EduVision: Journal of Innovations in Pedagogy and Educational Advancements
Volume 2, Issue 1, January 2026
brightmindpublishing.com
ISSN (E): 3061-6972

IMPROVING USE RESTRICTION WITH MODIFIED ATTRIBUTES-BASED ALGORITHMS

Haydarov Elshod Dilshod ugli
Head of the Department "Information Security" at Tashkent University of Information Technologies named after Muhammad al-Khwarizmi

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

Abstract
This article considers the issues of improving the process of restricting access in automated information systems of commercial banks. In order to eliminate the shortcomings of the traditional role-based access control (RBAC) method, which are associated with lack of flexibility and non-accountability of attributes, a modified algorithm is proposed, integrated with the attribute-based access control (ABAC) approach. The proposed method allows determining access rights based on user roles and attributes, as well as resource attributes. The article develops a two-stage algorithm for granting access rights and verifying access in information systems of commercial banks. This approach serves to increase the security of bank information resources, reduce unauthorized access, and optimize the process of authority management.

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

Introduction

Today, as a result of the rapid development of digital technologies, the information systems of commercial banks are becoming more complex, and the volume of data stored and processed in them is increasing sharply. Since banking information systems contain financial transactions, customer information, settlements and other resources of strategic importance, ensuring information security in these systems is one of the urgent issues. In particular, the correct and precise management of

EduVision: Journal of Innovations in Pedagogy and Educational Advancements
Volume 2, Issue 1, January 2026
brightmindpublishing.com
ISSN (E): 3061-6972

user access rights to system resources is considered one of the main components of information security.

In practice, the role-based access control (RBAC) model is often used to organize access restrictions in commercial bank information systems. In this model, users are assigned roles in accordance with their position or functional duties, and access rights to resources are determined precisely through these roles. Although the RBAC model is characterized by simplicity and ease of management, it is not flexible enough for the dynamic environment of modern banking information systems. In particular, one of the main shortcomings of this model is its inability to take into account individual user attributes, contextual factors, and resource characteristics [1].

To overcome this problem, the attribute-based access control (ABAC) model has been proposed, which defines access rights based on user, resource, and system attributes. Although the ABAC model provides a high level of flexibility, its full implementation in the information systems of large commercial banks may lead to increased management complexity and computational costs.

Therefore, in recent years, there has been increasing interest in hybrid approaches that combine the advantages of RBAC and ABAC models. This paper proposes a modified role- and attribute-based access restriction algorithm adapted for commercial banking information systems. In the proposed approach, the RBAC model is used as the main mechanism and is enriched with the attribute-based control capabilities of the ABAC model[2].

In the article, the processes of granting access rights to users and verifying access are developed as separate algorithms. These algorithms provide decision-making based on comparing user authentication, roles and attributes with resource attributes. As a result, the process of restricting access in banking information systems becomes more accurate, flexible and secure.

The implementation of the algorithm proposed in the article requires that the resources in the information system of commercial banks are generally stored in a distributed state in the database of commercial banks. Typically, the database of commercial banks is organized in a distributed state and is based on the principle of centralized management [3-4]. In the second step of the proposed algorithm, the user who is being implemented provides the system with his/her identifier and authenticator to access the automated information system, that is, passes

EduVision: Journal of Innovations in Pedagogy and Educational Advancements
Volume 2, Issue 1, January 2026
brightmindpublishing.com
ISSN (E): 3061-6972

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).

proposed above can be divided into two security-oriented algorithms for granting or verifying the authorization status of users in relation to resources in the system during access restriction in the information system of commercial banks. These are:

- Algorithm for granting access rights to information systems of commercial banks;
- algorithm for checking access to information systems of commercial banks;

commercial banks consists of the following sequence [5,6].

Step 1. Getting started.

Step 2. The user provides the system with his/her identifier and authenticator 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. Identify the user role in the information system of commercial banks r_j' and the user attributes in the information system of commercial banks .A_f

Step 4. Compare the user's role r_j' and attributes with A_f resource attributes in the information system of commercial banks.$A_{r'}$

Step 5. Access to the information system of commercial banks $K = f(A_f, A_{r'})$ using to determine.

Step 6. If the granted powers $f(A_f, A_{r'})$ correspond to the user, allow him to use the specified resources in the information system of commercial banks.

Step 7. Otherwise, the user will not be allowed to use the specified resources in the information system of commercial banks.

Step 8. Done.

The algorithm for verifying access to information systems of commercial banks consists of the following sequence.

EduVision: Journal of Innovations in Pedagogy and Educational Advancements
Volume 2, Issue 1, January 2026
brightmindpublishing.com
ISSN (E): 3061-6972

Step 1. Getting started.

Step 2. The user provides the system with his/her identifier and authenticator 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. Verify the user role in the automated information system of commercial banks r_j' and the user attributes in the information system of commercial banks .A_f

Step 4. Compare the user's role r_j' and attributes with A_f resource attributes in the information system of commercial banks.$A_{r'}$

Step 5. If the user's attributes in the commercial bank's information system A_f match the user's role in the commercial bank's information system, the user's r_j' access to the commercial bank's information system is considered valid.

Step 6. Otherwise, the user's access to the information systems of commercial banks will be considered invalid.

Step 7. Done.

Based on the proposed method and algorithm, a clear and flexible approach to managing access rights (authorizations) in the system, taking into account the user's role and attributes, is presented in the process of restricting access to information systems of commercial banks. This approach allows creating a new environment for ensuring the security of information (resources) in the information system of commercial banks and improving the level of information security in the system, and correctly and accurately managing the processes of user access to the system. By accurately performing the steps in the proposed algorithm, it is possible to further increase the security of the information system of commercial banks and optimize the permissions (authorizations) granted to users in the system [7].

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.

2 Shafiq, M., Tian, Z. Secure Access Control Mechanisms for Banking Systems. Future Generation Computer Systems, vol. 117, 2021.

EduVision: Journal of Innovations in Pedagogy and Educational Advancements
Volume 2, Issue 1, January 2026
brightmindpublishing.com
ISSN (E): 3061-6972

3 Ganiev S.K., Irgasheva D.Y. Model of the state of threats to the Access Control System // Bulletin of TUIT: Management and Communication Technologies. https://uzjournals.edu.uz/tuitmct/vol2/iss2/2/. 2019 2 (45). -P. 30-37.
4 Миляев, П.В. Мошенничество в банковской сфере.
5 Биолчева, П. Разработване и оценяване на проекти за повишаване на физическата сигурност на търговските банки. Автореферат, София, 2014.
6 ISO/IEC 27001:2022. Information Security Management Systems — Requirements**.**
7 F.B. Botirov, Sh.N. Kobiljonov, Analysis of the system for monitoring information security incidents of a bank, Scientific - technical and information-analytical journal TUIT, 2022, №3(63), pp. 70-79.