[3] E. Al Nuaimi, H. Al Neyadi, N. Mohamed, and J. Al-Jaroodi, "Applications of big data to smart cities", Journal of Internet Services and Applications, vol. 6, no. 1, Dec. 2015, DOI: 10.1186/s13174-015-0041-5.
[4] F. Zhongke, H. Xiaodong and L. Fang, "Forest Survey Equipment and Development of Information Technology", Transactions of the Chinese Society for Agricultural Machinery, vol. 46, no. 9, pp. 257-265, Jun. 2015, DOI: 10.6041/j.issn.1000-1298.2015.09.038.
[5] H. Guo, L. Wang, F. Chen, and D. Liang, "Scientific big data and Digital Earth", Chinese Science Bulletin, vol. 59, no. 35, pp. 5066-5073, Dec. 2014, DOI: 10.1007/s11434-014-0645-3.
[6] H. Coble, A.K. Mishra, S. Ferrell, and T. Griffin, "Big Data in Agriculture: A Challenge for the Future", Appl. Econ. Perspect. P., vol. 40, no. 1, pp. 79-96, Feb. 2018, DOI: 10.1093/aepp/ppx056.
[7] J. Zhao and J. Guo, "Big data analysis technology application in agricultural intelligence decision system" presented at Int. Conf. Cloud Computing and Big Data Analysis, Chengdu, China, Apr. 20-22, 2018.
[8] M. Das and S.K. Ghosh, "Deep-STEP: A Deep Learning Approach for Spatiotemporal Prediction of Remote Sensing Data", IEEE Geosci. Remote S., vol. 13, no. 12, pp. 1984-1988, Nov. 2016, DOI: 10.1109/LGRS.2016.2619984.
[9] M. Chi, A. Plaza, J.A. Benediktsson, Z. Sun, J. Shen, and Y. Zhu, "Big Data for Remote Sensing: Challenges and Opportunities", P. IEEE, vol. 104, no. 11, pp. 2207-2219, Sep. 2016, DOI: 1109/JPROC.2016.2598228
[10] X. Yao and G. Li, "Big spatial vector data management: a review", Big Earth Data, vol. 2, no. 1, pp. 108-129, Feb. 2018, DOI: 10.1080/20964471.2018.1432115.
[11] Y. Chen, C. Li, P. Ghamisi, X. Jia, and Y. Gu, "Deep Fusion of Remote Sensing Data for Accurate Classification", IEEE Geosci. Remote S., vol. 14, no. 8, pp. 1253-1257, Jun. 2017. DOI: 10.1109/LGRS.2017.2704625
[12] Y. Sun, H. Song, A. J. Jara and R. Bie, "Internet of Things and Big Data Analytics for Smart and Connected Communities," in IEEE Access, vol. 4, pp. 766-773, 2016. DOI: 10.1109/ACCESS.2016.252972

Rol Əsaslı Girişə (RBAC) Nəzarət Sisteminin bank domeninde implementasiyası

Abdullayev Qara
Azərbaycan Dövlət Neft və Sənaye Universiteti

Abstract

Bugün, banklar mailliyyə dövriyyəsinin tam ortasındadır. Belə ki, bankların pul transfer edilməsi, pulu saxlamaq və s kimi bir çox maliyyə yönümlü funksiyası vardır. Bu zaman serverlərlə təyin edilmiş insanların əlçatanlığı təhlükəsizlik baxımdan çox önəmlidir. Buna görə də RBAC (role-based access control), yəni rol əsaslı giriş nəzarəti personalın fəaliyyətinə nəzaret etmek məqsədli ən avtomatlaşdırılmış sistemdir. İT sistemlərində idarəetmə və səlahiyyətin paylanması üçün rol əsaslı giriş nəzarəti (RBAC) istifadə olunur.

Açar sözlər: təhlükəsizlik, verilənlər bazası, istifadəçi imtiyazları, rollar, imtiyazların idarə olunması, RBAC.

Müasir rəqamsal dünyada sözsüz ki təhlükəsizlik böyük narahatlıq doğurur. Rol əsaslı giriş nəzarəti ayrı-ayrı istifadəçilərə uyğun rollar təyin edir, eləcə də təyin edilmiş rollar üçün müəyyən giriş icazələri verir. Bununla da müəssisədə rəqəmsal məlumatın qorunması mexanizmi təmin olunur. Bu məqalə xüsusilə banklarda rolların əhəmiyyətini və təyin olunan rollarla bağlı təkamül dəyişikliklərini təsvir etməkdədir. Burada sözü gedən rol subyekt kimi müəyyən edilir və müvafiq əməliyyatlarla birlikdə rolların xüsusiyyətləri müəyyən edilir. RBAC, son dövrlərdə əhəmiyyətli tədqiqat mövzusu olan standart və ən vacib girişə nəzarət modelidir. Girişə nəzarət siyasəti dedikdə resurslara kimin daxil ola biləcəyi və hər bir istifadəçiyə nə qədər giriş icazəsinin verildiyi ilə bağlı qaydaları müəyyən edən bir sistemdir. Burada əsas diqqət Rol üzərində cəmlənmişdir. RBAC-ın əsas ideyası kimi rolun istifadəçilər və icazələr arasında aralıq modul olması çıxış edir. RBAC-da rollar istifadəçilərə (çoxdan çoxa üzrə) və icazələr müvafiq rola (çoxdan çoxa üzrə) təyin edilmişdir. RBAC sistemi, istifadəçinin rola və rolların da dataya əlaqələndirilmiş icazələrini istiqamətlənən iki fəqli müqayisə apararaq çevik nəzarətetmə və idarə imkanı verir. Əksər halda RBAC, rol iyerarxiyalarını dəstəkləyən formada qurulur. Bu quruluş bir rolun digər roldan müvafiq funksiyanı miras almasına yardım edir.

RBAC, icazələrin birbaşa istifadəçilərə deyil, təşkilat daxilindəki iş funksiyalarına uyğun gələn rollar vasitəsilə təyin edilməsi ideyasına əsaslanır. RBAC-da rol xüsusi hüquq və imtiyazlar toplusunu əhatə edir; rola təyin edilmiş istifadəçilər bu icazələrə avtomatik şəkild sahib olrlar. Dəyişikliklərin fərdi istifadəçi səviyyələrində deyil, yalnız rol səviyyəsində idarı olunması icazələrin bu metod vasitəsi ilə nizamlanmasını olduqca asanlaşdırır.

RBAC sisteminin əsas funksiyaları aşağıdakılardır:

- İstifadəçi idarəsi: RBAC istifadəçiləri müəyyən edərək onlara müvafiq icazələr vermək, eyni zamanda idarə etmək üçün struktur təqdim edir.
- Rol idarəsi: RBAC sistemində rolları müəyyən etmək, dəyişiklik etmək və silmək olduqca rahatdır. İcazə idarəetməsi: İcazələrin yaradılması və müəyyən olunması, onların müvafiq istifadəçilərə verilməsi və icazələrin geri alınması əsas funksiyalarından biridir.
- Girişə Nəzarət: RBAC sistemi nəzarət mexanizmi sayəsində istifadəçilərin öz rollarına və icazələrinə uyğun olaraq resurslara (fayllar, verilənlər bazası, serverlər, proqramlar və s.) girişinə nəzarət edir.
- Təhlükəsizlik Auditləri: RBAC, sistemdə təhlükəsizlik siyasətlərinin həyata keçirilməsində yardımçı olur və audit qeydlərini yaradır.

RBAC sistemi 4 əsas kompenenti özündə ehtiva edir:

- İstifadəçilər (user): RBAC sisteminin əsas aktoru istifadəçilərdir. Belə ki istifadəçi dedikdə sistemdəki real şəxslər və ya sistemlər nəzərdə tutulur. Hər istifadəçinin unikal bir identifikasiyası yaradılır.
- Rollar: Rollar istifadəçilərin ortaq funksiyalara sahib olduğu qruplardır. Misal üçün, bank sistemində “administrator”, “müstəri xidmətləri nümayəndəsi”, “maliyyə mütəxəssisi” və s. kimi rollar mövcud ola bilər. Bu halda hər rolun bir və ya birdən çox icazəsi, yəni səlahiyyəti ola bilər.
- İcazələr (permissions): İcazələr sistemdəki resurslara, verilənlər bazasına əlçatanlığı təmin edir.

Nümunə kimi demək olar ki bir bazaya bir istifadəçinin oxuma, digər istifadəçinin isə həm oxuma, həm də yazma icazəsi ola bilər. İcazələr rollarla əlaqələndirilir və hər rolun müvafiq bir icazıyı sahib olduğu icazə matrisi formalaşdırılır.

- İcazə matrisi: İcazə matrisini bir cədvəl kimi düşünə bilərik. Hansı ki, bu

cədvəldə rollar və icazələr əlaqələndirilmişdir. Beləcə hər rolun hansı icazəyə sahib olduğu bu matrisdə əksini tapır. Misal üçün, administrator rolunun bazada bütün funksionallıqlara icazəsi ola bilər. Cədvəl 1.1 və 1.2 icazə rol matrislərinə nümunə ola bilər:

Cədvəl 1. Rol cədvəli

Role ID	Role Name	Description
R_1	Admin	Administrator
R_2	Board of Director	Owner or administrator
R_3	Head Office Manager	Manager
R_4	Branch Manager	Manager
R_5	Remittance Counter Checker	Counter Checker
R_6	Withdraw Counter Checker	Counter Checker
R_7	Deposit Counter Checker	Counter Checker
R_8	Remittance Operator	Operator
R_9	Withdraw Operator	Operator
R_10	Deposit Operator	Operator

Cədvəl 2. İcazələrin növləri

Permission ID	Permission Name	Description
P_1	Read	View individual transaction, or read resources
P_2	Write	Fill data deals with account transactions
P_3	Edit	Update or modify existing resources
P_4	Delete	Cancel wrong transactions

P_5	Read report	Detail and summary report (monthly, annual) by branch
P_6	Execute	Calculate interest amount, execute resources
P_7	Approve	Check transactions step by step
P_8	Read all	Read all transactions
P_9	Execute	Define User Account, Trace Login/Logout time,

RBAC texnikasının komponentlərinə daha ətraflı baxaq.

Rollar. RBAC metodunun ən təməl və ən vacib tərkib hissəsini rollar təşkil edir. Rollar sistem daxilində istifadəçinin səlahiyyətlərini və məhdudiyyətlərini birlikdə müəyyən edən icazələr toplusu hesab edilə bilər. Hər hansı bir təşkilati şəraitdə RBAC-ın tam potensialından istifadə etmək üçün rolların strateji məqamlarının düzgün başa düşülməsi və həyata keçirilməsini başa düşmək vacibdir. Rollar təşkilatın iyerarxiyasını və funksional strukturunu dəqiq əks etdirmək üçün nəzərdə tutulmuşdur. Onlar konkret şəxslərə deyil, vəzifəyə və ya iş funksiyasına bağlanacaq qədər mücərrəddirlər. Bu abstraksiya təşkilat daxilində iş funksiyaları inkişaf etdikcə istifadəçilərə rollar asanlıqla təyin edilməs və ya yenidən təyin edilə bilməsi ilə yüksək çeviklik və miqyaslılığa imkan verir. Aşağıdakı şəkildəki misala nəzər salaq:

```
CREATE ROLE hr_manager;
CREATE ROLE finance_officer;
```

Şəkil 1.1

Şəkil 1.1-də insan resursları və maliyyə məmurları üçün müvafiq rollar yaratdıq.

```
-- Granting access to HR-related tables to the HR manager role
GRANT SELECT, INSERT, UPDATE ON employee_records TO hr_manager;

-- Granting access to financial tables to the finance officer role
GRANT SELECT, INSERT ON financial_records TO finance_officer;
```

Şəkil 1.2

Şəkil 1.2-də insan resursları roluna işçi qeydlərinin yerləşdiyi cədvəllər üçün yeni işçi məlumatlarının daxil olunması, mövcud məlumatların yenilənmədi və mövcud məlumatlara baxılması üçün, maliyyə məmurlarının roluna isə yeni maliyyə qeydlərinin daxil olunması və mövcud məlumatlara

baxılması üçün imtiyazlar verilmişdir. Hesab edək ki, bazadakı hər hansı bir istifadəçiyə bu imtiyazlar verilməlidir.

```
GRANT hr_manager TO alice;
GRANT finance_officer TO bob;
```

Şəkil 1.3

Hər hansı istifadəçiyə insan resurslarına və ya maliyyə məmurlarına məxsus imtiyazların verilməsini Şəkil 1.3-dəki kimi sadə şəkildə icra edə bilirik. Rolların effektiv dizayn olunması üçün aşağıdakı xüsusiyyətlərin nəzərə alınması vacibdir.

Fraqmentasiya(Granularity). Rol dizaynında kritik mülahizələrdən biri fraqmentasiya səviyyəsidir. Həddindən artıq geniş rol potensial olaraq ən az imtiyaz prinsipini pozaraq, həddindən artıq girişə gətirib çıxara bilər, həddən artıq detallı rollar isə idarə etmək çətinləşə bilər. Düzgün balansı tapmaq təşkilatın əməliyyatlarını və təhlükəsizlik tələblərini dərindən başa düşməyi tələb edir.

Ən az imtiyaz(Least Privilege). Hər bir rol ən az imtiyaz prinsipinə ciddi şəkildə riayət etmək üçün qurulmalıdır, yəni onun əlaqəli vəzifələrini yerinə yetirmək üçün lazım olan icazələrdən çox və ya az olmamalıdır. Bu, həddindən artıq geniş girişi icazəsi olan rollardan qaynaqlanan icazəsiz giriş və ya məlumatların pozulması riskini minimuma endirir.

Rol iyerarxiyası. Bir çox təşkilatlar rolların digər rollardan icazələri miras almasına imkan verən rol iyerarxiyalarını müəyyən etməkdən faydalanır. Məsələn, "Baş Menecer" rolu müəyyən yüksək səviyyəli icazələri əlavə edərkən "Menecer" rolunun bütün icazələrini miras ala bilər. Bu iyerarxik yanaşma əlaqəli rolların idarə edilməsini və ümumi strukturu sadələşdirə bilər. Müasir müəssisələrdə rolların idarə olunmasında aşağıdakı prinsiplər gözlənilməlidir

Rolların təyinatı və ləğvi. Rolların təyin edilməsi və ləğv edilməsi prosesi nəzarətdə saxlanılmalı və yoxlanılmalıdır. Rol təyinatındakı dəyişikliklər adətən işə qəbul, yüksəlişlər, köçürmələr və ya işlərin dayandırılması kimi hadisələrlə baş verir. Effektiv rol idarəetməsi bu dəyişikliklərin girişə nəzarət sistemində operativ və dəqiq əks olunmasını təmin edir. Müntəzəm Auditlər və Baxışlar. Rollar, imtiyazların azalmasına yol vermədən təşkilatın ehtiyaclarını qarşılamağa davam etməsini təmin etmək üçün müntəzəm olaraq nəzərdən keçirilməli və yoxlanılmalıdır. Bu, cari əməliyyat tələbləri və uyğunluq standartlarına uyğunlaşdırmaq üçün rol təriflərinə yenidən baxılmasını və bəlkə də yenidən nəzərdən keçirilməsini nəzərdə tutur.

Rolların dinamik təyinatı. RBAC texnikasının qabaqcıl tətbiqləri dinamik rol təyinatlarını özündə birləşdirə bilər, burada rollar yer, vaxt və xüsusi layihə tapşırıqları kimi kontekstual amillər əsasında avtomatik tənzimlənə bilər. Bu çeviklik təşkilatlara dinamik iş mühitlərində məhsuldarlığa mane olmadan təhlükəsizliyi qorumağa kömək edir. Rolların dinamik idarə olunmasının Oracle SQL-də tətbiqinə aid kiçir bir misala nəzər salaq. Tutaq ki, bir təşkilat audit dövründə məxfi məlumatlara müvəqqəti giriş icazəsi verməlidir. İT departamenti audit müddətində girişi artırmaq üçün verilənlər bazasında istifadəçi rollarını dinamik şəkildə dəyişə bilər. Şəkil 1.4-də göstərildiyi kimi adi işçilər üçün *regular_employee*, audit menecerləri üçün isə *audit_manager* rollarını yaradaq:

```
-- Create roles
CREATE ROLE regular_employee;
CREATE ROLE audit_manager;

-- Grant privileges to roles
GRANT SELECT ON financials TO regular_employee;
GRANT SELECT, INSERT, UPDATE ON financials TO audit_manager;
```

Şəkil 1.4

Şəkil 1.5-dəki audit prosesi başladıldığı anda *user_id* ilə identifikasiya olunan istifadəçinin rolu adi istifadəçidən audit menecer roluna dəyişdirilərək bu istifadəçinin imtiyazları dəyişdirilir. Audit prosesinin sonunda isə bu istifadəçinin rolu yenidən adi istifadəçi roluna qaytarılır:

```
CREATE OR REPLACE PROCEDURE Assign_Audit_Role(user_id IN VARCHAR2, start_audit IN BOOLEAN) IS
BEGIN
    IF start_audit THEN
        -- Grant audit_manager role
        EXECUTE IMMEDIATE 'GRANT audit_manager TO ' || user_id;
    ELSE
        -- Revoke audit_manager role and revert to regular_employee
        EXECUTE IMMEDIATE 'REVOKE audit_manager FROM ' || user_id;
        EXECUTE IMMEDIATE 'GRANT regular_employee TO ' || user_id;
    END IF;
END;
```

Şəkil 1.5

İcazələr. Oracle SQL nümunəsində əsas diqqət şərtlərin dəyişməsi əsasında dinamik olaraq rolların təyin edilməsi prosedurunun yaradılmasına yönəldilib (məsələn, auditin başlanması). Bu prosesin necə həyata keçirildiyini və daha da optimallaşdırıla biləcəyini araşdıraq. Dinamik Rol Təyinatı üçün SQL Proseduru. Assign_Audit_Role SQL proseduru auditin tələbi əsasında istifadəçi rollarının dinamik şəkildə dəyişdirilməsi üçün əsasdır. Prosedurun və onun potensiauzantılarının bölgüsü:

```
CREATE OR REPLACE PROCEDURE Assign_Audit_Role(user_id IN VARCHAR2, start_audit IN BOOLEAN) IS
BEGIN
    IF start_audit THEN
        EXECUTE IMMEDIATE 'GRANT audit_manager TO ' || user_id;
    ELSE
        EXECUTE IMMEDIATE 'REVOKE audit_manager FROM ' || user_id;
        EXECUTE IMMEDIATE 'GRANT regular_employee TO ' || user_id;
    END IF;
END;
```

Şəkil 2.1

Məqsəd və funksionallıq:

- Şərtə əsaslanan rolun təyin edilməsi: Prosedur iki parametr alır: user_id və start_audit.

start_audit-in DOĞRU və ya YANLIŞ olmasından asılı olaraq, o, rolları verir və ya ləğv edir.

- Dinamik SQL İcrası: Dinamik SQL ifadəsinin icrası üçün EXECUTE IMMEDIATE-dən

Istifadə edir, rol dəyişikliklərinin prosedur daxiletmələri əsasında dərhal tətbiq edilməsinə imkan verir.

- Təhlükəsizlik Təsirləri: İstifadəçi daxiletmələrinə (user_id) əsaslanan SQL əmrlərinin

birbaşa icrası SQL inyeksiyası kimi təhlükəsizlik risklərinə səbəb ola bilər. SQL sorğularını dinamik şəkildə qurmaq üçün birləşmədən istifadə edərkən girişləri təsdiqləmək və ya sanitarlaşdırmaq çox vacibdir.

RBAC-ın üstünlükləri və niyə onun effektiv və genişlənən giriş nəzarəti üçün üstünlük verilən seçim olaraq qaldığına nəzər yetirək:

1. Minimallaşdırılmış inzibati iş və sadələşdirilmiş idarəetmə. RBAC-ın əsas

üstünlüklərindən biri, icazələrin idarə edilməsi üçün tələb olunan inzibati işlərin mürəkkəbliyini və həcmini azaltmaq qabiliyyətidir. Hər bir istifadəçiyə fərdi icazələr təyin etmək əvəzinə, administratorlar müəyyən bir iş funksiyası üçün uyğun olan icazələr qrupunu təmsil edən rollar təyin edirlər.

2. Təkmilləşdirilmiş təhlükəsizlik. RBAC istifadəçilərin yalnız öz işlərini yerinə yetirmək üçün lazım olan girişi əldə etmələrini təmin edərək, ən az imtiyaz (PoLP) prinsipinə riayət etməklə təhlükəsizliyi artırır. Bu, icazələrin təsadüfi və ya bilərəkdən sui-istifadə riskini məhdudlaşdırır.

3. Ölçüləbilənlik və çeviklik. Təşkilatlar böyüdükcə onların İT infrastrukturu və istifadəçi

bazası inkişaf edir. RBAC, girişə nəzarət strukturlarında əhəmiyyətli dəyişikliklərə ehtiyac olmadan artan mürəkkəbliyə uyğunlaşan genişlənə bilən təhlükəsizlik modellərinə imkan verir.

4. Sabit və yoxlanıla bilən giriş nəzarəti. RBAC sistemləri istifadəçi icazələrini idarə etmək

üçün sabit yanaşma təmin edir. Eyni rolu olan hər bir istifadəçi eyni giriş hüquqlarına sahib olacaq, bu da auditləri və təhlükəsizlik yoxlamalarını asanlaşdırır. Təfərrüatlı qeydlər, rol təyinatları və dəyişikliklərin qeydləri audit tələblərini əlavə olaraq dəstəkləyir.

Ədəbiyyat

[1] Al-Kahtani, M., & Sandhu, R. (2013). A Model for Attribute-Based User-Role Assignment. Journal of Computer Security.

[2] Benantar, Messaoud. (2016). Access Control Systems: Security, Identity Management and Trust Models.

[3] Biuk-Aghai, Robert P. (2013). Security and Access Control Using Biometric Technologies.

[4] Coyne, E. J., & Davis, J. M. (2017). Role engineering for enterprise security management. Information Systems Security.
[5] Ferraiolo, D., Kuhn, R., & Chandramouli, R. (2014). Role-Based Access Control. Artech House.
[6] Gupta, P., & Seetharaman, A. (2019). The Business Impact of Role-Based Access Control: A Systematic Literature Review. Expert Systems with Applications.

MANAGING ACCESS IN DISTRIBUTED SYSTEMS: OVERVIEW

Tural Ahmadov , Kifayyat Mammadova

Abstract
This review provides a comprehensive analysis of access management (AM) methods in the field of information security. AM is a key aspect of protecting sensitive data and resources from unauthorized access. Understanding various AM models and mechanisms is crucial for designing effective security solutions. One of the main goals of the study is the diversity of AM approaches, analyzing models from traditional discretionary AM (DAM) and mandatory AM (MAM) to more newly developed models such as role-based AM (RBAM), attribute-based AM (ABAM), and policy-based AM (PBAM). Additionally, enforcement mechanisms like AM Lists (AML) are discussed. This research work is proposed as a valuable resource for researchers, practitioners, and administrators involved in information security and AM decision-making.
Keywords: access management; distributed systems; information security.

Introduction

In modern society, many digital innovations have transformed organizations and altered their operational structures, leading to the establishment of internal networks and connections to broader networks. The evolution of networks has provided businesses with efficient and effective communication solutions that require advanced Authentication and Authorization solutions for the storage of data [1]. Access Management (AM) is a solution to address information security issues by fulfilling specific security requirements to prevent unauthorized access to various resources. Since AM is a very active research field, this scientific work aims to explore existing technical solutions and application areas by examining issues surrounding reliable digital transformation strategies for organizations and enterprises.

Background and related work

AM is a valuable technique for protecting information security by determining who or what can see or use resources. According to the definition provided by NIST for AM [2]:
A usually automated set of procedures or processes that allow access to a particular space or data managed in conjunction with predefined policies and rules.'AM is considered the foundation of information security in fields including Cloud Computing and the Internet of Things. AM has the capability to monitor access to resources and effectively prevent unauthorized data flows [3].
According to Stallings and Brown [4], AM solutions can be designed with three main principles in mind:

–Identification - The process of verifying the correctness of specific access credentials of the user (subject) and various system objects.

–Authorization - The process of granting or denying access permissions for a system resource (object), deciding for what purpose the subject is trusted.

–Audit - An independent review that checks system logs or activities to understand the status of system management tools. Additionally, conducting an audit can help ensure compliance with established policies and operational procedures, detect security breaches, and provide recommendations for improving Information Security Management Systems (ISMS).