ISSN 1330-3651 (Print), ISSN 1848-6339 (Online) https://doi.org/10.17559/TV-20200516084319
Original scientific paper

Multi-Level Security Model Developed to Provide Data Privacy in Distributed Database Systems

Cigdem BAKIR*, Mehmet GUCLU

Abstract: Information security is related to efforts put in to avoid activities such as unauthorized usage, changing or disseminating of information by having access to these pieces of information. This should not be only thought as capturing of information but also as avoiding the violation of particulars such as integrity, availability, and confidentiality. Vulnerability that occurs in any one of these three basic elements will be evaluated as violation of information security. In this study with the aim to develop a multi-level access control method, Improved Bell-LaPadula security model has been adopted to distributed systems and hence, it was aimed to show how the property of confidentiality, being one of the three basic elements in information security, has been provided. The developed model proposed in the study has been applied on data cluster which has been obtained from real life. Performance of the proposed model has been compared with the performances of Role Based Access Control and Traditional Access Control models. As the obtained results were compared, it was observed that with the proposed model data were provided in a more secure and rapid way to be shared by the users.

Keywords: access control model; Bell-LaPadula model; distributed databases; role based access control

1 INTRODUCTION

Information security is defined as the avoidance of acts such as having unauthorized access to information, and using, changing or destroying the data, and it is composed of certain basic elements, namely confidentiality, integrity and availability [1]. Confidentiality is related to protection of information against its being accessed and read or used by unauthorized people. Integrity is related to avoiding the changing of information by unauthorized people and protecting its originality. Availability is the situation where information is only accessible to and usable by authorized people. We can generally state that many threats turn into attacks by benefiting from security deficits or weaknesses, and in order to prevent this type of attack damaging the operating system it is highly desirable to provide all of the above mentioned security elements. For this reason, no matter how securely a system is protected, the important issue is to determine the elements that can give rise to attacks and to take the required measures [2].

So far, we have seen developed the security models whose design has been specific to their application areas [3]. However, traditional security models cannot meet the requirements relating to the rapidly increasing numbers of systems that are becoming increasingly more complex. When the factors giving rise to this situation are examined, it is seen that making it mandatory to conduct very tight controls and inspections plays an important role in environments where sensitive information is kept, where inspection of information flow is not guaranteed, where data is not able to be shared in a secure and fast way, and where there is a significant loss of flexibility in the application area [4].

This study discusses the problems of loss of flexibility in access and of reduced allocation of resources among users, which are among the most common problems in real system applications [5]. The absence of an exceptionally flexible approval mechanism in existing access control models may impair the resource availability and work time efficiency of current applications, and limit their growth [6]. This study defines new security policies in addition to the security policies offered by the Bell-LaPadula model. With the proposed model, the aim was to increase the use of resources with access controls in a controlled and safe manner with the newly defined policies.

Distributed systems are different databases held in different locations but interconnected by a computer network. Many large-scale institutions and organizations prefer these systems. In our study, a more functional and suitable access control model has been developed by considering the weak points of traditional security models in real system applications. The main contribution of our study is a model that can be adopted by distributed database systems and that has been developed by defining new and multi-level access control procedures in addition to the security policies offered by the Bell-LaPadula model. Especially with regard to distributed database systems, the aim was to adopt the developed model to the real systems in a more flexible and effective way to deliver the requirements of confidentiality relating to data.

The remaining part of this study has been organized in the following way: Relevant studies are covered in section 2, section three covers distributed database and security models. Details of the proposed and improved, multi-level security model for distributed systems are given in section 4, and the experimental study is shown in section 5. Finally, the evaluation and conclusions are given in section 6.

2 RELATED WORKS

Security concerns related to databases and especially distributed databases have been evaluated in various studies [8]. In some of the studies in particular, security problems relating to each of the two system types were evaluated separately and were focused on the weak points of each system with respect to security [7]. In these studies it was emphasized that distributed database systems faced various security problems, such as multi-level access control, confidentiality, reliability, integrity and recovery [8].

Naeem et al. [9] used a team-based access control (TMAC) model and an extended role-based access (RBAC) model in order to increase common sharing and to

increase confidentiality of information. In the study on confidentiality, sharing and rule-based metrics for both models related to access control and privacy issues were compared, and their results were evaluated.

In another study [10], protection of confidentiality and security requirements relating to the role-based access control (RBAC) security model have been examined. In order to support secure health services, a health service integration platform (u-HCSIP) was designed and an RBAC-based security model was applied in this design. The applicability of the RBAC-based u-HCSIP, which was proposed by analyzing the work flow, was verified.

In current Distributed Control System (DCS) environments, it is difficult to comply with the principle of least privilege, since access control principles are distributed among many heterogeneous systems [11]. In some studies, the main difficulties in progress towards a more complete and manageable access control model in distributed systems have been mentioned [12]. In one study, an access control architecture that could be adapted by the Industrial Control System (ICS) community was presented so that each access could be checked against the policies complying with the principle of least privilege [13]. In this proposed architecture, the aim was to protect central policy management and every connected field device. Bertolissi, C. and Fernandez, M. [14] defined a metamodel for access control design taking into account the special requirements of distributed environments. In the study, a framework was proposed for the implementation of access control policies that take into account the local policies determined by each member of a distributed system consisting of several sites, each of which protects its own resources.

Dasgupta et al. [15] established an access control graphic primarily based on mutual relationships between employees and their roles within the organization. Afterwards a series of approval mechanisms were developed to approve the access request of a user at a specific time. The proposed multi-user approval strategy was evaluated with two empirical data clusters and the reported outcomes showed the ability to select non-repetitive approvers for user access under different institutional and environmental constraints.

An access control mechanism was designed in the cloud environment by considering the behavior of the honey bees that prevents intruders from entering their hives [16]. In the study, new attribute-based access control for cloud security was introduced through the Bell-LaPadula Model-inspired by the honey bee behavior [17].

In published literature, in recent years, various studies using different techniques in line with the above-mentioned goals have been conducted. In our study, unlike those studies, the users' past actions, interactions between individuals, trust values or users' requests for access were not considered; special rights and powers were defined to meet the requirements of users in accordance with the changing commercial conditions, business requirements and organizational structure. In this current study, the aim was to dynamically change the security policies that were initially decided on, and increase the availability and sharing of resources in a safe and controlled manner by giving users special rights and powers at different access levels. The most important contribution of the study is that it was based on providing flexibility to sector applications by operating an exceptional multi-level approval mechanism.

3 DISTRIBUTED DATABASE AND DATA SECURITY

3.1 Distributed Database

We call the system that can serve the users as a single system by working in communication and coordination among the servers, although data logically linked to one another is distributed on different servers, as a distributed database system [18]. Each one of the storage units shown in Fig. 1 can be a computer and while these computers can be present in the same environment, they can also be placed at remote points that can communicate with computer net. The place where the data being accessed is stored is not known by the client. In Fig. 1, we also demonstrated the communication between server and clients by integrating database security into distributed systems.

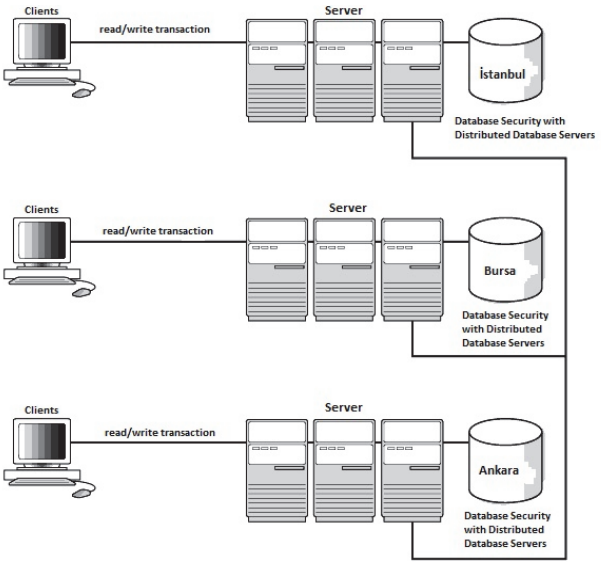

Figure 1 Database security with distributed systems servers and clients

Two types of distributed database systems can be defined, homogeneous database system and heterogeneous database system [14].

3.1.1 Homogeneous Database System

In Fig. 2, all servers use the same Database Management System (DBMS) product.

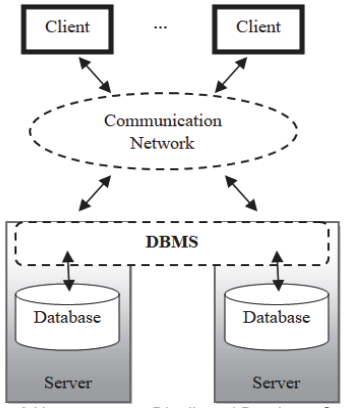

Figure 2 Homogeneous Distributed Database System

It is seen by the user as a single system. With this approach it is enabled for a new site to be easily added to distributed database management system and for more than one site to benefit from parallel processing capacity [19]. Its usage, design and easy management are among its advantages. Its disadvantage is that it is difficut for many institutions to force the homogeneous environment.

3.1.2 Heterogeneous Database System

Fig. 3 shows the database system which integrates different central DBMS types through one communication net. It is not required for all sites to use the same DBMS product. Each site can use different schemes and software. Sites may not be aware of one another and they may provide only limited opportunities for cooperation in their processing. System contains different DBMSs that support different data models (relational, hierarchical or network) that operate in different computer systems such as main computers and micro computers . Its advantage is that in a global center big data coming from different data centers can be stored, remote access can be made by using general scheme, and different DBMSs are used in each node. Its disadvantage is that its management and design are difficult [20].

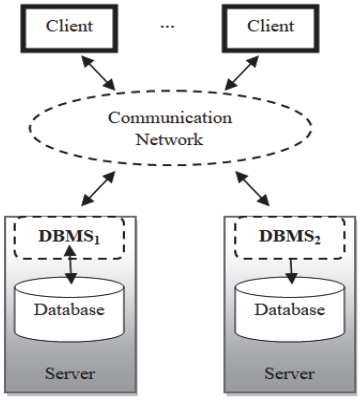

Figure 3 Heterogeneous Distributed Database System

3.2 Security Models

3.2.1 Role Based Access Control Model

Roles are defined according to the tasks and responsibilities of users within an organization, and authorization to have access to resources and its limitations is shaped according to these roles. Users have certain authorizations as per the roles being defined for them. In this model with the roles of users that are shaped by being correlated with their tasks, it is enabled to use expressions such as 'Human resources specialist screens personal staff files' instead of expressions such as '*X* user has reading and writing authorizations in relation to *Y* object'. Since roles are limited with the tasks, in the model "minimum authorization" principle is applied.

In Fig. 4, the relationship between users, roles and authorizations is shown. Authorizations are the transactions that can be applied on objects (systems, servers, files, applications etc.) and they are defined for the roles. By assigning roles to the users, it is enabled for them to have certain authorizations. For each role authorization is given for having access to one or more number of sources and one or more number of roles are assigned for each user.

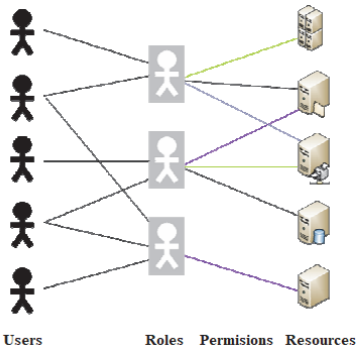

Figure 4 Role Structure

3.2.2 Traditional Access Control Model

Traditional access control models are shown in Fig. 5. Traditional access control model is divided into two as being 'mandatory access control' and 'Discretionary access control'. In Mandatory Access Control Model, access of users to the resources is controlled in accordance with certain rules being predetermined by central authority [9]. This type of access control is widely observed in military confidentiality classification. In the Discretionary Access Control Model, users can give access authorizations to other users within limits being assigned to them or they can determine limitations (Fig. 5). This type of access control is commonly seen in folder and file authorizations of operating systems [9].

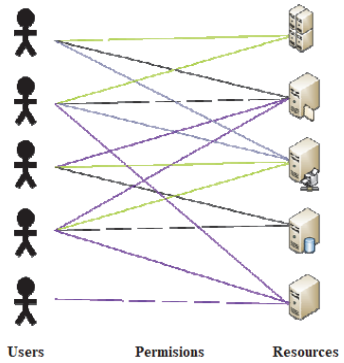

Figure 5 Traditional Authorization

3.2.3 Bell-Lapuda Model

Subjects define the users and systems in relation to security. In this study subjects have been defined as user or actor. Objects define all kinds of source data on which processes such as reading, writing, erasing, and updating can be done [21]. For each object and actor a specific level of security has been defined. Actor can perform defined processes on the objects that are available at the security level which has been defined for the actor.

While a model for which more than one security level has been defined can be used in various operating systems to ensure confidentiality, it also comes out as being the mandatory access model being required to be used to ensure access control especially in public institutions relating to security and in the military applications [22]. In the model assets are composed of two types of classes

being actors and objects. It is aimed to avoid actors to have unauthorized access to objects requiring high level of security and to avoid security violations. In order to categorize assets, hierarchical classification methods which we frequently encounter are used and assets are qualified as per their security classes. For example to classify the assets security classes such as top secret, the secrets, confidential and unclassified, have been defined meaning that each asset within the system has a security label. Model tells which authorizations the actor has in relation to which object as per security class and which processes it can realize [22].

In the model shown in Fig. 6, authorizations of actors in relation to objects are shown. With this shape the access rights and authorizations of users in relation to classified objects are being defined. In another way of expressing it, while an actor can realize reading and writing operations on the object at its own level, it can only realize reading operations on the object that is below its own security level (Maintaining the integrity of an upward report in the hierarchy) [23]. In addition, an actor can only realize additional operations to the objects that are above its own security level (Such as not being able to change an instruction but adding distribution areas).

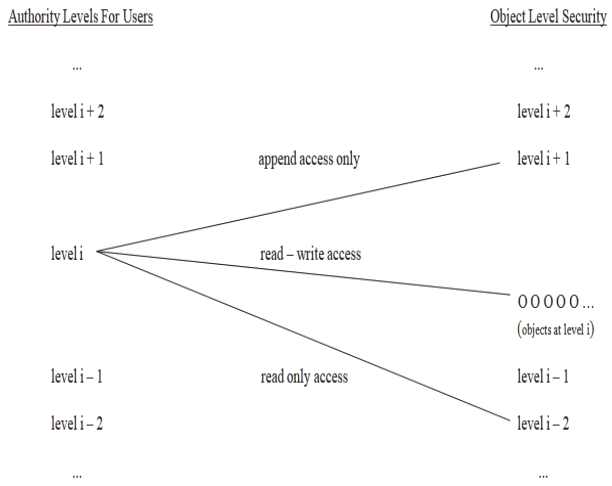

Figure 6 Access privileges between actor, object and this pair

Definition: Let $A = \{a_1, a_2, a_3, ..., a_n\}$ be the actor cluster and let $O = \{o_1, o_2, o_3, ..., o_m\}$ be the object cluster. Let two assets which are u and v, be any two assets that are chosen from the combined cluster ($u, v \in A \cup O$). If we define the security level of an asset with $gs()$ function: If $gs(u) > gs(v)$, we state that asset u is dominating over asset v. Various security policies offered by Bell-LaPadula model and security classes where actor or object will be present have been mentioned below.

a) Security Policies:

Simple Security Property: An actor cannot realize reading process on objects having high level of sensitivity [24]. Security policies are shown in Fig. 7.An actor can only realize reading operations on the objects which are at its own security level or below its security level (Fig. 7).

Simple security property can only be defined with "No Read Up" rule [24]. An actor can only read the objects security class of which it dominates or the objects with which it is at the same level (Fig. 11). But if the object is dominating over the actor no reading can be done. For example, ordinary personnel cannot read data which are at confidential level.

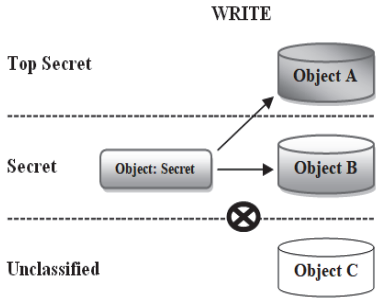

Figure 7 Simple Security Property

Star Property: An actor cannot realize reading operation on the objects having low level of sensitivity [24]. In Fig. 8, an actor can only realize reading operations on the objects which are at its own security level and which are above its own security level.

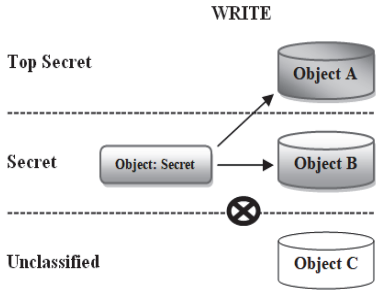

Figure 8 Star Property

In Fig. 8, star property can be defined with "No Write Down" rule [25]. An actor can only write on the objects which are dominating over its own security class or which are at the same level (Fig. 10). But if the actor is dominating over the object, no writing can be done. For example, top secret data cannot be written on the unclassified files (which the actors can read).

Strong Star Property: An actor cannot realize both reading and writing operations on the objects which have both low and high level of sensitivity [24]. In Fig. 9, an actor can only realize reading and writing operations on the objects which are at its own security level.

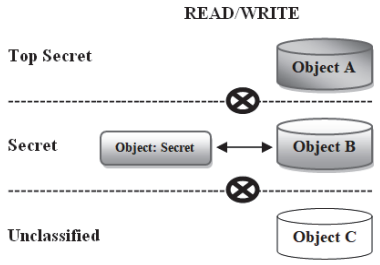

Figure 9 Strong Star Property

b) Security Policies:

Security policies are shown in Fig. 10. Security classes where an actor or an object can be present define its security level. The levels that are available within classification are Top Secret, Secret, Confidental, Unclassified (Fig. 10).

Reading process is only possible for objects that are at its own level or below it. Writing process is only possible for the objects that are at the actor's level and above it. This means that an actor can both read and write on an object which is at its own level [26].

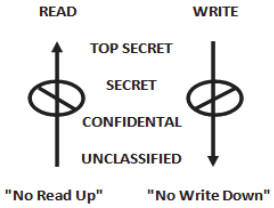

Figure 10 Security Classes

When these security policies are realized, it will be avoided for sensitive information to pass to the objects at lower level and in this way confidentiality will also be provided [27]. Likewise, changes or additions will be prevented when going up in the hierarchy in findings or experimental results.

4 EXPANDING THE RECOMMENDED MULTILEVEL ENCHANCED SECURITY MODEL TO DISTRIBUTED SYSTEMS

In this section by applying our proposed enhanced security model to distributed databases, we will realize the steps for providing confidentiality property of data in distributed systems, as well. Fig. 11 shows databases of an institution in its branches that are located in different cities. The situation of being able to carry out reading and writing operations on objects stored in a database held by a branch is limited with the rights and powers given to the employees in that branch.

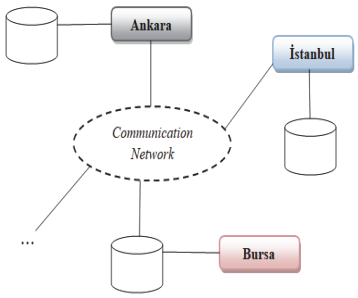

Figure 11 Distributed databases location of an institution

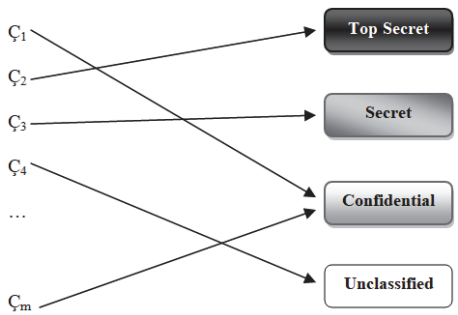

Figure 12 Assign security level to employees

In Fig. 11 for example, let Istanbul, Bursa, etc be the cities where branches of a security institution are located and let Ankara be the headquarters unit. In Fig. 12, a security level is assigned to each employee in a branch depending on his position. In Fig. 13, there are hidden objects in the database which is stored at each branch and a security level is assigned to the objects which are hidden in this database. Security levels are classified under 4 categories: Top Secret, Secret, Confidential and Unclassified.

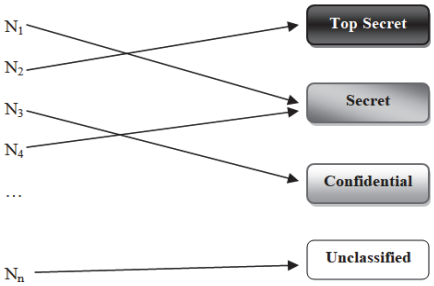

Figure 13 Assign security level to objects

Branch workers of a company are shown in $C = \{C_1, C_2, ..., C_m\}$ cluster and objects are shown in $N = \{N_1, N_2, ..., N_n\}$ cluster.

4.1 Scenarios

x and y, define any two assets that are selected from $Ç$ and N clusters, respectively. Reading and writing operations define R and W symbols and $G()$ function defines the security level.

Scenario 1 (S1): Each branch worker can only realize reading operation on the objects that are assigned to the security level which is equivalent to its own security level or which is below (Simple Security Property), meaning that if the security level of an employee (C_x) is equal to the security level of object to which it has access (N_y) or if it is below it, the employee can screen this object (Fig. 7).

$$G(x) \leq G(y) \geq \text{Authorization}[x] = \{R\}_y \quad (1)$$

Scenario 2 (S2): Each branch worker can only realize writing operation on the objects being assigned for security level which is equal to its own security level or above it (Star Property) meaning that if the security level of an employee ($Ç_x$) is equal to the security level of an object to which it has access (N_y) or if it is above it, the employee can realize operations on this object (Fig. 8).

$$G(x) \geq G(y) \geq \text{Authorization}[x] = \{W\}_y \quad (2)$$

Scenario 3 (S3): Each branch worker can realize reading and writing operations on the objects being assigned to a security level which is equivalent to its own security level, together (Powerful Star Property), meaning that if the security level of an employee ($Ç_x$) is equal to the security level of object to which it has access (N_y), the employee can screen that object and can realize operations on that object (Fig. 9).

$$G(x) = G(y) \geq \text{Authorization}[x] = \{R, W\}_y \quad (3)$$

4.2 Private Rights and Authorizations

If no private arrangements are made, a branch worker does not have authorization to realize operations on the

objects belonging to another branch (such as the situation where an employee at Bursa Branch cannot have access to objects at Istanbul branch). But by being authorized by the headquarters unit or by realizing an agreement (protocol) between two units, a branch worker can also have certain rights at the other branch. In Tab. 1, authorization levels of employees are shown as per the branches. Those working at Ankara unit have been gathered under groups of $A1$ (Ankara Top Secret), $A2$ (Ankara Secret), $A3$ (Ankara Confidential) and $A4$ (Ankara Unclassified) according to their security levels, those working at Istanbul branch have been gathered under groups of $I1$ (Istanbul Top Secret), $I2$ (Istanbul Secret), $I3$ (Istanbul Confidential) and I4 (Istanbul Unclassified) according to their security levels, and those working at Bursa branch have been gathered under groups of $B1$ (Bursa Top Secret), $B2$ (Bursa Secret), $B3$ (Bursa Confidential) and $B4$ (Bursa Unclassified) according to their security levels.

Private Situation 1 ($O1$: Between headquarters-branch): Headquarters unit has the same authorizations at other branches as in the headquarters (It is at the same level as per the security level).

Table 1 New levels of authority for Special Case 1

	Ankara	Istanbul	Bursa
Top Secret	$A1$	$I1$, $A1$	$B1$, $A1$
Secret	$A2$	$I2$, $A2$	$B2$, $A2$
Confidential	$A3$	$I3$, $A3$	$B3$, $A3$
Unclassified	$A4$	$I4$, $A4$	$B4$, $A4$

In accordance, a headquarters employee has the rights and authorizations of all branch workers having security levels that are equivalent to its own security level. In Tab. 1, it is seen that as Ankara is the headquarters unit, all of the workers in this unit are also classified in the group where other branch workers having equivalent security levels have been gathered.

Private situation 2 ($O2$: Between branch and branch): By being authorized by the headquarters unit or by means of a protocol being made, any branch worker has the rights and authorizations of worker of another branch, having security level which is equivalent to its own security level. (For example let k be Istanbul worker and let i be Bursa worker. If $G(i) = G(k)i$, k may have authorizations of i).

In Tab. 2, it is seen that a branch worker ($I1_k$) who is part of Istanbul Top Secret ($I1$) group, is also part of Bursa Top Secret ($I1$) group due to $O2$.

Table 2 New levels of authority for Special Case 2

	Ankara	Istanbul	Bursa
Top Secret	$A1$	$I1$, $A1$	$B1$, $A1$, $I1_k$
Secret	$A2$	$I2$, $A2$	$B2$, $A2$
Confidential	$A3$	$I3$, $A3$	$B3$, $A3$
Unclassified	$A4$	$I4$, $A4$	$B4$, $A4$

Table 3 New levels of authority for Special Case 3

	Ankara	Istanbul	Bursa
Top Secret	$A1$	$I1$, $A1$	$B1$, $A1$
Secret	$A2$	$I2$, $A2$	$B2$, $A2$
Confidential	$A3$	$I3$, $A3$	$B3$, $A3$
Unclassified	$A4$	$I4$, $A4$, $B3_z$	$B4$, $A4$

Private Situation 3 ($O3$: Between branch-branch, Severance difference): By being authorized by headquarters unit or by means of an agreement that is made between two units, worker of any branch can have the rights and authorizations of another branch worker, having a security level which is below its own security level. (For example let Bursa employee be z and Istanbul employee be y. If $G(z) > G(y)$, z may have authorizations of y).

In Tab. 3, it is seen that a branch worker ($B3_z$) who is part of Bursa Confidential ($B3$) group is also part of Istanbul Unclassified ($I4$) group due to $O3$.

Table 4 New levels of authority for Special Case 4

	Ankara	Istanbul	Bursa
Top Secret	$A1$	$I1$, $A1$	$B1$, $A1$
Secret	$A2$	$I2$, $A2$	$B2$, $A2$, $I3_x$
Confidential	$A3$	$I3$, $A3$	$B3$, $A3$
Unclassified	$A4$	$I4$, $A4$	$B4$, $A4$

Private Situation 4 ($O4$: Between branch branch): By being authorized by headquarters unit or by means of an agreement that is made between two units, worker of any branch can have the rights and authorizations of another branch worker, having a security level which is above its own security level. (For example let Istanbul worker be x and Bursa worker be t. If $G(x) < G(t)$, x may have authorizations of t).

In Tab. 4, it is seen that a branch worker who is part of Istanbul Confidential ($I3$) group is also part of Bursa Secret ($B2$) group due to $O4$.

4.3 Application of Scenarios as per Defined Rules (Private Situations)

A user can take part in the authorization lists of other branches with an authorization that is equivalent to or lower or higher than its authorization level at the branch where he is positioned within frame of a private situation or a protocol being concluded between the branches. User access levels being determined by considering this situation are shown in Tab. 5.

Table 5 User Access Level

	Ankara	Istanbul	Bursa
Top Secret	$A1$	$I1$, $A1$	$B1$, $A1$, $I1_k$
Secret	$A2$	$I2$, $A2$	$B2$, $A2$, $I3_x$
Confidential	$A3$	$I3$, $A3$	$B3$, $A3$
Unclassified	$A4$	$I4$, $A4$, $B3_z$	$B4$, $A4$

Private authorization levels which are assigned to users as per the authorizations given by headquarters unit or by means of an agreement that is concluded between two units are kept in protocol files. Protocol files are defined with PD symbol. Protocol files which have been created as per Tab. 5 have been given in Tab. 6 and Tab. 7.

Table 6 Protocol file to be kept in Bursa branch (PD)

Istanbul	Bursa
$I1$	$B1$, $I1_k$
$I3$	$B2$, $I3_x$

Table 7 Protocol file to be kept in Istanbul branch (PD)

Istanbul	Bursa
$I4$, $B3_z$	$B4$

After authorization levels of each user within communication net determined for the branch or branches, list of users who will have access at security levels of Top Secret, Secret, Confidential and Unclassified relating with that branch will be kept in the files at each relevant branch.

In these files which we name as access rights files, information about users who can have access to each security level of a branch and the branch to which the users are connected with and their security levels at these branches are stored. Access rights file is defined with E symbol. Access rights file, which has been created for each branch, is shown in Tab. 8, Tab. 9 and Tab. 10.

Table 8 User access rights file (EA) in the central unit

A_1	$A1_1, A1_2, \ldots, A1_p$
A_2	$A2_1, A2_2, \ldots, A2_r$
A_3	$A3_1, A3_2, \ldots, A3_s$
A_4	$A4_1, A4_2, \ldots, A4_u$

A_1, A_2, A_3 *and* A_4, represent the 1th, 2nd, 3rd and 4th (Top secret, secret, confidential, unclassified). $A1_1$, $A1_2$, …, $A1_p$ show all users at A_1 authorization level. $A2_1$, $A2_2$, …, $A2_r$: A_2 show all users at A_2 authorization level. $A3_1$, $A3_2$, …, $A3_s$: A_3 show all users at A_3 authorization level. $A4_1$, $A4_2$, …, $A4_u$: A_4 show all users at A_4 authorization level.

In Fig. 14, for the access of a user located in Ankara unit to the unit where he is present, access rights file relating only to his own unit (E_A) is controlled, while in case of his having access to a different unit, both E_A and the access rights file being kept at the unit where he wishes to have access (E_I for Istanbul branch and/or E_B for Bursa branch) are controlled. In Fig. 14, access control procedure for the users in Ankara unit is shown. K_A: shows all users in Ankara unit.

Furthermore, it is decided whether the access rights file is updated or not by reviewing the protocol files. If there is a contradictory authorization situation in the protocol file (PD) and access rights file (E), access request of user is considered as being unauthorized and it is rejected. In a contrary situation if there is an authorization being defined for the user in access rights file and if this authorization is being supported by the protocol file, the user can have access to the relevant authorization level of that branch. This control mechanism is valid for all branches.

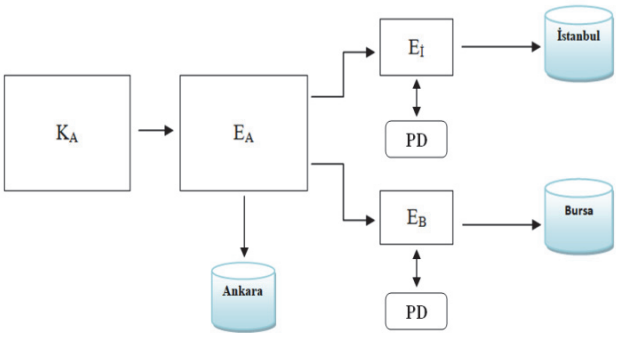

Figure 14 Access control procedure of users in the Ankara unit

Table 9 User access rights file (EI) in the Istanbul unit

$İ_1$	$I1_1, I1_2, \ldots, I1_a, A1$
$İ_2$	$I2_1, I2_2, \ldots, I2_b, A2$
$İ_3$	$I3_1, I3_2, \ldots, I3_c, A3$
$İ_4$	$I4_1, I4_2, \ldots, I4_d, A4, B3_z$

I_1, I_2, I_3 *and* I_4 represent 1th, 2nd, 3rd and 4th authorization levels (Top secret, Secret, Confidential, Unclassified). $I1_1$, $I1_2$, …, $I1_a$, $A1$ show all users at I_1 authorization level. $I2_1$, $I2_2$, …, $I2_b$, $A2$ show all users at I_2 authorization level. $I3_1$, $I3_2$, …, $I3_c$, $A3$ show all users at $İ_3$ authorization level. $I4_1$, $I4_2$, …, $I4_d$, $A4$, $B3_z$ show all users at I_4 authorization level.

In Fig. 15, while only E_I access rights file is controlled for accessing of a user located in Istanbul branch to his own unit, in case of having access to a different unit both E_I and access rights file that is kept at the unit where he wishes to have access (E_A for Ankara unit and E_B for Bursa branch) will be controlled. In Fig. 15 access control procedure for users in Istanbul branch has been shown. K_I shows all users at Istanbul branch.

B_1, B_2, B_3 *and* B_4 show 1th, 2nd, 3rd and 4th authorization levels at Bursa branch (Top secret, Secret, Confidential, Unclassified) by representation. $B1_1$, $B1_2$, …, $B1_e$, $A1$, $I1_k$: show all users at B_1 authorization level. $B2_1$, $B2_2$, …, $B2_f$, $A2$, $I3_x$ show all users at B_2 authorization level. $B3_1$, $B3_2$, …, $B3g$, $A3$, B_3 show all users at B_3 authorization level. $B4_1$, $B4_2$, …, $B4_h$, $A4$ show all users at B_4 authorization level.

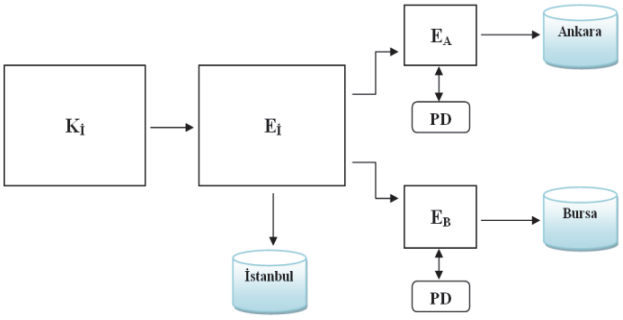

Figure 15 Access control procedure of users in the Istanbul unit

Table 10 User access rights file (EB) in the Bursa

B_1	$B1_1, B1_2, \ldots, B1_e, A1, I1_k$
B_2	$B2_1, B2_2, \ldots, B2_f, A2, I3_x$
B_3	$B3_1, B3_2, \ldots, B3_g, A3$
B_4	$B4_1, B4_2, \ldots, B4_h, A4$

In Fig. 16, while only E_B access rights file is controlled for accessing of a user located in Bursa branch the unit where he is present, in case he will have access to a different unit both E_B and access rights file that is kept at the unit where he wishes to have access (E_A for Ankara unit and E_I for Istanbul branch) are controlled. In Fig. 16 access control procedure for users at Bursa branch is shown. K_B shows all users at Bursa branch.

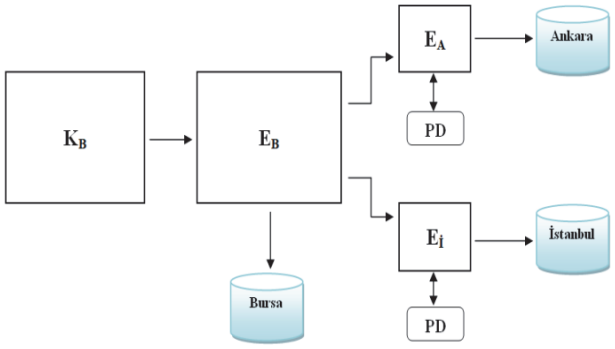

Figure 16 Access control procedure of users in the Bursa unit

The privileges assigned to a unit with private authorization or by means of an inter-branch protocol are only valid for the workers in that unit. In another way of

saying it, a user who is authorized at 1th, 2nd, 3rd or 4th level in a different unit with private protocols cannot have the private rights and authorizations of workers present at the branch where he is authorized, as being valid for another branch. As it is shown in Fig. 17, while a user (X_1) present in X unit can have access to Y unit due to his having an authorization in Y unit, and a user present in Y unit (Y_1) can have access to Z unit due to his having an authorization at Z unit, since although ancak X birimindeki X_1 user in X unit has an authorization at Y unit, this user will not have the authorization of Y_1 user present at Y unit, regarding his authorization being valid for Z unit, it can be stated that X_1 user cannot have access to Z unit.

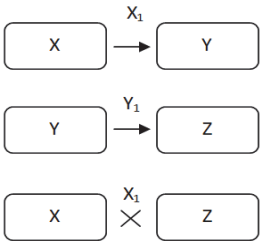

Figure 17 Authorization between X_1 and Y_1

As a conclusion, if we would interpret the authorization levels given in Tab. 5 in accordance with access procedures being explained above within the scope of security policies introduced with the advanced security model.

According to Scenario 1:

Istanbul worker at "Top secret" security level ($I1$), can only realize reading operation on the objects being available at all security levels at Bursa branch due to Istanbul and $O2$ rule.

Istanbul worker at "Confidential" security level ($I3$), can only realize reading operation on objects available at "Top secret", "Secret", "Confidential" and "Unclassified" security levels at Bursa branch due to "Confidential" and "Unclassified", $O4$ rules at Istanbul branch.

Bursa worker at "Confidential" security level ($B3$), can only realize reading operation on the objects available at "Unclassified" security levels at Istanbul branch due to "Confidential" and "Unclassified", $O3$ rules at Bursa branch.

According to Scenario 3:

Istanbul worker at "Top secret" security level ($I1$) can only realize reading operation on objects available at "Top secret" security level at Bursa branch due to Istanbul and $O2$ rule.

Istanbul worker at "Confidential" security level ($I3$), can only realize reading operation on objects that are available at "Secret" and "Top secret" security levels at Bursa branch due to "Confidential", "Secret" and "Top secret", $O4$ rule at Istanbul branch.

Bursa worker at "Confidential" security level ($B3$), can only realize reading operation for objects that are available at all security levels at Istanbul branch due to "Confidential", "Secret" and "Top secret", $O3$ rule at Bursa branch.

According to Scenario 3:

Istanbul worker at "Top secret" security level ($I1$), can realize both reading and writing operations on the objects that are available at "Top secret" security level at Bursa branches due to Istanbul and $O2$ rule.

Istanbul worker at "Confidential" security level ($I3$), can realize both reading and writing operations on objects that are available at "Secret" security level at Bursa branch due to "Confidential", $O4$ rule at Istanbul branch.

Bursa worker at "Confidential" security level ($B3$), can realize both reading and writing operations on objects that are available at "Unclassified" security levels at Istanbul branch due to "Confidential", $O3$ rule at Bursa branch.

In all cases that may come out of the scenarios that are specified above, it is not possible for users to have access to objects and to realize operations on the objects.

As it can be seen, while standard policies being offered by the model can be applied to distributed systems by means of proposed security model that has been determined for a system being established on distributed database, it can be made possible for users being equipped with private rights and authorizations to have access to objects at levels above the existing security levels and to transmit information to levels below existing security levels in a controlled way.

5 EXPERIMENTAL STUDY

In this study, real data sets obtained from public institutions providing health and justice services were used, and the performance of the proposed access control model and other methods were evaluated according to the results obtained from each data set. Two data sets obtained from different sectors used in the study were pre-processed, and each user and object included in the data set was classified according to their security parameters. The classification process was based on the real classification criteria of businesses. The data set obtained from the health sector consisted of 430 users and 55,300 objects, and the data set obtained from the justice sector consisted of 292 users and 72,988 objects. The data sets are expressed as the Health Data Set and the Justice Data Set.

5.1 Experimental Analysis

Along with the proposed model, other access control models were also run on a platform providing a real distributed system, and all models were separately applied to the three data sets. The performance levels of the methods were analyzed by comparing the access level results (reading, writing, reading and writing, etc.) obtained for all models applied to each data set with the access level results of the sector from which the data set was obtained. The performance evaluation of the methods applied to datasets was based on the accuracy of access level and the access rate determination percentages of each method.

5.2 Performance Results for the Proposed Model

The test results of the proposed model on the health and justice data sets are presented in Tab. 11. With the proposed model, the access level results were determined correctly in 98.20% of cases for the health data set and in 97.82% of cases for the justice data set, and in addition, the

access rate for both data sets was measured at 0.85 and 0.91 seconds, respectively.

When the results of the proposed model were evaluated, it can be said that the proposed model provided the correct access level to the data set of two different sectors in 90% or more cases. Furthermore, it was observed that the access rate to the object increased as the number of objects in the data set increased.

Table 11 Access level and access speed results

Dataset Used Model	Accuracy Rate / %	Access Speed / sec
Health Data	98.20%	0.85
Justice Data	97.82%	0.91

5.3 Performance Results for Traditional Access Control Models

The test results of the Role-based access control, Discretionary and Mandatory access control models on the health and justice data sets are presented in Tab. 12, Tab. 13 and Tab. 14.

Table 12 Access level and access speed results (RBAC)

Data Used Set	Access Level / %	Access Speed / sec
Health Data	91.10%	0.87
Justice Data	93.23%	0.95

Table 13 Access level and access speed results (DAC)

Data Used Set	Access Level / %)	Access Speed / sec
Health Data	90.88%	0.87
Justice Data	90.52%	0.92

Table 14 Access level and access speed results (MAC)

Data Used Set	Access Level / %	Access Speed / sec
Health Data	90.69%	0.85
Justice Data	91.96%	0.91

5.4 Performance Evaluation

It was observed that the proposed model provided more successful results in determining the correct access level and improved access rates compared to other techniques, and as can be seen in Fig. 18 and Fig. 19, it determined the correct access level rates in both data sets in a higher percentage of cases compared to other models, while its access rate performance was also higher. When the results were evaluated, it can be said that the proposed model provided a technique that was more consistent in authorization and gave faster results in sharing information compared to other existing techniques.

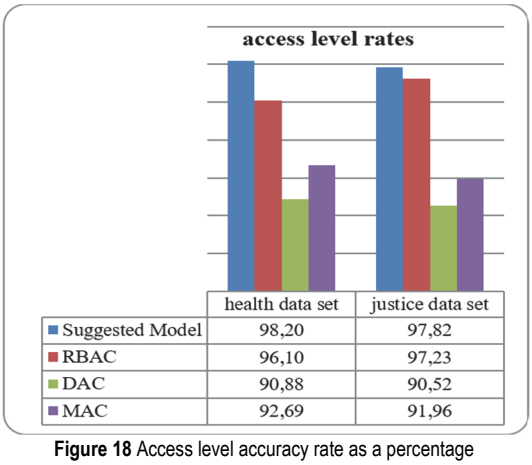

Figure 18 Access level accuracy rate as a percentage

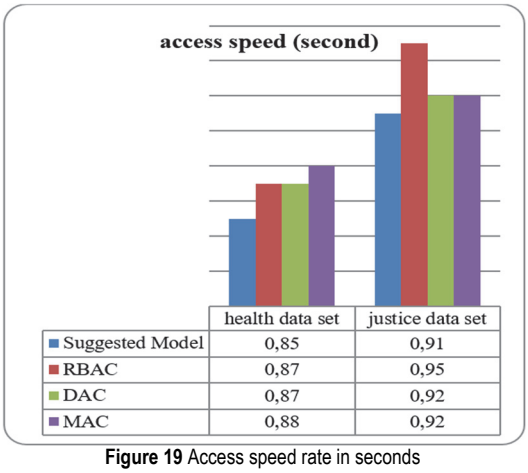

Figure 19 Access speed rate in seconds

6 EVALUATION AND CONCLUSION

With the proposed enhanced security model which we examined in the study, evaluation has been made on confidentiality aspect of information, as being one of the basic elements of information security. Security policies offered by the model have been applied to distributed database systems and hence, examinations have been made on who can have access to objects being kept in different physical environments and how they can access them.

At this point we can state that positive aspect of the study is that in distributed systems data are shared with users in a secure and rapid way and that unless tight controls and inspections are required, flexibility in applications has been provided in great extent by definite specific private rights and authorizations for the users. The weak aspect of the study can be considered such that security model which has been applied to distributed systems by being extended has been especially modelled with the aim to protect confidentiality of data and that other security particulars have been kept in the background (availability, integrity).

In the conducted study it is being avoided for a user to have access to security levels that are above its own security level and to transmit information to security levels below its own security level. For other information sources supervised authorizations can be defined by means of private protocols and security model policies can be made valid also for these sources (objects).

In the continuation of study, the availability and integrity aspects, being among the basic elements of information security will also be examined. Furthermore, a research will be made on the issue of how other security models will be spread to distributed database systems.

7 REFERENCES

[1] Andress, J. (2011). The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice. *Elsevier Inc*., USA.

[2] Nemati, H. (2007). Information Security and Ethics: Concepts, Methodologies, Tools and Applications. Information Science Reference, USA. https://doi.org/10.4018/978-1-59904-937-3

[3] Whitman, M. E. & Mattord, H. J. (2012). Principles Of Information Security, Course Technology, Cengage Learning, USA.

[4] Vijayalakshmi, K. & Javalakshmi, V. (2021). Shared Access Control Models for Big Data: A Perspective Study and Analysis. *Advances in ıntelligent Systems and Computing book series (AISC)*, *1272*, 397-410. https://doi.org/10.1007/978-981-15-8443-5_33

[5] Ghamdi, H. F. & Than, T. (2020). Information security governance challenges and critical success factors: Systematic review. *Elseiver Computers & Security*, *99*, 1-39. https://doi.org/10.1016/j.cose.2020.102030

[6] Gunjan, B., Vijayalakshmi, A., Jaideep, V., & Shamik, S. (2019). Deploying ABAC Policies Using RBAC Systems. *Journal of Computer Security*, *27*(4), 483-506. https://doi.org/ 10.3233/JCS-191315

[7] Xiang, Y., Chonka, A., & Deng, R. H. (2011). A Generic Framework for Three-Factor Authentication: Preserving Security and Privacy in Distributed Systems. *IEEE Transactions on Parallel and Distributed Systems*, *22*(8), 1390-1397, 2011. https://doi.org/ 10.1109/TPDS.2010.206

[8] Kim, D. & Solomon, M. G. (2016). Fundamentals of Information Systems Security. *Jones and Bartlett Publishers Inc.*

[9] Naeem, W., Shah, M. A., & Malik, A. K. (2015). Privacy-Preserving in Collaborative Working Environments. *Proceedings of the IOARP International Conference on Communication and Networks, London, United Kingdom*, 76-83.

[10] Shin, M. S., Jeon, H. S., Ju, Y. W., & Jeong, S. P. (2015). Constructing RBAC Based Security Model in u-Healthcare Service Platform. *The Scientific World Journal*, *2015*(12), 1-13. https://doi.org/ 10.1155/2015/937914

[11] Kotari, M., Chiplunkar, N. N., & Nagesh, H. R. (2016). Framework of security mechanisms for monitoring adaptive distributed systems. *IOSR Journal of Computer Engineering (IOSR-JCE)*, *18*(4), 25-36. https://doi.org/ 10.9790/0661-1804012536

[12] Reid, J., Cheong, I., Henrickson, M., & Smith, J. (2014). A novel use of RBAC to protect privacy in distributed health care information systems. *ACM Transactions on Information and System Security*, 403-415. https://doi.org/10.1007/3-540-45067-X_35

[13] Huh, J. H. (2016). Next-Generation Access Control for Distributed Control Systems. *IEEE Internet Computing*, *20*(5), 28-37. https://doi.org/ 10.1109/MIC.2016.105

[14] Bertolissi, C. & Fernandez, M. (2014). A metamodel of access control for distributed environments: Applications and properties. *Information and Computation*, *238*(2), 187-207. https://doi.org/ 10.1016/j.ic.2014.07.009

[15] Dasgupta, D., Roy, A., & Ghosh, D. (2018). Multi-user permission strategy to access sensitive information. *Elsevier Information Sciences*, *423*(C), 24-49. https://doi.org/10.1016/j.ins.2017.09.039

[16] Chow, S. M., Lee, J. H., & Subramanian, L. (2009). Two-Party Computation Model for Privacy-Preserving Queries over Distributed Databases. *Network and IT Security Conference NDSS Symposium*, San Diego, California, USA.

[17] Balamurugan, B., Shivitha, N. G., Monisha, V., & Saranya, V. (2015). A Honey Bee behaviour inspired novel Attribute-based access control using enhanced Bell-Lapadula model in cloud computing. *Innovation Information in Computing Technologies (ICIICT)*, Chennai, India. https://doi.org/ 10.1109/ICIICT.2015.7396064

[18] Kotari, M. & Chiplunkar, N. N. (2020). Investigation of Security Issues in Distributed System Monitoring. *Springer Information Sciences*, 609-634. https://doi.org/ 10.1007/978-3-030-22277-2_24

[19] Zhang, Y., Ye, X., Xie, F., & Peng, Y. (2009). A practical database intrusion detection system framework. *In Computer and Information Technology* , Xiamen, China, 342-347. https://doi.org/ 10.1109/CIT.2009.69

[20] Yang, L., Wang, J., Tang, Z., & Xiong, N. N. (2019). Using Conditional Random Fields to Optimize a Self-Adaptive Bell-LaPadula Model in Control Systems. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *1*(1), 1-15. https://doi.org/10.1109/TSMC.2019.2937551

[21] Crampton, J., Leung, W., & Beznosov, K. (2006). The secondary and approximate authorization model and its application to Bell-LaPadula policies. *ACM Symposium on Access Control Models and Technologies*, California, USA.

[22] Ferraiolo, D. F., Cugini, J. A., & Kuhn, D. R. (1995). Role-Based Access Control (RBAC): Features and Motivations. National Institute of Standards and Technology-U. S. Department of Commerce, Gaithersburg.

[23] Thomas, W. (1999) Foundations of Software Science and Computation Structures. FoSSaCS: International Conference on Foundations of Software Science and Computation Structure, Amsterdam, The Netherlands. https://doi.org/10.1007/3-540-49019-1

[24] Thuraisingham, B. (2000). Security for Distributed Databases. *Information Security Technical Report, The MITRE Corporation*, 95-102. https://doi.org/10.1016/S1363-4127(01)00210-2

[25] Bertino, E. & Sandhu, R. (2005). Database Security-Concepts, Approaches and Challenges. *IEEE Transactions on Dependable and Secure Computing*, *2*(1), 2-19. https://doi.org/ 10.1109/TDSC.2005.9

Contact information:

Mehmet GUCLU
Yildiz Technical University,
Davutpasa Street, 34220, Istanbul, TURKEY
E-mail: mehmetguclu007@gmail.com

Cigdem BAKIR
(Corresponding author)
Yildiz Technical University,
Davutpasa Street, 34220, İstanbul, TURKEY
E-mail: cigdem.bakir@erzincan.edu.tr