Providing Access Isolation to Information in the Database

https://doi.org/10.3991/ijim.v17i14.36073

Akanov Arman[1](✉), Sagindykov Kakim[2]
[1] Alikhan Bokeikhan University, Semey City, Kazakhstan
[2] L.N. Gumilyov Eurasian National University, Nur-Sultan, Kazakhstan
akanov-87@list.ru

Abstract—Most modern database management systems (DBMS) provide the ability to restrict user access to database objects. The problems of restricting access to individual records are arising increasingly in connection with the growing need for flexibility in restricting access in modern databases, including when using them to store information classified as state or commercial secrets. Currently, these tasks are solved individually, and there are no commonly formalized approaches to designing such access restrictions. The study aims to reduce the design time for database schemes when it is necessary to restrict access to individual records of the database tables and improve the quality of the designed schemes by using the proposed algorithms. Questions about the design of the protected databases with the use of access restrictions to separate records are considered. Both restriction of illegal access to records, and granting false camouflage information instead of required is considered. The proposed software package will consist of 2 main parts: a database and a client application. To differentiate access, the study proposed the use of a record-protecting lock.

Keywords—client-server, database, database management system, model, software

1 Introduction

Most modern database management systems (DBMS) provide the ability to restrict user access to database objects, which include tables, views, packages, stored procedures, sequences, and schemas [1-4]. At the same time, the issues of restricting access to individual records of the database tables have not been given due attention. Particular DBMS, such as Linter, provide the possibility to set security labels on database table records. Most commercially used DBMSs do not have these capabilities [5-7].

The use of the standard SQL language in relational databases makes it possible to perform the same actions on different DBMS, executing identically formed queries. Thus, nowadays correctly designed information systems can be ported between several DBMS [8-11]. The problems of restricting access to individual records are arising increasingly in connection with the growing need for flexibility in restricting access in modern databases, including when using them to store information classified as state or

commercial secrets. Currently, these tasks are solved individually, and there are no commonly formalized approaches to designing such access restrictions [12-15].

The study aims to reduce the design time for database schemes when it is necessary to restrict access to individual records of the database tables and improve the quality of the designed schemes by using the proposed algorithms and methods for restricting access, which restrict various access models.

To achieve the aim, the following problems must be resolved:

- analysis of possible ways to restrict access with the choice of the most suitable for a specific task and compatible with most relational databases;
- the choice of means of access restriction implementation, which allows implementing access restriction on most DBMS.

2 Materials and methods

Providing differentiation of access to information in databases within the organization ensures the full-fledged work of all its users over the network, business process management, support for life cycles and document versions, and dynamic management of access rights [16-18].

As an example, let's consider a software package for automating the work of the selection committee. The software package should perform the following tasks:

1. At the preparatory stage of the work of the selection committee, it should enter the results of the entrance exams into the database. A diagram of decision options is shown in Figure 1. Information that is entered into the Database at this stage:
   - Full name of the applicant;
   - Faculty/School, in which the applicant intends to enroll;
   - The score received by the applicant.

   Based on this information, the PC Operator can generate various reports.

2. At the stage of accepting documents, it should enter information about applicants into the Database. On the diagram of solution options (Figure 1), this interaction is described in the algorithm of the PC Operator and the Applicant and the solution "The applicant's record-keeping". During document submission, it may be necessary to enter the exam results into the Database (the extended connection between the options "The applicant's record-keeping" and "Add exam result"). Information entered into the Database at this stage:
   - specialty for which the applicant wishes to enroll;
   - a list of specialties that the applicant agrees to enter, if he/she can not enroll in the main specialty;
   - citizenship;

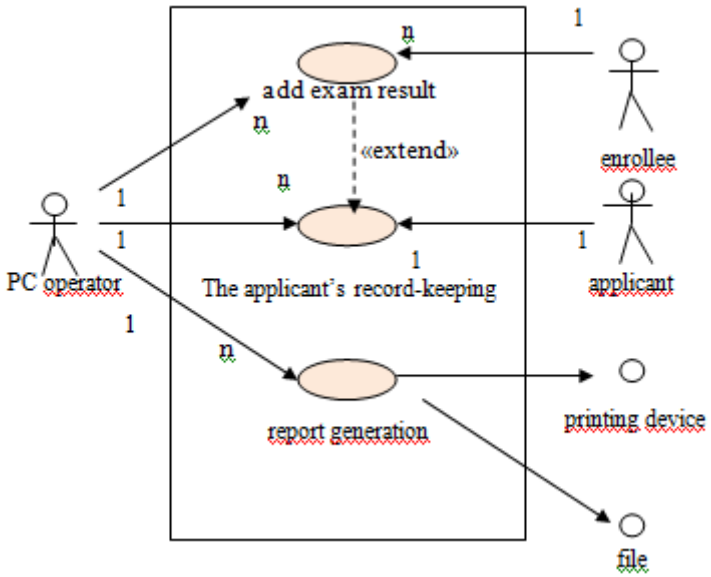

Fig. 1. Diagram of choosing the solution options

- gender (female, male);
- date of birth;
- address of the applicant;
- information about parents (full name, date of birth, address of residence);
- passport data;
- number of the certificate and year of graduation from school (university);
- the original or a copy of the certificate has been submitted;
- form of education (fee-based or state grant);
- contract number (for a fee-based form of education);
- date of signing the contract;
- refusal to participate in the competition (for a fee-based form of education);
- the result of the interview (for a fee-based form of education);
- participation of the applicant in testing.

3. At the stage of the examinations, the test results and exam results, information on admission to the specialty based on the test results, and competition are entered into the Database. Based on this information, the PC Operator can generate various reports. The applicant's record-keeping options include:
   - Submission of an application by the applicant.
   - Submission of all necessary documents.
   - Withdrawal of applicants' documents.

At any stage of the selection committee's work, the PC Operator can generate various reports. The actors in the "Report Generation" solution are the PC Operators,

who generate reports, the dean's office, the IT department, the chancellory, the first-aid post, and the departments (the actors to whom the reports are sent).

4. Restricting users' access to information in the Database. All users can be divided into the following categories:
   - DBMS administrator - a person who is responsible for the creation of a database, technical control of the operation of the DBMS, and determines the rules of security and data integrity. The administrator gets access to all data in the database.
   - The administrator of the central admission committee - is a person who has the right to view, add, and change any data in the database. This person plays the role of an actor "PC Operator" at the preparatory stage of the selection committee's work (collecting information about the Olympiads held and entering these data into the database).
   - The user of the central admission committee is a person who has the right to view the data on applicants entering the university. This person can perform part of the "PC Operator" actor duties (it is allowed to implement the "Report Generation" system option, Figure 1)
   - The administrator of the admission committee within a faculty - is a person who has the right to view, add, and change data about applicants entering this faculty. This person plays the role of a "PC Operator" actor at the second stage of the selection committee (receiving documents) and the third stage (conducting exams).
   - The user of the admission committee within a faculty is a person who has the right to view the data on applicants entering this faculty. This person can perform part of the "PC Operator" actor's duties in the second and third stages of the selection committee's work (it is allowed to implement the "Report Generation" system option, Figure 1).

Since the admission committee of the university consists of a central admission committee and several admission committees of faculties, which can be physically located in different classrooms (even in different buildings), our software package should consist of several parts that can interact via a local area network (LAN).

3 Results

Based on the terms of reference and the above-mentioned facts, the software package will consist of 2 main parts: a database and a client application (Figure 2).

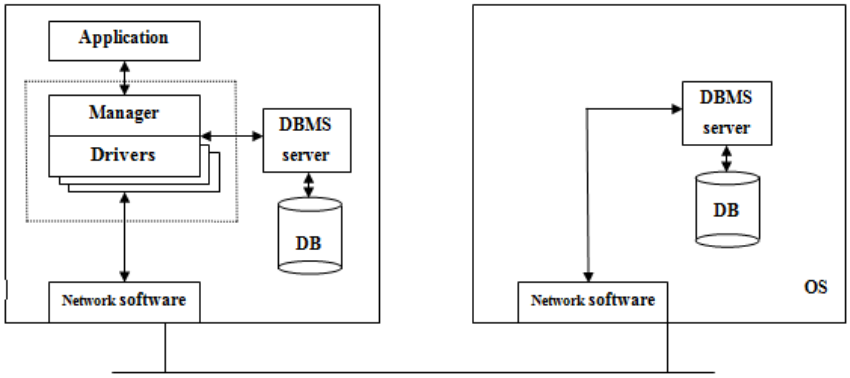

Fig. 2. The structure of the software package

According to the terms of reference, all users can be divided into the following categories:

- DBMS administrator - responsible for creating the database;
- The administrator of the Central Admission Committee (ACAC) - has the right to view, add, and change any data in the database;
- The user of the Central Admissions Committee (UCAC) - has the right to view the data on applicants;
- The administrator of the admission committee of the faculty (AACF) - has the right to view, add, and change the data on applicants entering the faculty;
- The user of the admission committee of the faculty (UACF) - has the right to view the data on applicants entering the faculty;

It is necessary to delimit access to database data according to the categories of users. To do this, we will develop rules for differentiating access to data from the database:

- All users have the right to access the **Faculty** and **Exam** reading tables. Only ACAC has access to recording, updating, or deleting.
- All users have access to read s**pecial** tables. Users of the ACAC and UCAC have the right to read all records. AACF and UACF users can read only those records that relate to their faculty. Only ACAChave access for recording, updating, or deleting.
- All users have access to the **ExamResult** and **DPUser** tables. Users of the ACAC and UCAC have the right to read all records. AACF and UACF users can read only those records that relate to their faculty. ACAC has access to recording, updating, or deleting all records, whereas AACF has access only to those records that relate to their faculty.
- All users have access to read the **Abiturient** and **AbiturientSpec** tables. Users of the ACAC and UCAC have the right to read all records. AACF and UACF users can read only those records that relate to their faculty. Only AACF has access to recording, updating, or deleting.

Based on the rules of access control, we determine that it is necessary to differentiate access for all database users (except the Administrator) to various table records by *selecting, updating, deleting,* and *inserting.* The access criteria will be:

- The user belongs to the user category.
- The user is a member of the faculty.

To store these criteria, we will add another table to the database - **SecureUser**, which will contain the username (which corresponds to the username under which the person will register in the system), the category, and the faculty to which he/she belongs (only for AACF and UACF). The final information model of the system database, which is in the third normal form, is shown in Figure 3.4.

We will provide access control in two ways:

- Introduction of roles, with the help of which we will provide separate access to tables.
- Introduction of **Row Level Security (RLS)**, a mechanism that uses a selection condition (predicate) when querying database tables. This mechanism consists of two parts - creating a function that generates a selection predicate by username and linking this function with the target table, listing the actions for which this function should be performed.

3.1 Secure user table

Table 1 includes information about database users.

Table 1. Fields

Attribute	Data Type	PKEY	FKEY	NOT NULL	UNIQUE	Description
user_id	NUMBER	X		X	X	Key field
user_name	VARCHAR2(64)			X	X	Username
adm	NUMBER			X		User category
id_fac	NUMBER		X	X		Faculty to which the user belongs. Link to the record in the table **Faculty**

Codes for the **adm** field:

0 - DB Administrator, DBMS Administrator

1 - Administrator of the Central Admission Committee (ACAC)

2 - User of the Central Admissions Committee (UCAC)

3 - Administrator of the admission committee of the faculty (AACF)

4 - User of the admission committee of the faculty (UACF)

Role restrictions:
— For ACAC, UCAC, AACF, UACF – only reading.

Field access predicates for users:
— For ACAC, UCAC, AACF, UACF – «user_name».

3.2 Faculty table

Table 2 includes information about the faculties of the university.

Table 2. Faculty information

Attribute	Data Type	PKEY	FKEY	NOT NULL	UNIQUE	Description
fac_id	NUMBER	X		X	X	Key field
fac_name	VARCHAR2(64)			X		Faculty name
fac_num	NUMBER			X	X	Faculty number
Deleted	NUMBER			X		Record deleted

Role restrictions:
— For UCAC, AACF, UACF - only reading.

3.3 Special table

The table includes information on specialties that an applicant can apply for.

Table 3. Specialties in the university

Attribute	Data Type	PKEY	FKEY	NOT NULL	UNIQUE	Description
spec_id	NUMBER	X		X	X	Key field
spec_name	VARCHAR2(64)			X		Specialty name
spec_num	NUMBER			X	X	Specialty number
id_fac	NUMBER		X	X		Faculty to which the specialty belongs. Link to the record in the table **Faculty**
Deleted	NUMBER			X		Record deleted

Role restrictions:
— For UCAC, AACF, UACF - only reading

Field access predicates for users:
— For AACF, UACF - "**UserTable** [login = user_name] .fac_id = id_fac".

3.4 Exam table

The table includes information about the entrance exams.

Table 4. Information about entrance exams

Attribute	Data Type	PKEY	FKEY	NOT NULL	UNIQUE	Description
exam_id	NUMBER	X		X	X	Key field
exam_date	DATE			X		Exam date
id_base	NUMBER		X	X		The base on which the exam was conducted
Deleted	NUMBER			X		Record deleted

Role restrictions:

— For UCAC, AACF, UACF - only reading

3.5 Exam result table

The table includes information about the exam results.

Table 5. Exam results

Attribute	Data Type	PKEY	FKEY	NOT NULL	UNIQUE	Description
result_id	NUMBER	X		X	X	Key field
id_exam	NUMBER		X	X		The exam at which this result was obtained. Link to the record in the Exam table.
id_dpuser	NUMBER		X	X		The person who received the given result. Link to the DPUser table record.
id_fac	NUMBER		X	X		Faculty for which the exam is being conducted. Link to the record in the Faculty table.

Role restrictions:

— For UCAC, AACF, UACF – only reading.

Field access predicates for users:

— For AACF, UACF - "(**UserTable** [login = user_name] .fac_id = id_fac) | (**UserTable** [login = user_name] .fac_id = Base [Exam [id_exam] .id_base] .id_fac) "(the faculty for which the exam is being conducted, or the faculty that owns the base on which the exam was conducted, matches the desired one).

3.6 DP user table

The table includes information about users.

Table 6. Information on users

Attribute	Data Type	PKEY	FKEY	NOT NULL	UNIQUE	Description
user_id	NUMBER	X		X	X	Key field
first_name	VARCHAR2(64)			X		First name
last_name	VARCHAR2(64)			X		Last name
middle_name	VARCHAR2(64)			X		Middle name
user_dp	NUMBER			X		Type of pre-university preparation
deleted	NUMBER			X		Record deleted

Role restrictions:

— For UCAC, UACF – only reading.

Field access predicates for users:

— For AACF, UACF - "the faculty for which at least one exam of this faculty was conducted, or the applicant has applied for this faculty, but he/she does not yet have exam results (determined through the AbitSpec and Spec tables), coincides with the desired one."

3.7 Abiturient table

The table includes information about applicants who have applied for admission to the university.

Table 7. Admission Applicants

Attribute	Data Type	PKEY	FKEY	NOT NULL	UNIQUE	Description
abit_id	NUMBER	X		X	X	Key field
id_user	NUMBER		X	X	X	Link to record in DPUser table
id_spec	NUMBER		X			The specialty for which he is enrolled. Link to recording in the Special table.
create_date	DATE			X		Date of submission of documents
drop_date	DATE					Date of return of documents
certificate_real	NUMBER			X		Original passport or copy submitted
cetrificate_number	NUMBER			X		Certificate number

Attribute	Data Type	PKEY	FKEY	NOT NULL	UNIQUE	Description
cetrificate_good	NUMBER			X		In the certificate, all marks are higher than 6 points (according to a 12-point system)
school_end_date	DATE			X		Graduation year
school_type	NUMBER			X		Type of secondary educational institution
nationality	VARCHAR2(32)			X		
address	VARCHAR2(512)			X		
address_type	NUMBER			X		
birthday	DATE			X		
sex	NUMBER			X		Sex
privel	NUMBER			X		Privileges
foreign_leng	NUMBER			X		What foreign language was studied at school
contract	NUMBER			X		fee-based or state grant form of education
pay_date	DATE					Contract payment date
sum	NUMBER					Contract payment amount
contrakt_number	NUMBER					Contract number
reject_con	NUMBER					Refusal to participate in the competition
zachislen	NUMBER			X		Enrolled or not
zachislen_con	NUMBER					Enrolled by competition or early admission
test1	NUMBER					The applicant goes to the first test
test2	NUMBER					The applicant goes to the second test
test_result	NUMBER					Test results
deleted	NUMBER			X		Record deleted

Role restrictions:

— For ACAC, UCAC, UACF - only reading.

Field access predicates for users:

— For UACF - "the applicant has applied for this faculty, (determined through the AbitSpec and Spec tables)".

3.8 Abiturient spec table

The table includes information about the specialties for which the applicant wants to enroll.

Table 8. Choice of Program specialties of applicants

Attribute	Data Type	PKEY	FKEY	NOT NULL	UNIQUE	Description
abitsp_id	NUMBER	X		X	X	Key field
id_abit	NUMBER		X	X	X	An applicant who wishes to enter a certain specialty. Link to the record in the Abiturient table.
id_spec	NUMBER		X	X		The specialty for which the applicant wishes to enroll. Link to the record in the Special table.
prior	NUMBER			X		Specialty priority
deleted	NUMBER			X		Record deleted

Role restrictions:
- For ACAC, UCAC, UACF - only reading.

Field access predicates for users:
- For UACF - "The specialty belongs to the desired faculty (determined through the Spec table".

Thus, the differentiation of access to data using the introduction of roles and RLS provide flexible and effective protection of information in the database.

4 Conclusion

During the analysis of the access control rules, it can be seen that different users can simultaneously access data from the database. Therefore, a data-sharing mechanism must be provided. Access to different users for reading the same set of data does not have any negative consequences. It is necessary to delimit access for recording, updating and deleting. In my case, it is necessary to delimit access to the ExamResult and DPUser tables from the users of ACAC and AACF. These users have the right to change the contents of these tables.

To differentiate access, the study proposed the use of a record-protecting lock, which protects an object from being imposed on it by other operations of a complete lock or a recording lock. This kind of locking allows someone who previously "captured" the object to complete the modification of the object. In the future, during the development of software, it must be kept in mind that the introduction of such a lock can lead to deadlocks, and it is necessary to take measures to resolve them (seize resources in strict order).

5 References

[1] Vasiliev, V. G. (2007). Object-Oriented Databases: An Inside View // Computers + Programs (3rd ed.).

[2] Akcil, U., Uzunboylu, H., & Kinik, E. (2021). Integration of Technology to Learning-Teaching Processes and Google Workspace Tools: A Literature Review. Sustainability, 13(9), 5018. https://doi.org/10.3390/su13095018

[3] Minett, B. T. (2007). Software Development. Translation from English MVU. Lvov-Dnepropetrovsk.

[4] Connolly, T., & Begg, C. (2014). Database Systems: A Practical Approach to Design, Implementation, and Management (6th ed.). Pearson

[5] Maklakov, S. V. (2009). Bpwin and Erwin. Case - information systems development tools. DIALOG-MEPhI.

[6] Uzunboylu, H., & Gundogdu, E. G. (2018). A Content Analysis Study on Pre-School Education and Instructional Technologies. International Journal of Innovative Research in Education, 5(4), 119–128. https://doi.org/10.18844/ijire.v5i4.3974

[7] Yakubu, M. B., DanAzumi, H., Bulama, M., & Hassan, A. (2019). Intrusion tolerance model against higher institution database. Global Journal of Information Technology: Emerging Technologies, 9(1), 20–28. https://doi.org/10.18844/gjit.v9i1.4060

[8] Magayon, V. C., Saccuan, R. & Carbonell, A. (2021). Expectation vs. reality: A sentiment analysis of students' experience on distance learning. International Journal of Learning and Teaching, 13(4), 260–275. https://doi.org/10.18844/ijlt.v13i4.5979

[9] Rosli, R., & Siregar, N. C. (2022). Teacher professional development on science, technology, engineering, and mathematics: A bibliometric analysis. Contemporary Educational Researches Journal, 12(1), 01–17. https://doi.org/10.18844/cerj.v12i1.5417

[10] Turkkan, H. (2021). The significance of typography in data visualization. Global Journal of Computer Sciences: Theory and Research, 11(1), 12–23. https://doi.org/10.18844/gjcs.v11i1.5030

[11] Yildiz, E. P., Cengel, M., & Alkan, A. (2020). Current trends in education technologies research worldwide: Meta-analysis of studies between 2015-2020. World Journal on Educational Technology: Current Issues, 12(3), 192–206. https://doi.org/10.18844/wjet.v12i3.5000

[12] Ceker, E., & Ozdamli, F. (2021). Features and characteristics of problem-based learning. Cypriot Journal of Educational Sciences, 11(4), 195–202. https://doi.org/10.18844/cjes.v11i4.1296

[13] Noormohammadi, B. (2019). On the relationship between Iranian EFL Teachers' attitudes towards the Book series''Prospect'' taught in Iran's Schools and their TKT (Teaching Knowledge Test). Global Journal of Foreign Language Teaching, 7(1), 18–33. https://doi.org/10.18844/gjflt.v7i1.1235

[14] AY, G. (2020). Evaluation of views regarding pharmacy information management systems implementation and systemic issues in community pharmacies. International Journal of Emerging Trends in Health Sciences, 4(1), 68–76. https://doi.org/10.18844/ijeths.v4i1.4522

[15] Pascu, L., Simo, A., & Vernica, A. M. (2019). Integrating Microsoft IoT, machine learning in a large-scale power meter reading. International Journal of New Trends in Social Sciences, 3(1), 10–16. https://doi.org/10.18844/ijntss.v3i1.3815

[16] Kelkay, A. D., & Endris, A. (2020). Model-based instruction to improve the concept of students on human anatomy: Primary School, Ethiopia. International Journal of Learning and Teaching, 12(2), 72–85. https://doi.org/10.18844/ijlt.v12i2.4618

[17] Yakubu, M. B., DanAzumi, H., Bulama, M., & Hassan, A. (2019). Intrusion tolerance model against higher institution database. Global Journal of Information Technology: Emerging Technologies, 9(1), 20–28. https://doi.org/10.18844/gjit.v9i1.4060

[18] Aravind, V. R., & McConnell, M. K. (2018). A computer-based tutor for learning energy and power. World Journal on Educational Technology: Current Issues, 10(3), 174–185. https://doi.org/10.18844/wjet.v10i3.3558

6 Authors

Akanov Arman is a Ph.D. candidate, specialty "Informatics", educational institution "Alikhan Bokeikhan University", Abay street 107, 071405, Semey city, Kazakhstan (akanov-87@list.ru, https://orcid.org/0000-0002-5323-1705).

Sagindykov Kakim is an Ass. professor, specialty "Informatics", L.N. Gumilyov Eurasian National University, Ablaihana street 6/5, 01, Nur-Sultan, Kazakhstan (ksagin@mail.ru, https://orcid.org/0000-0003-3315-798X).

Article submitted 2022-09-12. Resubmitted 2022-10-12. Final acceptance 2022-10-13. Final version published as submitted by the authors.