Improving the method of detecting insider attacks on the organization's information resources

Vitalii Savchenko[1,*,†], Valeriia Savchenko[1,†], Roman Vozniak[2,†] and Oleksandr Sampir[2,†]

[1] *State University of Information and Communication Technologies, Solomianska street, 7, 03110, Kyiv, Ukraine*

[2] *The National Defence University of Ukraine, Air Force avenue, 28, Kyiv, 03049, Ukraine*

Abstract

The article deals with the problem of detecting insider attacks on the organization's information resources. This article is a continuation of the authors' publication, which proposed a method for detecting malicious activity based on the statistical measure IDF (Inverse Document Frequency) and calculating the cosine similarity of two vector assets. The authors show that this similarity-based approach works well in organizations where employees' access rights to the organization's information resources do not overlap. However, in the case of using shared resources or masking the activity of an insider, this approach is not very effective. The authors of the article propose an improved method, the difference of which is the presence of two matrices: the matrix of permissions and the matrix of real access. The difference of such matrices expressed as a percentage of the user's total access to information assets makes it possible to calculate a measure of the user's malicious activity. Input data for the technique is information from IDS intrusion detection systems. The simulation results based on the given examples show that the improved method is more adequate compared to the cosine similarity method, which makes it possible to use it in a wide range of applications. The method allows you to determine the abnormal activity of users in the organization, which makes it possible to detect insider attacks at an early stage. The method can be used by information security administrators for further analysis of user activity.

Keywords

information asset, information resource, insider, abnormal user behavior, cosine similarity

1. Introduction

In today's digital world, where access to information is becoming increasingly important for the successful operation of organizations, user interaction with information resources is becoming a key factor in efficiency and security. Organizations invest significant effort in developing and maintaining systems that provide access to data and resources for their employees and customers. However, the detection of anomalies in this interaction can have a significant impact on the security and functionality of these systems. Anomalies in interaction with an organization's information resources can include a wide range of events, from unusual user activity to potential cyber attacks or security breaches. Understanding, detecting, and responding in a timely manner to such anomalies become critical to ensuring the reliability of information systems.

In this study, we will consider the method of determining anomalies of user interaction with the organization's information resources. The study is a continuation of our previous publication [1], where we already proposed a method for detecting anomalies in the activity of information system users. It is aimed at identifying insiders, which will help increase the security and efficiency of

Information Technology and Implementation (IT&I-2024), November 20-21, 2024, Kyiv, Ukraine

[*] Corresponding author.

[†] These authors contributed equally.

savitan@ukr.net (V. Savchenko); savchenko.valeriya@gmail.com (V. Savchenko); Romeros80@ukr.net (R. Vozniak); Sampir1984@ukr.net (O. Sampir)

0000-0002-3014-131X (V. Savchenko); 0000-0003-1921-2698 (V. Savchenko); 0000-0002-3789-2837 (R. Vozniak); 0000-0002-3564-1997 (O. Sampir)

information systems of organizations by identifying and solving anomalies in their interaction with users.

2. Problem statement

The general problem of identifying anomalies in the interaction of users with the organization's information resources is that this task is complex and requires an integrated approach due to several key reasons:

- Variety of Anomalies: Anomalous user behavior can take many forms, including unusual patterns of information access, unusual activity, unauthorized access attempts, or insider threats. The diversity of these anomalies makes their detection difficult.
- Volume of data: Organizations have huge volumes of data generated as a result of user interaction with information systems. Analyzing these large volumes of data to detect anomalies requires powerful processing and analysis tools.
- Dynamics of change: User behavior and the structure of information systems can change over time. What was normal yesterday may become an anomaly today. You need a system that can adapt to changes in the environment.
- Data heterogeneity: User interaction data can be presented in different formats and sources. Combining them and processing them to detect anomalies can be difficult due to differences in data structures and types.
- Need for accuracy: Anomaly detection requires high accuracy because misinterpretation can lead to misclassification of normal behavior as abnormal or vice versa.
- Ensuring privacy: When detecting anomalies, the confidentiality and privacy of user data must be preserved, which can make it difficult to implement some analysis methods.

Since these problems are complex and diverse, the detection of anomalies in the interaction of users with information resources requires the use of various methods of data analysis, machine learning, and the development of specialized systems to effectively solve this problem.

3. Related works overview

Anomaly detection is a direction that is becoming more and more relevant every year. There are various ways of detecting anomalies in the activity of information system users. Most of them are based on the analysis of various technical indicators, such as network activity, use of peripheral devices, system load, intensity of interaction with information systems, etc.

In the article [1], we investigated the intrusion detection method based on the calculation of the similarity of user actions. The disadvantage of the previous study is that, despite its advantages, the proposed method is poorly protected against deception by unscrupulous users, as it is based on the calculation of the similarity coefficient of the user's actions using cosine similarity. This approach allows the attacker to easily imitate loyal activity, thereby leveling off his malicious activity. Our other paper [2] investigates the detection of insider attacks based on the time parameters of the protection system. In this publication, we conclude that detection of such an attack is possible only when the defense system is able to react faster than the attacker.

The article [3] provides a comprehensive review of the existing literature, which examines recent advances in anomaly detection methods for detecting security threats in cyber-physical systems. The authors analyze 296 articles devoted to the detection of anomalies and identify the shortcomings of various detection methods, including: limited resources, lack of standardized communication protocols, heterogeneity of technologies and protection systems, different information security policies. The authors of the article [4] propose approaches to the classification of anomaly detection methods in modern attack detection systems. It is shown that the methods of detecting anomalies in modern attack detection systems are not sufficiently elaborated in terms of the formal attack model, and, therefore, it is quite difficult for them to strictly evaluate such properties as computational complexity, correctness, and completeness.

The authors of the publication [5] evaluate anomaly detection methods based on the aspect of their applicability to various systems with the minimization of the user input. The obtained results show that the most effective method of detecting anomalies, which can be transferred to different systems and minimizes the user's work, are systems based on machine learning. The publication [6] defines three main methodological areas for diagnosing anomalies (machine learning, deep learning, statistical approaches) and summarizes exactly how the corresponding models are used to detect anomalies. In addition, the authors explain which specific application areas are typically addressed by anomaly detection in the context of cloud computing environments and which relevant public datasets are often used for evaluation.

In [7], the authors propose an intelligent system for detecting anomalies and identifying smart home devices using collective communication. The concept of the system's operation is based on obtaining benefits from the integration of smart homes into a social network in terms of increasing the security of both a single smart home and the entire social network of connected smart homes. Publication [8] proposes an unsupervised method that was developed to detect anomalies when information is not labeled or classified. Information extraction approaches based on machine learning, developed for the implementation of the anomaly detection system, were used.

Currently, intrusion detection systems (IDS - Intrusion Detection System) are increasingly being implemented in the practice of organizations. Their work is based on the use of a database of attack patterns (signatures) and machine learning methods. In addition, such systems can register a set of data characterizing the interaction of employees with the organization's information assets and have proven themselves well in solving the problem of detecting anomalies.

The article [9] describes a study of log mining in the field of microservices technologies with the detection of anomalies from logs, that is, events that require deeper inspection by analysts. The authors propose a new approach to finding numerical representations of computer logs without making assumptions about the format of the underlying data and without requiring programming knowledge. The article [10] presents a distributed approach for real-time anomaly detection in large-scale environments. The method has the ability to detect consistent and quantitative anomalies within a multi-source streaming log.

The purpose of this article is to improve the previously proposed method of detecting anomalies of user interaction with the organization's information resources, which would allow using the results of modern intrusion detection systems (IDS) and would be simple enough for practical implementation by information security administrators.

4. The method of detecting insider attacks on the organization's information resources

4.1. General approach

As before, we will take as a basis the methodology based on the use of a bipartite graph [1, 11] to display the interaction of users (employees of the organization) with assets (information systems) on the basis of network data collected by the IDS system.

The set of users will be denoted by $U = \{u_1, \dots, u_n\}$, the information assets will be defined as the set $A = \{a_1, \dots, a_n\}$, and the set of users who accessed to assets a_i over a certain period of time will be defined as the set U_{A_i}. We denote as G_{A_i} - a complete graph U_{A_i}, where the value of the weight between pairs of vertices is the value of similarity.

A bipartite graph reflecting the fact of users' access to assets is denoted by a binary matrix A_U. At the same time $A_U(i, j) = 1$, if the user u_i accesses the a_i asset, and $A_U(i, j) = 0$ if not. It is suggested to use the statistical measure IDF (Inverse Document Frequency) to assess the connection of users with assets. As a measure of IDF I_{DF}, it is suggested to take a sigmoidal function in the form:

$$I_{DF}(U_i) = \frac{1}{1+e^{\frac{\gamma}{2}-\frac{\gamma E \times U_i}{|A|}}}, \tag{1}$$

where $E = (1,1,\ldots,1)$ is unit vector of dimension m; $|A|$ is a power of set A; U_i is a column i-user of the matrix A_S (access vector); γ is a sensitivity coefficient of the function.

The matrix obtained after the transformation will be denoted by I_{DF}^{UA}. The similarity between pairs of users can be obtained based on their access vectors. To measure the similarity of two vector assets, it is suggested to use cosine similarity [12]:

$$C(u_i, u_j) = \frac{I_{DF}(U_i) \times I_{DF}(U_j)}{\|I_{DF}(U_i)\| \times \|I_{DF}(U_j)\|} = \frac{\sum_{k=1}^{m} I_{DF}(U_{i,k}) \times I_{DF}(U_{j,k})}{\sqrt{\sum_{k=1}^{m}\left(I_{DF}(U_{i,k})\right)^2} \times \sqrt{\sum_{k=1}^{m}\left(I_{DF}(U_{j,k})\right)^2}}. \tag{2}$$

Given two feature vectors X and Y, the cosine similarity can be represented using the scalar product and the norm. When a user interacts with an organization's information assets, the cosine similarity of two users ranges from 0 to 1, since the angle between the two frequency vectors cannot be greater than 90°. Cosine similarity is effective as an evaluation measure, especially for sparse vectors, since only non-zero values are taken into account [10].

As a result of the calculations, a similarity matrix of user interaction with information assets will be obtained. It is assumed that if one of the users is an intruder, then his actions will be reflected in the similarity matrix. Around each asset, an individual group of users is formed who work with it and refer to it. To calculate the similarity between groups of users, it is necessary to calculate the average similarity between all pairs of users (total user similarity):

$$C\left(G_{A_k}\right) = \frac{\sum_{i=1}^{n} \sum_{j=1}^{n} C(U_i, U_j)}{\left|U_{A_k}\right| \times \frac{U_{A_k}-1}{2}}, \forall U_i \neq U_j \in U_{A_k} \forall U_j, \tag{3}$$

where $\left|U_{A_k}\right|$ is number of users in the group.

If $C\left(G_{A_k}\right)$ has a high value, it means that users have a strong engagement with asset a_k. To detect anomalous user actions, it is necessary to determine the average similarity for the subgroup $C\left(G_{A_k}\right), \forall i \vee j = k$, in which a single user k is compared with other users, and to determine the rating of this user relative to the average value for the organization:

$$R(u_k, A) = \frac{C\left(G_{U_k}\right) - C\left(G_{A_k}\right)}{C\left(G_{A_k}\right)} \times 100\%, k = 1, \ldots, m, \tag{4}$$

where $C\left(G_{U_k}\right)$ is the subset of users that are compared to user u_j. The larger the value of $R(u_k, A)$, the more likely that user u_j's access to assets a_i is abnormal.

The proposed technique for detecting abnormal user actions based on network data analysis can be presented in the form of a sequence of steps:

1. Building sets of users and assets.
2. Construction of a bipartite interaction graph.
3. Calculation of the statistical measure of IDF.
4. Calculation of the similarity matrix of user actions.
5. Calculation of the overall similarity of user actions.
6. Detection of abnormal actions.

4.2. Algorithm for detecting anomalies in the interaction of users with the organization's information assets (Algorithm of similarity)

1. $A_U \leftarrow \begin{bmatrix} a_{u_{1,1}} & \cdots & a_{u_{1,n}} \\ \vdots & \ddots & \vdots \\ a_{u_{m,1}} & \cdots & a_{u_{m,n}} \end{bmatrix}$ – forming a matrix of user access to assets.
2. $\gamma \leftarrow$ – entering the sensitivity value of the algorithm.
3. $m = Length[A_U]$ – determining the number of assets.
4. $n = Length[A_{U_i}]$ – determining the number of users.
5. $E \leftarrow (1, \dots, 1_m)$ – forming a unit vector.
6. $I_{DF}(U) = Table\left[\frac{1}{1+e^{\frac{\gamma}{2}-\frac{\gamma E\times Table\left[\left\{a_{u_{i,j}}\right\},\{m\}\right]}{m}}}, \{j,n\}\right]$ – determination of the IDF parameter.
7. $I_{DF}(A_U) = Table\left[If\left[a_{u_{i,j}} = 1, I_{DF}(U)_i, 0\right], \{i,n\}, \{j,m\}\right]$ – substitution of $I_{DF}(U)$ values to the matrix of sigmoidal functions.
8. $C(u_i, u_j) = Table\left[\frac{\sum_{k=1}^{m} I_{DF}(A_U)_{k,i} \times I_{DF}(A_U)_{k,j}}{\sqrt{\sum_{k=1}^{m}\left(I_{DF}(A_U)_{k,i}\right)^2} \times \sqrt{\sum_{k=1}^{m}\left(I_{DF}(A_U)_{k,j}\right)^2}}, \{i,n\}, \{j,n\}\right]$ – calculation of the similarity matrix for user actions.
9. $C(G_{U_k}) = Table\left[\frac{1}{n-1}\sum_{j=1}^{n} If\left[i = j, 0, C(u_i, u_j)\right], \{i,n\}\right]$ – determining the similarity of the actions of individual users.
10. $\overline{C}(G_{U_k}) = \frac{1}{n}\sum_{i=1}^{n} C(G_{U_k})_i$ – determination of the average value of the similarity of user actions.
11. $R(u_k, A) = Table\left[\frac{C(G_{U_k})_i - \overline{C}(G_{U_k})}{\overline{C}(G_{A_k})} \times 100\%, \{i,n\}\right]$ – detection of abnormal actions by individual users.

4.3. Improvement of the method (Advanced method)

Despite the obvious advantages, such an approach, which is based on determining the similarity of the actions of individual users, has significant disadvantages, in particular:

1. The approach works well in those organizations where information resources are clearly demarcated between employees. That is, sets of information resources of individual employees do not overlap.
2. In this model, the impact of suspicious employee access to the organization's resources can be neutralized by the appropriate combination of access to authorized resources.

In order to avoid the mentioned shortcomings, it is suggested to improve the method as follows.

To control user access to the organization's resources, we introduce an access matrix $A_A = \begin{bmatrix} a_{a_{1,1}} & \cdots & a_{a_{1,n}} \\ \vdots & \ddots & \vdots \\ a_{a_{m,1}} & \cdots & a_{a_{m,n}} \end{bmatrix}$. The elements of this matrix denote: $A_A(i,j) = 1$, if the user u_i is granted access to asset a_j, and $A_A(i,j) = 0$, if not.

The actual access of users to assets will still be determined by the matrix $A_U = \begin{bmatrix} a_{u_{1,1}} & \cdots & a_{u_{1,n}} \\ \vdots & \ddots & \vdots \\ a_{u_{m,1}} & \cdots & a_{u_{m,n}} \end{bmatrix}$.

To determine the malicious activity of users, we will calculate the difference between the matrices $M = A_A - A_U$. As a result, we will get a matrix, the elements of which will be numbers from the set $M \in \{-1,0,1\}$, where: $m_{i,j} = -1$ in the case of malicious user activity; $m_{i,j} = 0$ – the user has made legal access to the authorized assets; $m_{i,j} = 1$ – the user did not access the authorized assets.

Let's count the number of "-1" values in each column of the matrix M and divide these values by the number of "1" values in each column of the matrix A_A. We will present the obtained results in percentage ratio. This is necessary in order to take into account the general activity of users: for a user with a limited scope of access, even a single malicious access will produce a result similar to a user with wide access rights to the organization's resources.

5. Simulation and discussion of results

As before, we will consider the effect of the technique on an abstract example [13]. Assume that the organization has 10 users and 15 information assets. Then the bipartite graph of user interactions with information assets can be described by a binary matrix A_S of dimension 15×10.

Let's consider and compare the main scenarios of the application of the two methods.

5.1. Scenario 1

Two groups of users work with authorized information assets and their actions regarding access to the assets do not overlap. However, one of the users (#5) is trying to access asset #8, which he does not have permission to access. In addition, user #5, knowing the algorithm for detecting anomalies in user interaction, tries to bypass the protection system, for which he does not use one of the allowed resources, for example, asset #1. These two situations can be described by matrices of access [14]

$$A_U^a = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \mathbf{1} & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}, \quad A_U^b = \begin{bmatrix} 1 & 1 & 1 & 1 & \mathbf{0} & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \mathbf{1} & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}, \qquad (5)$$

where matrix columns denote users of the organization; the rows of the matrix indicate the organization's assets; values of "1" in blue color indicate assets to which users are allowed to access; value "0" in black color – assets to which access is prohibited.

According to Scenario 1, the matrix A_U^a of formula (5) describes the attempt of user #5 to access the prohibited asset #8. Matrix A_U^b of formula (5) is the attempt of user #5 to access asset #8 bypassing the security system by ignoring the asset #1 allowed to him.

In the case of A_U^a, the application of the algorithm immediately gives a result in which the abnormality of the behavior of user #5 is 7.2% against the background of the rest of the users, whose degree of abnormality ranges from −3.4% to +1.3% (Figure 1). This clearly indicates anomalous behavior of this user, which may be an indication of an insider threat [15].

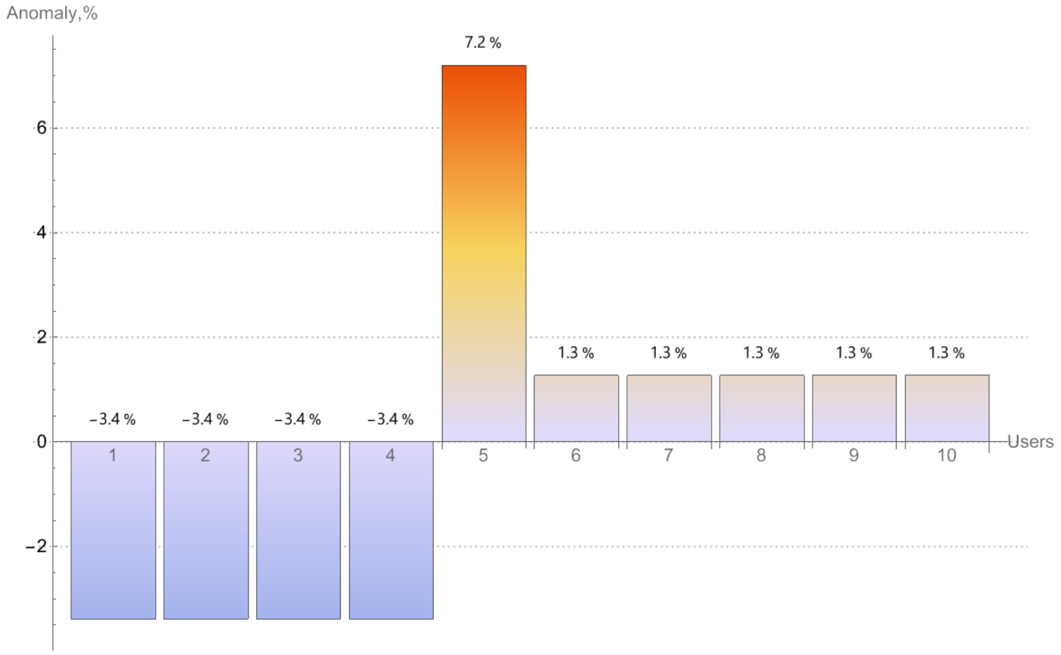

Figure 1. Calculating the abnormality of user behavior #5 using the similarity algorithm.

In the situation A_U^b, when user #5 tries to bypass the protection system, for which he does not use one of the permitted resources, for example, asset #1, when calculating the abnormality of the behavior of user #5, the algorithm will give an erroneous result (Figure 2) . In this case, for user #5, the degree of abnormality will be only 1.9% and therefore, against the background of general indicators from −4.0% to 2.8%, it will be impossible to recognize an insider attack [16].

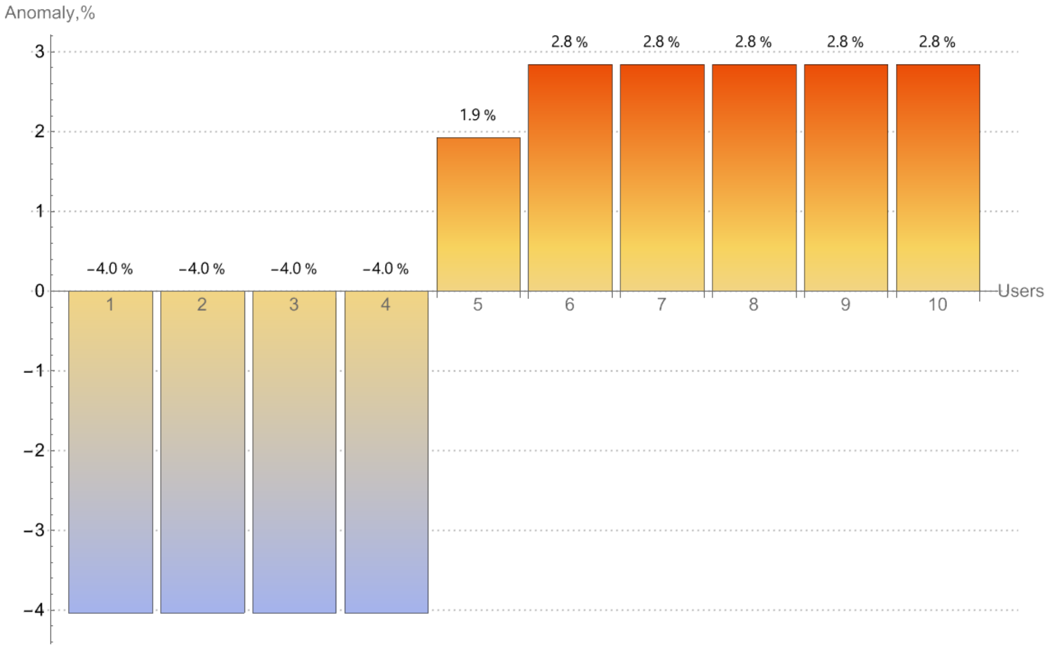

Figure 2. Calculating the abnormality of the behavior of user #5 using the similarity algorithm when he tries to bypass the protection system.

In the same situation, when applying the improved methodology, in both cases (when user #5 access is attempted without bypassing the protection system and with the protection system bypassed), we get a result that clearly indicates the anomalous behavior of user #5 (Figure 3).

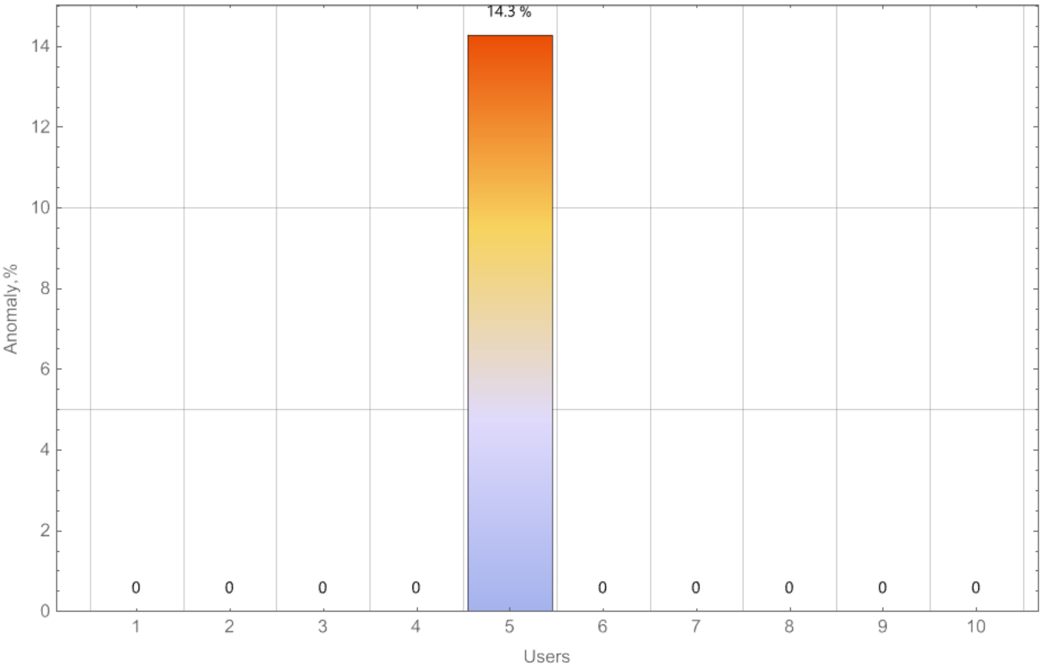

Figure 3. Calculating the abnormality of user behavior #5 using an improved method.

5.2. Scenario 2

In the previous scenario, the organization's information assets were clearly demarcated between users. However, this situation in most organizations is the exception rather than the rule. As a rule, when performing tasks, employees of organizations very often use common resources. In this case, the application of the method based on the similarity matrix [17] gives extremely contradictory results that cannot be interpreted.

As in Scenario 1, we denote the access rights of users to the assets of the organization by the matrix A_A^c. The fact of user access to assets is denoted by the access matrix A_U^d. In the matrix of actual access, let's mark with red symbols "1" attempts of users to gain unauthorized access to assets, and with "0" symbols in brown – authorized assets that were not used by users. In this case, the matrices A_A^c and A_U^d, as an example, can have the form

$$A_A^c = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}, A_U^d = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}. \quad (6)$$

We simulate the situation described by matrices (6) using the similarity algorithm and the improved method. The results of modeling using the similarity algorithm and the improved method are shown in Figure 4 and Figure 5.

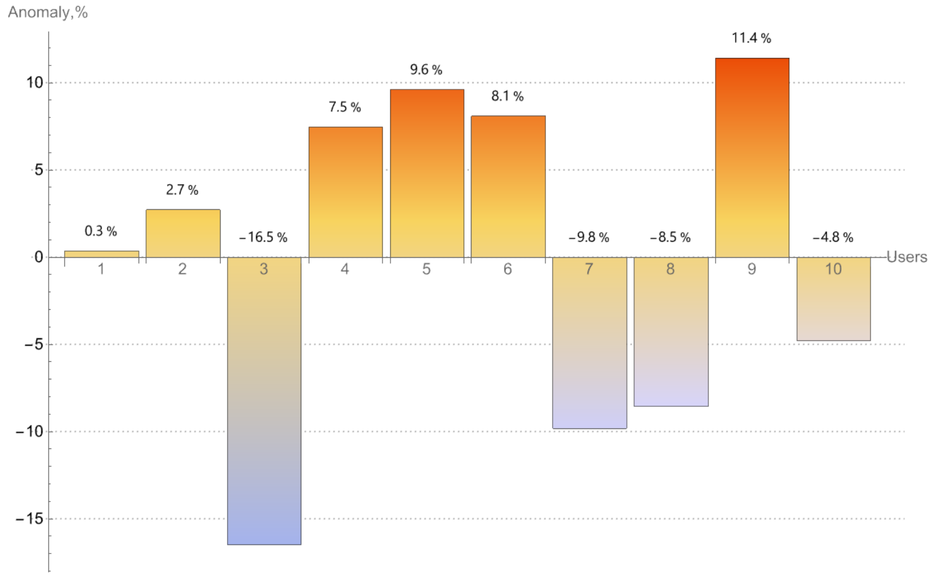

Figure 4. Calculating anomalies using the similarity algorithm.

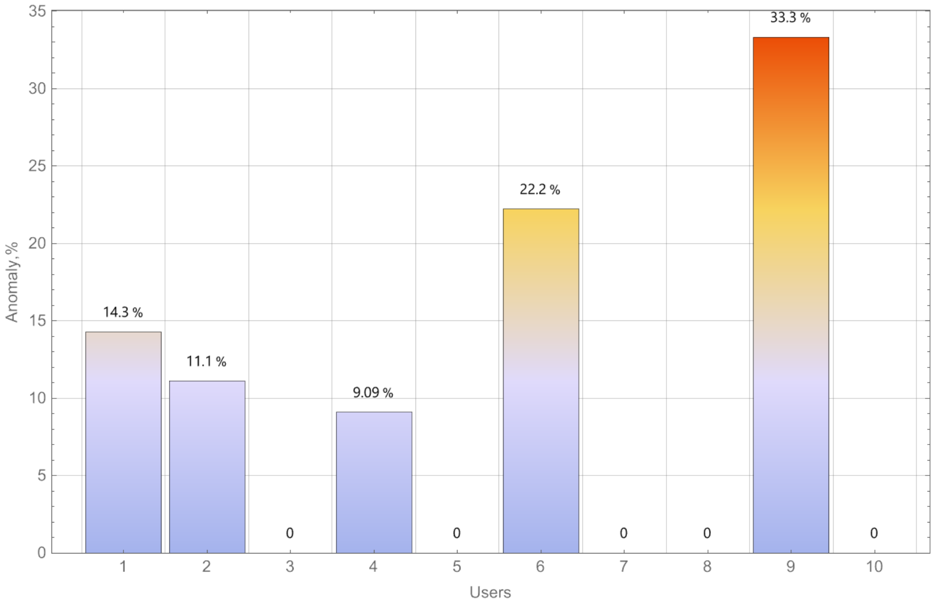

Figure 5. Calculating of anomalies according to the improved method.

As we can see from Figure 4, in the case when the access rights of different users overlap (when users can use shared resources), the similarity algorithm gives results that do not unambiguously indicate anomalies in user behavior. At the same time, the results in Figure 5 fully reproduce the pattern of malicious activity described by the matrix A_U^d. At the same time, the system can also determine the level of malicious activity [18, 19]. In particular, the matrix A_U^d of formula (6) shows that attempts to gain unauthorized access to the organization's assets were made by users #1, #2, #4, #6, #9. At the same time, user #6 made 2 such attempts, and user #9 made three such attempts. The results of the application of the improved technique give indicators for user #6 at the level of 22.2%, and for #9 − 33.3%. At the same time, for other malicious actions of users #1, #2, #4, the result is within 9.09...14.3%, which clearly distinguishes more dangerous users against the background of less dangerous ones. The separation of suspicious activity into different levels is important from the point of view of identifying real insiders, because in this case it is possible to reject those users who make unintentionally erroneous actions with information assets. In this way, the system will be more protected against false alarms.

6. Conclusions

The improved method given in this article makes it possible to unambiguously determine that the user's interaction with some information asset of the organization is anomalous. This, in turn, may indicate a possible insider attack. The results of the application of the improved method may be transferred to the information security administrator for further analysis and action. It is assumed that in some cases such an approach will not allow to reliably determine whether a given activity is a malicious activity, since such an analysis does not take into account the context of interaction and the reason for its occurrence, in addition, other, personal characteristics of a specific user are not taken into account. In any case, the application of this technique is advisable in combination with the analysis of other indicators that allow determining the presence of the user's propensity for malicious activity, for example, taking into account the loyalty of the staff.

By integrating real-time monitoring and behavior profiling, the technique can serve as an early warning system, flagging users whose actions deviate significantly from established norms. This can allow security administrators to intervene promptly, reducing response times and minimizing potential damage. Moreover, combining this method with context-aware analysis and psychological profiling could provide a more holistic approach to insider threat management, balancing technological detection with an understanding of human factors.

Future research in this area could explore the integration of machine learning techniques with the proposed method to enhance the detection of insider threats in more complex organizational environments. Specifically, incorporating predictive analytics and anomaly detection algorithms could improve the system's ability to identify patterns of malicious behavior even when insiders attempt to mask their activity.

Declaration on Generative AI

The authors have not employed any Generative AI tools.

References

[1] V. Savchenko, E. Smolev, D. Gamza, The method of detecting anomalies of user interaction with the organization's information resources, Modern information security 4(56) (2023) 6–12. doi:10.31673/2409-7292.2023.030101.

[2] V. Savchenko, V. Savchenko, T. Dzyuba, O. Matsko, I. Novikova, I. Havryliuk, V. Polovenko, Time Aspect of Insider Threat Mitigation, Advances in Military Technology 19(1) (2024) 149-164. doi:10.3849/aimt.01830.

[3] N. Jeffrey, Q. Tan, J. R. Villar, A Review of Anomaly Detection Strategies to Detect Threats to Cyber-Physical Systems, Electronics 12 (2023) 3283. doi:10.3390/electronics12153283.

[4] I. V. Ruban, V. O. Martovytskyi, S. O. Partyka, Classification of anomaly detection methods in information systems, Weapon systems and military equipment 3(47) (2016) 100–105. URL: https://openarchive.nure.ua/server/api/core/bitstreams/7c434471-942c-40a7-b70c-0cc2655a42fe/content.

[5] V. O. Horbenko, and V. M. Tkach. “Methods of detecting abnormal user behavior in information systems.” Transactions of Theoretical and applied problems of physics, mathematics and

informatics: XVI All-Ukrainian scientific and practical conference of students, postgraduates and young scientists 26–27.04 (2018): 51–52. URL: https://ela.kpi.ua/handle/123456789/25237.

[6] T. Hagemann, and K. Katsarou. "A Systematic Review on Anomaly Detection for Cloud Computing Environments." Transactions of 3rd Artificial Intelligence and Cloud Computing Conference (AICCC 2020) Kyoto, Japan 18–20.12 (2020). doi:10.1145/3442536.3442550

[7] A. O. Nicheporuk, A. A. Nicheporuk, O. S. Savenko, A. D. Kazantsev, An intelligent system for detecting anomalies and identifying smart home devices using collective communication, Electrical and computer systems 34(110) (2021) 50-61. URL: https://eltecs.op.edu.ua/index.php/journal/article/download/3196/1118/

[8] H. L. Mezones Santana, T. E. Cobeña Macias, M. A. Quimiz Moreira, Anomaly Detection Method in Computer Systems by Means of Machine Learning, in: M. Zambrano Vizuete (Ed.), Innovation and Research – A Driving Force for Socio-Econo-Technological Development, Lecture Notes in Networks and Systems, 511 (2022). doi:10.1007/978-3-031-11438-0_32.

[9] M. Cinque, R. Della Corte, A. Pecchia, Micro2vec: Anomaly detection in microservices systems by mining numeric representations of computer logs, Journal of Network and Computer Applications 208 (2022) 103515. doi:10.1016/j.jnca.2022.103515.

[10] A. Vervaet, "MoniLog: An Automated Log-Based Anomaly Detection System for Cloud Computing Infrastructures." IEEE transactions of 37th International Conference on Data Engineering (ICDE) (2021). URL: https://ieeexplore.ieee.org/document/9458872.

[11] M. A. Polyanychko. "Methodology for detecting anomalous interaction of users with information assets for detecting insider activity." Proceedings of communication educational institutions 6(1) (2020): 94–98. doi:10.31854/1813-324X-2020-6-1-94-98.

[12] A. Singhal. "Modern Information Retrieval: A Brief Overview." Bulletin of the IEEE Computer Society Technical Committee on Data Engineering 24(4) (2001): 35–43. URL: http://singhal.info/ieee2001.pdf.

[13] V. Savchenko, V. Akhramovych, T. Dzyuba, S. Laptiev, N. Lukova-Chuiko, and T. Laptieva. "Methodology for Calculating Information Protection from Parameters of its Distribution in Social Networks." IEEE 3rd International Conference on Advanced Trends in Information Theory (ATIT), Kyiv, Ukraine, (2021) 99–105, doi: 10.1109/ATIT54053.2021.9678599.

[14] G. Saunders, M. Hitchens, V. Varadharajan, Role-Based Access Control and the Access Control Matrix, Operating Systems Review 35 (2003) 145–157. doi: 10.1007/978-3-540-39927-8_14.

[15] B. Viswanath, A. Bashir, M. Crovella, S. Guha, K. P. Gummadi, B. Krishnamurthy, and A. Mislove. "Towards detecting anomalous user behavior in online social networks." Proceedings of the 23rd USENIX Security Symposium (USENIX Security) (2014) 223–238. URL: https://www.researchgate.net/publication/310793105_Towards_detecting_ anomalous_user_behavior_in_online_social_networks.

[16] L. Daubner, M. Macak, R. Matulevičius, B. Buhnova, S. Maksović, T. Pitner, Addressing insider attacks via forensic-ready risk management, Journal of Information Security and Applications 73 (2023) 103433. doi: 10.1016/j.jisa.2023.103433.

[17] P. Alves, C. Sales, M. Ashworth, Does outcome measurement of treatment for substance use disorder reflect the personal concerns of patients? A scoping review of measures recommended in Europe, Drug and Alcohol Dependence 179 (2017) 299–308. doi: 10.1016/j.drugalcdep.2017.05.049.

[18] L. Ko, D. M. Divakaran, Y. Liau, V. Thing, Insider Threat Detection and its Future Directions, International Journal of Security and Networks 12 (2016). doi: 10.1504/IJSN.2017.10005217.

[19] V. Sosnovyy, N. Lashchevska, Detection of malicious activity using a neural network for continuous operation, Cybersecurity: Education, Science, Technique 3 (2024) 213–224. doi: 10.28925/2663-4023.2024.23.213224.