International Journal of Software Innovation
Volume 8 • Issue 1 • January-March 2020

Use of Purpose and Role Based Access Control Mechanisms to Protect Data Within RDBMS

Suraj Krishna Patil, D.K.T.E. Society's Textile and Engineering Institute, Ichalkaranji, India

Sandipkumar Chandrakant Sagare, D.K.T.E. Society's Textile and Engineering Institute, Ichalkaranji, India

Alankar Shantaram Shelar, D.K.T.E. Society's Textile and Engineering Institute, Ichalkaranji, India

ABSTRACT

Privacy is the key factor to handle personal and sensitive data, which in large chunks, is stored by database management systems (DBMS). It provides tools and mechanisms to access and analyze data within it. Privacy preservation converts original data into some unknown form, thus protecting personal and sensitive information. Different access control mechanisms such as discretionary access control, mandatory access control is used in DBMS. However, they hardly consider purpose and role-based access control in DBMS, which incorporates policy specification and enforcement. 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 to resources based on purpose for which data can be accessed. It regulates execution of queries based on purpose. The PuRBAC system uses the policies of both, i.e. PuBAC and RBAC, to enforce within RDBMS.

KEYWORDS

Access Control, Privacy, Purpose, Query Rewriting, Role

1. INTRODUCTION

Nowadays, the large chunks of personal and sensitive data of individuals are stored and processed through online surveys and online product purchases. The organizations handling such data must take care of the privacy of individuals. Privacy preservation is the main requirement in processing personal and sensitive data (Byun & Li, 2008; Kabir & Wang, 2009; Colombo & Ferrari, 2014). 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 with access control is that each database user gets access to a subset of databases to which they can query and get data that they required.

For any Information Management System, the major requirement is protecting the information and resources from unauthorized users. The organizations that handle such sensitive information must take care of the privacy of individuals. The privacy-preserving is the key requirement in processing personal and sensitive data (Byun & Li, 2008; Kabir & Wang, 2009; Colombo & Ferrari, 2014). The

DOI: 10.4018/IJSI.2020010105

privacy preservation is the prerequisite in exchanging information. The main objective of privacy preservation is to transform original data into some anonymous form to protect sensitive information. To achieve data privacy, it is necessary to identify the type of information that is going to be protected and where that information is exposed.

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 (Colombo & Ferrari, 2014). Purpose of access is one of the major components in privacy which considers data as a key factor in access control decisions (Jafari et al., 2011). 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 (Colombo & Ferrari, 2015). It enforces fine-grained access control on the basis of 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.

The Purpose and Role Based Access Control (PuRBAC) model helps in bridging the gap between security and privacy-oriented data protection (Colombo & Ferrari, 2015). The Purpose Based Access Control (PuBAC) allows system access to the users based on the purpose for which they are accessing the data. The Role Based Access Control (RBAC) allows system access only to authorized users. RBAC gives privileges to the users based on their role in the organization. The PuBAC and RBAC together will enforce fine-grained access control on basis of purpose of access, actions executed by SQL (Structured Query Language) queries on accessed data, categories of data and role of the user. It regulates the execution of SQL (Structured Query Language) queries based on purpose and role-based privacy policies. Only authorized and authenticated users can access the data from the system. 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 access to resources (Kabir et al., 2010). The Role Based Access Control (RBAC) regulates 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.

Data is an important asset for any organization. Loss of information can lead to direct or indirect losses. So, Privacy is a key requirement in the applications that collect and process personal and sensitive data of individuals. Preserving the privacy and providing access control mechanisms to achieve security is a need for database management systems (DBMS). To maintain data quality and data privacy we need different access control mechanisms. Providing personal data according to the user purpose for which they are to be used. The purpose to access the data is must be accurate and complete. Access control mechanisms are needed to protect personal and sensitive data from unauthorized access. The PuRBAC model introduces a framework that integrates action aware purpose and role-based access control mechanisms into Relational Database Management Systems. The PuRBAC model is the combination of two existing systems i.e. Purpose Based Access Control (PuBAC) and Role Based Access Control (RBAC). The PuRBAC uses the advantages of both the existing systems and enforces the policies within RDBMS.

2. LITERATURE REVIEW

J. Byun and N. Li (2008) 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