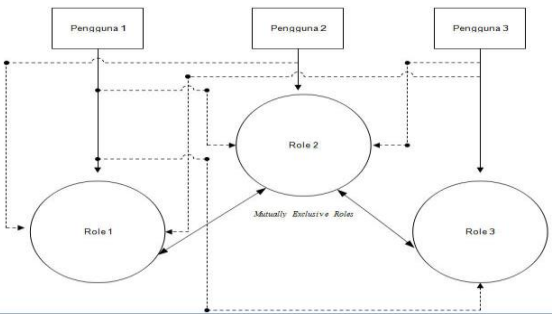


Gambar 1. Hambatan Hak Akses di MER

3 SKENARIO UJI COBA

Model yang diajukan dan dijelaskan secara terperinci dengan mengikuti skenario digambarkan di bawah ini. Ilustrasi gambar di bawah ini diproses secara lengkap dan dilakukan oleh *role*. Seperti contoh melibatkan tiga pengguna dan tiga *role* dengan hak akses yang ganda. Misalkan kita memiliki tiga pengguna yaitu pengguna1, pengguna2 dan pengguna3 serta mempunyai otoritas untuk mengaktifkan tiga *mutually exclusive roles* yaitu Role1, Role2 dan Role3. Setiap pengguna akan mengaktifkan salah satu dari tiga *mutually exclusive roles*, pengguna tersebut tidak dapat mengaktifkannya baik itu sebagian maupun keseluruhan *role* yang ada dalam session yang sama sesuai dengan definisi DSD standar.

Pada gambar 2 pengguna1 ingin mengaktifkan Role1 dan pengguna2 mengaktifkan Role2 begitu juga pengguna3 mengaktifkan Role3. Tanda panah putus-putus memperlihatkan pengguna tidak dapat mengaktifkan *role* diakibatkan pelaksanaan DSD dari segi *mutually exclusive roles*. Akibat penerapan DSD pada tingkat *role*, pengguna RBAC kehilangan ranah otoritas mereka



Gambar 2. Tugas Pengguna dalam *Mutually Exclusive Roles*

Penerapan ranah otoritas pengguna mengalami kekurangan besar dalam mengimplementasikan DSD dari segi *mutually exclusive,* diakibatkan oleh pengguna RBAC kehilangan bagian dari ranah otoritas mereka. Sekarang kita akan menganalisa skenaria model yang peneliti usulkan dengan mengimplementasikan DSD pada tingkat *mutually exclusive permissions*.

4 HASIL UJI COBA

Hambatan hak akses dengan menggunakan *mutually exclusive permissions* (MEP) hak akses HA4 dan HA5 berasal dari normalisasi *role* yaitu normalisasi R2 dan normalisasi R3. Pengguna berwenang untuk mengaktifkan semua role yaitu R1, R2, dan R3 dan juga berhak mengaktifkan *role* R1 atau nomalisasi R2 dan R3 yang disebabkan oleh *mutually exclusive roles* (MER) dalam mengimplementasikan DSD.

Perhitungan rangkaian ranah otoritas yang tersedia dalam hak akses dalam mengimplementasikan DSD. Kedua hak akses dipisahkan seperti yang terlihat di table 2 di bawah ini. Hak akses negatif memiliki tindakan negatif ditetapkan pada suatu objek yang menggantikan hak akses positif dan memiliki kegiatan positif sesuai dengan ketetapan pada objek yang sama sebagai hak akses negatif. Hak akses positif mempunyai hak akses negatif kemudian akan dibatalkan serta dihapus dari ranah pengguna RBAC.

Hak akses dalam kegiatan “baca”
HA1 = Baca (obj1)
HA2 = Tulis (obj2)
HA3 = Cetak (obj7)
HA4 = Baca (obj2)
HA5 = Baca (obj7)

Roles
R1 = {HA1, HA2, HA3}
R2 = {HA4}
R3 = {HA5}

Pengguna
P1 = {R1, R2, R3}

Hambatan dalam Hak akses
MEP = {HA4, HA5}

Menentukan ranah kewenangan untuk pengguna P1= {S1, S2}
S1 = {R1, R2}
S2 = {R1, R3}

Tabel 1. Pembuatan role baru dan hak akses baru dalam Kegiatan Baca

S1	S2
R1 + R2	R1 + R3
HA1 + HA2 + HA3 +HA4	HA1 + HA2 + HA3 + HA5
Baca(obj1) + Tulis(obj2) + Cetak(obj7) + Baca(obj2)	Baca(obj1) + Tulis(obj2) + Cetak(obj7) + Baca(obj7)
Baca(obj1) + Tulis(obj2) + Cetak(obj7)	Baca(obj1) + Tulis(obj2) + Cetak(obj7)
R1	R1

Dari hasil perhitungan kalkulasi yang telah dibuat, hak akses positif dan hak akses negatif sama-sama memiliki potensi dalam penyelesaikan suatu permasalahan dalam melakukan akses. Tetapi mempunyai dampak yang berbeda di mana yang telah dibahas sebelumnya bahwa hak akses positif memberikan wewenang ke pengguna dan hak akses negatif membatasi wewenang ke pengguna. Hak akses negatif tidak akan memberikan manfaat apapun tanpa menggunakan hak akses positif. Hak akses negatif sangat baik diterapkan jika saat hak akses positif diterapkan juga pada objek yang disimpan dalam struktur pohon direktori. Sehingga objek akan selalu terhubung satu sama lainnya melalui beberapa hirarki.

5 KESIMPULAN

Penggunaan DSD dengan *mutually exclusive roles* rawan terjadinya manipulasi diakibatkan tidak membatasi hak akses pengguna berbeda dengan *mutually exclusive permissions* dapat membatasi hak akses pengguna.

Dengan menggunakan DSD *mutually exclusive permissions* dua *role* yang berbeda tidak dapat diaktifkan oleh pengguna yang sama walaupun *session*nya berbeda.

6 DAFTAR PUSTAKA

[1] Habib, M.A. 2011. **Role inheritance with object-based DSD**. Int. J. Internet Technology and Secured Transactions, 3, 2:149-160

[2] Strembeck, M. 2004. **Conflict Checking of Separation of Duty Constraints in RBAC - Implementation Experiences**, In Proc. of the Conference on Software Engineering (SE)

[3] Rotenberg, L.J. 1974. **Making computers keep secrets.** Ph.D. Th., MIT, MAC TR-115

[4] Khayat. E.J., Abdallah. A. E. 2005. **A Formal Model for Flat Role Based Access Control,** IFIP International Federation for Information Processing Volume 173. pp 233-246

[5] Roskos, J.E, Boone, J.M and Mayfield. T. 1989. **Integrity in Tactical and Embedded Systems. Institute for Defense Analyses**, HQ 89-034883/1

[6] Hawkins, D.I, Best. R.J and Coney, K.A, 1983. **Consumer Behavior, Business Publications**, P lano, Texas

[7] Ferraiolo, D, Kuhn. D, and Chandramouli, R., 2003, **Role-Based Access Control**, Artech House, Computer Security Series

[8] DoD 5200.28-STD Department of Defense. 1985. **Trusted Computer System Evaluation Criteria (Orange Book)**, National Computer Securit y Center