Accuracy-Constrained Privacy-Preserving Row Level Access Control Mechanism for Relational Data

Desai Bhoomi A.[1] Rathod Vidhi C.[2] Mrs. Kalyani Adwadkar[3]
[1,2]Student [3]Head of Dept.
[1,2,3]Department of Information Technology
[1, 2,3]Sigma Institute of Engineering Vadodara, Gujarat, India

Abstract— this particular system is used to protect the sensitive data of an organization that they are maintaining in their day to day life. This system prevents the misuse of confidential data from authorized user. Before this system is introduced, Access Control Mechanisms is used that assures only that the authorized information is accessed by the user, However, Confidential information can still be misused by authorized users to compromise the privacy of consumers. This concept of privacy-preservation for sensitive data requires the enforcement of several privacy policies and/or the protection against identity disclosure by satisfying some privacy requirements.

Key words: Access control, privacy, k-anonymity, query evaluation, Anonymization, Privacy preservation

I. INTRODUCTION

Organizations collect and analyze consumer data to improve their services. Access Control Mechanisms (ACM) is used to ensure that only authorized information is available to users. However, sensitive information can still be misused by authorized users to compromise the privacy of consumers. The privacy protection mechanism ensures that the privacy and accuracy goals are met before the sensitive data is available to the access control mechanism. The permissions in the access control policy are based on selection predicates on the QI attributes. The policy administrator defines the permissions along with the imprecision bound for each permission/query, user-to-role assignments, and role-to permission assignments.

II. ACCESS CONTROL FOR RELATIONAL DATA

A. *Table level Access Control Mechanism:*

1) Tuple Level:

When evaluating user queries, assume a model called Truman. In this model, a user query is modified by the access control mechanism and only the authorized tuples are returned.

2) Column level:

It allows queries to execute on the authorized column of the relational data only

3) Cell level:

It is implemented by replacing the unauthorized cell values by NULL values [3].

B. *Role-based Access Control:*

Fig. 1: Role Based Access Control

The permissions on objects based on roles in an organization.

1) U = user1, user2, user3 where U is a set of Users.
2) R = role1, role2, role3 where R is a set of Roles.
3) P = permission1, permission2, permission3 where P is a set of Permission [3].

C. *Attributes:*

1) Identifier:

Attributes which is uniquely identify an individual. These attributes are completely removed from the anonymized relation [1].

2) Quasi-identifier (QI):

Attributes, that can potentially identify an individual based on other information available to an adversary. QI attributes are generalized to satisfy the anonymity requirements [3].

3) Sensitive attribute:

Attributes that if associated to a unique individual will cause privacy breach [1].

D. *Anoymity Definitions:*

1) Equivalence Class (EC):

It is a set of tuples having the same QI attribute values [3].

2) K-anonymity Property:

An anonymized table satisfies the k-anonymity property if each equivalence class has k or more tuples [3].

3) Query Imprecision:

Difference between the numbers of tuples returned by a query evaluated on an anonymized relation and the number of tuples for the same query on the original relation [3].

4) Query Imprecision Bound:

It is the total imprecision acceptable for a query predicate and is preset by the access control administrator.

5) Query Cut:

The splitting of a partition along the query interval values. For a query cut using Query, both the start of the query interval and the end of the query interval are considered to split a partition along the dimension [1].

Select randomly queries and store it into Query Cut set and divide it into equal intervals which are called Uniform Query set [3].

III. PRIVACY PROTECTION MECHANISM

PPM ensures that the privacy and accuracy goals are met before the sensitive data is available to the access control mechanism.

A. *Privacy Protection Module:*

It anonymizes the data to meet privacy requirements and imprecision constraints on predicates set by the access control mechanism [1].

B. *L-diversity:*

It is a form of group based anonymization that is used to preserve privacy in data sets by reducing the granularity of a data representation. This reduction is a tradeoff that results in some loss of effectiveness of data management or mining algorithms in order to gain some privacy [2].

C. K-anonymity:

A table T_ satisfies the k-anonymity property if each equivalence class has k or more tuples [1].

IV. PURPOSE

This particular system is used to protect the sensitive data of an organization that they are maintaining in their day to day life, so this system prevents the misuse of confidential data from authorized user. This system is useful for the organization which works on Database and primary need is to provide the role based security on database. Also provides privacy preservation on confidential data of organization.

V. PROPOSED SYSTEM

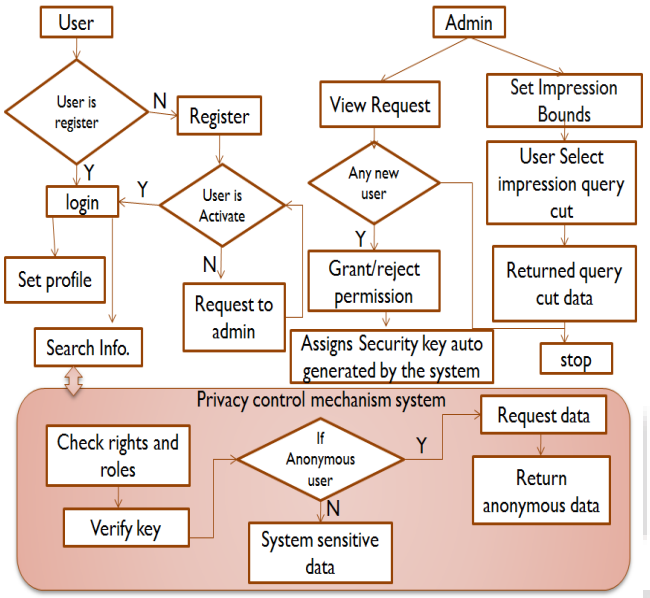

Fig. 3: System flow

First of all the users within the organization register themselves in the system and the registration request goes to admin. Only after the admin grant the permission user will be able to login into the system.

After logging into the system users can set their profile or search for the information. At the time when user requests for information the system check rights and role of that user if he/she has rights to access the requested information the key will be verified and based on that the system will give an access to either sensitive information or an anonymous data within their imprecision bound. This key will be auto generated by the system when admin grants the permission.

VI. CONCLUSION

An accuracy-constrained privacy-preserving access control framework for relational data has been proposed. The framework is a combination of access control and privacy protection mechanisms. The access control mechanism allows only authorized query predicates on sensitive data. The privacy preserving module anonymizes the data to meet privacy requirements and imprecision constraints on predicates set by the access control mechanism.

REFERENCES

[1] Zahid Pervaiz, Walid G. Aref, Senior Member, Arif Ghafoor, Fellow, and Nagabhushana Prabhu, "Accuracy-Constrained Privacy-Preserving Access Control Mechanism for Relational Data", IEEE TRANSACTIONS, VOL. 26, NO. 4, APRIL 2014.

[2] Ankitha.N.Kulkarni, Ashwini.S, Vidhyashree.S, Chandrashekar. "K.TAccuracy-Constrained Privacy-Preserving Access Control Mechanism for Health Care Systems",IJARCCE *Vol. 4, Issue 5, May 2015*

[3] Madhuri S. Lambe, Vrunda K. Bhusari," Accuracy-Constrained Privacy-Preserving Cell Level Access Control Mechanism for Relational Data", Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

[4] B. Fung, K. Wang, R. Chen, and P. Yu, "Privacy-Preserving Data Publishing: A Survey of Recent Developments", *ACM Computing Surveys*, vol. 42, no. 4, article 14, 2010.

[5] Machanavajjhala, D. Kifer, J. Gehrke, and M. Venkitasubrama- niam, "L -Diversity: Privacy Beyond k-anonymity," *ACM Trans. Knowledge Discovery from Data*, vol. 1, no. 1, article 3, 2007.

[6] P. Samarati, "Protecting Respondents' Identities in Microdata Release," *IEEE Trans. Knowledge and Data Eng.*, vol. 13, no. 6, pp. 1010-1027, Nov. 2001.

[7] S. Chaudhuri, R. Kaushik, and R. Ramamurthy, "Database Access Control & Privacy: Is There a Common Ground?" Proc. Fifth Biennial Conf. Innovative Data Systems Research (CIDR), pp. 96-103, 2011.

[8] T. Iwuchukwu and J. Naughton, "K-Anonymization as Spatial Indexing: Toward Scalable and Incremental Anonymization," Proc. 33rd Int'l Conf. Very Large Data Bases, pp. 746-757, 2007.

