IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727,
PP 16-19
www.iosrjournals.org

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

M. N. Kale[1], Kunal N. Dhoot[2], Kajal P. Kale[3], Pallavi N. Kale[3], Shraddha S. Rasal[4]

[1,2,34,](Information Technology, Pad .Dr .V .V. Vikhe Patil College of Engineering Ahmednagar / Savitribai Phule Pune University, India)

Abstract : *Access Control Mechanism provide security to information from unauthorized users. Even authorized person may illegally use the data to dispose the privacy of individuals to whom the data belongs to. Privacy Protection Mechanism [PPM] anonymize the relation to prevent identity and attributes disclosure. Privacy Protection Mechanism needs to satisfy the constrained like imprecision bound along with privacy requirements. For satisfy privacy requirements it needs suppression and generalization techniques of anonymization algorithm.*

Our aim is to develop such system that based on anonymization algorithm. The system allows users to retrieve the data based on their roles using Roll Based Access Control. By using trial and error logic for anonymization algorithm, which will results into increase in accuracy rate and minimization of imprecision bound.

Keywords – *Privacy, Data Anonymity, Security, Information Protection.*

I. INTRODUCTION

Group of persons collect and analyze consumer data to improve their services. Access Control Mechanism are used to ensure that only authorized information is available to users. Authorized users can also be illegally use the information, to avoid this, the proposed system provide privacy preservation policies by satisfying some privacy requirements. The database security areas faces various new difficulties. Factors such as the evolution of security concerns, the "disintermediation" of access to data, new computing paradigms and applications, such as grid-based computing and on demand business, have introduced both new security requirements and new contexts in which to apply and possibly extend current approaches.[8]

A PPM can use suppression and generalization of relational data to anonymize and satisfy privacy requirements E.g., k-anonymity [9] and l-diversity [7], against identity and attribute disclosure.

The contributions of the paper are as follows. First, we formulate the accuracy and privacy constraints as the problem of k-anonymous Partitioning with Imprecision Bounds (k-PIB) and give hardness results. Second, we introduce the concept of accuracy-constrained privacy-preserving access control for relational data. Third, we propose heuristics to approximate the solution of the k-PIB problem and conduct empirical evaluation.

II. VIRTUAL PRIVATE DATABASE IN ORACLE9IR2

The Oracle9*i* database builds upon 14 separate security evaluations of its server software.

Oracle7 introduced many features which enabled application developers to limit data access based on well known security concepts, such as "least privilege."[2] The principle of least privilege states that users should have only the minimum allowance set required to perform their jobs, and no more.

These features include:

- Granular privileges as a means of limiting access rights
- Roles to provide ease-of-administration (by encapsulating groups of privileges)
- Views to provide content- or context-based data access
- Stored procedures to enable well-formed business transactions, without direct privilege grants

While many of these features can be used to enforce least privilege, and provide access control at a level greater than table-level these features aren't always well-suited to access control at much finer levels of granularity

The Virtual Private Database (VPD) is the aggregation of server-enforced, fine-grained access control, together with a secure application context in the Oracle9i database server.

It gives a flexible mechanism for building applications that enforce the security policies customers want enforced, only where such control is necessary. By dynamically appending SQL statements with a predicate, VPD limits access to data at the row level and ties the security policy to the table itself.

III. FINE GRAINED AUTHORIZATION THROUGH PREDICATED GRANTS

This system introduced a model for fine-grained authorization based on adding predicates to authorization permissions. This model supports predicated authorization to specific columns, cell-level authorization with nullification, authorization for function execution, and grants with grant option. This model also includes other new features, such as query defined user groups, and authorization groups, which are designed to simplify administration of authorizations. This model is designed to be a strict generalization of the current SQL authorization mechanism [3].

Fine-grained access control, which restricts access to only the information in some rows of a table, and further to only information in certain columns within those rows, is required in practically all database applications. As an example, a HR application has to ensure that employees can see only rows corresponding to their own data, and managers can additionally see some columns (such as salary) of rows corresponding to their employee's data. Fine-grained authorization is traditionally implemented by application programs, with no role for the database system.

Characteristics:

- Clear and simple semantics.
- Compatibility with existing SQL security model, with minimal changes
- The ability to deal with huge numbers of application users, not just a set of constant database users/roles.
- Low impact on existing application code.

This system is designed to meet the above requirements, and has several novel aspects:

- An extension of the SQL authorization grant model to include predicates. Predicates can be applied on any form of grant, including read and update of rows, and execution of functions and procedures. Current SQL authorization is a special case of predicated authorization, with the predicate being “true”.
- Column-level authorization, including variants that allow:

1. Nullification of values based on predicates, which enables cell-level security, and
2. Authorization on aggregates, while restricting authorization on the underlying data.

- Mechanisms to support administration of systems with huge numbers of application users and database objects including

1. Query-defined user groups.
2. Authorization groups, which allow a group of tuples that together constitute a business object to be granted as a unit.

IV. MONDRIAN MULTIDIMENSIONAL K-ANONYMITY

This system offers a new multidimensional Model, which gives an additional degree of flexibility not seen in past (single-dimensional) methods. Often this flexibility leads to great-quality anonymizations, as Measured both by general-purpose metrics and more proper estimation of query answerability.

Optimal multidimensional anonymization is NP-hard. However, system offer a easy greedy approximation algorithm, which shows that this greedy algorithm frequently leads to more desirable anonymizations than exhaustive optimal algorithms for two single-dimensional models.[4]

The essential goal of k-anonymization is to protect the privacy of the individuals to whom the data belongs. However, subject to this constraint, it is important that the released data remain as “useful” as possible. The major addition of this system is new multidimensional recoding model and a greedy algorithm for k-anonymization.

V. K-ANONYMIZATION AS SPATIAL INDEXING: TOWARD SCALABLE AND INCREMENTAL ANONYMIZATION

This paper propose that *k*-anonymizing a data set is remarkably similar to building a spatial index over the data set, so similar as a matter of fact is that classical spatial indexing techniques can be used to anonymized data sets.

Observation with this application recommends the R-tree index-based approach turnout a batch anonymization algorithm that is orders of magnitude more efficient than formerly proposed algorithms and has the improvement of supporting incremental updates. Lastly, it show that the anonymizations generated by the R-tree approach do not sacrifice quality in their search for efficiency; in fact, by several previously observed quality metrics, the compact partitioning properties of R-trees generate anonymizations superior to those generated by previously observed anonymization algorithms.[5]

K-anonymity has been proposed as a means to protecting privacy in data releases. Put simply, the private data set is modified so that each record is identical from at least $k-1$ other records. Identicalness is defined in terms of any set of attributes that can be used to uniquely identify an individual. This set of attributes has been called a *quasi-identifier.*

The main thing in this algorithm is to venture a striking parallel between the "classical" area of database indexing and the almost new data Privacy research domain, *k*-anonymity.

VI. CONCLUSION OF LITERATURE SURVEY

To perform literature survey we had studied, following four system:
1. The virtual private database in oracle 9iR2
2. Fine grained authorization through predicated grants
3. Mondrian multidimensional k-anonymity
4. K-anonymization as spatial indexing: Toward scalable and incremental anonymization

VII. ARCHITECTURE

Access Control Mechanism [ACM] is necessary to obtain secrecy, integrity, and availability goals. This mechanism is illustrated in Fig.1 (arrows represent the direction of information flow).

The privacy protection mechanism ensures that the privacy and accuracy objectives 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 Quasi-Identifier (QI) attributes. The policy administrator define the permission along with the imprecision bound for each permission/query, user-to-role assignment, and role-to permission assignment. The presence of the imprecision bound ensures that the authorized data has the desired level of accuracy. The imprecision bound information is not shared with the users because knowing the imprecision bound can result in violating the privacy requirements. The privacy protection mechanism [PPM] is required to meet the privacy requirement along with the imprecision bound for each permission [1].

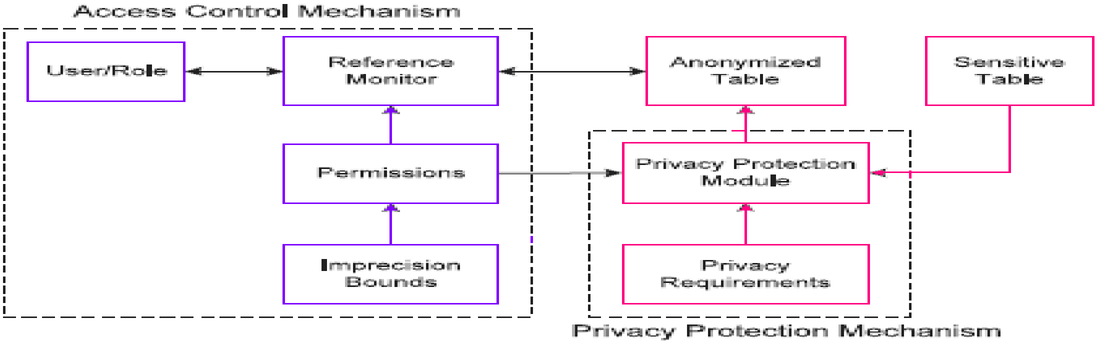

Fig.1 Accuracy Constrained Privacy-Preserving Access Control Mechanism

The Access Control Enforcement by reference monitor can be of the following two types:
1. Relaxed
2. Strict

This system focuses on relaxed enforcement. However the proposed s for anonymization are also applicable for strict enforcement because the proposed heuristics minimize the overlap between partitions and queries.

VIII. ALGORITHM 1: TOP DOWN HEURISTIC 1 (TDH1)

The objective of Top-Down Selection Mondrian (TDSM) is to minimize the total imprecision for all queries while the imprecision bounds for queries not considered. In TDSM, consider a partition that overlaps a query. In this TDH1 heuristic, we propose to distribute the partition along the query cut and after that choose the dimension along which the imprecision is minimum for all queries. The query used for the cut needs to selected, if multiple queries overlap a partition. If imprecision is greater than zero for the partition that are sorted based on imprecision bound and query with minimum imprecision bound is selected.

In Top-Down Heuristic 1(TDH1) algorithm, first whole tuple space is added to the set of candidate partitions. Next, in the query overlapping the candidate partitions with minimum imprecision bound and imprecision greater than zero is selected. In while loop, checks for a possible split of the partition along query intervals. If possible cut is found, then resulting partition are added to candidate partition, else the candidate partitions is checked for median cut.

IX. ALGORITHM 2: TOP DOWN HEURISTIC 2 (TDH2)

In Top-Down Heuristic 2(TDH2) algorithm, the query bounds are updated when partitions are added to the output.

In Top-Down Heuristic 2(TDH2) algorithm, the concept of depth first (preorder) traversal is used. Initially prefer the queries which is smaller bounds. Initially, the tuple space is added to the set of candidate partition. There are two difference in TDH1 and TDH2.First, the depth-first tree traversal for the 'for' loop is preorder. Second, when partitions are added to the output, the query bounds are updated.

X. CONCLUSION

The access control mechanism allows only authorized query predicates on sensitive data. The privacy preserving mechanism anonymizes the data to meet privacy requirements and imprecision constraints on predicates set by the access control mechanism [ACM].

REFERENCES

[1] "Accuracy-Constrained Privacy-Preserving Access Control Mechanism for Relational Data" Zahid Pervaiz, Walid G. Aref, Senior Member, IEEE, Arif Ghafoor, Fellow, IEEE, and Nagabhushana Prabh.

[2] K. Browder and M. Davidson, "The Virtual Private Database in oracle9ir2," Oracle Technical White Paper, vol. 500, 2002.

[3] S. Chaudhuri, T. Dutta, and S. Sudarshan, "Fine Grained Authorization through Predicated Grants," Proc. IEEE 23rd Int'l Conf. Data Eng., pp. 1174-1183, 2007.

[4] K. LeFevre, D. DeWitt, and R. Ramakrishnan, "Mondrian Multidimensional K-Anonymity," Proc. 22nd Int'l Conf. Data Eng., pp. 25- 25, 2006.

[5] 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.

[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] A. 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.

[8] E. Bertino and R. Sandhu, "Database Security-Concepts, Approaches, and Challenges," IEEE Trans. Dependable and Secure Computing, vol. 2, no. 1, pp. 2-19, Jan.-Mar. 2005.

[9] "Approximation Algorithms for k-Anonymity" Gagan Aggarwal,Tomas Feder,Rajeev Motwani,Rina Panigraphy.