Analysis of Existing Vulnerabilities in Information Reception, Processing and Transmission Systems in a Distributed Database

Sadikov Sh.M.

Tashkent University of Information Technologies named after Muhammad Al-Khwarizmi Associate professor

ABSTRACT

The article examined the problems associated with the reception of information in the distributed database, violations in the process of information processing in the distributed database of corporate network users, the interaction of MBBT systems, the interconnection of various data in the repository, as well as problems with B health with quality storage of data.

Keywords: distributed database, information processing, MBBT, data warehouse, DSS (Decision Support System), operational analytical data.

In a distributed database, data loss (violation of their integrity) can be observed at any stages of information collection, registration, control, processing, transmission of information through communication channels. To prevent data loss during storage, special measures are taken to protect data carriers from mechanical damage and physical influences (such as magnetic fields).

The main causes of violations in the process of information processing in the distributed database of corporate network users are:

beat the whistle;

failure and failure of equipment (failure of electronic equipment, deletion of files, violation of data when entering the memory space through unprocessed access, etc.);

insufficient accuracy or errors in the source data, in the generalization of intermediate and output data of the moment;

the incompatibility of the mathematical models being implemented with real-world processes, the approximate nature of the methods used in solving problems on a computer (in particular, iterative methods),

errors in programs.

The choice of specific methods and means of management included in the technological process depends on the importance of Information, its structural organization, size, stability and other characteristics. Each process can be carried out with the following results:

without introducing additional distortions;

with additional breakdowns of the “window” type, converting the broken bit sequence to the original unbroken bit;

with the introduction of additional breakdowns.

To determine the likelihood of these results, it is necessary to analyze the possible threats to the loss of integrity in the process of information annotation in the distributed database under consideration. The distributed database provides detailed information about the existing threats in several scientific works. Therefore, it is necessary to consider the threats and vulnerabilities to the distributed database in connection with the multilevel architecture in the distributed database only

below, new technologies for information processing and new requirements for the form of data presentation.

For a corporate information system, client-server architecture is important. Today, Oracle, Microsoft SQL Server, and DB2 servers are more commonly used in qaragna to other servers. The basic principle of operation of these servers is based on multilevel architecture, combining multilevel architecture with Internet/Intranet technologies can be seen in Figure 6.

The lower layer provides client applications designed to perform functions and perform presentation logic. The middle layer is an application server that manages application logic and performs data processing logic database operations. The top level is a remote specialized database server dedicated to data processing services and file operations.

Vulnerabilities in a distributed database that can cause a violation of the integrity of information can be found in many ways in practice. These are, first of all, vulnerabilities associated with incorrect administration of the access control system. This includes:

the absence of mechanisms for protecting traffic in the clock;

lack of mechanisms to control the use of user accounts in the clock, both on the server and by the client;

the absence of mechanisms for dynamically controlling the values of security attributes of the clock.

Traffic protection refers to the confidentiality, integrity, reliability, usability and threat protection of information being transmitted and the continuous exchange of information. When using Internet technologies, a lack of traffic protection mechanisms often leads to attacks aimed at network nodes, as well as an effective analysis of traffic, changing the data to be transmitted.

The lack of protection of Service data in a distributed database, the use of password authentication, the ability to run CGI scripts and Java applets, uncontrolled import and export of data to external systems, the absence of mechanisms for detecting attacks at the physical level can adversely affect the whole and the security of the information system as a whole.

A user's hatti actions caused by ignorance of prohibited actions can lead to loss of integrity; for example, allowing clients to set up sessions with the server in large numbers or uncontrolled, which can lead to loss of performance. Due to data loss due to lack of memory and unauthorized access of the attacker to the journal, violation of the integrity of the audit system Journal, as well as shortcomings in the organization of security domain allocation, can lead to access to the address fields of unauthorized entities, code or data of protective equipment.

Finally, the lack of integrity control in protection systems can lead to changes in data protection tools and operating system kernel performance algorithms. Violation of the protection system can also occur due to failures in the information system itself and the absence of mechanisms for restoring the safe state of the protective equipment, as well as mechanisms for checking the integrity of these tools.

Information processing processes in a distributed database in connection with new requirements for mbbt can be carried out using various technologies and involve many actions. In addition, each action can create an additional risk to information security.

For example, the simplest way to work with a distributed database is to load read-only data. Only one computer is responsible for updating all data, but copies of the data only for reading can be sent to multiple computers. The complex processing method allows you to update the same data in different places. In this case, three types of distributed update conflicts may arise.

In the first contradiction case, two different computers can create a series with the same values of some attributes, that is, the identity is broken.

In the case of a second conflict, it is possible to indicate that the same line on two computers will be updated.

In the third conflict case - a deleted line on one computer on another can be updated.

To resolve update conflicts, it is necessary to allocate a special computer that monitors all updates. Conflicts are resolved through Mbbt proprietary tools or applications similar to triggers. In exceptional cases, the conflict is manually recorded and resolved. At the same time, many rows in databases operating in practice can hang in an uncertain position, which leads to a decrease in the bandwidth of the Enterprise Information System.

None of the conflict resolution methods solve the problem of ensuring the atomicity of transactions in a distributed database. In order for a transaction to be atomat, no updates must be kept until all the transaction's actions are saved. This means that each computer must conditionally record its updates and wait for the distributed transaction manager to report that the actions of all other computers have also been recorded. For this, a two-phase fixation algorithm is used. If updates have to be reversed when resolving a conflict, a distributed transaction may not be completed for several hours or even days. Thus, in the process of updating, originality, integrity and usability can be involuntarily impaired.

With the advent of high-capacity personal computers, it became possible to download large amounts of data to computers of users and departments for local processing of enterprise data. Users can request this data using local MBBT, as well as import them into spreadsheets, financial analysis programs, graphs, and other applications. The downloaded data cannot be updated, they can only be used for requests and reports.

Downloading data brings data closer to the user and increases the efficiency of its use, and also increases the risk of computer crimes (illegal copying, illegal access to the network) due to the difficulty of coordination, consistency and access control.

The need to process operational analytical data led to the creation of information repositories. A Data Warehouse (Data Warehouse) (MO) includes not only data, but also tools, procedures, training, personnel and other resources that facilitate access to data.

The main goal of the data warehouse is to increase the value of the information assets of the enterprise. The data warehouse stores parts of the work data and provides it in a user-friendly format. It can be extracts from databases and files, as well as scanned images of documents, records, photos and other non-digital information.

Data warehouse (MO) is used to store, merge, generalize, modify, and communicate data to users using analysis and decision-making tools such as OLAP. OLAP (Online Analytical Processing) is not a single software product, but a set of concepts, principles and requirements that lie on the basis of software products that facilitate access to data to analysts.

Data Quality Assurance is a complex problem in data repositories for the following reasons;

when combining data from different sources, the result may be inconsistencies due to differences in the temporal properties and domains of the source data;

the data warehouse includes many application programs related to various fields, among which the export and import of data can be done incorrectly;

a shortage of information storage self-management tools.

Given the potential value of the data, the issue of data management has become an urgent issue. The main problems of data management are that there are many types of data, the main categories of data are not clear, the same data can have many descriptions and formats, changes in information, often in parallel, political and organizational issues complicate the solution of operational problems. Data collection takes a lot of time and money.

New technologies require new forms of data presentation. Thus, Decision Support Systems based on DSS (Decision Support System) are created in the database, depending on the detailed level of information, operational data, collected and generalized data are distinguished.

Operational data is stored in a relational database, sufficiently normalized and

optimized to support operations that occur in daily operations, such as the presence of material in the warehouse, the number of parts produced, etc.being updated very frequently.

In ensuring distributed database security, operational data and DSS data can be designed for a variety of purposes. Therefore, their format and structure differ. Operational data differs from DSS data in three ways. These are:

time range;
detailing gorge;
multi-dimensionality of the moment.

Operational data covers a very short time. Their level of detail is very high; they are practically atomic. There is no multidimensionality, or to some extent it can be ensured by associating it with many tables. Operational data is often associated with update transactions. The query size is small, simple, but requires a quick response. Since the data model is relational, the data must be normalized. Otherwise, it can lead to recurrent, rapidly changing data anomalies. Normalization results in the creation of a large number of tables, each containing a minimum set of attributes. Despite the fact that the main requirement for operational data is processing speed - productivity, the guaranteed reliability (accuracy) of this data is also important. The main purpose of DSS is to be able to handle queries that are frequent and complex. Therefore, the data model in DSS must be multidimensional.

In multidimensional imaging, the main data structure is the data cube. The database consists of one or more of these cubes. The cube has two or more independent dimensions that define a kind of coordinate system for the data space it displays. Coordinates on a given measure are represented by the values of the relevant data attribute, and hierarchical relationships can be established on this set of values. The set of coordinates of different sizes corresponds to the data values at cubic points, which are called Elements. The presence of a hierarchy of values of measurement "coordinates" allows you to sum the values of the relevant data, analyze the data at one level or another with details.

Foydalanilgan adabiyotlar ro'yxati

1. Ross Anderson "Security Engineering: A Guide to Building Dependable Distributed Systems" 2014.
2. Charlie Kaufman, Radia Perlman, and Mike Speciner "Network Security: Private Communication in a Public World" 2013
3. George S. Oreku "Database Security: Concepts, Approaches, and Challenges" 2015
4. Hassan A "Database Security and Auditing: Protecting Data Integrity and Accessibility" 2021
5. Sushil Jajodia and Bhava "Database Security: Status and Prospects" 2002
6. Alton Chung and Sheng-Uei Guan "Database Security: From Legacy Systems to Blockchain Technology" 2021
7. John R. Vacca "Computer and Information Security Handbook" 2021
8. George S. Oreku "Database Security: Concepts, Approaches, and Challenges" 2014