



Data Protection through Access Control Mechanisms: A Survey Paper

Prof. S. K. Patil, Prof.S.B.Bhagate, Prof.P.M.Gavali

Department of Computer Science and Engineering, DKTE's Textile and Engineering Institute,
Ichalkaranji, India

Abstract— *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. There are different access control mechanisms available in database management systems like discretionary access control, mandatory access control, role based access control etc. Discretionary access control mechanism is based on data owner's discretion. In Mandatory access control mechanism user and resources are classified with security labels. In role based access control the data is assigned as per the role of users in organization. Based on sensitivity of data any class of access control can be used in various applications. Data security is the protection of database from unauthorized users. Only the authorized persons are allowed to access the database. The users are allowed to access a part of database i.e., the data that is related to them or related to their department.*

Keywords— *Privacy, Access Control, Sensitive data, Security*

I. 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 in processing the personal and sensitive data [1],[2],[3].The database management system plays a vital role in storing the data. Access Control is any mechanism by which a system grants or revokes the right to access some data, or perform some action. Normally, a user must first Login to a system, using some Authentication system. Next, the Access Control mechanism controls what operations the user may or may not make by comparing the User ID to an Access Control database. 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 get access to subset of 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 helps in bridging the gap between security and privacy oriented data protection[6].It enforces fine grained access control on basis of purpose of access, actions executed by SQL queries on accessed data, categories of data and role of 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) is used to regulate the access to resources based on the roles of individual users within an enterprise. 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 purpose for which data can be accessed. It regulates execution of SQL queries based on purpose. It helps to achieve privacy as well as security of data.

II. METHODOLOGIES OF ACCESS CONTROL MECHANISM

Byun and N.Li [1] proposed the reference purpose based model for relational DBMS which regulates the access based on purpose compliance. In this model, purpose information associated with a given data element specifies the intended use of the data element. A key feature of model is that it allows multiple purposes to be associated with each data element and also supports explicit prohibitions, thus allowing privacy officers to specify that some data should not be used for certain purposes. 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 enforce privacy and enable customers to maintain control over their data. This model works on the conditional purposes. The conditional purpose is applied along with allowed purpose and prohibited purpose. It allow user to use some data with purpose and condition. It uses conditional purpose and the association of different purposes with a data element. 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 database on the compliance of the purposes for which data are processed with those for which they are collected. The privacy is achieved through the PuRBAC module that operates in between user and the database system. Such a module intercepts all kinds of storage and processing requests issued by users and handles them according to purpose based privacy policies. 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 on the basis of the access complies with the obligations defined for the accessed data. Privacy policies are specified in terms of 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 support action aware purpose based access control within relational database management system. The proper policies should be defined to regulate the execution of queries based on the actions (i.e., combinations, aggregations, filtering) that are executed on data. It allows regulating the access to data performed by SQL queries based on access purpose of query and category of data. Data can be characterized by different sensitivity levels like identifier, quasi identifier, sensitive, generic etc. An access control model is proposed to regulate the access to data performed by SQL queries based on: the access purposes of the query to be executed, the types of actions that the query should execute on data, and the categories of the data jointly accessed during the execution. On the basis of category of data the access can also be provided. 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 extracts 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 useful for internal access control within organization as well as information sharing between organizations. This model also does not support for action aware policies.

III. MODELS

A. Access Control Models

This performs the following tasks-

- a) Defining set of purposes which are used in policy specification and enforcement
- b) Specifying purpose based authorizations for validating user and administrator
- c) Classifying data into different data categories used for access control purposes e.g. Identifier, Quasi identifier, Sensitive and Generic

This Module defines the set of purposes which are helpful in policy specification and its enforcement for data privacy. To maintain the quality and privacy of data there must be proper authorization. The unauthorized user can misuse the data which violates the privacy of individual. This module will specify authorization based on purposes to validate user and admin. The module also classifies the data which regulates access control. The different data categories are identifier data, quasi identifier data, sensitive data and generic data. Identifier data allow to directly identifying personal data. Quasi identifier identifies personal information by accessing all elements in set together along with some external data. Sensitive data is those data which collects individual's personal information. Generic data collects information that does not belong to any other categories [6].

B. Policy Management Module

Policies specify for which purpose the data can be accessed, type of actions that can be executed on data & categories of data that can be jointly accessed. Policies are fine grained i.e. they refer to single data item in each tuple. This module provides policy specification requests (e.g. add policy, add/edit action type) as well as handle updates if set of purposes are modified. Both user and admin policies are defined in this module. It just manages the policies of user and admin. The proper policies manage the execution of queries on accessed data. The module allows accessing the data jointly by joint access constraints (e.g.aggregation, combinations, filtering).Privacy policies are specified in terms of users, actions, purposes and roles.

C. Enforcement Module

This module will enforce access control by means of SQL query rewriting. The original SQL query will be modified or rewritten after it passing to query signature model. A query signature model describe types of actions that are performed by query on accessed data. It will allow verifying the compliance of actions performed by queries with the policies specified for accessed data. This module should monitor, block or modify 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 have been authorized to the processing [6].

IV. CONCLUSION

In this article, we discussed different access control models for data protection based on the purpose & role of individuals. We discussed idea of purpose and role in the organizations within relational database management systems. The different access control models regulate the data access by using purpose compliance and role compliance. Based on the category of data present in relational database management system the access to data is also controlled. Data protection provides the secure infrastructure based on access control models. The purpose and role of individual plays an important role in data protection within relational database management systems.

REFERENCES

- [1] J.Byun and N.Li, "Purpose based access control for privacy protection in 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, p
- [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.