

**A MULTILEVEL COMBINED MODEL OF USE RESTRICTION
BASED ON MATRIX AND NEURAL NETWORKS**

Kobiljanov Sh.N.

Independent researcher at Tashkent University of
Information Technologies named after Muhammad al-Khwarizmi

Abstract

This in the article commerce banks information in systems use restriction process improvement Bell– LaPadula for the purpose and Biba security models combination based on working issued many level approach matrix and artificial neuron to networks based model offer Offer done method user and information security degrees mathematician vector and matrices using expression opportunity gives and this the process artificial intellect technologies using to automation conditions creates . Neuron network in the model user and information security degrees entrance parameters as taken away , hidden layer through permission to give or restriction decision is formed . As a result commerce banks information in systems of information confidentiality and integrity one at the time provision , as well as use management process flexibility and accuracy increase opportunity is created .

Keywords: information security, commerce banks, use limitation, Bell – LaPadula model, Biba model, neuron networks, matrix model, confidentiality, integrity, artificial intellect.

Nowadays, the activities of commercial banks are organized on the basis of digital technologies, and their information systems process a large amount of important and confidential information. This information includes information on financial transactions, personal data of customers, account status and internal management processes of the bank. Therefore, ensuring information security in the information systems of commercial banks, in particular, maintaining the confidentiality and integrity of information, is one of the most urgent tasks.

Access restriction mechanisms play an important role in ensuring information security. These mechanisms strictly regulate the access rights of users to system resources and prevent unauthorized reading, writing, or modification. In practice, classical security models such as Bell–LaPadula and Biba are widely used to ensure access restriction. While the Bell–LaPadula model is mainly focused on

ensuring data confidentiality, the Biba model is focused on protecting data integrity [1].

However, in modern banking information systems, it is not enough to use only one security model. Because banking systems require both confidentiality and integrity of data at the same time. In this regard, the development of a method for limiting multi-level access by combining the Bell–LaPadula and Biba models is an urgent scientific issue. In the proposed approach, the security levels of the user and data are compared, and read and write operations are allowed only if the levels are equal.

This paper examines the possibility of representing this combined approach using a matrix model. The user and data security levels are represented by vectors and matrices, and the access restriction rules are mathematically formulated. In addition, the possibility of implementing the proposed method using artificial neural networks is also investigated. The neural network model accepts user and data security levels as input parameters, processes them in the hidden layer, and forms an authorization or denial decision in the output layer[2].

The proposed matrix and neural network-based approach will serve to automate the access control process in commercial banks' information systems, increase flexibility, and reduce errors related to the human factor. As a result, a new, effective, and modern model of ensuring information security in banking information systems will be formed.

One of the advantages of the proposed method is that it can be expressed in the form of matrices and can be used in artificial intelligence methods due to the presence of two or more input elements to the input parameters (since the number of perceptrons receiving the input elements of neural networks is required to be two or more, it is possible to introduce two rules for the input values, i.e., reading and writing rules, into the input layer of the neural network) [3].

The proposed method can be expressed in matrix form as follows.

$F = \{f_1, f_2, \dots, f_n\}$ - a set of users in the information system of commercial banks;
 $M = \{m_1, m_2, \dots, m_l\}$ - collection of data in the information system of commercial banks;

Since the transposed matrix must be used, it is recommended to express the above t_f and t_m in terms of v_f and in order to avoid misunderstandings in the following expressions v_m . Accordingly, the vector formed by them will be as follows:

V_f – a vector representing the security levels of users in the information system of commercial banks;

$$V_f = [v_{f_1}, v_{f_1} \dots v_{f_n}]^T \tag{1}$$

V_M – A vector representing the security levels of information in the information systems of commercial banks.

$$V_d = [v_{d_1}, v_{d_1} \dots v_{d_l}]^T \tag{2}$$

here: T –transposed matrix.

and data v_m in the information systems of commercial banks v_f are taken as a matrix.

$$V_f = v_{f_i}, \text{ and } V_m = v_{m_j} \tag{3}$$

If $V_f = V_m$ so, the user in the information system of commercial banks will f_i only m_j be able to read and write information, and its matrix will be represented in the following form:

$$\text{Read} = [v_{f_1}, v_{f_1} \dots v_{f_n}]^T = [v_{d_1}, v_{d_1} \dots v_{d_l}]^T \tag{4}$$

Based on the above, it can be said that if the user's security level and the security level of the data in the information system of commercial banks are equal, the user will have read and write permissions[4].

In addition, the proposed method is expressed using the neural network method as follows. When expressing the proposed method using the neural network method, information about the security level granted to the user and the security level of the information is created in the input layer to control access in the information system of commercial banks using a neural network. After that, the hidden layer of the neural network helps to determine the authority (permission) of the user in the information system of commercial banks to use the information in the system. In the output layer of the neural network, a decision is made on the acceptance of the request sent to the user for authorization (permission), that is, granting or denying permission.

The data for the neural network input layer is as follows:

$$x_1 = t_f, \quad x_2 = t_m \tag{5}$$

The hidden layer of a neural network is calculated using the following expression:

$$z = w_1 * t_f + w_2 * t_m + b \tag{6}$$

here:

z — the output signal of the hidden layer of a neural network.

w_1 and w_2 — weights. Weights in a neural network ($w_1, w_2, \dots w_n$)— These are the parameters that are learned during the training process of the network, which determine the importance (or influence) of the input data. In each neural network, there are connections (synapses) between neurons from the input layer to the

output layer, and each connection has its own weight. These weights are learned during the training process of the network and help the model produce accurate and correct results. [5]

b- bias, this quantity is used to adjust the output function of the neuron.

Hidden layer neurons are used to optimize the principles of the Bell-LaPadula and Biba models and compare the security levels between users and data in the information system of commercial banks.

The output layer of a neural network is calculated using the following expression:

$$y = \sigma(w_1 * z_1 + w_2 * z_2 + \dots + w_m z_m + b) \quad 7$$

here:

y- the size of the user's access permission (1 or 0) to access information in the information system of commercial banks.

σ - activation function.

z_1, z_2, \dots, z_m — the output signal of the hidden layer of a neural network.

w_1 and w_2 — weights.

b— the bias of the output layer of the neural network.

The relationship between the activation function σ and the output signal of the hidden layer of a neural network .z

$$\sigma(z) = \frac{1}{1 + e^{-z}} \quad 8$$

This function is used to determine the output, the permission, because its result is in the range $y = 0$ and $y = 1$, which indicates whether the user is allowed or not, that is, if the output value of the neural network $y = 1$ is, the user in the information system of commercial banks is allowed to access the relevant information in the system, otherwise, if the user's security level is lower than the security level of the information in the system he wants to use $y = 0$, the value is accepted and permission to use the information is not granted, that is, the use is restricted.

The proposed method, as a result of combining the Bell-LaPadula and Biba models, shows that the relationship between the security levels of users in the information system of commercial banks and the security levels of data can be applied in both matrix and neural network methods. It can be seen that the conditions for performing read and write operations on users in the information system of commercial banks can be implemented both in the matrix method and in the neural network method, and in the proposed multi-level combined method

of access restriction, the user has access to only information equal to his security level [6].

The main advantage of the proposed method over existing methods is explained by the following two features. These features are:

1. Security levels are provided . Commercial banks require that the security level between the user and the data in the information system be equal, since both the Bell-LaPadula and Biba models provide incompatible restrictions. This means that a user with read permission is only allowed to read data within his security level , and a user with write permission is only allowed to write to data within his security level.

2. Ensuring integrity and completeness. The proposed multi-level combined method of access restriction allows to ensure both confidentiality and integrity of information using one method at the same time . The user in the information system of commercial banks can not only read and write information, but also perform all operations in accordance with their security levels [7, 8].

The Bell-LaPadula and Biba models in the information system of commercial banks, in turn, allows maintaining the confidentiality and integrity of information in this information system during the process of access restriction in the information system.

References

- 1 Bishop, M. Computer Security: Art and Science (2nd Edition). Addison-Wesley, 2021.
- 2 Goodfellow, I., Bengio, Y., Courville, A. Deep Learning. MIT Press, 2022.
- 3 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
- 4 Kumar, R., Singh, A. AI-Based Access Control for Financial Information Systems. International Journal of Information Security, vol. 24, 2023.
- 5 Zhang, Y., Li, X. Formal Analysis of Bell-LaPadula and Biba Hybrid Models. Journal of Information Security and Applications, vol. 58, 2021.
- 6 Botirov F.B., Kobiljonov Sh.N., The problem of monitoring the state of information security of the automated banking system, Science and Education in Karakalpakstan, 2022 №4/2 ISSN 2181-9203. pp. 80-85.

- 7 L. Esmaeili and A. H. Golpayegani, “A novel method for discovering process based on the network analysis approach in the context of social commerce systems,” J. Theor. Appl. Electron. Commer. Res., vol. 16, no. 2, pp. 34–62, 2021.
- 8 Ji Kun, Dou Shixin. Research on the innovative development of digital RMB smart contracts of Postal Savings Bank of China [J]. Postal Research, 2025, 41 (1): 53 – 57.