DEVELOPMENT OF ROLE-BASED ACCESS CONTROL ALGORITHMS IN INFORMATION SYSTEMS OF COMMERCIAL BANKS

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 thesis is devoted to the issues of access restriction and access rights management in information systems of commercial banks . The study covers the structure and mechanism of operation of two main algorithms aimed at correctly granting users access rights to the information system and preventing unauthorized access - access rights granting and access restriction checking algorithms. The process of assigning permissions to users based on the role-based access control (RBAC) approach is described, and the relationships between users, roles, and resources are analyzed. Also, the possibilities of ensuring the confidentiality and integrity of information in information systems through the use of RBAC and ABAC models and integration with the Bella–LaPadula security model are substantiated. The results of the study serve to increase the efficiency of access management in information systems of commercial banks, strictly control permissions , and strengthen the level of information security.

Keywords: Commercial banks, information system, access control, access restriction, RBAC, ABAC, access rights, roles, resources, information security.

The algorithm for granting access rights to the information system of commercial banks, in turn, protects users from incorrect access rights when logging in to the system, and the second algorithm, which works as a separate module for each user who successfully logs in to the system, directs the algorithm for checking access restrictions to the information system of commercial banks. This, in turn, serves to increase the reliability of the protection mechanism [1] .
The algorithm for granting access rights to the information system of commercial banks looks like this:

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. The user's role in the information system is determined.

Step 4. The user is provided with access rights (authorizations) appropriate to the assigned role.

Step 5. Permissions are granted to the resources in the information system that the user can use.

Step 6. Done.

The algorithm for checking access restrictions to the information system of commercial banks looks like this (it is carried out based on the matrix presented above).

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. Access rights k_{ij} – are checked.

Step 4. If $k_{ij} = 1$ so, f_i–user– $r_j$is granted access (use) to the resource.

Step 5. If $k_{ij} = 0$ yes, f_i–user– $r_j$is not granted access (use) to the resource.

Step 6. Done .

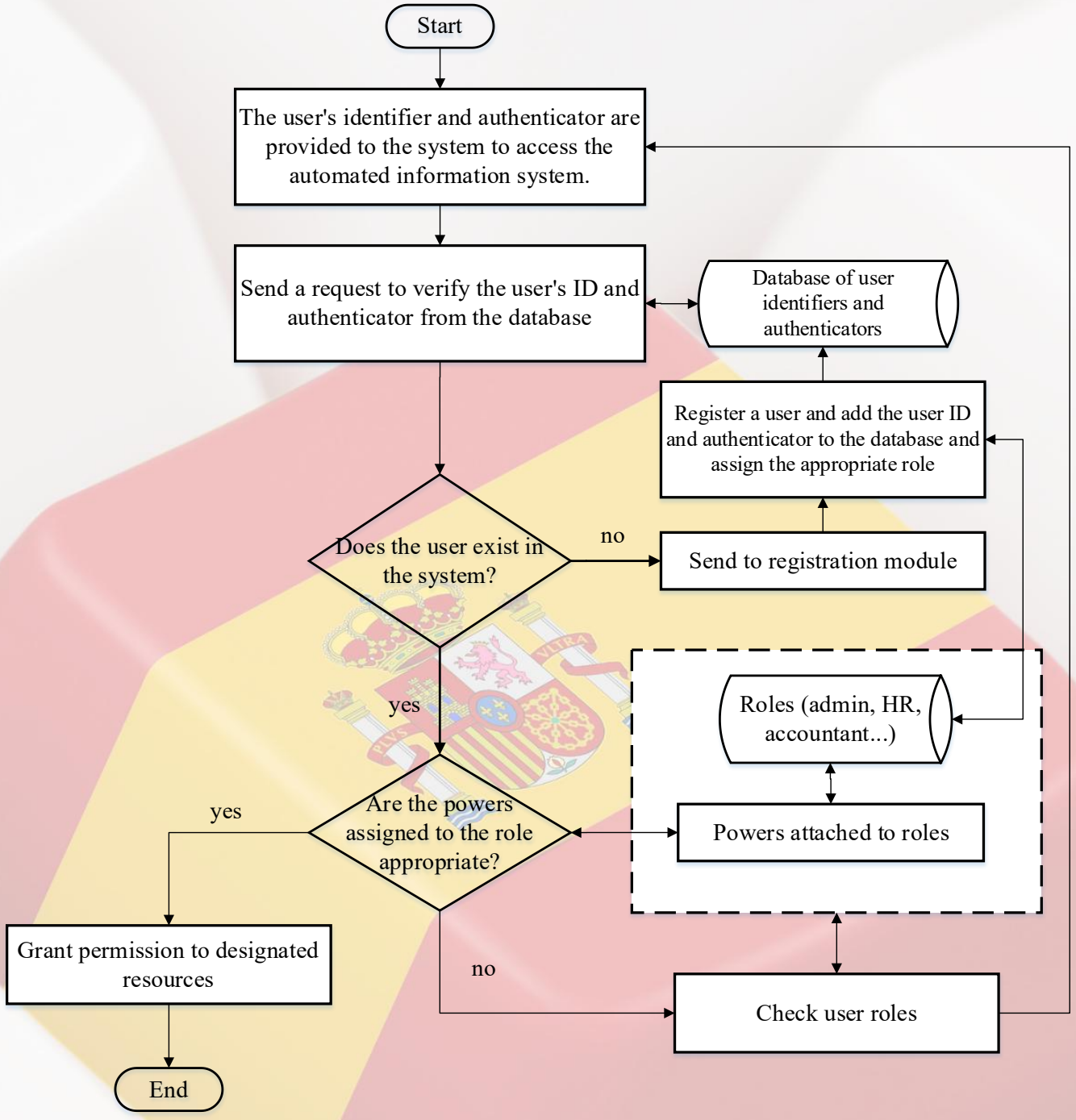

Figure 1. Block diagram of the algorithm for granting access rights to the information system of commercial banks.

The block diagram of the algorithm for checking access restrictions to the information system of commercial banks is similar to the block diagram of the algorithm for providing access rights to the information system of commercial banks, presented in Figure 1, with the main difference that the final result $k_{ij}$is obtained depending on the value of the parameter representing the access right. Usually, roles are formed in the information system depending on the field of activity of the organization [2] . Roles in the information system are formed mainly in accordance with the position specified in the approved structure of the organization.

Each role created in the information system represents a corresponding position, and the powers assigned to the role are formed based on the functional tasks in the job description and assigned to the role [3,4]. During the registration process of users in the information system of commercial banks, they are assigned to roles in the system depending on their position, and the powers assigned to the role are provided to the user.

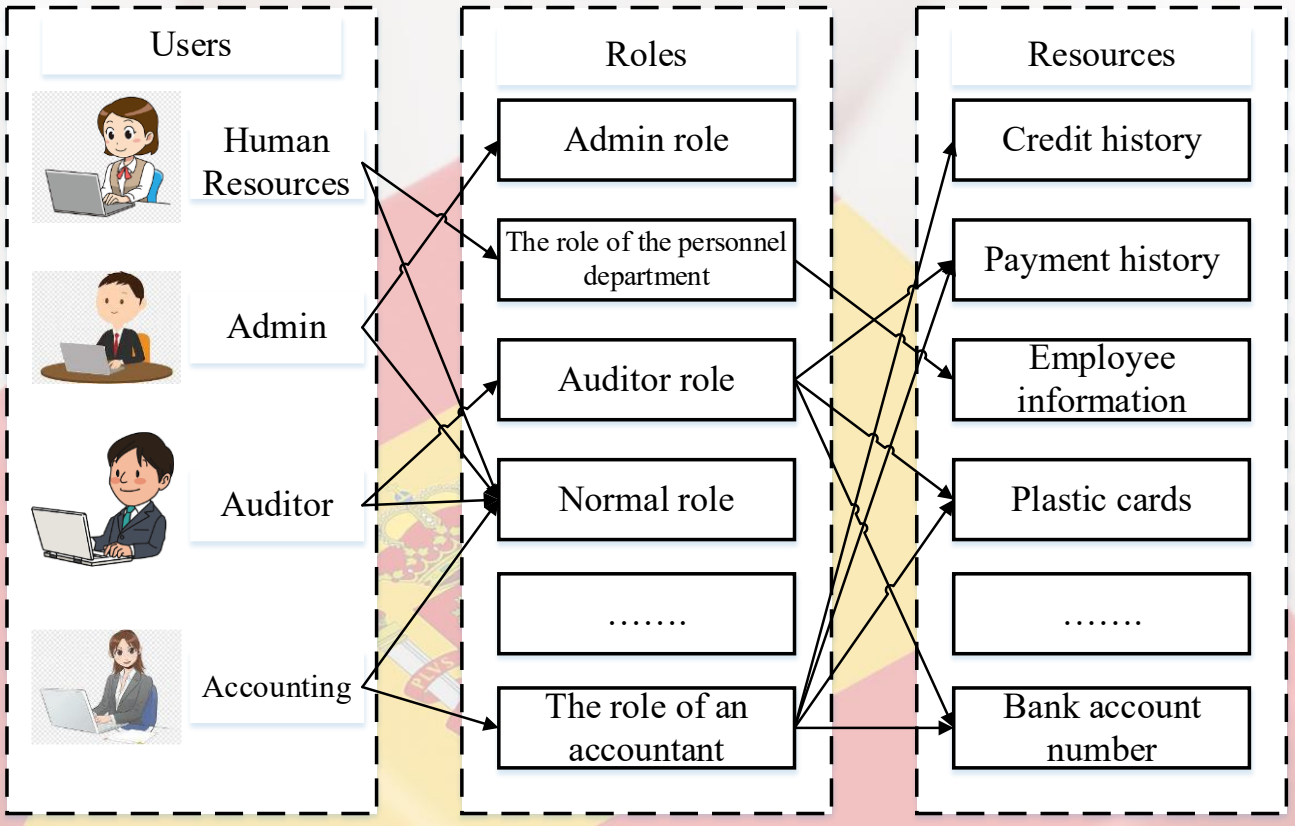

Figure 2. Example relationships between users, roles, and resources.

In order to reliably control the processes of restricting access in the information systems of commercial banks, it is recommended to use the methods recommended in the first chapter for managing access in the process of providing information security by using the resources in the system and granting authorizations to users, and the use of the Bella-LaPadula methods in the process of ensuring the integrity and confidentiality of information in the information system, as well as the use of the RBAC and ABAC methods, as well as the use of the Bella-LaPadula methods, as a basis for a comparative analysis[5]. Based on this, it is recommended to develop new methods and algorithms based on the improvement of the RBAC and ABAC methods in the process of managing access in the information systems of commercial banks, and to use the above-mentioned mathematical model of access control as a mathematical model of the developed method or algorithm. The proposed new method creates an opportunity to increase the efficiency of access control systems by partially eliminating the shortcomings of the RBAC and ABAC methods.

References

1 Stallings W. Network Security Essentials: Applications and Standards. – Pearson Education, 2019.
2 I. Ghafir, J. Saleem, M. Hammoudeh, H. Faour, V. Prenosil, S. Jaf, S. Jabbar and T. Baker. "Security threats to critical infrastructure: The human factor". The Journal of Supercomputing, vol. 74, no. 10, pp. 4986-5002, 2018.
3 Климович В.П. Финансы, денежное обращение и кредит: Учебник 2006.
4 Ross Anderson "Security Engineering: A Guide to Building Dependable Distributed Systems" 2012.
5 Hu V., Kuhn R., Ferraiolo D. Attribute-Based Access Control (ABAC). – NIST Special Publication 800-162, 2014.