Educator Insights: A Journal of Teaching Theory and Practice
Volume 2, Issue 1, January 2026
brightmindpublishing.com
ISSN (E): 3061-6964
Licensed under CC BY 4.0 *a Creative Commons Attribution 4.0 International License.*

IMPROVING ACCESS RESTRICTIONS IN COMMERCIAL BANKS INFORMATION SYSTEMS USING A MODIFIED ROLE-BASED METHOD

Irgasheva D. Ya.
Director of the Network center for retraining and Professional Development of Pedagogic Personnel at the Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, DSc, Professor

Kobiljanov Sh. N.
Independent researcher at Tashkent University of Information Technologies named after Muhammad al-Khwarizmi

Abstract
This article considers the issue of eliminating the existing shortcomings of the role-based access control (RBAC) method, which is widely used in the process of access control in information systems of commercial banks. In order to reduce these shortcomings, a modified (hybrid) approach based on a combination of RBAC and attribute-based access control (ABAC) methods is proposed. The proposed method allows determining access rights taking into account the roles of users, as well as their attributes, resource attributes and system attributes. The article develops a mathematical model of the modified method, a set of basic parameters and an algorithm designed for information systems of commercial banks. The proposed approach increases flexibility in the use of bank information resources, enhances the level of security and reduces the risk of unauthorized access.

Keywords: Information security, access control, RBAC, ABAC, hybrid access control, commercial banks, information system, access rights, attributes, role model.

Introduction

In order to eliminate the shortcomings of the role-based access control method for limiting access, it is proposed to modify, that is, improve, this method. Accordingly, by improving the RBAC method using a combination of RBAC

Educator Insights: A Journal of Teaching Theory and Practice
Volume 2, Issue 1, January 2026
brightmindpublishing.com
ISSN (E): 3061-6964
Licensed under CC BY 4.0 *a Creative Commons Attribution 4.0 International License.*

(Role-Based Access Control) and ABAC (Attribute-Based Access Control), which are used to limit users' access rights to system resources, it is possible to further increase the reliability of ensuring security in the information systems of commercial banks . The proposed method can be called a modified or improved or hybrid method. Since the RBAC method is taken as a basis and its shortcomings are eliminated using the ABAC method, it is considered appropriate to call it a modified role-based access control method since the mathematical hardware used in the method belongs to the RBAC method [1].

The modified version of the proposed method restricts access rights (authorizations) to information systems of commercial banks based on user roles and attributes. This approach implements the restriction of user roles using RBAC and attributes using ABAC. Since the proposed method uses two existing methods, it is first necessary to determine the main parameters of the two existing methods used in the proposed method, since which parameters are taken from which method reflects the advantages and disadvantages of that method [2].

Typically, in the RBAC method, users in the information system of commercial banks have different roles, and each role provides access to certain resources in the information system, that is, the access rights (authorizations) of system users to resources are assigned through their role in the system. Based on this, it is necessary to determine the following parameters, which are:

$F = \{f_1, f_2, \dots f_n\}$- a set of users in the information system of commercial banks;

$R' = \{r'_1, r'_2, \dots r'_m\}$- a set of roles in the information system of commercial banks;

$V = \{v_1, v_2, \dots v_k\}$- a set of competencies in the information system of commercial banks;

$F \to R'$- the connection between users and roles in the information system of commercial banks;

$R' \to V$- the connection between roles and authorities in the information system of commercial banks.

From these links, it can be seen that when a user logs into the information system of commercial banks, his role determines the access rights to a specific resource in the system. In the ABAC method, attributes are defined for users, resources and other elements in the system, and access is restricted based on the defined attributes. According to the ABAC method, access rights to the system are determined based on the attributes of each user in the information system of commercial banks. In the proposed method, it is necessary to define the following

Educator Insights: A Journal of Teaching Theory and Practice
Volume 2, Issue 1, January 2026
brightmindpublishing.com
ISSN (E): 3061-6964
Licensed under CC BY 4.0 *a Creative Commons Attribution 4.0 International License.*

parameters in the ABAC method for accessing the relevant attributes of the ABAC method, which are [3] :

$A_f = \{a_{f1}, a_{f2}, \dots\ a_{fn}\}$- a set of attributes of users in the information system of commercial banks;

$A_{r'} = \{a_{r'1}, a_{r'2}, \dots\ a_{r'm}\}$- a set of attributes of resources in the information system of commercial banks;

$A_t = \{a_{t1}, a_{t2}, \dots\ a_{tk}\}$- a set of attributes of the information system of commercial banks.

In accordance with these parameters, access rights to the information system of commercial banks according to the ABAC method $K$are determined by the following expression.

$$K = f\left(A_f, A_{r'}, A_t\right) \quad 1$$

Here f, it is a function that provides access based on user attributes, resource attributes, and system attributes in the information system of commercial banks.

Based on the determined parameters of these two methods in the process of access management in the information system of commercial banks, the main parameters of the proposed method are formed, that is, the parameters of the modified role-based access restriction method are determined, which are[4]:

$F = \{f_1, f_2, \dots\ f_n\}$- a set of users in the information system of commercial banks;

$R' = \{r'_1, r'_2, \dots\ r'_m\}$- a set of roles in the information system of commercial banks;

$A_f = \{a_{f1}, a_{f2}, \dots\ a_{fn}\}$- a set of attributes of users in the information system of commercial banks;

$A_{r'} = \{a_{r'1}, a_{r'2}, \dots\ a_{r'm}\}$- a set of attributes of resources in the information system of commercial banks;

$V = \{v_1, v_2, \dots\ v_k\}$- a set of competencies in the information system of commercial banks;

$F = f\left(R',\ A_f, A_{r'}\right)$- authorization based on the roles and attributes of users in the information system of commercial banks.

role-based access restriction method in accordance with these parameters, access rights to the information system of commercial banks are determined based on the following conditions[5].

Educator Insights: A Journal of Teaching Theory and Practice
Volume 2, Issue 1, January 2026
brightmindpublishing.com
ISSN (E): 3061-6964
Licensed under CC BY 4.0 *a Creative Commons Attribution 4.0 International License.*

$$A_{f_i} \rightarrow R'_{r'_j} \text{ and} f(A_f, A_{r'}) \quad 2$$

Here:

A_{f_i}user attributes in the information system of commercial banks ;f_i

$R'_{r'_j}$the right to access the resource corresponding to the role of the user in the information system of commercial banks ;r'_j

$f(A_f, A_{r'})$- a function for verifying access to the system based on the user's role and attributes in the information system of commercial banks.

The algorithm of the proposed method is implemented in the following sequence.

Step 1. Getting started.

Step 2. The user provides his/her identifier and authenticator to the system to access the information system, that is, he/she undergoes identification and authentication. If the user is a new user in the system, he/she will be redirected to the user registration module.

Step 3. Determine the user's role in the information system of commercial banks $.r'_j$

Step 4. Check user attributes in the information system of commercial banks A_f. and $A_{r'}$check resource attributes.

Step 5. Check resource attributes in the information system of commercial banks $.A_{r'}$

Step 6. Verify authorization using the access function (access authorization function) $.f(A_f, A_{r'})$

Educator Insights: A Journal of Teaching Theory and Practice
Volume 2, Issue 1, January 2026
brightmindpublishing.com
ISSN (E): 3061-6964
Licensed under CC BY 4.0 *a Creative Commons Attribution 4.0 International License.*

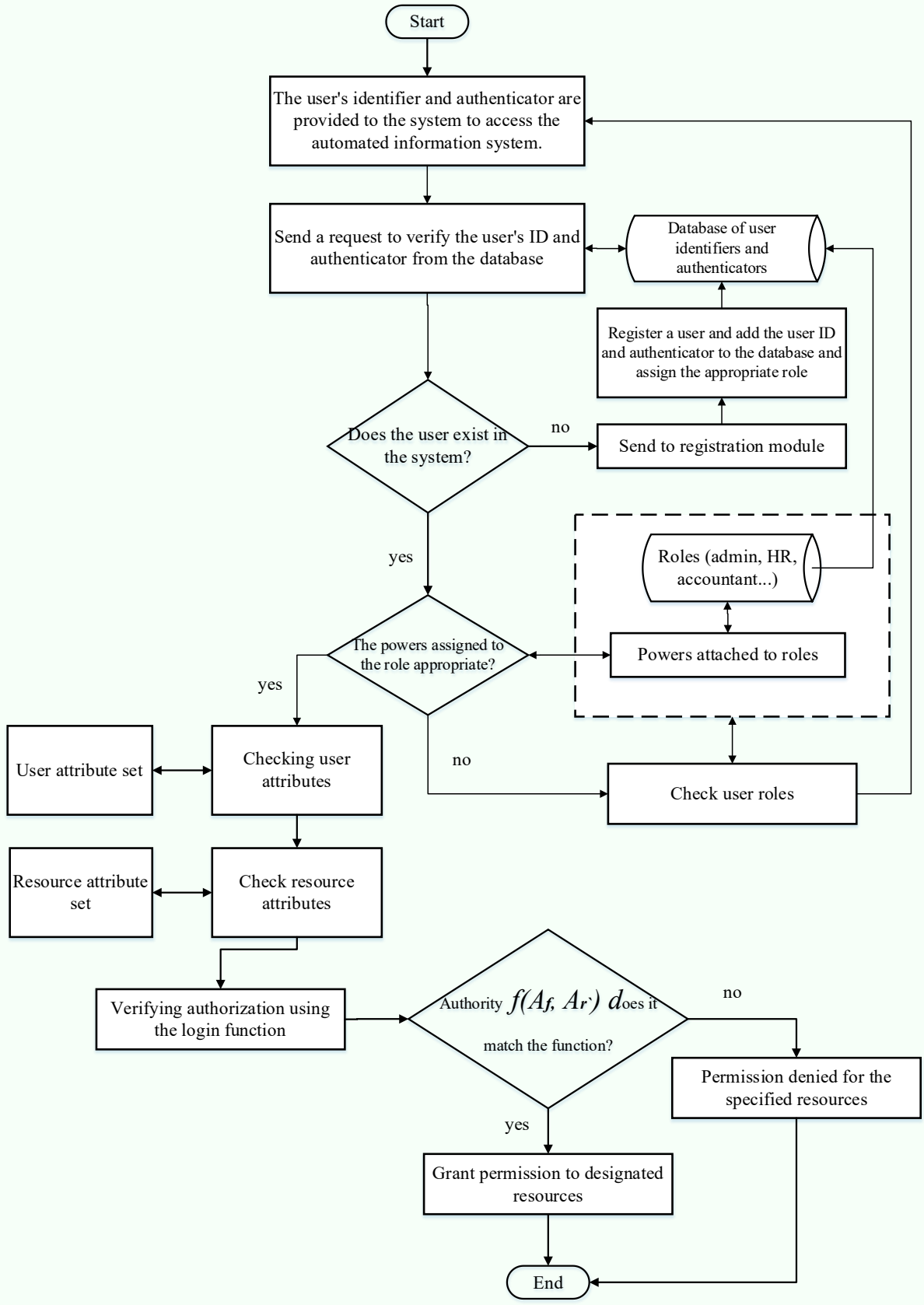

Figure 1. Block diagram of the modified role-based access restriction algorithm.

Educator Insights: A Journal of Teaching Theory and Practice
Volume 2, Issue 1, January 2026
brightmindpublishing.com
ISSN (E): 3061-6964
Licensed under CC BY 4.0 *a Creative Commons Attribution 4.0 International License.*

Step 7. If the access function corresponds to $f(A_f, A_{r\prime})$the user role in the information system of commercial banks $r_j'$and simultaneously provides access to the user attributes $A_f$and resource attributes in the information system of commercial banks $A_{r\prime}$, the access right in the information system of commercial banks, that is, the use of the specified resources, is allowed.

Step 8. If the access function $f(A_f, A_{r\prime})$corresponds to $A_f$the user role in the information system of commercial banks but does not provide access to the user attributes $r_j'$and resource attributes in the information system of commercial banks $A_{r\prime}$, the access right in the information system of commercial banks, that is, the use of the specified resources, is not allowed.

Step 9. Done.

It is required that the resources in the information system of commercial banks are generally stored in a distributed state in the database of commercial banks . Usually, the database of commercial banks is organized in a distributed state and is based on the principle of centralized management [6]. In the second step of the proposed algorithm, the user, who is implemented, provides his/her identifier and authenticator to the system to enter the automated information system , that is, passes identification and authentication. If the user is a new user in the system, it is recommended to update the roles assigned to him/her and the powers attached to these roles at a certain time interval (3 months, 6 months, 1 year) when directing the user to the registration module. The main reason for this is that the assigned role is assigned depending on the position, and the powers attached to the role are formed depending on the function of the position. During the specified time interval, additional functions may be added or reduced to the employee's position (role).

References

1. P. K. Paul and P. S. Aithal. “Database security: An overview and analysis of current trend”. International Journal in Management and Social Science, vol. 4, no. 2, pp. 53-58, 2019.

Educator Insights: A Journal of Teaching Theory and Practice
Volume 2, Issue 1, January 2026
brightmindpublishing.com
ISSN (E): 3061-6964
Licensed under CC BY 4.0 *a Creative Commons Attribution 4.0 International License.*

2. Hu, V. C., Ferraiolo, D., Kuhn, D. R. Guide to Attribute Based Access Control (ABAC) Definition and Considerations. NIST Special Publication 800-162, NIST, 2020.
3. Bozarov Farhod “Bank faoliyati avtomatlashtirilgan axborot tizimlari va texnalogiyalari” 2021
4. Shafiq, M., Tian, Z., Bashir, A. K. Security and Privacy of Banking Systems: Access Control Perspectives. Future Generation Computer Systems, vol. 118, 2021.
5. Ross Anderson “Security Engineering: A Guide to Building Dependable Distributed Systems” 2012
6. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements.