European Journal of Interdisciplinary Research and Development
Volume-18 August 2023
Website: www.ejird.journalspark.org ISSN (E): 2720-5746

# METHOD AND ALGORITHM FOR DETECTING NETWORK ATTACKS ON THE DISTRIBUTED DATABASE OF CORPORATE NETWORK USERS

Sadikov Sh.M.
Associate Professor of
Tashkent University of Information Technologies
named after Muhammad al-Khwarizmi

**Abstract**:
The article identifies network attacks on the distributed database of corporate network users, researches the effects of external and internal threats within the organization's information system, and analyzes effective protection measures against network attacks on the database. A partition scheme has been developed in the area section of the distributed database, and an algorithm for detecting SQL injection attacks on the distributed database has been developed.

**Keywords**: corporate network, distributed database, SQL injection, comparison matrix, risk, OTP.

## Introduction

Detection of network attacks on the distributed database of corporate network users is a process that requires a comprehensive approach, taking into account the effects of external and internal threats within the organization's information system. In order to effectively protect corporate network users from network attacks against the distributed database, it is necessary to know the probability of attacks against the information stored in the database and having a certain value throughout its life cycle. will be done.

Continuous analysis of network attacks on the distributed database of corporate network users and elimination of deficiencies in the protection mechanism based on the results of the analysis is of great importance in ensuring the security of the entire information system. However, there are no mathematical models that can accurately determine the probability of network attacks against the database. In practice, models can work based on certain criteria. It is no secret that if the parameters of a new type of attack that do not meet the criteria are encountered, the system considers them as anomalies, as a result of which the number of anomalies increases, which, in turn, leads to a decrease in the efficiency of the system to detect new types of attacks. As we know, any model is designed for some object (there is no universal protection model that can be applied to all objects) and must work with specific threshold values and specific parameters for use in the model. . However, the parameters that identify database-targeted attacks are not clear. There are several main reasons for this.

1. It is impossible to systematize the factors of network attacks on the distributed database of corporate network users, the reasons for their occurrence based on a specific criterion. Each protection requires a different approach and a different parameter. In addition, the model, method and algorithm of the attacker who has carried out attacks so far is incomplete, unclear, and the likelihood of attacks is low.

2. It is difficult to identify vulnerabilities in a distributed database in one part, i.e., when dividing the common database into certain parts according to their relevance at the time of distribution. This ensures successful implementation of network attacks on the distributed database of users of the corporate network.

In the process of detecting network attacks of corporate network users on the distributed database, that is, the presence of information that requires simultaneous processing in all parts of the distributed database, and the decomposition of factors affecting the security of the database in the form of a level, i.e. hierarchy first of all, it is necessary to form a protection hierarchy. Typically, a distributed database of corporate network users follows the hierarchy below.

Hierarchy analysis method can be used to detect the network attacks of corporate network users on the distributed database, and the probability of network attacks on the database can be determined based on the success of the attack. In this case, an important role is played by which part of the distributed database the attack corresponds to.

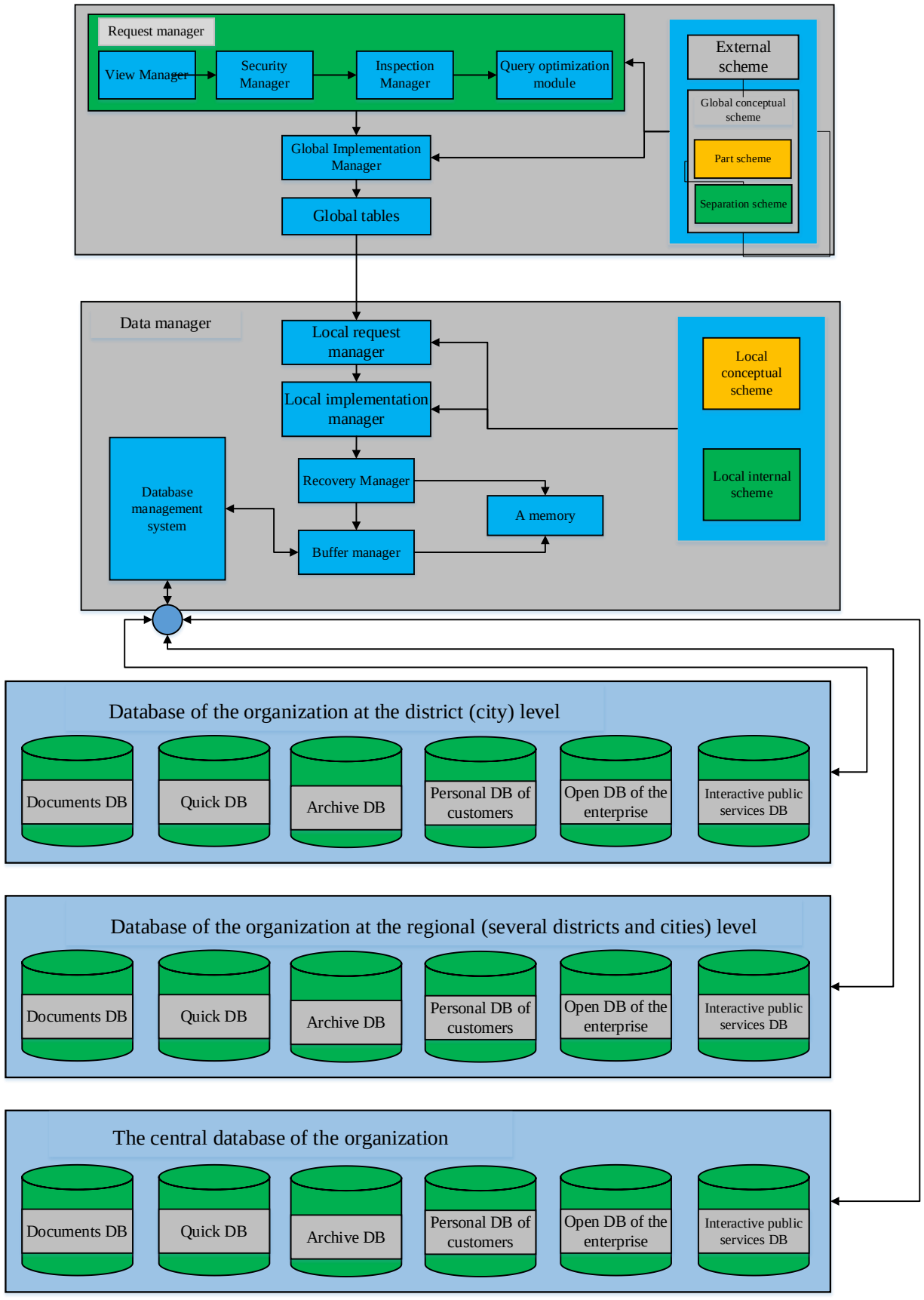


Figure 1. Partitioning scheme of a distributed database in the cross-section of regions

After determining the division of the distributed database of corporate network users into regions, in order to determine the network attacks on these databases, it is necessary to calculate the matrices of pairwise comparison based on the models presented in Chapter 3 for each of the following levels. These levels are:

- level of assets in a distributed database (A)
- level of resources in the distributed database (R)
- employee level (H) in the distributed database
- third-party level (U) in a distributed database
- level of attack on a distributed database (Attack)
- level of threats in the distributed database (T)
- level of vulnerabilities in the distributed database (Z)
- the level of risk in the distributed database (Risk)

This is followed by the level of detection of network attacks on the distributed database of individual enterprise network users and additional communication at the resource and user group level and between departments.

$$A = \begin{pmatrix} 1 & a_1/a_2 & \dots & a_1/a_n \\ a_2/a_1 & 1 & \dots & a_2/a_n \\ \vdots & \vdots & \dots & \vdots \\ a_n/a_1 & a_n/a_2 & \dots & 1 \end{pmatrix}, \quad (1)$$

where A is the pairwise comparison matrix of asset level in detecting network attacks on distributed database of corporate network users.

$$A_c = \begin{pmatrix} a_1^c \\ a_2^c \\ \vdots \\ a_n^c \end{pmatrix}, \quad (2)$$

where A_c-A are the normalized eigenvectors of the priority matrix.

$$\forall a_i \in A, \quad i = 1, 2, \dots . n:$$

$$R = \begin{pmatrix} 1 & r_1/r_2 & \dots & r_1/r_k \\ r_2/r_1 & 1 & \dots & r_2/r_k \\ \vdots & \vdots & \dots & \vdots \\ r_k/r_1 & r_k/r_2 & \dots & 1 \end{pmatrix}, \quad (3)$$

where R is the pairwise comparison matrix of the resource level in detecting network attacks on the distributed database of corporate network users.

$$R_c = \begin{pmatrix} r_1^1 & r_1^2 & \dots & r_1^n \\ r_2^1 & r_2^2 & \dots & r_2^n \\ \vdots & \vdots & \dots & \vdots \\ r_k^1 & r_k^2 & \dots & r_k^n \end{pmatrix}, \quad (4)$$

where A_c-A is the matrix of normalized eigenvectors of the priority matrix.

$$\forall r_j \in R, \quad j = 1, 2, \dots . k:$$

$$H = \begin{pmatrix} 1 & {}^{h_1}/_{h_2} & \dots & {}^{h_1}/_{h_k} \\ {}^{h_2}/_{h_1} & 1 & \dots & {}^{h_2}/_{h_k} \\ \vdots & \vdots & \dots & \vdots \\ {}^{h_k}/_{h_1} & {}^{h_k}/_{h_2} & \dots & 1 \end{pmatrix} \quad (5)$$

where H is the pairwise comparison matrix of employee level in detecting network attacks against distributed database of corporate network users.

$$H_c = \begin{pmatrix} h_1^1 & h_1^2 & \dots & h_1^n \\ h_2^1 & h_2^2 & \dots & h_2^n \\ \vdots & \vdots & \dots & \vdots \\ h_k^1 & h_k^2 & \dots & h_k^n \end{pmatrix}, \quad (6)$$

where H_s-H is the matrix of normalized eigenvectors of the priority matrix.

$$\forall h_j \in H, \qquad j = 1, 2, \dots . k:$$

$$U = \begin{pmatrix} 1 & {}^{u_1}/_{u_2} & \dots & {}^{u_1}/_{u_k} \\ {}^{u_2}/_{u_1} & 1 & \dots & {}^{u_2}/_{u_k} \\ \vdots & \vdots & \dots & \vdots \\ {}^{u_k}/_{u_1} & {}^{u_k}/_{u_2} & \dots & 1 \end{pmatrix}, \quad (7)$$

where A is the third-party level pairwise comparison matrix for detecting network attacks against distributed databases of corporate network users.

$$U_c = \begin{pmatrix} u_1^1 & u_1^2 & \dots & u_1^n \\ u_2^1 & u_2^2 & \dots & u_2^n \\ \vdots & \vdots & \dots & \vdots \\ u_k^1 & u_k^2 & \dots & u_k^n \end{pmatrix}, \quad (8)$$

where U_c-U is the matrix of normalized eigenvectors of the priority matrix.

$$\forall u \in U, \qquad j = 1, 2, \dots . k:$$

$$Hujum = \begin{pmatrix} 1 & {}^{huj_1}/_{huj_2} & \dots & {}^{huj_1}/_{huj_k} \\ {}^{huj_2}/_{huj_1} & 1 & \dots & {}^{huj_2}/_{huj_k} \\ \vdots & \vdots & \dots & \vdots \\ {}^{huj_k}/_{huj_1} & {}^{huj_k}/_{huj_2} & \dots & 1 \end{pmatrix}, \quad (9)$$

where Attack is a pairwise comparison matrix of the attack level in detecting network attacks on a distributed database of corporate network users.

$$Hujum_c = \begin{pmatrix} huj_1^1 & huj_1^2 & \dots & huj_1^n \\ huj_2^1 & huj_2^2 & \dots & huj_2^n \\ \vdots & \vdots & \dots & \vdots \\ huj_k^1 & huj_k^2 & \dots & huj_k^n \end{pmatrix}, \quad (10)$$

where 〖Attack〗_s is the matrix of normalized eigenvectors of the Attack priority matrix.

$$\forall huj_j \in Hujum, \qquad j = 1, 2, \dots . k:$$

$$T = \begin{pmatrix} 1 & t_1/t_2 & \dots & t/t_k \\ t_2/t_1 & 1 & \dots & t_2/t_k \\ \vdots & \vdots & \dots & \vdots \\ t_k/t_1 & t_k/t_2 & \dots & 1 \end{pmatrix}, \quad (11)$$

bu yerda $T$ – korporativ tarmoq foydalanuvchilarining taqsimlangan ma'lumotlar bazasiga bo'ladigan tarmoq hujumlarini aniqlashda tahdid darajasining juft taqqoslanish matritsasi.

$$T_c = \begin{pmatrix} t_1^1 & t_1^2 & \dots & t_1^n \\ t_2^1 & t_2^2 & \dots & t_2^n \\ \vdots & \vdots & \dots & \vdots \\ t_k^1 & t_k^2 & \dots & t_k^n \end{pmatrix}, \quad (12)$$

bu yerda $T_c - T$ ustuvorliklar matritsasining normallashgan xususiy vektorlari matritsasi.

$$\forall t_j \in T, \qquad j = 1, 2, \dots . k:$$

$$Z = \begin{pmatrix} 1 & z_1/z_2 & \dots & z_1/z_k \\ z_2/z_1 & 1 & \dots & z_2/z_k \\ \vdots & \vdots & \dots & \vdots \\ z_k/z_1 & z_k/z_2 & \dots & 1 \end{pmatrix}, \quad (13)$$

bu yerda $Z$ – korporativ tarmoq foydalanuvchilarining taqsimlangan ma'lumotlar bazasiga bo'ladigan tarmoq hujumlarini aniqlashda zaiflik darajasining juft taqqoslanish matritsasi.

$$Z_c = \begin{pmatrix} z_1^1 & z_1^2 & \dots & z_1^n \\ z_2^1 & z_2^2 & \dots & z_2^n \\ \vdots & \vdots & \dots & \vdots \\ z_k^1 & z_k^2 & \dots & z_k^n \end{pmatrix}, \quad (14)$$

bu yerda $Z_c - Z$ ustuvorliklar matritsasining normallashgan xususiy vektorlari matritsasi.

$$\forall z_j \in Z, \qquad j = 1, 2, \dots . k:$$

$$Risk = \begin{pmatrix} 1 & risk_1/risk_2 & \dots & risk_1/risk_s \\ risk_2/risk_1 & 1 & \dots & risk_2/risk_s \\ \vdots & \vdots & \dots & \vdots \\ risk_s/risk_1 & risk_s/risk_2 & \dots & 1 \end{pmatrix}, \quad (15)$$

where Risk is a pairwise comparison matrix of the level of risk in detecting network attacks on the distributed database of corporate network users.

$$Risk_c = \begin{pmatrix} risk_1^1 & risk_1^2 & \dots & risk_1^k \\ risk_2^1 & risk_2^2 & \dots & risk_2^k \\ \vdots & \vdots & \dots & \vdots \\ risk_s^1 & risk_s^2 & \dots & risk_s^k \end{pmatrix}, \quad (16)$$

where 〖Risk〗_c-Risk is the matrix of normalized eigenvectors of the priority matrix.

$$\forall risk_v \in Risk, \qquad v = 1, 2, \dots . s:$$

After this step, a network attack on the distributed database of corporate network users is determined according to expression (17).

$$the\ result = \begin{pmatrix} \sum_{j=1}^{n} a_j^c * & r_i^c * h_i^c * & u_i^c * huj_i^c * & t_i^c * z_i^c * & risk_1^c \\ \sum_{j=1}^{n} a_j^c * & r_i^c * h_i^c * & u_i^c * huj_i^c * & t_i^c * z_i^c * & risk_2^c \\ \sum_{j=1}^{n} a_j^c * & r_i^c * h_i^c * & u_i^c * huj_i^c * & t_i^c * z_i^c * & risk_s^c \end{pmatrix} \quad (17)$$

Identifying network attacks on the distributed database of corporate network users and eliminating them helps to increase the efficiency of the company's information security system. SQL injection attacks made up the largest number of attacks against the database. According to statistics for the last five years, 81 percent of database attacks were SQL injection attacks, and the remaining 19 percent were other types of attacks. Therefore, it is appropriate to test the developed method in the process of identifying and eliminating attacks of this type. The algorithm of the method developed for detecting this type of attacks is implemented in the following sequence. In this case, the program developed to detect the attack can be implemented in any programming language. The performance technology is similar to the IPS algorithm, the main difference from which is that the concept of weight is included for the commands, and it is decided on the basis of the concept according to the decision level.

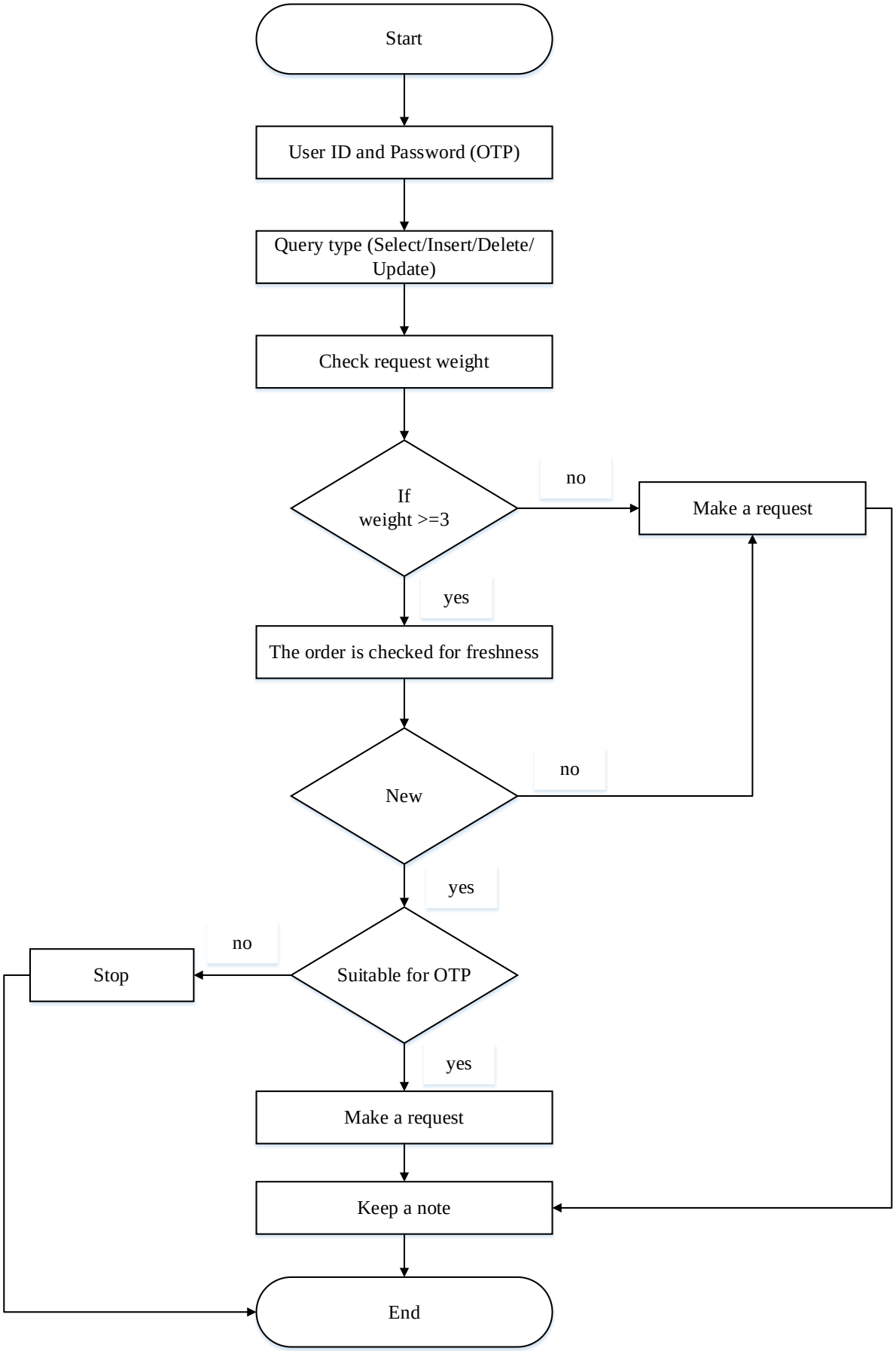
Start
User ID and Password (OTP)
Query type (Select/Insert/Delete/ Update)
Check request weight
If weight >=3
no
Make a request
yes
The order is checked for freshness
New
no
yes
Suitable for OTP
no
Stop
yes
Make a request
Keep a note
End

Figure 2. Block diagram of the SQL injection attack detection algorithm.

The more important the command, the greater the weight and accordingly the OTP (One Type Password) is required. The scheme of operation of the algorithm is given below.

1. Start.
2. Obtain User Id and Password (OTP).
3. Analysis of the request (in this case, it is determined which command was given by the request, i.e. Select/Insert/Delete/Update).
4. Checking the weight of the request (in this case, the weight increases according to the frequency of the sent request, the weight decreases when the frequency, that is, how quickly the number of this request is sent).
5. The check condition is executed (that is, the condition is as follows: if the weight is equal to or greater than 3, go to step 6, otherwise, go to step 9 if the condition is fulfilled).
6. The order is checked for freshness.
7. Check according to the following condition (if the request is new, go to step 8, otherwise, go to step 11).
8. If the OTP matches, proceed to step 9, otherwise, proceed to step 11.
9. Implementation of the request.
10. Record keeping.
11. That's it.

The block diagram of this algorithm is as follows.

As a result of detection of SQL injection attacks, it will be possible to protect against most of the network attacks on the distributed database of corporate network users. In addition, as a result of protection from these attacks, not only the efficiency of information security systems increases, but also the efficiency of the information system within the entire activity of the enterprise increases. The main reason for this is that MBBT provides integration of several systems in the information exchange system of the enterprise.

**List of used literature**

1 Yirui Wu, Dabao Wei and Jun Feng “Network Attacks Detection Methods Based on Deep Learning Techniques: A Survey” 28 Aug 2020, https://doi.org/10.1155/2020/8872923
2 Iqbal H. Sarker “Machine Learning for Intelligent Data Analysis and Automation in Cybersecurity: Current and Future Prospects” Annals of Data Science, 19 september 2022
3 Sadikov Sh.M. “Classification of information security thereats in the database” Innovate research in modern education, Canada 2023.
4 Sadikov Sh.M. “Analysis of existing vulnerabilities in information reception, processing and transmission systems in a distributed database” In volume 21, of. Eurasian Journal of Engineering and Technology(EJET) Belgium, August, 2023, ISSN(E): 2795-7640
5 Hassan A “Database Security and Auditing: Protecting Data Integrity and Accessibility” 2021
6 Sadikov Sh.M. “Comparative Analysis of Database security assurance models from unauthorized actions and quantitative assessment of integrity” Texas Journal of Engineering and Technology, 2023, ISSN NO: 2770-4491

7 Alton Chung and Sheng-Uei Guan "Database Security: From Legacy Systems to Blockchain Technology" 2021
8 John R. Vacca "Computer and Information Security Handbook" 2021.