ISSN NO: 2770-4491
Date of Publication:08-08-2023

Comparative Analysis of Database Security Assurance Models from Unauthorized Actions and Quantitative Assessment of Integrity

Sadikov Sh.M.
Tashkent University of Information Technologies
named after Muhammad Al-Khwarizmi Associate professor

Annotation: the article examines the processes of ensuring the security of the database, the creation and research of the database of users of the protected corporate network, one of the important tasks in ensuring the security of the database of users of the corporate network is the provision of Information Integrity, models of ensuring security.

Keywords: database, corporate network, privacy, integrity usability, security models, table, index, Harrison-Ruzzo Ulman's discretionary, Bella-La Padula, Clark Wilson .

Database security models are important in the database security process. One of the main areas of Information Security is to define the roles of database users and to control their proper use of the powers granted to them based on the roles provided, and to limit their use if necessary. It is advisable to use security models to have this capability, it is to create a formal model of Information Security.

As a result of the development of digital technologies, attackers (hackers) are gaining access to a database security breach or sufficient damage to the protection mechanism using modern tools. In order to avoid such situations, it is necessary to improve current database security models or develop new models. A model of Information Security used to ensure database security is understood as a formal description of security policies. Security policy means that their implementation, taking into account the general set of procedures and rules that strictly determine the process of processing information, provides protection against a certain set of taxids, attacks. Security models are important in the creation and research processes of the database of protected corporate network users, as they provide a systematic-technical approach that covers the solution of the following extremely important issues;

selection and justification of the basic principles of the protected database architecture, which determine the mechanisms for the implementation of electronic information protection tools and methods in the information system of the enterprise;

approval of the features of the protective system based on ensuring compliance with the information security policy (standards, requirements, criteria) of the enterprise;

an important component of the protected database produced for the enterprise is the formation of a formal detailed list of the security policy that is being calculated.

In the process of applying security modellalry to database security assurance, attention should be paid to the main two concepts. These concepts are the concepts of object and subject. These concepts can also be interpreted in different scientific articles, depending on the place of use of the information system. This error does not calculate the concept, for example, it is interpreted as the subject of Use and the object of use in the process of limiting use or distribution of roles in computer systems. In the process of ensuring the security of the database as a whole, the totality of linkage relations between objects and entities used in the analysis of security models determines the state of the system.

One of the important tasks in ensuring the security of the database of corporate network users is to ensure the integrity of information. The concept of integrity is considered one of the key concepts for database systems and security systems. Maintaining integrity is important even in systems where the number of users is very low. In this field of scientific research, brogan scientists interpret this concept in different ways. For example, the concept of integrity of information according to the Hoffman tariff was explained by the correspondence of information in the initial document to information in the system. The totality of information according to the Deita tariff is explained by the accuracy and authenticity of information. In

ISSN NO: 2770-4491
Date of Publication:08-08-2023

other data, however, da whole is defined as the property of maintaining the structure or content of information or software at the time of transmission or storage, and it is this last tariff that is reflected in many scientific works in this area, since this tairf covers the life cycle of information.

It is usually assumed that every optional a message forms a certain equivalence class in its semantic content. In this, the property of preserving the whole is explained as follows: the transmitted message A is said to have retained the whole if the a_1 message received as a result of the transmission belongs to the A message equivalence class. In accordance with the requirement for information security, the problem of protecting database systems consists in developing methods and tools that ensure the fulfillment of three interconnected features of the system. These are:

privacy;
totality;
usefulness.

These characteristics are associated not only with each other, but also with the characteristics of the information being processed: relevance, accuracy, reliability and timely delivery. Thus, security means that authorized users are allowed to perform the necessary actions, and integrity means that these actions are correct. Violation of integrity leads to loss or falsification of the usability of information. Loss of privacy violates the inviolability of personal data, the parameters of belonging and accuracy will be strictly related to the parameters of timely transmission and reliability, respectively. The organization's information security policy should include tools to implement all of these features, as each is necessary to effectively protect the database. However, while security methods are well implemented in existing Mbbts, integrity preservation methods require a lot to be taken into account.

The task of ensuring integrity provides a set of measures aimed at preventing the intentional modification or destruction of information used by the Management Information System or decision support system. The issues of maintaining the integrity of the database are closely related to the issues of access control, in many cases the same mechanisms are used to solve them.

Corporate network beneficiationswhich in order to protect privacy and integrity in the process of ensuring the security of a distributed database, it is necessary to know the lower sizes;

table;
view;
index;
cluster;
table area;
role;
reverse segment;
database objects such as library etc.

Also active objects (procedure, function, package and trigger) are widely used. Among these, the trigger is of particular importance. A Trigger is a stored procedure that is performed automatically when a related event occurs. Typically, when performing INSERT, DELETE, UPDATE operations related to the execution of event addition, update, and deletion phrases, auto-start creates additional verification and programmable control capabilities of completed operations. At the same time, triggers can be applied not only to dynamically verify the integrity of the data and implement additional access control rules, but also to create an illegal copy of the attacker's actions, in particular, the entered data.

The same functions are implemented from the analysis of functional dependencies, integrity constraints, and key values by SQL injection protection mechanisms (the request to enter the UNION construct into SQL statements returns confidential information). Usability threats can also lead to a violation of the whole. Security models are also used to solve this problem, for example, using the specificity of the primary keys, not created by the system, we can create a situation in which it will be impossible to enter new entries in the table. When updating the corresponding entries, Oracle MBBT can create a lockout, which, for example, leads to failure in the transaction, if the external key is not indexed.

The definitions cited above do not provide a quantitative estimate of the information integrity in a database of corporate network users. Maintaining integrity refers to a set of rules that the user should not violate. The rules must be specified in some convenient language and stored in the system directory, while

ISSN NO: 2770-4491
Date of Publication:08-08-2023

the MBBT must control compliance with the established rules. Usually the rules are in their structure in the form of models.

Today, the following security models are used.

1. Kharrison-Ruzzo Ulmanningdiscretionary model.
2. Gauger-Gezinger model.
3. Bella - La Padula model.
4. Biba model.
5. Clark Wilson model.
6. Millen model.
7. Sutherland model.
8. Safety roll model

2-table.

Comparative analysis of security models used to ensure database security.

Criteria / Security Modeli name	Kharrison-Ruzzo Ulman discretionary model	Giger-dizayner modeli	Bell-LaPadula model	Biba model	Klark Uilson model	Millen model	Sazerlend model	Safety roll model
Privacy protection	-	+	+	-	-	-	+	+
Integrity Protection	+	+	-	+	+	-	+	+
Usability protection	-	-	-	-	-	+	-	+
Possibility of flexibility	+	+	+	-	+	-	+	+
Ease of foaming is difficult	+	-	-	-	+	+	-	+
Easy to fool	-	+	+	+	-	-	+	-
Introduction complex	+	-	-	-	+	+	-	+
The introduction is simple	-	+	+	+	-	-	+	-
It is difficult to give powers	+	+	-	-	+	+	+	+
It is easy to give powers	-	-	+	+	-	-	-	-

The security models mentioned above are used in the process of ensuring the security of the database, but among them there is the following feedback on what will be used in the process of ensuring the security of the distributed database. In doing so, the most commonly used Bell-LaPadula integrity model among these models allows for multilevel database protection and is designed to handle subjects requiring access to data and objects (files, records, Fields) based on a matrix of input classes, hierarchical and non-hierarchical component relations. The basic prinstip of this model is explained in short by the phrase “do not write down, do not read from above” (which means that according to this whole model, users can only create objects on their own or at a lower whole level. At the same time, users can view content only at their own level or cannot view it at a higher level) as well as include two limitations.

the first is called the simple privacy feature. In this, non-hierarchical components (input objects) at each level are automatically assigned to all higher levels.

ISSN NO: 2770-4491
Date of Publication:08-08-2023

a second limitation, known as a complex property, is that information pertaining to any level of security can never be recorded to an object with a lower level of security. The entry level is a hierarchical component (e.g. unclassified secret, confidential, top secret).

This model was developed to ensure data security from unauthorized actions. In addition the Biba integrity model was developed by Kenneth Biba in 1977 with the aim of bypassing the weaknesses of the Bell-LaPadula model. It is a system designed to safely move a computer system from one state to another, describing a set of access control rules. According to it, data and objects are grouped into ordered Whole levels, and then two restrictions are placed on their interaction.

1. The simple integer axiom states that an object of a given level of the whole cannot read an object of a lower level.

2. The axiom of complex whole states that an object of given integer level should not write to higher-order objects.

This model is designed to increase the level of data integrity storage. The main goal of maintaining integrity:

not allowing data to be changed by unauthorized entities;
preventing unauthorized modification of information by authorized entities;
to have internal and external significance.

The Gauger-Gezinger model is based on automata theory. According to it, the system can switch from one allowed state to only a few other states with each action. The subjects and objects in this protection model are divided into groups - domains, and the transition of the system from one state to another is carried out only according to a table of permissions indicating what operations the subject can perform. This model uses transactions that ensure the overall integrity of the system when the system moves from one state to the other.

The Sazerland model of protection focuses on the interaction of subjects and information flows. It has many allowed case combinations and a set of starting positions. This model studies the behavior of several compositions of functions from one state to another.

In Information Security theory, the Clark-Wilson model is central. Clark-Wilson's integrity model serves as the basis for the specification and analysis of computer system security policies.

Information security is ensured by preventing data elements in the system from being corrupted by random errors or intentional modifications. The integrity policy describes how to safely store data elements in a system from one state to another, and defines the competencies of different users in the system. The Model defines the rules of validity and certification that form the basis of the integrity policy. In this model, integrity policy refers to the totality of transactions. The principle of separation of tasks (works, functions, operations) requires that the transaction Authenticator and the implementer be different objects. The Model includes a number of basic constructs that represent data elements and processes that operate on these data elements.

These integrity models are more suited to ensuring the confidentiality of information than the information integrity. Bell-La Padula and Biba models are more useful, for example, to prevent high levels of information from being disseminated and distorted in data classification systems at important objects of state organizations. In contrast, the Clark-Wilson model is more in line with business and manufacturing processes, in which maintaining the integrity of the data is important at any level of classification.

Since integrity is important in ensuring the security of a distributed database, a quantitative assessment of integrity is necessary on the basis of these models. From this, it is necessary to develop a model for assessing information security in terms of protecting the integrity of data. It is proposed to measure the integrity of the data with the possibility of a violation of the integrity in the process of processing the relevant data.

The development of methods for determining such probabilities is a complex process. This is due to the complexity and versatility of the objects they describe in a distributed database, the complexity of software and technical tools, including protective ones, the complexity of an adequate algorithmic description of data processing, storage and transmission processes in modern data processing systems.

Almost every process of information processing in a distributed database requires the determination of the following probabilities:

ISSN NO: 2770-4491
Date of Publication:08-08-2023

the possibility of reliably presenting information when performing a functional task;
the probability of providing the necessary information for a certain period of time;
the probability that the database will fully reflect certain types of real account objects;
the possibility of the absence of hidden random errors in the data under investigation;
the likelihood that there will be no hidden random errors by users or digital technology technicians before or during the completion of the task;
the likelihood that there will be no hidden virus exposure before or during the execution of the task, and the completion of the task will not be interrupted by prevention against the virus;
the possibility of maintaining its relevance during the use of information;
the possibility of preventing unauthorized access;
the possibility of maintaining privacy and integrity.
safety and integrity maintenance.

Each of the random events described by these probabilities can be considered as an alternative to some a_i from set a, which contributes to maintaining the data integrity. For all a_i∈a, the so-called optimization criterion (or parameter) can be given a function z(A), which has the property that if a_1>a_2, then 〖Z(a〗 _2)>z(a_1). For the entire set of alternatives A={a_1,a_2,...a_n}, a target function in the form Z=f(A)→ max or min is introduced.

The choice of any alternative has certain consequences (storing the data integrity), and the given criterion z(a) numerically represents the estimate of these consequences. The best alternative is a^* option with the highest criterion value:

when a∈is A, a^*=argmaxz(a). (1.1)

The question of determining the Optimal solution a^* also depends on the set A and the type of Criterion. In practice, the complexity of the task of determining the best alternative increases significantly, since it is often necessary to evaluate according to several criteria, and not bittalab. Then several criterion functions Z_I=f_I (a) Where i = 1, n, one generalized quantitative property-supermezon , the scaler function of the vector argument,

Z_0=〖z_0 (f〗 _I (a)) must be assembled, where i=1,n, (1.2

In this case the additive

Z_0=∑_(i=1)^n▒(〖p_i f〗 _i (a))/b_i (1.3)

or multiplicative functions are used

Z_0=∏_(i=1)^n▒(f_i 〖(a)^ ^ (p_i)) /b_i (1.4)

Where b_i is the value that ensures the normalization of different gender criteria, p_i is the weight, which describes the contribution of a particular criterion to supercritical.

p_i∈(0,1], ∑_(i=1)^n▒p_i =1 (1.5)

The weight of the initial indicators in the Integral index depends on their distribution and the correlation between them.

If the processed information resource is a discrete random variable, then the whole characteristic a_i is the probability of converting the true value of the message into some other a_j, i.J. This probability condition is p_ij=p(a_j/a_i).

The total probability of breaking the whole depends on the aprior probability distribution over the p_bb possible message ensemble:

P_bb h∑_(i=1)^M▒ 〖 P (a_i) p(a_j/a_i)〗 (1.6)

List of literature used

1 George S. Oreku “Database Security: Concepts, Approaches, and Challenges” 2014.
2 William Stallings “Cryptography and Network Security: Principles and Practice” 2013
3 David W. Chadwick “Secure Multi-Party Non-Repudiation Protocols and Applications” 2015
4 Hassan A “Database Security and Auditing: Protecting Data Integrity and Accessibility” 2021
5 Ravi S. Sandhu “Database Security and Integrity” 1994
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

ISSN NO: 2770-4491
Date of Publication:08-08-2023