International Journal of Security and Its Applications
Vol.8, No.3 (2014), pp. 163-174
http://dx.doi.org/10.14257/ijsia.2014.8.3.18

Database Security Model in the Academic Information System

Ema Utami[1] and Suwanto Raharjo[2]

[1]*Departement of Magister of Informatics Engineering of The College of Information Systems and Computer Science of AMIKOM Yogyakarta Indonesia,*
[2]*Departement of Informatics Engineering of Institute Science and Technology AKPRIND Yogyakarta, Indonesia*
[1]*ema.u@amikom.ac.id,* [2]*wa2n@nrar.net*

Abstract

Database plays an important role on both web-based or desktop based academic information system (AIS) in Indonesian higher education institutions (HEI). Nowadays web-based AIS dominates in Indonesian HEI, almost every HEI uses web-based AIS with relational database management system (RDBMS) as database software. Relational database systems such as Oracle, MySQL, MS SQL Server or PostgreSQL are familiarly used as database management system in the AIS. There are many researches on development of AIS in HEI but none of them is discussing database security and integrity. This research will perform the analysis of database security model that could be used in AIS such as table constraints, table relationships and role-based access control (RBAC).

Keywords: *AIS, database security, database integrity, RBAC*

1. Introduction

Academic information system (AIS) is a software intended to process the academic data of an educational institution. AIS in a tertiary education is generally used to manage the student academic data starting from registration as students, plan their study, to look at the study result as well as judicium and graduation process. Most of tertiary education institutions use web-based AIS connected to intranet or internet. Research on AIS design in Indonesia is largely found in Google search engine (http://scholar.google.com), even AIS research for elementary and secondary schools have been published. Yet, from those researches there is no research about security on AIS especially database security. This research will discuss about data based security model on AIS in Indonesia specifically on tables related with the study plan and study result processes in tertiary education institutions.

2. Related Paper

Some related research is discusses about AIS development in Indonesian tertiary (higher) education institutions [1-3]. Research about AIS security has been done previously but it is in terms of authenticity method [4]. Another research discusses the other security method that is AIS result document security [5]. Technical document of information system development is also used as a reference in this research [6]. Previous research has not discussed the database security especially on the database related to the study plan and study result processes. The research in the reference shows that it is web-based AIS which is developed by using web-based programming with PHP as language programming and MySQL as its database management system (DBMS) software. The global research on relational database security

ISSN: 1738-9976 IJSIA
Copyright ⓒ 2014 SERSC

have been studied such as using hash function to assure the confidentiality and integrity [7], watermark [8, 9], encryption [10], Access control [11] and multilayer security [12].

3. Methodology

This research is the theoretical review from the existing research about AIS in tertiary education institutions and especially about database security. AIS in tertiary education institutions is a software aimed at managing academic data of tertiary education institutions from student registration until graduation. In the academic data management, there are some processes that can be done by students, among them are:

1. Heregistration
2. Looking at the schedule
3. Looking at the lecture attendance amount
4. Planning the study
5. Looking at the study result
6. Printing the transcript

Discussion about the existing reference is focused on the problems of the study plan and study result processes of the students in tertiary education institutions. Processes in AIS related with this research are: planning the study, changing the study plan, printing the study plan card, looking at the study result, printing the study result per semester and printing the transcript. The study plan process is a process where students choose the lectures in one semester saved in the course selection sheet (CSS). The students who have studied for minimal 1 semester will be able to look at the study result saved in the course result sheet (CRS). The students who have had marks can look at the study result and print either the study result or the transcript per semester. Discussion is done in the database security used especially in the data integrity aspect. This research will see the security aspect from database design used, namely: key choosing, table relation design, constraint usage, database authenticity and database role usage. This research limits on the database security and does not discuss about the application security model used. The flowchart of the research process can be described in Figure 1.

4. Findings and Discussion

The study plan and result process in AIS are an important process in AIS. The process is often done because the study plan is conducted every semester. The study plan starts from the administrative process done by students to fulfill the requirement to do the study plan, for instance paying the tuition. Students who are allowed to do the study plan can do the following processes:

1. Choosing the offered lectures and fulfilling the requirement to take
2. Choosing the schedule they want
3. Changing the study plan

The study plan process has generally been determined in a certain period in which the students can change the study plan data taken. After the study plan fulfillment, the input data cannot be changed. The change of the study plan fulfillment data can be done again in the determined period. The diagram of the fulfillment and the changing of the study plan plot can be seen in Figure 2.

 Copyright ⓒ 2014 SERSC

Based on the references, the design of database table related with the process and the study result generally has similarity, that is using 4 main tables which are related each other, namely tables of *student*, *css*, *crs* and *courses* [3, 6, 1]. The relationship among the 4 tables can be described in Figure 3. Yet, there is also a research using a design where *css* and *crs* tables are made in one table by giving an additional grade column in *css* table.

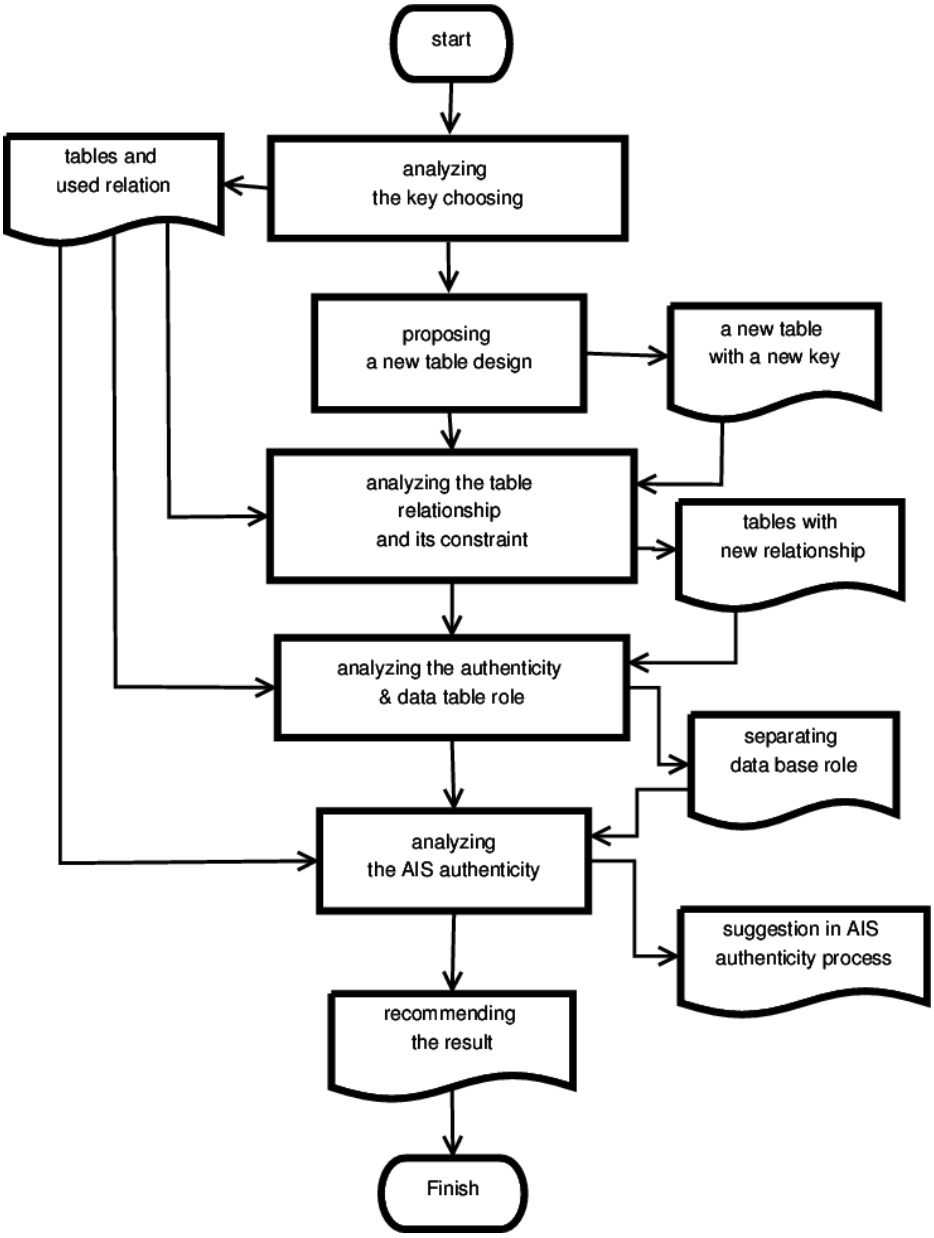

Figure 1. The Research Process Flowchart

4.1. Key Choosing

The references show that *ccs* and *crs* tables use PRIMARY KEY constraint in the form of a column commonly called *cssid* and *crsid* which are related each other, with *cssid* in *crs* table as FOREIGN KEY (Figure 3). From Figure 3, it is possible to form composite primary

Copyright ⓒ 2014 SERSC

key, that is a combination of *sid* (student number), *ac_year* (academic year), *courseid* and *semester* columns in *css* table. Yet, the substituted primary key (surrogate key) which generally uses generated data type by the program is used in the database design like in the research reference [1-3]. Figure 4 shows methods of the primary key usage.

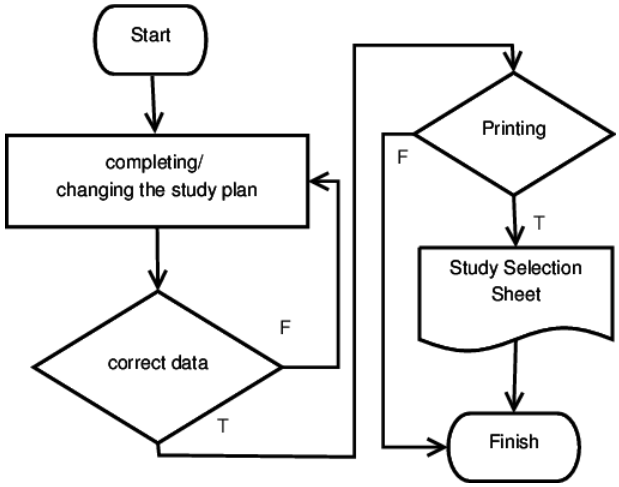

Figure 2. The Study Plan Flowchart

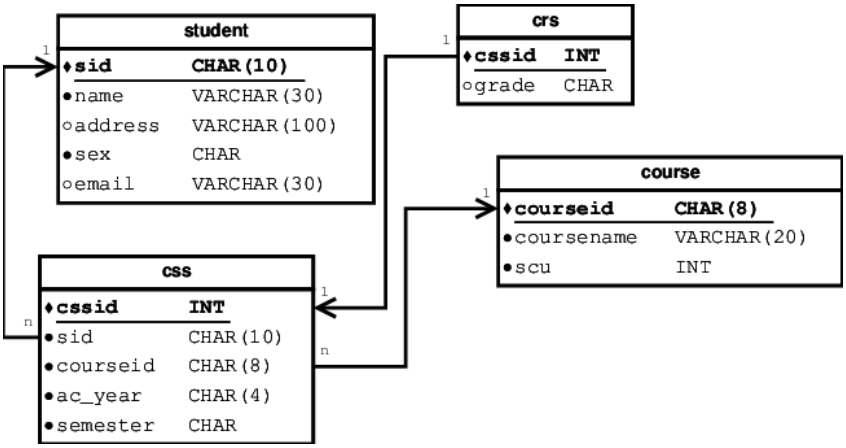

Figure 3. The Table Relationship

The surrogate primary key will have a weakness in which *css* table will enable the redudancy, that is in columns *sid*, *ac_year*, *courseid* and *semester*. Table 1 shows the possibility data redudancy where the table does not break the given constraint in *css* table with *cssid* as primary key.

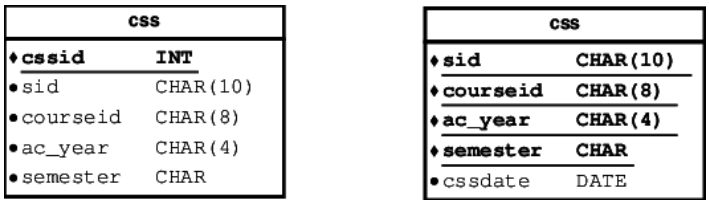

Figure 4. *css* Table with the Surrogate and Composite Primary Key

Copyright ⓒ 2014 SERSC

Data integrity assurance will be better if composite primary key is used in *css* table, that is by using *sid, ac_year, courseid* and *semester* as the primary key. If it is forced to use surrogate primary key, UNIQUE constraint in *sid, ac_year, courseid* and *semester* can be given to guarantee the data integrity. The SQL command is used to force data integrity using both methods shown in Figure 5.

Table 1. Data Redudancy

cssid	sid	courseid	ac year	semester
1	12.52.1234	TIF-1201	2012	1
2	12.52.1234	TIF-1201	2012	1
3	12.52.1234	TIF-1201	2012	1
4	12.52.1235	TIF-1201	2012	1
5	12.52.1235	TIF-1201	2012	1

UNIQUE Constraint	**Composite Key**
CREATE TABLE css (cssid INT PRIMARY KEY, sid CHAR(10), courseid CHAR(8), ac_year CHAR(4), semester CHAR, UNIQUE (sid, courseid, ac_year, semester));	CREATE TABLE css (sid CHAR(10), courseid CHAR(8), ac_year CHAR(4), semester CHAR, cssdate DATE, PRIMARY KEY (sid, courseid, ac_year, semester));

Figure 5. SQL Command

4.2. Tables Relationship and Constraints

Table relationship in Figure 3 shows that *css* table correlates with *student* table, all reference papers related to this research generally have similar relationship. *sid* column in *css* table as the foreign key depends on *sid* column as the primary key in students table. This relation guarantees that only students who have been recorded in *student* table can input the study plan data in *css* table. Yet, this method cannot limit that only students who have the right to process the study plan can input the data in *css* table.

The limitation on who can be saved in *css* table will generally be done in programming level by checking whether the students have been authenticated and have fulfilled the administrative requirement. Thus, if that relation method is viewed from the database security, it has a weakness that can damage the data integrity, where all students in the *student* table have possibility to be input in the *css* table.

The student separation that has fulfilled the requirements to do the study plan can be done to solve this problem. For instance the *study* table can be made to record data from the students who have re-registered and fulfilled the requirement to plan the study and it is used as a reference table by the *css* table. Figure 6 shows the additional *study* table used as the reference table from the *css* table.

Copyright ⓒ 2014 SERSC

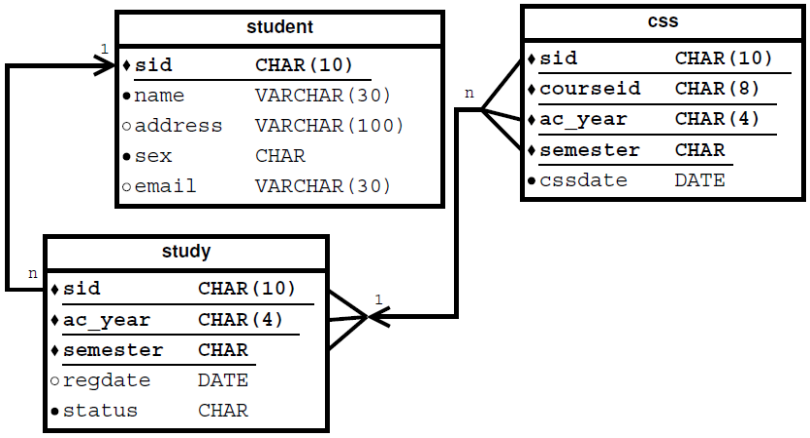

Figure 6. *css* and *study* Table Relationship

Hierarchy relationships in Figure 6 will guarantee that only students who have been listed in the *study* table have the right to input data in the *css* table. The hierarchy relationship model can guarantee the data integrity in the *css* table. Same with the *crs* table, this table is separated from the *css* table. The composite primary key usage will maintain the data integrity in *crs* table. Data that can be inputted in the *crs* table will only match the *css* table. Figure 7 is a relationalship picture between the *css* and *crs* table. The separation between the *css* and the *crs* table will make the role easier.

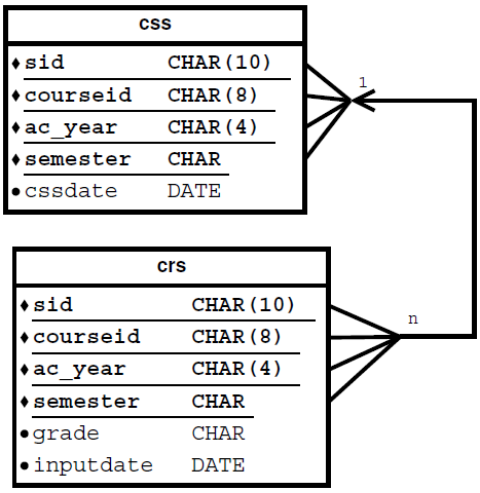

Figure 7. *css* and *crs* Table Relationship

Besides using the relationship tables, data input limitation in a table can be used to maintain the data integrity by using CHECK constraint [13] and procedural language (PL) that can be a TRIGGER. The study plan process will generally limit the amount of semester credit unit (CSU) that a student can take. The limitation of courses taken commonly depends on grade point (GP) of the previous semester and the prerequisite of a course that will be taken. *course* table that has *scu* column and correlates with the *css* table (Figure 8) will be used to count GPA (Grade Point Average) and how many the semester credit unit can be taken.

 Copyright ⓒ 2014 SERSC

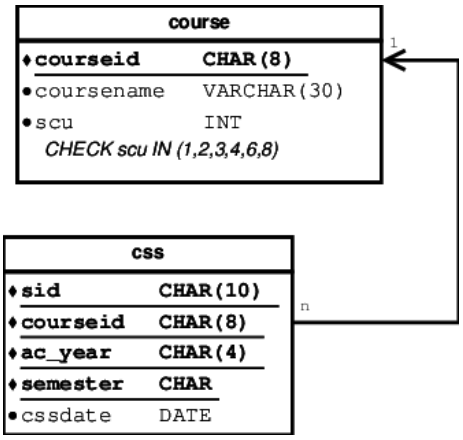

Figure 8. *css* and *course* Table Relationship

The *scu* column with INTEGER data type can limit the value that might be inputted by CHECK constraint and is adjusted with the curriculum policy. Besides limiting the *scu* value, the total *scu* limitation taken can use the PL such as PL/SQL in Oracle, Transact SQL in MS SQL or PL/PgSQL in PostgreSQL. PL enables users to calculate the grade point of the previous semester. The function to count the grade point can be embedded in a TRIGGER or CHECK constraint which can limit the data input. If the *scu* amount has passed the limit, the data input can be denied. Figure 9 shows the SQL command to create table uses CHECK constraint of which function is named *checkgp* used to calculate the grade point of the previous semester.

```
CREATE TABLE css (
sid CHAR(10),
courseid CHAR(8),
ac_year CHAR(4),
semester CHAR,
cssdate DATE,
PRIMARY KEY (sid, courseid , ac_year, seemester),
CONSTRAINT check_gp CHECK (checkgp (sid, courseid, ac_year, semester)));
```

Figure 9. CHECK Constraint to Limit Data Input

CHECK constraint in *css* table (Figure 9) will calculate the grade point of the previous semester in *crs* table and sum total *scu* in *css* table. If the previous grade point and total *scu* in the current semester already pass the limitiation, a new row will not be able to be inserted. The error message generated by this CHECK constraint is shown on Figure 10.

```
INSERT INTO css VALUES ('12.52.1234', 'TIF-1205', '2013', '2') ;
ERROR: new row for relation "css" violates check constraint "check_gp"
```

Figure 10. Error Message

The lecture prerequisite CHECK or TRIGGER constraint can be used to allow or deny the data inputted in the *css* table. Yet, this method have a weakness that is, where a higher education institution made a policy for the students to take *scu* more than what is determined. So as the use of CHECK and TRIGGER constraints as the prerequisite will collide if there is a policy that allows the student to take a lecture without taking the prerequisite. This special case often occurs. For example when there is a transferred student, the database is sometimes

Copyright ⓒ 2014 SERSC

forced to receive the data in which according to the rule, it is not allowed. But if the rule is fixed and cannot be violated, CHECK and PL constraints can become a considerable option. Further research is needed to test the accuracy, especially the data input speed that might be affected by the limitation.

4.3. Database Role

Web-based AIS application commonly uses server side scripting programming such as PHP, ASP, JSP or others which is connected to DBMS software. In the references, it is not found methods used to connect the database system. The connection from PHP to DBMS can be done with some methods such as ODBC, ADODB, PEARDB, or PDO. The relational description among a user, application and AIS database system is shown in Figure 11.

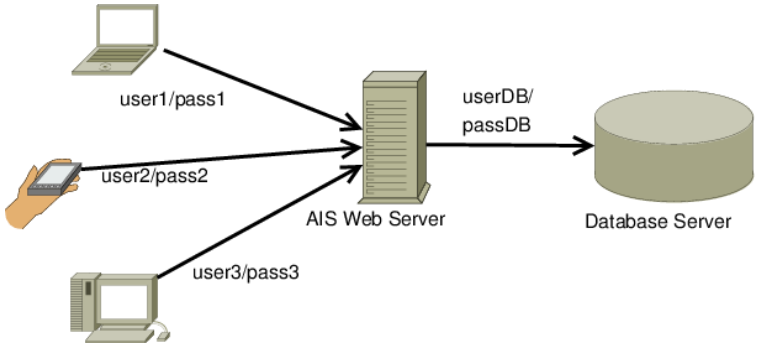

Figure 11. Database and Application Connection

From Figure 11, it is seen that there are 2 forms of authenticity, namely:
1. AIS application authenticity
2. Database authenticity

AIS authenticity is the authenticity used to validate whether a student deserves to enter into the system or not, whereas database authenticity is a validation from AIS application to access its database. There is no direct connection between AIS authenticity and database authenticity. PDO can be used by PHP based application from 5.0 PHP version. Now PDO becomes a connection method to Relational DBMS (RDBMS) suggested for the security reason. The use of one statement in PDO can minimize the threat from SQL Injection [14]. It is the strength of PDO from the database security side. PDO supports some RDBMS such as MySQL, MSSQL, PostgreSQL, Sysbase, etc. The connection example from AIS application that uses PHP and PDO to be connected with MySQL can be seen in Figure 12.

```
<?php
$dbh = new PDO('mysql : host=localhost;
dbname=nameDB', $username, $password);
?>
```

Figure 12. MySQL Connection using PDO

Figure 12 shows that the application uses 1 database, 1 host, 1 user and 1 password which are saved in a PHP file. The user name in $*username* variable can generally be used in AIS that is the user of the *nameDB* database owner with the *password* adjusted. As the database owner of *nameDB*, the owner has the full role of the database. Traditional identity-based

 Copyright ⓒ 2014 SERSC

mechanisms are useless for web databases and also for most of the web applications are used high privileges user [15].

Figure 11 dan 12 show that any AIS user that is authenticated will be connected to the same DBMS. The connection to the database that only uses 1 kind of role with the full access right to the database that will enable the security problem towards the database. The example of the problem is that the *css* table is possible to be changed in an undefined time. Because there is no limitation of database user access to the *css* table, it is possible for the user to change the data in the *css* table.

There is no discussion about using of the database role in the existing Indonesian research references. Each RDBMS has the ability to manage users access right in the database which is usually called role based access control (RBAC). RBAC is widely used in computer system security and can be used to protect privacy [16]. By using RBAC, RDBMS can give the access right to a user in the database in accordance with what the database owner wants. RBAC itself has been one of ANSI standards in 2004. RBAC enables database owner to give the access limitation to the user who uses it to connect to the database. For example: scenarios that can be used to secure the database by RBAC are:

1. Giving a special access right at the process of the study plan and change.
2. Giving a special access right for the process to see the study result.

In general, RBAC enables to make special users who are related to the database connection for specific need. Figure 13 shows the illustration of the RBAC usage in AIS.

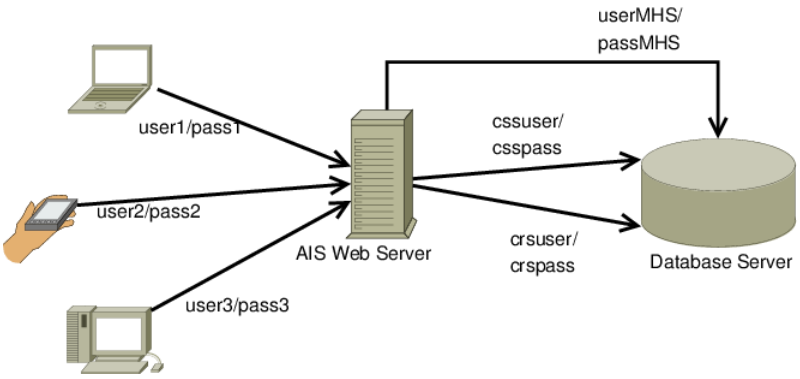

Figure 13. Implementation of RBAC in the AIS

In AIS, the study plan process is done on schedule and through page or specific menu therefore the specific process is possible to use specific connection of the study plan in which Figure 13 is represented by *cssuser* and *csspass*. The *cssuser* has the access right to do SELECT, INSERT, UPDATE and DELETE in the *css* table. After the study plan is finished, *cssuser* can be non-activated by the database owner, so *cssuser* cannot be used anymore. Besides the study plan process, other processes can use *generaluser*, user that has certain limitation, for instance: the user cannot change the *css* table. Another example is the process to see the study result, a user who accesses in the *crs* table can use *crsuser* that has the access right to do SELECT only in the *crs* table. Table 2 shows the sample of the rule with RBAC that can be applied in AIS related to the study plan and result processes.

By using RBAC, only users who have the right can change the value from a table, so this method deserves to be used to keep the database integrity. This method needs the programming side to separate the processes in AIS. Each process is grouped and matched

Copyright ⓒ 2014 SERSC

with its access right by connecting to the different database suitable with each user's right. Thus the connection to the database is not sole like in general connection but it can be more than one kind of connection in accordance with the number of the access right groups.

Table 2. Access Right based on Role

Role Name	Access Right
cssRole	Is allowed to write in the *css* table Is allowed to change in the *css* table Is allowed to delete in the *css* table Is allowed to read only in the *crs* table Is not allowed to do anything in another table
crsRole	Is allowed to read only in the *crs* table Is not allowed to do anything in another table
stdRole	Is allowed to read only in the *css* and *crs* tables Is allowed to change the personal data in the suitable table Is not allowed to do anything in another table

4.4. AIS Authenticity

This research does not discuss about the methods and processes of the application authenticity connected to the database used in the process of the study plan. Before the students can process the study plan or see the study result they have passed, students must login first to AIS system. In some AIS, the process related to the study plan is separated from other processes, so that the authenticity for the study plan and other processes are separated with the different login page. By this method, login page to process the study plan is only activated when the schedule of the study plan comes. But there is possibility to keep on using one same authenticity page for all processes in AIS. The menu for the study plan will not be active if it is not in the study plan period. In the database security aspect there is no difference in the use of login page which is separated from other processes. Discussion about reference finds out that the table design used to process the authenticity
can be divided into 3 models, namely:

1. User table is separated with the student table without relationship.
2. User table is separated with the student table with relationship.
3. User and student tables are in single table.

The method of the authenticity table in AIS does not have direct correlation with the database security, especially in the data integrity problem. Yet, correlating the student authenticity table with the *student* table will have benefit that only students who are included in the *student* table will be accepted by the system. Users who are not students cannot enter the system, the student users who are related with the *student* table bring consequences that AIS users who are not students, for instance administrator must be separated in table. The sample of table relation which can be used for AIS authenticity can be seen in Figure 14.

By separating student and administrator users in the different table, we can implement the roles in both tables. For example student users with the *stdUser* role are allowed to change the *login* table to change the password, but the role is not allowed to see the *administrator* table. Using this method enables to keep the data security in the tables better.

 Copyright ⓒ 2014 SERSC

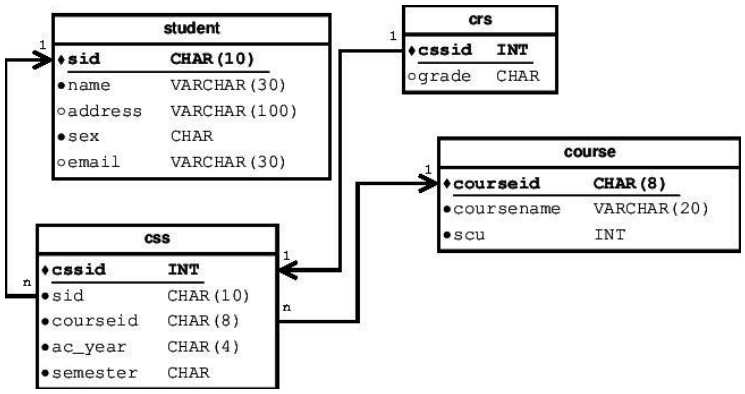

Figure 14. User Table Relationship

5. Conclusion

Data in AIS especially the process related to the study plan and result are vital data in a HEI. Having good data in which the integrity is well kept is the basic thing to take the concise decision. The supervision of the data integrity in RDBMS becomes a must. Limiting the data input in order that the coming data are suitable with the requirement and defined regulation is one of the ways to maintain the database integrity. The good planning of the primary key can maintain tables to receive data without being redundant. Data input in the table which has relationship with another table will be denied if there is no reference data. The accurate relationship design among tables can be used as one of the methods to maintain the data integrity. The same with CHECK constraint and PL usage, they can be implemented in TRIGGER to be used to maintain the table in AIS to be a strong table. Rule making or database role is possible to be applied in AIS application which is synchronized with the module or menu from application. The study plan menu related to certain database role which only has certain access can be used to maintain data in order not to be changed by users without the right.

References

[1] J. and R. A. Triyono, "Pembangunan Sistem Informasi Kartu Rencana Studi (KRS) dan Kartu Hasil Studi (KHS) Online pada Sekolah Tinggi Ilmu Tarbiyah Nahdlatul Ulama (STITNU) Pacitan", IJCSS-Indonesian Journal on Computer Science Speed-FTI Universitas Surakarta, vol. 10, no. 1, **(2012)**.
[2] F. R. Noviandi, "Pengembangan Sistem Informasi Akademik Fakultas Teknik Universitas Tanjungpura", Jurnal Sistem dan Teknologi Informasi (JustIN), vol. 1, no. 1, **(2013)**.
[3] Y. Y. Joefrie and P. P. Kalatiku, "Desain Basis Data Sistem Informasi Akademik di Fakultas Teknik Universitas Tadulako", FORISTEK, vol. 2, no. 2, **(2013)**.
[4] A. Masykur, K. I. Satoto and R. R. Isnanto, "Analisis Keamanan Sistem Informasi Akademik Fakultas Teknik Universitas Diponegoro Versi 0.4 Tahun 2005", Undergraduate thesis, Universitas Diponegoro, **(2011)**.
[5] H. Ahmaddul, E. Sediyono and K. I. Satoto, "Rancang Bangun Sistem Pengamanan Dokumen pada Sistem Informasi Akademik Menggunakan Digital Signature dengan Algoritma Kurva Eliptik", Masters thesis, Universitas Diponegoro, **(2012)**.
[6] Y. Utama and Tim, "ICT Content dan Sistem Informasi, Pengembangan Sistem Informasi Akademik Universitas Sriwijaya", Technical documentation, **(2008)**.
[7] L.-X. Xu, D. Sun and D. Liu, "Study on Methods for Data Confidentiality and Data Integrity in Relational Database", Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference, vol. 1, **(2010)**.
[8] I. Kamel and K. Kamel, "Toward Protecting the Integrity of Relational Databases", Internet Security (WorldCIS), 2011 World Congress IEEE, **(2011)**.

Copyright ⓒ 2014 SERSC

[9] A. Khan and S. A. Husain, "A Fragile Zero Watermarking Scheme to Detect and Characterize Malicious Modifications in Database Relations", The Scientific World Journal, vol. 2013, **(2013)**.
[10] E. Shmueli, R. Vaisenberg, Y. Elovici and C. Glezer, "Database Encryption: An Overview of Contemporary Challenges and Design Considerations", ACM SIGMOD Record, vol. 38, no. 3, **(2010)**.
[11] R. Thion and S. Coulondre, "A Relational Database Integrity Framework for Access Control Policies", Journal of Intelligent Information Systems, vol. 38, no. 1, **(2012)**.
[12] M. H. Abdel-Aziz, I. M. El-Henawy and A. M. Mostafa, "Interactive Multi-layer Policies for Securing Relational Databases", Information Society (i-Society), 2012 International Conference, IEEE, **(2012)**.
[13] S. De Capitani di Vimercati, P. Samarati, S. Jajodia and R. B. Knode, "Database Security. Encyclopedia of Software Engineering", **(2001)**.
[14] D. Popel, "Learning PHP Data Objects", Packt Pub Limited, **(2007)**.
[15] A. Bouchahda, N. Le Thanh, A. Bouhoula and F. Labbene, "Enforcing Access Control to Web Databases", Computer and Information Technology (CIT), 2010 IEEE 10th International Conference, IEEE, **(2010)**.
[16] M.-Y. Chen, C.-C. Yang and M.-S. Hwang, "Privacy Protection Data Access Control", International Journal of Network Security, vol. 15, no. 6, **(2013)**.

Authors

Dr. Ema Utami, S.Si, M.Kom**,** received the S.Si, M.Kom and Doctoral degrees in Computer Science from Gadjah Mada University, Yogyakarta, Indonesia in 1997, 2002 and 2010 respectively. Since 1998 she has been a lecturer in STMIK AMIKOM Yogyakarta, Indonesia. Her areas of interest are Natural Language Processing, Computer Algorithms, and Database Programming.

Suwanto Raharjo, S.Si, M.Kom, is a lecturer in Informatics Engineering of Institute Science and Technology AKPRIND Yogyakarta, Indonesia. His areas of interest are database, database programming and Linux operating system.

 Copyright ⓒ 2014 SERSC