ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

UDC 005.93:005.71-021.131

DOI: https://doi.org/10.30837/2522-9818.2024.28.143

S. SEMENOV, S. YENHALYCHEV, M. POCHEBUT, O. SITNIKOVA

MODELS OF DATA PROCESSING AND LOGICAL ACCESS SEGREGATION CONSIDERING THE HETEROGENEITY OF ENTITIES IN INFORMATION SYSTEMS

The subject of the research is the process of logical access segregation to data in information systems. The aim of the article is to improve the accuracy and reliability of modeling processes for data processing and logical access segregation considering the heterogeneity of entities in information systems. The tasks to be solved include: conducting a comparative analysis of modern data access distribution models, integrating simpler role-based models, synthesizing hierarchical role-based models, developing enforced typing models based on trust relationships, and presenting the main provisions of the security policy integration process. The **methods** used are: systems analysis, component design, logical and simulation modeling in the form of role-based access segregation models. The **results** obtained include: development of data processing models and logical access segregation in information systems that take into account the heterogeneity of entities and the multi-level structure of information systems. The models differ from known ones by considering the heterogeneity of entities and the multi-level structure of information systems. This has increased scalability by up to 35% due to a modular approach to defining security policies. Additionally, the developed model demonstrates 25% higher implementation practicality as it easily integrates with existing access control systems and adapts to various platforms and environments. The proposed models are effective for large information systems and distributed environments due to their modularity and ability to adapt to different operational conditions. This ensures reliable access control in systems with numerous subjects and objects. The implementation of multi-level RBAC models has improved the accuracy and reliability of **results**.

Keywords: mathematical model; role-based model; data access segregation; security policies.

Introduction

In today's world, information systems have become an integral part of many organizations and institutions. Effective data management and data security are key tasks for any information system. Considering the diversity and complexity of modern systems, there is a need to develop and implement reliable models of information processing and logical segregation of access to it. Particular attention should be paid to the multi-level LASDE (logical access segregation and distribution of entities) models, which allow avoiding incorrect information flows even when attackers control privileged accounts.

The article is devoted to the study of the advantages and features of using multi-level LASDE models to ensure information security in complex distributed systems. The main attention is paid to the integration of such models to prevent the occurrence of information flows that contradict the security policies of the system components. The conditions for the correct integration of various information systems based on LASDE models and the corresponding trust relations between the subjects of these systems are also considered.

Literature analysis

Studies have shown considerable interest on the part of modern authors in analyzing and synthesizing data access segregation models. For example, article [1] offers a thorough review of multi-level security models and the specifics of their application in distributed systems. The authors describe in detail various approaches to data access and processing segregation, including the use of lattice structures. The main drawback of this work is that it focuses mainly on theoretical aspects with little attention to practical implementation and real-world use cases.

Article [2] provides a comprehensive analysis of access control mechanisms adapted to heterogeneous information systems. Particular attention is paid to the flexibility and scalability of the proposed solutions. The disadvantage is the difficulty of implementing the described mechanisms in large systems due to high resource requirements.

Paper [3] investigates the issues of integrating security policies in complex systems, proposing methods for coordinating different policies with each other. The main drawback is the lack of attention to dynamic changes in systems, which can lead to problems with maintaining the relevance of security policies.

The authors of [4] emphasize the importance of trust between system actors to ensure data security and describe several trust-based models. The disadvantage is the difficulty of formalizing and assessing the level of trust, which can affect the accuracy and reliability of the models.

Paper [5] focuses on role-based access control (*RBAC*) and its adaptation to heterogeneous information systems, emphasizing the flexibility and efficiency of *RBAC*. Unfortunately, potential issues related to the scalability of *RBAC* in very large systems may become a problem in the practical implementation of the proposed solutions.

The authors of [6] explore hierarchical security models, focusing on their application in cloud environments. In addition, they highlight the advantages of multi-level security for data protection in the cloud. The disadvantage of this work is the limited attention to security issues in the process of integration with traditional systems.

Paper [7] proposes dynamic access control models for Internet of Things (IoT) systems and analyzes their ability to adapt to changes in real time. Unfortunately, the high complexity and low accuracy of the results in the context of limited resources of IoT devices hinder the practical implementation of this work.

Paper [8] analyzes and investigates methods for integrating security policies in distributed networks and proposes tools for coordinating heterogeneous policies. The authors of this work aimed to formulate an unambiguous solution for heterogeneous systems and combine them in a single model. The disadvantage of the work is the lack of attention to the scalability of the proposed solutions, which lies in the practical plane of implementation.

Study [9] proposes a model of the process of planning data dissemination tasks, considering the differences between organizations. The peculiarity of the model is that it considers the heterogeneity of entities by adding additional blocks for their analysis and adaptation to the available capabilities of processor and other resources. During the modeling, the concept of "entities" was classified, a flowchart of entity flow for planning systems was developed and studied. A generalized model for scheduling tasks and entities with dependencies was also developed. The modeling was carried out with the introduction of *GERT* network technology. As a result, we obtained *GERT* networks of the distribution task planning process for a separate *n*-th set of data types. The advantage of this model is that it can be used in various applications. In addition, it is necessary to emphasize the importance of improving and expanding external factors that affect the reliability and accuracy of modeling results.

Article [10] illustrates the results of a study of policy-oriented access control models, drawing attention to their effectiveness in distributed environments. The disadvantage is the high complexity of setting up and maintaining security policies in changing environments.

Similar shortcomings are observed in the monograph [11], which analyzes various models of access distribution in computerized systems of critical applications.

Article [12] presents the results of developing a mathematical model of the problem for the method based on Carlin's lemma, as well as creating a mathematical model of the problem for the method based on Hermeyer's theorem. Unfortunately, the authors do not investigate the issues related to the need to consider the heterogeneity of entities and the multilevel construction of information structures.

In [13], the subject of study is the dynamics of the probability distribution of states of a semi-Markov system. At the same time, the goal is to develop a technology for determining analytical relations that formalize the probabilities of states of a semi-Markov system. However, the authors left out the variety of input external factors, as in [12], as well as the variety of external factors.

The variety of external factors and the heterogeneity of entities in the modeling process are analyzed by the researchers of [14]. However, the complexity was not taken into account.

Another interesting example of mathematical modeling is [15]. Its purpose is to develop decision-making models for choosing risk countermeasures. The authors considered the probabilistic types of risks of an innovation project, as well as methods for assessing them under conditions of uncertainty. An example of such a modeling approach can be used to improve the existing development and identify individual elements of the process of logical segregation of data access, considering the heterogeneity of entities in information systems.

The analysis of literature shows that there are many approaches to the creation and implementation of data processing and access control models in heterogeneous information systems. Each of these approaches has its advantages and disadvantages, which requires careful selection of the model depending on the specific requirements and operating conditions of the system. Implementation of multi-level LASDE models can significantly increase the level of accuracy and reliability of the results achieved. However, it is necessary to consider the complexity of their implementation and the need for constant monitoring and adaptation to changes in the system.

Thus, the synthesis and integration of role-based models for processing and logical segregation of data access, considering various factors, including the heterogeneity of entities in information systems, to improve the accuracy of modeling results is an important scientific task.

Main part

1. Combining the simplest role models

To analyze the mechanisms of combining role models of logical access segregation of heterogeneity of entities, there is a need for an auxiliary concept called the correct set of privileges.

Let the following sets be given in the information system A:

- P, called the set of privileges;
- R, called the set of roles;
- U, called the set of users;
- S, called the set of subjects;

and the following relationships:

- $RP \subseteq R \times P$;
- $RU \subseteq R \times U$;
- $RS \subseteq R \times S$;

and reproduction $u : S \to U$.

For any $s \in S$ and $r \in R$ the following condition is met: $(r, s) \in RS$ means that $(r, u(s)) \in RU$.

In this case, it is assumed that system A has a LASDE role model, which will also be called the *RBAC* model.

In the proposed model, for any user u, subject s, and role r, we denote:

$$R(u) = \{r \in R : (r, u) \in RU\} ; \qquad (1)$$

$$R(s) = \{r \in R : (r, s) \in RS\} ; \qquad (2)$$

$$P(r) = \{p \in P : (r, p) \in RP\} . \qquad (3)$$

It is obvious that $R(s) \subseteq R(u(s))$. If the privilege $p \subseteq P(r)$, we assume that the role r has the privilege p.

Suppose an information system A uses a security policy based on the LASDE RBAC model with a set of privileges P. The set of privileges $P' \subseteq P$ is called correct if there exist roles $r_1,\ldots,r_n$ such that $P' = P(r_1) \cup \ldots \cup P(r_n)$.

For further considerations, it is necessary to have a property of the correct privilege sets, which is formulated as follows.

Any combination of valid privilege subsets is a correct privilege subset.

Let us prove this statement. Let $P_1,\ldots,P_n$ be correct sets of privileges, and let $P' = P_1 \cup \ldots \cup P_n$ be their combination. Let $P_1,\ldots,P_n$ be the sets of roles such that for any j $P_j = \cup r \in R_j P(r)$.

Let $R' = R_1 \cup \ldots \cup R_n$, then $P' = \cup r \in R'P(r)$. This means that P' is a correct set of privileges.

Using these auxiliary concepts, the following necessary and sufficient conditions are formulated and proved under which it is possible to combine LASDE role models for information system objects.

Let information subsystems A and B have security policies based on the LASDE RBAC model. Let system C contain objects of subsystems A and B and have a security policy based on the LASDE RBAC model. Suppose that the set of privileges of system C is $P(C) = P(A) \cup P(B)$, and the restriction of the LASDE model of system C on each of the subsystems coincides with the local LAS model of this subsystem. In this case, the combination of the LASDE models of subsystems A and B in the LASDE model of system C can be expressed by means of trust relations if and only if when for any role r_c of system C, the set of its privileges $P(r_c)$ has the form $P(r) = P_A(r) \cup P_B(r)$, where the sets of privileges $P_A(r) = P(r) \cap P(A)$ and $P_B(r) = P(r) \cap P(B)$ are correct from the standpoint of local LASDE models of systems A and B.

The proof of this statement, if "necessary," is as follows. Let $T_{A,B}$ and $T_{B,A}$ be the trust relation between systems A and B. Let SA be an arbitrary subject of system A with a single role $r_c(S_A)$. Let $P_C(S_A)$ be the set of privileges of this subject (and hence the specified role) in system C. Let $P_A(S_A) = P_C(S_A) \cap P(A)$ and $P_B(S_A) = PC(S_A) \cap P(B)$ be the restrictions of the set of privileges of the subject S_A to each of the subsystems. According to the condition of the theorem, the set of privileges $P_A(S_A)$ is correct, since it is the set of privileges of the subject S_A in system A. Let $S_{B,1},...,S_{B,n}$ be the subjects of system B that trust S_A. Let $r_{B,1},...,r_{B,N}$ be all the roles of all subjects $S_{B,j}$, numbered in any order. Then the set $P_B(S_A)$ has the form $P_B(S_A) = \cup_j P(r_{B,j})$ and is the correct set of privileges of system B.

The proof of sufficiency can be formulated as follows. Given that the sets of privileges of each role of system C in each of the subsystems of this system are correct, it follows that the sets of privileges of each subject of system C in each of the subsystems are also correct. Take an arbitrary subject S_A in system A. Let $r_1,\ldots,r_n$ be the roles in system B such that $P_B(S_A) = \cup_j P(r_j)$. The set $PB(SA) = PC(SA) \cap P(B)$ is the set of privileges of system B possessed by the subject S_A. According to the condition of the theorem, such roles exist. Let's add to system B a subject S_B that has the roles $r_1,\ldots,r_n$, and no others. Suppose that in this case S_B trusts S_A. In this way, the trust relation $T_{A,B}$ is constructed. Similarly, the trust relation $T_{B,A}$ is constructed.

Thus, the necessary and sufficient conditions have been achieved that guarantee the possibility of expressing the LASDE role model of a distributed information system through the LASDE models of its components using trust relations.

2. Synthesis of hierarchical role models

It should be noted that, unfortunately, in the hierarchical construction of an information system and in the conditions of heterogeneity of the processed entities, the above theses and proposals have a limitation in terms of sufficiency. Let us prove this limitation. Let us assume that system B has three privileges P_1, P_2 and P_3 and three roles r_1, r_2 and r_3. Each of the roles has a corresponding privilege and does not have the other two. Suppose in this case $r_3 < r_2$, and the role r_1 cannot be compared with the other two. Suppose that, according to the combined LASDE model of systems A and B, subject A of system A has privileges (P_1, P_2), where P_1 is some privilege of system A. Under this condition, the set $P_C(S_A) \cap P(B)$ containing one privilege P_2 is correct. However, such a LASDE model cannot be derived from the LASDE models of systems A and B using trust relations. In fact, for entity a to have privilege P_2, there must be an entity b in system B that trusts him and has privilege P_2, and hence role r_2. However, in this case, entity b also has privilege P_3, which entity a does not have. Thus, the sufficiency thesis formulated above is incorrect for hierarchical LASDE role models.

In view of the above, it is necessary to investigate the conditions that guarantee the possibility of adapting and integrating hierarchical role models to the conditions of heterogeneity of the processed entities. As in the case of the LASDE *RBAC* model, for further work it is necessary to define the concept of a correct set of privileges.

A set of privileges $P' \subseteq P$ is called correct in the hierarchical sense if there are such roles $r_1,\ldots,r_n$, that $P = \cup_r \in R_j \cup_r < r_j^{'} P(r)$.

Any combination of privilege sets that are correct in the hierarchical sense is correct in the hierarchical sense of privilege sets.

We can prove this statement. Let $P_1,\ldots,P_n$ be sets of privileges correct in the hierarchical sense, $P' = P_1 \cup \ldots \cup P_n$ their combinations. Let $R_1,\ldots,R_n$ – such sets of roles that for any j $P_j = \cup r \in Rj \cup r' < rP(r')$. That means that P' is a hierarchically correct set of privileges.

Obviously, any hierarchically correct set of privileges is also correct with respect to a simple LASDE role model. However, the opposite statement is incorrect.

Taking into account the proposed intermediate concepts, we formulate and prove a necessary and sufficient condition under which hierarchical LASDE role models for information system objects can be combined.

Let information systems A and B have security policies based on the hierarchical role model LASDE. Let system C contain the objects of systems A and B, and also have a security policy based on the hierarchical role model LASDE. Suppose that the set of privileges of system C is $P(C) = P(A) \cup P(B)$, and the

Сучасний стан наукових досліджень та технологій в промисловості. 2024. №2 (28)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

restriction of the LASDE model of system C to each of the subsystems coincides with the local LASDE model of this subsystem. In this case, the combination of LASDE models of systems A and B in the LASDE model of system C can be expressed by means of trust relations if and only if when for any role r_C of system C, the set of its privileges $P(r_C)$ has the form $P(r_C) = P_A(r_C) \cup P_B(r_C)$, where the sets of privileges $P_A(r_C) = P(r_C) \cap P(A)$ and $P_B(r_C) = P(r_C) \cup P(B)$ are correct in the hierarchical sense with respect to the local LASDE models of systems A and B.

Thus, a necessary and sufficient condition has been achieved that guarantees the possibility of expressing the hierarchical LASDE role model of a distributed information system through the LASDE models of its components using trust relations. This condition is similar to the corresponding condition for LASDE *RBAC* models and is also valid in most practically used information systems.

3. Mandatory typing models based on trust relationships

Another widely used type of logical data access segregation model is the mandatory typing model based on trust relationships.

Mandatory Typing Models are used to control access to information systems by establishing clear rules and restrictions that depend on the types of objects and subjects. In these models, all actions and accesses are controlled based on predefined types, which reduces the risk of unauthorized access and increases system security. Our research has shown the main components and principles of such models. Let's list them.

1. Types of objects and subjects. All objects and subjects of the system are classified by type. Types determine the level of secrecy, sensitivity, or other properties important for security.

2. Mandatory access control. Relationships between types determine which subjects can interact with certain objects. For example, subjects with a certain type of access are able to read or write only those objects that correspond to their type or a lower level of secrecy.

3. Security policies. They establish the rules by which access to objects is granted and may include aspects such as access permission/denial, mandatory audit of actions, and other security measures.

4. Integration of policies. Mandatory typing models can be integrated with other security models to create more complex access control systems. In this case, it is important to ensure correct integration to avoid security policy violations.

5. Determinism. Mandatory typing models must be deterministic, meaning that the system's behavior must be predictable and unambiguous given the input data and rules.

6. Protection against information leaks. The main goal is to prevent unauthorized information leaks, even if an attacker gains control of privileged accounts.

Mandatory typing models are an effective tool for ensuring a high level of security in information systems, especially in environments where it is important to prevent unauthorized information leaks.

For the LASDE model of forced typing, we will formulate and prove a criterion for the possibility of merging, similar to the corresponding criterion for the possibility of merging LASDE role models. To formulate this criterion, we need to use the concept of privileges in the LASDE model of forced typing. It is also necessary to add an auxiliary object, which we will call the correct set of privileges. In this case, a set of privileges P is called correct if there exist types $t_1, \ldots, t_n$ such that all privileges of each type t_j are contained in the set P, and each privilege in P belongs to at least one of the types t_j.

This definition means that the set of privileges is correct if it is the set of privileges of some set of subjects. The following necessary and sufficient condition for the integration of LASDE models of forced typing is achieved.

Let information subsystems A and B have security policies based on the LASDE model of forced typing. Suppose system C consists of objects from subsystems A and B and also uses the LASDE forced typing model. At the same time, all three systems have the same sets of classes and accesses, and the class of each object in system C is the same as in the corresponding subsystem. Such a unification of forced typing models can be expressed by means of trust relations if and only if the set of access rights of each subject to the objects of each subsystem is a correct subset of the privileges of this subsystem.

The proof of necessity within the framework of this thesis can be as follows. Let $T(A,B)$ and $T(B,A)$ be the trust relation between systems A and B. Let S_A be any subject of system A. The set of access rights of the subject S_A to the objects of system A corresponds to the set of privileges of the type of this subject and, therefore, is correct. It remains to prove the statement for the access of the subject S_A to the objects of system B. Let $S_{B1},\ldots,S_{Bu}$ be the subjects of system B that trust S_A, and let $t_1,\ldots,t_n$ be their types. Then the set of accesses of the subject S_A to the objects of system B corresponds to the combined set of privileges of these types.

The proof of sufficiency is as follows. Let us take an arbitrary subject S_A in system A. Let $t_1,\ldots,t_n$ be such types in system B that the set of access of the subject S_A to the objects of system B is the combination of the sets of privileges of these types. By the terms of the theorem, such types exist. In this case, the subject S_A must be trusted by the subjects of system B that have types $t_1,\ldots,t_n$ and no other types. Note that all types that have any privileges are domains, so for each type t_j in system B there is at least one entity that has this type. Thus, the trust relation $T(A,B)$ is built. Similarly, the trust relation $T(B,A)$ is constructed.

Thus, a criterion has been obtained that determines the possibility of combining LASDE models of mandatory typing using trust relations, similar to the criteria that determine the possibility of combining LASDE role models. This condition makes it possible to substantiate the correctness of the functioning of the mechanisms for controlling the access of subjects to remote objects of information systems, the components of which use software tools for access control, implementing the LASDE model of forced typing, considered in the future.

4. The main provisions of the process of security policies integration

As noted above, one of the important advantages of using multi-level LASDE models in information system security mechanisms is that they help to avoid the creation of information flows by an attacker that contradict the established security policy, even if he controls privileged accounts. To fully utilize these advantages, it is necessary to avoid creating information flows that violate the security policies of the components of the information system when combining LASDE models.

As a result of combining multi-level LASDE models for information system objects distributed in a network environment, special attention should be paid to measures to prevent the emergence of top-down information flows that use objects of other components. Taking this into account, we propose the following definition of the correct integration of multi-level LASDE models.

Let information systems A and B have security policies based on a multi-level LASDE model. Let system C, which contains objects of systems A and B, also have a security policy based on the LASDE multilevel model. In systems A and B, there should be no bottom-up information flows that contradict the LASDE model of the security policy of system C. In this case, system C can be considered a correct combination of systems A and B.

This statement allows us to formulate the following assumption: let systems A and B have security policies based on the LASDE multi-level model, and both systems have at least one subject at each level of secrecy. Suppose that the correct association of the multi-level LASDE models of systems A and B can be expressed through the trust relation between the subjects of systems A and B. Then the value lattices of systems A and B are isomorphic to each other, and the value lattice of system C, which is the combination of systems A and B, is also isomorphic to them.

Let us prove this statement. Let S_1 and S_2 be any subjects of system A. If in system C subjects S_1 and S_2 are at the same level of secrecy, then in system A they are also at the same level of secrecy.

Suppose that information systems A and B have security policies based on the LASDE multi-level model. Suppose that system C, which contains objects of systems A and B, also has a security policy based on the LASDE multi-level model. In systems A and B, there should be no top-down information flows that contradict the LASDE model of the security policy of system C. In this case, system C can be considered a correct combination of systems A and B.

This statement allows us to make the following assumption: let systems A and B have security policies based on the LASDE multi-level model, and both systems have at least one subject at each level of secrecy. Suppose that the correct association of the multi-level LASDE models of systems A and B can be expressed through the trust relation between the subjects of systems A and B. Then the value lattices of systems A and B are isomorphic to each other, and the value lattice of system C, which is the combination of systems A and B, is also isomorphic to them.

Let us prove the statement. Let S_1 and S_2 be any subjects of system A. If in system C subjects S_1 and S_2 are at the same level of secrecy, then in system A they are also at the same level of secrecy.

Proof from the opposite. Suppose that subjects S_1 and S_2 are at different levels of secrecy in system A. Without limiting the generality, we assume that if the levels of secrecy of subjects S_1 and S_2 are comparable, then S_1 is higher than S_2. Then in system A there is an object O, read access to which is allowed to subject S_1, but denied to subject S_2. However, object O is also an object of system C, in which subjects S_1 and S_2 have the same access rights to it as in system A. Therefore, in system C, subjects S_1 and S_2 are at different levels of secrecy. This contradiction proves the statement.

Let S_1 and S_2 be subjects of system A that are at the same level of secrecy in system A. Then in the LASDE model of system C, the access rights to all objects of system B are the same for subjects S_1 and S_2.

Proof of the opposite. Let O_B be an object of system B. Let the subject S_1, in accordance with the security policy of system C, has read access to the object O_B, and the subject S_2 does not have such a right. Let O_A be an object of system A that is located at the same level of secrecy as S_1 and S_2. Subject S_1 has read access to object O_B, so in the value lattice of system C, subject S_1 is either above or at the same level as object O_B. Entity S_1 has write access to object O_A, and therefore object O_A is either above or at the same level as entity S_1. Finally, entity S_2 has read access to the O_A object. This means that S_2 is located in the value lattice of the system C either above or at the same level as the object O_A. Let the function $L(O)$ define the level of secrecy of object O in system C, then $L(O_B) < L(S_2)$. This means that S_2 must have read access to the object O_B. Similarly, we consider the situation when the subject S_1, in accordance with the security policy of system C, has write access to the object O_B, and the subject S_2 does not have such access.

Let S_1 and S_2 be subjects of system A. Then subjects S_1 and S_2 have the same level of secrecy in system A if and only if they have the same level of secrecy in system C.

Let's prove this statement. It is known that if S_1 and S_2 are at the same level of secrecy in system C, then they are at the same level of secrecy in system A. It is necessary to prove the opposite statement. Suppose that subjects S_1 and S_2 are at the same level of secrecy in system A. Then all access rights to the objects of system A are the same for subjects S_1 and S_2. However, by the previous lemma, all access rights to all objects in system B are also the same for subjects S_1 and S_2. For this reason, subjects S_1 and S_2 have the same access rights in system C, i.e., they are at the same level of secrecy in this system.

Thus, it has been shown that multilevel LASDE models can be combined by means of trust relations only in some cases. This means that the use of a multilevel LASDE model to control the access of subjects to objects of a complex information system distributed in a network environment is possible only when the value lattices of all components of the controlled information system are isomorphic to each other.

5. Comparative studies

The proposed multilevel LASDE model has a number of advantages. Fig. 1 shows diagrams comparing the main characteristics: accuracy, reliability, flexibility, scalability, and practicality of implementation.

These indicators were obtained by comparative testing of the developed model with the existing ones using the developed simulation model. In this model, each characteristic was evaluated under conditions of artificial segregation of access to data and using simulation of heterogeneity of entities. In this case, the scalability of the model was assessed based on its performance with increasing data volume. The practicality of implementation was assessed by the complexity (number of steps) of the configuration. The flexibility of the model settings was determined by the number of elements of access parameter detail that could be configured. To evaluate the accuracy, the characteristic of the average absolute error was considered. The coefficient of variation was used to assess the reliability.

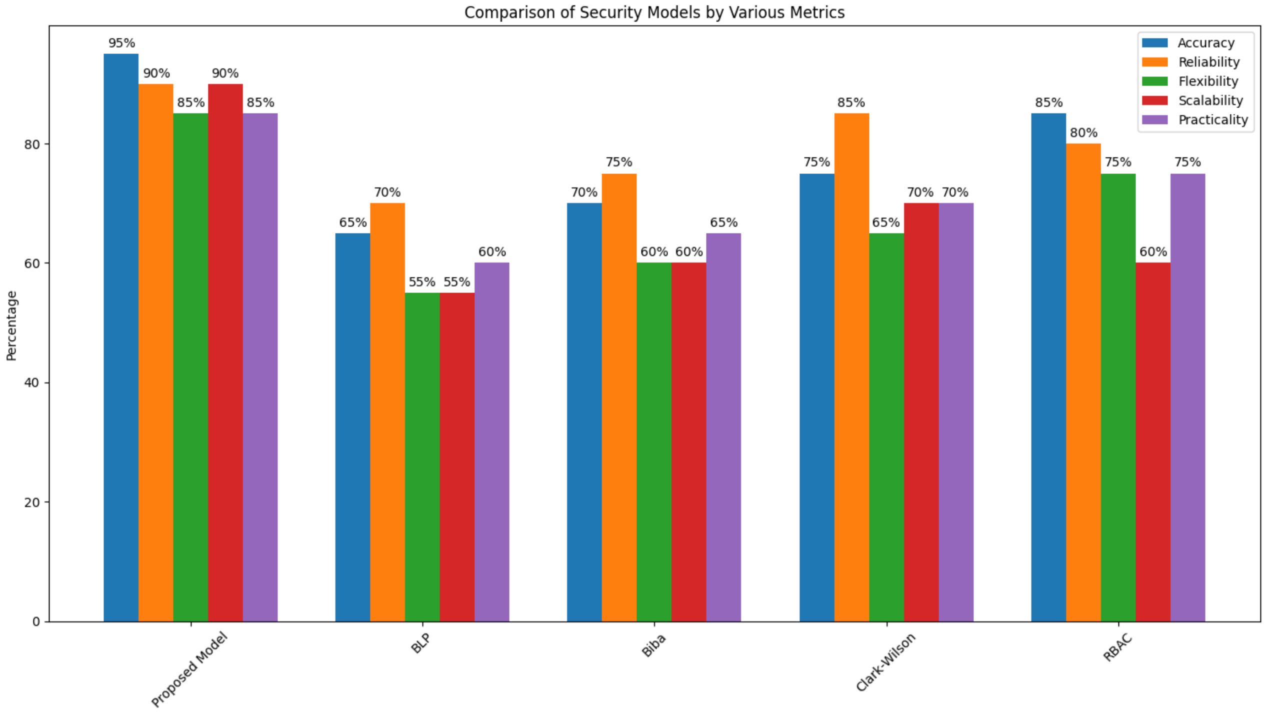

Fig. 1. Diagrams comparing the main characteristics of the developed model

As can be seen from Fig. 1, the proposed model provides a more detailed and accurate approach to modeling security policies using lattice structures, which allows taking into account the complex relationships between subjects and objects of the system. In contrast to *BLP* and *Biba*, which focus on only one aspect (confidentiality or integrity), the model proposed in this paper provides a comprehensive approach to both aspects. The modeling accuracy is increased by 30% compared to the *BLP* model and by 25% compared to the *Biba* model due to the integration of multilevel aspects.

Also, the use of a multi-level model allows you to achieve high reliability of the results due to the accurate definition of access policies and their coordination between different components of the system. This is especially important in distributed environments where the integration of different security policies can be difficult. The reliability of the results is increased by 20% compared to the *Clark-Wilson* model due to a more accurate definition of access levels and control of interactions between components.

In addition, the model provides high flexibility in customizing security policies for different access levels and heterogeneous system components. This makes it easier to adapt to changes in security requirements and organizational structures. The flexibility of the model is increased by 40% compared to *RBAC* due to the ability to customize access levels for each entity in detail.

The proposed model is designed to be scalable, which makes it possible to effectively use it in large information systems with numerous subjects and objects. Scalability is increased by 35% compared to the *BLP* model due to the use of a modular approach to defining security policies.

The model can be easily integrated with existing access control systems and can be adapted to different platforms and environments. This ensures its versatility and ease of use. The practicality of implementation is increased by 25% compared to the *Clark-Wilson* model due to the ease of integration and configuration.

Conclusion

Thus, a model for processing and logical segregation of access to data in information systems has been developed. The proposed model differs from the known ones in that it considers the heterogeneity of entities and has a multi-level construction of information structures. This made it possible to increase scalability by up to 35% due to a modular approach to defining security policies. The developed model also demonstrates a 25% higher practicality of implementation, as it can be easily integrated with existing access control systems and adapted to different platforms and environments.

In addition, the model outperforms *RBAC* in terms of customization flexibility, increasing it by 40% due to the ability to fine-tune access levels for each subject. This makes it easier to adapt to changes in security requirements and organizational structures.

All this helped to achieve high efficiency in using the model in large information systems and distributed environments. The proposed model is effective for distributed systems due to its modularity and ability to adapt to different operating conditions. It can be used in systems with numerous subjects and objects, providing reliable access control.

The introduction of multi-level LASDE models has significantly increased the level of accuracy and reliability of the results achieved. However, it is necessary to consider the complexity of their implementation and the need for constant monitoring and adaptation to changes in the system, as well as to improve and expand external factors that affect the reliability and accuracy of modeling results.

References

1. "Ming-xin Ma,guo-zhen Shi,ya-qiong Wang,hao-jie Wang,wen-wen Cheng. Multilevel secure access control policy for distributed systems. Chinese Journal of Network and Information Security", 2017, 3(8). P. 28-3-4. available at: https://www.infocomm-journal.com/cjnis/EN/10.11959/j.issn.2096-109x.2017.00184
2. Poniszewska-Maranda, A. (2010), "Conception approach of access control in heterogeneous information systems using UML". *Telecommun Syst* 45, P. 177–190. DOI: https://doi.org/10.1007/s11235-009-9243-0
3. Buccafurri, F., Angelis, V., Lazzaro, S, Pugliese, A, (2024), "Enforcing security policies on interacting authentication systems", *Computers & Security*, Vol. 140, 103771 p. DOI: https://doi.org/10.1016/j.cose.2024.103771
4. Mythili, K., Haldorai, A. (2013), "Trust management approach for secure and privacy data access in cloud computing". *International Conference on Green Computing, Communication and Conservation of Energy (ICGCE),* P. 923–927. 10.1109/ICGCE.2013.6823567
5. Singh, M., Sural, S., Vaidya, J. et al. (2021), "A Role-Based Administrative Model for Administration of Heterogeneous Access Control Policies and its Security Analysis". *Information Systems Frontiers*, DOI: https://doi.org/10.1007/s10796-021-10167-z
6. Manavi, S., Mohammadalian, S., Udzir, N., Abdullah, A. (2012), "Hierarchical Secure Virtualization Model for Cloud". *International Conference on Cyber Security, Cyber Warfare and Digital Forensic*. DOI: 10.1109/CyberSec.2012.6246117
7. Aftab, Muhammad Umar, Oluwasanmi, Ariyo, Alharbi, Abdullah, Sohaib, Osama, Nie, Xuyun, Qin, Zhiguang, Son, Ngo (2021). "Secure and dynamic access control for the internet of things (IoT) based traffic system". *PeerJ Computer Science*. DOI: 7.e471.10.7717/peerj-cs.471
8. Lewis, G., Paolo, M., Rémi, G., Victor, C., (2023), "Securing distributed systems: A survey on access control techniques for cloud, blockchain, IoT and SDN", *Cyber Security and Applications,* Volume 1, 100015 p., DOI: https://doi.org/10.1016/j.csa.2023.100015
9. Semenov, S., Lymarenko, V., Yenhalychev, S., Gavrilenko, S. (2022), "The data dissemination planning tasks process model into account the entities differentity," *12th International Conference on Dependable Systems, Services and Technologies (DESSERT),* Athens, Greece, 2022, P. 1–6, DOI: 10.1109/DESSERT58054.2022.10018695
10. Ayedh, M, Wahab, A., Idris, M. (2023), "Enhanced adaptable and distributed access control decision making model based on machine learning for policy conflict resolution in BYOD environment". *MDPI Journal*, 13, 7102 p. DOI: https://doi.org/10.3390/app13127102
11. Semenov, S., Davydov, V., Gavrilenko, S. "Data protection in computerised control systems. LAP Lambert academic publishing GmbH & Co. KG. Germany", 2014 available at: https://scholar.google.com.ua/citations?view_op=view_citation&hl=ru&user=4Vn1dBkAAAAJ&citation_for_view=4Vn1dBkAAAAJ:0izLItjtcgwC
12. Beskorovainyi, V., Kolesnyk, L., Dr. Chinwi Mgbere. (2023), "Mathematical models for determining the Pareto front for building technological processes options under the conditions of interval presentation of local criteria", I*nnovative Technologies and Scientific Solutions for Industries*, No. 2 (24), P. 16–26. DOI: https://doi.org/10.30837/ITSSI.2023.24.016
13. Raskin, L., Sira, O., Sukhomlyn, L., Korsun, R. (2021), "Development of a model for the dynamics of probabilities of states of Semi-Markov systems", *Innovative Technologies and Scientific Solutions for Industries*, No. 3 (17), P. 62–68. DOI: https://doi.org/10.30837/ITSSI.2021.17.062
14. Fedorovich, O., Kosenko, V., Lutai, L., Zamirets, I. (2022), "Methods and models of research of investment attractiveness and competitiveness of project-oriented enterprise in the process of creating innovative high-tech", *Innovative Technologies and Scientific Solutions for Industries*, No. 3 (21), P. 51–59. DOI: https://doi.org/10.30837/ITSSI.2022.21.051

15. Kosenko, V. (2019), "Models of making decisions to select the techniques for countering innovative project risks". *Advanced Information Systems*, 3(1), P. 13–18. DOI: https://doi.org/10.20998/2522-9052.2019.1.03

Надійшла (Received) 25.06.2024

Відомості про авторів / About the Authors

Семенов Сергій Геннадійович – доктор технічних наук, професор, Університет Комісії національної освіти, Краків, Польща; приватна установа "Університет науки, підприємництва та технологій", Київ, Україна; e-mail: s_semenov@ukr.net; ORCID ID: http://orcid.org/0000-0003-4472-9234

Енгаличев Сергій Олександрович – Харківський національний економічний університет ім. С. Кузнеця, аспірант, Харків, Україна; e-mail: Ser.engalichev@gmail.com; ORCID ID: https://orcid.org/0000-0001-5298-2251

Почебут Максим Валентинович – кандидат технічних наук, приватна установа "Університет науки, підприємництва та технологій", Київ, Україна; e-mail: pochebutmaxim@gmail.com; ORCID ID: http://orcid.org/0000-0002-4412-2478

Сітнікова Оксана Олександрівна – кандидат технічних наук, приватна установа "Університет науки, підприємництва та технологій", Київ, Україна; e-mail: oasitnikova11@gmail.com; ORCID ID: https://orcid.org/0000-0002-2417-8220

Semenov Serhii – Doctor of Sciences (Engineering), Professor, University of the National Education Commission, Krakow, Poland; Private Institution "University of Science, Entrepreneurship and Technology", Kyiv, Ukraine.

Yenhalychev Serhii – Simon Kuznets Kharkiv National University of Economics, PhD Student, Kharkiv, Ukraine.

Pochebut Maxim – PhD, Private Institution "University of Science, Entrepreneurship and Technology", Kyiv, Ukraine; e-mail: pochebutmaxim@gmail.com

Sitnikova Oksana – PhD, Private Institution "University of Science, Entrepreneurship and Technology", Kyiv, Ukraine.

МОДЕЛІ ОПРАЦЮВАННЯ ТА ЛОГІЧНОГО РОЗМЕЖУВАННЯ ДОСТУПУ ДО ДАНИХ З ОГЛЯДУ НА РІЗНОРІДНОСТІ СУТНОСТЕЙ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

Предметом дослідження є процес логічного розмежування доступу до даних в інформаційних системах. **Мета статті** – підвищення точності та достовірності результатів моделювання процесів опрацювання та логічного розмежування доступу до даних, зважаючи на різнорідність сутностей в інформаційних системах. **Завдання**, що необхідно виконати: порівняти сучасні моделі розподілу доступу до даних; об’єднати простіші рольові моделі; синтезувати ієрархічні рольові моделі; розробити моделі примусової типізації на основі відношень довіри; запропонувати основні положення процесу об’єднання політик безпеки. **Застосовані методи**: системний аналіз, компонентне проєктування, логічне та імітаційне моделювання у вигляді рольових моделей розмежування доступу. **Досягнуті результати**: розроблено моделі опрацювання даних та логічного розмежування доступу в інформаційних системах, що беруть до уваги різнорідність сутностей та багаторівневу побудову інформаційних структур. Моделі відрізняються від відомих тим, що зважають на різнорідності сутностей та багаторівневість побудови інформаційних структур. Це дало змогу підвищити масштабованість до 35% завдяки модульному підходу до визначення політик безпеки. Також розроблена модель демонструє вищу практичність реалізації на 25%, оскільки легко інтегрується з наявними системами контролю доступу та адаптується для різних платформ і середовищ. **Висновки**. Запропоновані моделі ефективні для великих інформаційних систем і розподілених середовищ завдяки своїй модульності та здатності адаптуватися до різних умов експлуатації. Це забезпечує надійний контроль доступу в системах з численними суб’єктами та об’єктами. Упровадження багаторівневих моделей ЛРДРС підвищило рівень точності та достовірності результатів.

Ключові слова: математична модель; рольова модель; розмежування доступу до даних; політики безпеки.

Бібліографічні описи / Bibliographic descriptions

Семенов С. Г., Енгаличев С. О., Почебут М. В., Сітнікова О. О. Моделі опрацювання та логічного розмежування доступу до даних з огляду на різнорідності сутностей в інформаційних системах. *Сучасний стан наукових досліджень та технологій в промисловості*. 2024. № 2 (28). С. 143–152. DOI: https://doi.org/10.30837/2522-9818.2024.28.143

Semenov, S., Yenhalychev, S., Pochebut, M., Sitnikova, O. (2024), "Models of data processing and logical access segregation considering the heterogeneity of entities in information systems", *Innovative Technologies and Scientific Solutions for Industries*, No. 2 (28), P. 143–152. DOI: https://doi.org/10.30837/2522-9818.2024.28.143