Impact Factor Value: 4.029 ISSN: 2349-7084
International Journal of Computer Engineering In Research Trends
Volume 4, Issue 8, August-2017, pp. 336-340 www.ijcert.org

Protecting Data in Relational Database Management System using Purpose and Role-Based Access Control

Suraj Krishna Patil[1], Suhas B. Bhagate[2]
[1]Master of Engineering Student, Computer Science & Engineering, TEI, Ichalkaranji, 416115, India
[2]Assistant Professor, Computer Science & Engineering, TEI, Ichalkaranji, 416115, India.

surajkpatil45@gmail.com[1], suhas.bhagate@gmail.com[2]

Abstract:- **Background/Objectives**: Privacy is a key requirement in handling personal and sensitive data. The Database Management System (DBMS) stores such kind of data and also provides tools to access and analyze this data.

Methods/Statistical analysis: The Role-Based Access Control (RBAC) regulates the access to resources based on the roles of individual users. Purpose Based Access Control (PuBAC) regulates the access based on the purpose for which data can be accessed. It regulates the execution of queries based on purpose.

Findings: From the result, it is observed that some records accessed by considering the purpose and role-based access control are less than some records accessed by original and purpose based access control query result. The system is more secure than the previous one.

Improvements/Applications: This work can be used in the organizations, government, and private offices academic institutes. It can be extended to support big data and conditional purpose based access control.

Keywords: Privacy, Access Control, Query Rewriting

1. Introduction

Nowadays, the large amount of personal and sensitive data of individuals are stored and processed. The organizations that handle such data must take care of privacy of individuals. The privacy-preserving is the key requirement for processing the personal and sensitive data [1],[2], [3].The database management system plays a vital role in storing the data. The database supports various access control mechanisms such as discretionary, mandatory which are operating at different levels of tables to the cells or tuples in the database. The idea of access control is that each database user gets access to a subset of the database to which they can query and get data that they required.

Within Database Management Systems (DBMS), privacy policies regulate the collection, access, and disclosure of the stored personal, identifiable and sensitive data. Policies specify actions that must be executed or conditions that must be satisfied before or after data are accessed [4]. Purpose of access is one of the major components in privacy which consider data as a key factor in access control decisions [5]. There are different access control mechanisms are available like discretionary, mandatory which provides privacy. The purpose and role based access control model help in bridging the gap between security and privacy oriented data protection[6].It enforces fine-grained access control by the purpose of access, actions executed by SQL queries on accessed data, categories of data and role of the user. It regulates the execution of SQL queries based on purpose and role-based privacy policies. Data categories are also used to regulate access control.

Access control is used to protect the personal and sensitive information of individuals. It is the process of limiting the access to resources [7]. The Role-Based Access Control (RBAC) regulates the access to resources based on the roles of individual users within an organization. This can restrict system access to authorized users only. Roles are created according to functions in the organization. The Purpose Based

Access Control (PuBAC) regulates the access based on the purpose for which data can be accessed. It regulates the execution of SQL queries based on purpose. It helps to achieve privacy as well as the security of data.

2. Literature Review

J.Byun and N.Li [1] proposed the reference purpose based model for relational DBMS which regulates the access based on purpose compliance. The access is granted if the purposes for which the accessed data have been collected comply with purposes for which the queries accessed data. The privacy protection is based on the idea of purpose. The model determines access purpose by using role attributes and conditional roles. This model does not cope with other elements of privacy such as obligations and complex conditions.

M.E.Kabir and H.Wang [2] proposed model which extract more information from customers by providing a secure privacy policy. This model enforces privacy and enables customers to maintain control over their data. This model works for the conditional purposes. Purposes play a significant role in privacy preservation of database management systems. It is useful for internal access control within an organization as well as information sharing between organizations. This model does not support for role-based access control mechanism.

P.Colombo and E.Ferrari [3] proposed the framework for automatic generation of enforcement monitors for purpose and role-based privacy policy and their integration into DBMS. This model regulates the execution of SQL queries based on purpose and role-based privacy policies. In this, DBMS should regulate accesses to the database on the compliance of the objectives for which data are processed with those for which they are collected. This model also does not support for action aware policies.
P.Colombo and E.Ferrari [4] proposed model which performs runtime enforcement of privacy policies that include obligations within relational database management systems. This model should monitor, block or modify the execution of SQL commands by the access complies with the obligations defined by the accessed data. Privacy policies are specified regarding users/roles, actions, purposes, and conditions. This model does not support for action aware policies.

M.Jafari, P.W.Fong, R.Safavi-Naini, K.Barker, and N.P.Sheppard [5] proposed model which enforces purpose based privacy policies in a business system. The purpose of an action is determined by its situation within other inter-related actions. Actions and their relationships can be modeled by action graph which is based on business processes in a system. Purpose of access is one of the major components in privacy preservation which consider users data as a key factor in access control decisions.

P.Colombo and E.Ferrari [6] proposed model which supports aware action purpose based access control within relational database management system. It allows regulating the access to data performed by SQL queries based on access purpose of query and category of data. It supports policy specification and enforcement. The enforcement is achieved through query rewriting. It does not support for role based access control.

M. Kabir, H. Wang, and E. Bertino [7] proposed model extract more information from customers by providing secure policies. A role-involved conditional purpose-based access control (RCPBAC) allows users to use some data for certain purpose with conditions. This access control can be used for internal access control within the organization as well as information sharing between organizations. This model also does not support for action aware policies.

3. System Design

The system architecture is as follows-

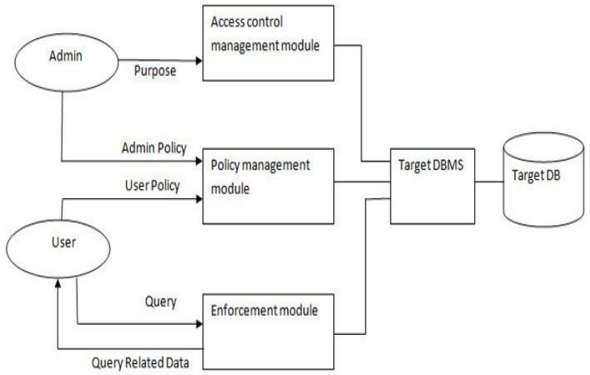


Figure 1. System Architecture

The system composed of following modules-

1) Access Control Management Module
2) Policy Management Module
3) Enforcement Module

Access Control Management Module

Access control management module defines the set of purposes which are helpful in data privacy. To maintain the quality and privacy of data, there must be proper authorization. So it also specifies authorization based on purposes and roles to validate user and admin. Different roles and purpose set are created required for policy specification. It also classifies the data which regulates access control into different data categories. The different data categories are identifier data, quasi-identifier data, sensitive data and generic data. The identifier data allow the user to direct access to data. The quasi-identifier data can be accessed by joint access with external data. The sensitive data is not disclosed to any user as it is confidential. The generic data is any other data which does not belong to a category mentioned above.

Policy Management Module

Policy Management module provides policy specification requests. The proper policies manage the

execution of queries on the accessed data. The different policies are assigned to roles and purposes. The module allows accessing the data jointly by joint access constraints. Privacy policies are specified regarding users, purposes, and roles. When a user tries to access the data from the system, then user policies are compared with the policies assigned to their role and purpose.

Enforcement Module

Enforcement module enforces access control using SQL query rewriting. The original SQL query is parsed, and then it is modified or rewritten according to role and purpose. It also monitors, block or modifies the execution of SQL queries. It ensures that SQL queries are executed in such a way that the purposes for which data are processed comply with the purposes for which they are collected, and the user who requests the query execution belongs to a role that has been authorized to the processing.

4. Implementation

Algorithm for Parsing SQL Query

The SQL query is breaking down into different components is as follows-

1. Replace "; " by " " in SQL query.
2. To check whether SQL query is valid or not, check the length of the query. If the length of the query is less than SELECT clause then it is invalid query otherwise it is a valid query.
3. Check the index of FROM clause to get the column names. If the index of FROM is -1 then returns the error else get the column names.
4. To get the table name, find the index of WHERE clause. If the index of WHERE clause is -1 then table names are present between FROM clause to the end of SQL query, otherwise it is present the FROM clause and WHERE clause.
5. If WHERE clause is present then search for different clauses like having, order by, group by, etc. to get the condition. So if the index of having/ order by / group by is not -1 then substring between WHERE clause to the end of query gives the condition.

Algorithm for SQL Rewriting

The SQL Query rewriting works as follows-

1. Initialize the rewritten query to SELECT clause.
2. As per purpose and role, take the available columns and accessible tables from "Accessible_Columns" and "Accessible_Table" tables respectively.
3. During the parsing of SQL Query, the columns and tables are stored in TABLE_NAME and COLUMNS.
4. Do policy matching by comparing COLUMNS with Accessible_Column and select Only matching columns from COLUMNS table. Append this column names to SELECT clause.
5. Append FROM clause to initialized rewritten query.
6. Do policy matching to get table names. So that compares TABLE_NAMES with "Accessible_Table" table. Append this table names after FROM clause.
7. Append the condition for which WHERE clause is appended after the table names.
8. After appending the WHERE clause, simply append the condition according to role and purpose to the rewritten query.

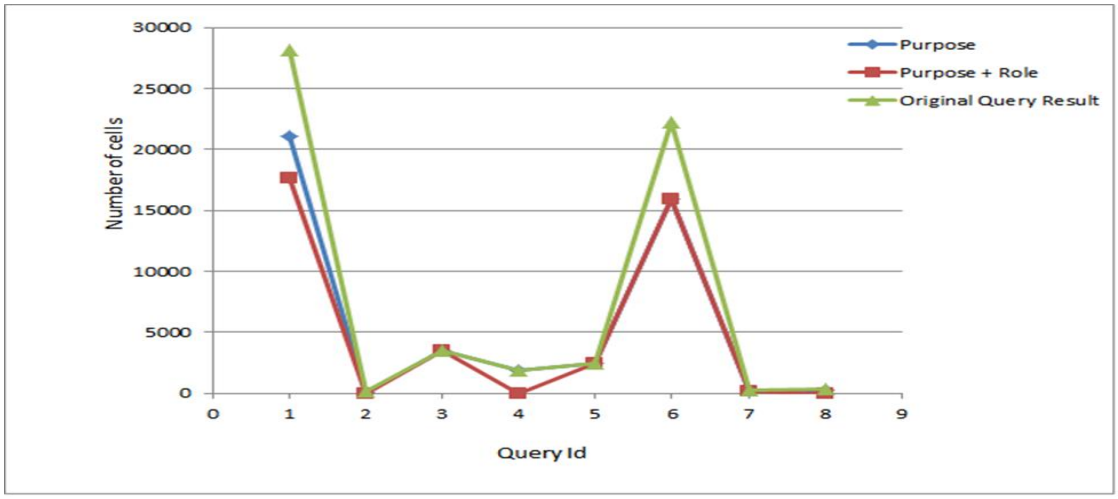
5. Experimental Result

The program is implemented in JAVA. The experiments are carried out using NetBeans 8.1 with MySQL Workbench database on a single machine with windows 7 operating system. The database consists of college domain records. Student, Exam, Result, Placement tables are present in the database. Following queries are executed on the same database-

Query Id	Query
1	select * from student
2	select * from placement
3	select count(roll_no) from student
4	select distinct DOB from student
5	select count(city) from student where a not city like 'Michal karanji.'
6	select roll_no, first_name,middle_name,last_name,city,caste,mob_no from student where not roll_no like '%cmpn%'
7	select first_name, middle_name, last_name, prn, exam_type from student,exam,appear where student.roll_no = appear.roll_no and exam.exam_no = appear.exam_no
8	select first_name, middle_name, last_name,city,mob_no, com_nm, com_add, sal from student, placement,place where student.roll_no = place.roll_no and placement.com_id = place.com_id

Table: Sample Queries

We have identified following statistics for Clerk role and Student Information purpose.



From the result, it is observed that some records accessed by considering the purpose and role-based access control are less than some records accessed by original and purpose based access control query result. The system is more secure than the previous one.

6. Conclusion

This paper control into RDBMSs. The framework regulates the access to the data performed by SQL queries based on the role and access purposes of the query to be executed and category of the data. It supports to specify policies and enforcing them. SQL query rewriting achieves the enforcement based on role and purpose of the user. The future work includes- i) Conditional purpose based access control ii) Support for big data

References

1. J.Byun and N.Li, "Purpose based access control for privacy protection in a relational database system," VLDB J., vol.17, no.4, pp. 603–619, 2008.

2. M.E.Kabir and H.Wang, "Conditional purpose based access control model for privacy protection," in Proc. 20th Australian Conference Australian Database, 2009, vol.92, pp. 135–142.

3. P.Colombo and E.Ferrari, "Enforcement of purpose based access control within relational database management systems," IEEE Transactions Knowledge Data Engineering, vol.26, no.11, pp.2703-2716, Nov 2014.

4. P.Colombo and E.Ferrari, "Enforcing obligations within relational database management systems", IEEE Transactions Dependable secure computing, vol.11, no.4, pp.318-331, Jul/Aug 2014.

5. M. Jafari, P. W. Fong, R. Safavi-Naini, K. Barker, and N. P. Sheppard, "Towards defining Semantic foundations for purpose-based privacy policies," in Proc. 1st ACM Conf. Data Appl. Security Privacy, 2011, pp. 213-224.

6. P.Colombo and E.Ferrari, "Efficient enforcement of action-aware purpose-based access control within relational database management systems," IEEE Transaction Knowledge Data Engineering, vol. 27, no.08, pp. 2134-2147, Aug 2015.

7. M. Kabir, H. Wang, and E. Bertino, "A role-involved conditional purpose-based access control model," in E-Government, E-Services and Global Processes, series IFIP Advances in Information and Communication Technology, vol. 334, M. Janssen, W. Lamersdorf, J. Pries-Heje, and M. Rosemann, Eds. Springer, 2010.

8. V.Nikitha, P.Jhansi , K.Neelima and D.Anusha ," Data sets preparing for Data mining analysis by SQL Horizontal Aggregation,"

International Journal of Computer Engineering In Research Trends.,vol.3,no.9,pp. 225-229,2014.

9. Neelima Kuderu, Dr. Vijaya Kumari," Relational Database to NoSQL Conversion by Schema Migration and Mapping ,"International Journal of Computer Engineering In Research Trends.,vol.3,no.9,pp. 506-513,2016.

10. Jollu Jayachandrudu,M.Sri lakshmi,Dr.S.Prem Kumar," Enhanced Independent Access to Encrypted Cloud Databases ,"International Journal of Computer Engineering In Research Trends.,vol.2,no.9,pp. 589-593,2015.

