Scientific Journal Impact Factor (SJIF) : 1.711
International Journal of Modern Trends in Engineering and Research
ISSN (ONLINE) : 2349 - 9745 ISSN (PRINT) : 2393 - 8161

AN EFFECTIVE FRAMEWORK FOR EXTENDING PRIVACY-PRESERVING ACCESS CONTROL MECHANISM FOR RELATIONAL DATA

Morla Dinesh[1], Shaik. Jumlesha[2]
[1]*M.Tech (S.E), Audisankara College Of Engineering &Technology*
[2]*M. Tech (C.S.E), Audisankara College Of Engineering &Technology*

Abstract - User may have to compromise the privacy of data or info. The privacy preservation will be achieved through anonymization techniques like generalization or suppression. Beside privacy the exactness of the licensed information is vital. The aim of the work is to bring in higher security and minimum level of exactness to the retrieved information, for that during this paper an effective framework for extending privacy preserving access control mechanisms enforced with extra constraint on every selection predicate known as in precision bounds. New approaches to prevent the misuse of sensitive data by the approved users and bring in each privacy and security of the sensitive data. New approach has investigated privacy-preservation from the anonymity aspect. The access control mechanisms and privacy preservation mechanisms defend the info from unauthorized or third party user. Once there's a lack in privacy preserving mechanism (PPM) and information is shared with others, the licensed visualize extending the planned privacy-preserving cell level access control. Today's quick growing world, the malicious intent or hacking purpose as well increasing. Thus there's a desire to supply a higher security to our system.

Keywords: k-anonymity, privacy preserving, Access control

I. INTRODUCTION

ORGANIZATIONS collect and analyze consumer information to boost their services. Access Control Mechanisms (ACM) is used to ensure that only authorized information is available to users. However, sensitive data will still be misused by licensed users to compromise the privacy of consumers. The concept of privacy-preservation for sensitive data can require the enforcement of privacy policies or the protection against identity disclosure by satisfying some privacy requirements [1]. During this paper, we investigate privacy-preservation from the anonymity aspect. The sensitive information, even after the removal of identifying attributes, is still liable to linking attacks by the licensed users [2]. Anonymization algorithms make use of suppression and generalization of records to satisfy privacy requirements with minimum distortion of micro data. The anonymization techniques [3], [4] can be used with an access control mechanism to make sure both safety and privacy of the sensitive information. The privacy is achieved at the cost of accuracy and imprecision is introduced in the authorized information under an access control policy. We use the concept of imprecision bound for each permission to define a threshold on the amount of imprecision that can be tolerated. The heuristics planned in this paper for extending privacy-preserving access control are also related in the environment of workload-aware anonymization. The anonymization for uninterrupted data publishing has been studied in literature [5]. During this paper the spotlight is on a static relational table that is anonymized only once. To show our approach, role-based access control is supposed. However, the concept of accuracy constraints for permissions can be applied to any privacy-preserving protection policy, e.g., discretionary access control.

II. BACKGROUND

Based on anonymity, role-based access management and privacy definitions supported anonymity is over-viewed. Query evaluation semantics, inexactness, and therefore the Selection Mondrian algorithm [3] are explained.

A relation T = {A1;A2; : : : ;An} where Ai is an attribute, T* is the anonymized translation of the relation T. Consider T is a static relational table. The attributes can be of the following types:

- Identifier: Attributes which is uniquely determine a personal. These attributes are totally removed from the anonymized relation.
- 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.
- Sensitive attribute: Attributes, that if associated to a unique individual will cause a privacy breach.

A) Anonymity Definition

- **Equivalence Class** (EC): It is a set of tuples having the similar QI attribute values.
- **K-anonymity Property:** An anonymized table satisfies the k-anonymity property if each equivalence class has k or more tuples [2].
- **Query Imprecision:** variation between the number of tuples returned by a query evaluated on an anonymized relation and the amount of tuples for the same query on the original relation.
- **Query Imprecision Bound:** It is the total imprecision satisfactory for a query predicate and is fixed by the access control administrator.
- **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.

III. ACCURACY CONSTRAINED PRIVACY PRESERVING ACCESS CONTROL

An accuracy-constrained privacy-preserving access control mechanism, illustrated in Fig1. (Arrows represent the direction of data flow), is proposed. The privacy protection mechanism ensures that the privacy and accuracy goals are met before the sensitive information is accessible to the access control mechanism. The permissions within the access management policies are supported choice predicates on the QI attributes. The policy administrator defines the permissions beside the imprecision bound for every permission/query, user-to-role assignments, and role-to permission assignments [6].

The specification of the imprecision bound ensures that the accepted information has the desired level of accuracy. The imprecision bound information isn't shared with the users as a result of knowing the imprecision bound could end up in violating the privacy demand. The privacy protection mechanism is needed to fulfil the privacy demand at the side of the imprecision bound for every permission.

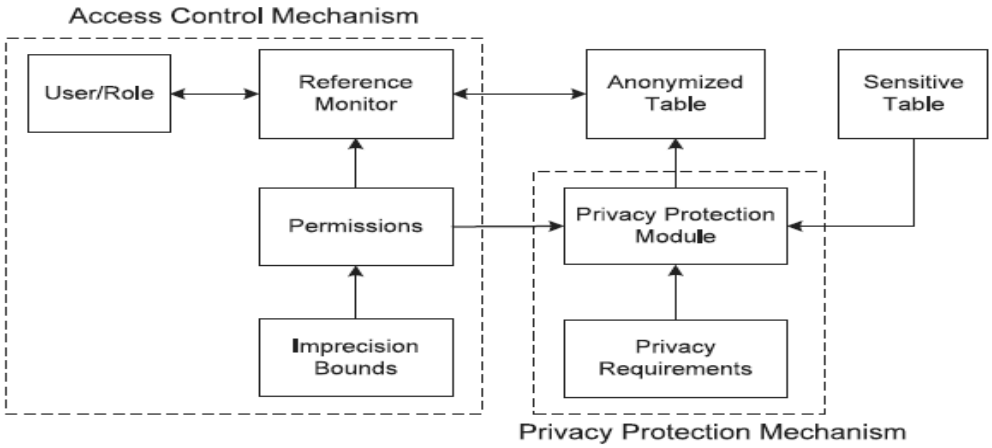

Fig 1: Accuracy-constrained privacy-preserving access control mechanism.

A). Access Control Enforcement

The correct tuple values in a relation are replaced by the generalized values subsequent to the anonymization process. During this case, access control enforcement over the generalized data has to be defined.

- *Relaxed*: Use overlap semantics and let access to all or any partitions that are overlapping the permission.
- *Strict*: Use enclosed semantics to authorize access to exclusively those partitions that are totally encircled by the permission.

Both of these schemes have their own strengths and weaknesses. Relaxed enforcement violates the authorization predicate by giving access to additional tuples on the other hand it is helpful for applications where low cost of a warning is tolerable as compared to the risk related to a missed event. On the other hand, strict enforcement is appropriate for applications where a high risk is related to a false alarm as compared to the value of a missed event. Associate example could be a false arrest just in case of breaking and entering. During this paper, the focal point is on relaxed enforcement. But the planned strategies for anonymization are valid for strict enforcement because the considered heuris-tics decrease the overlap between partitions and queries. We have a tendency to any assume that under relaxed enforcement if the imprecision bound is violated for permission then that permission isn't assigned to any role.

B). Probabilistic Analysis for Access Control Enforcement

During this section, the relaxed management of access control is analyzed probabilistically. The access management policy administrator sets the imprecision bound for every query and needs that the imprecision bound for the smallest amount of queries be desecrated by PPM. The policy administrator would possibly revise the imprecision bounds for queries and further relax the access management policy if it's recognized with a high chance that an outsized range of queries be able to breach the bounds and access requests for roles are going to be denied.

IV. PROPOSED ENHANCEMENTS

An Effective Framework for Extending Privacy-Preserving Access Control Mechanism for Relational Data is an amalgamation of access control and privacy protection mechanisms. Individual sensitive information is simply inferred by an attacker. Defending data privacy is a vital problem, in micro-data sharing. Anonymization is to defend entity privacy, with negligible impact on the quality of the ensuing information. This framework construct an anonymous outlook based on an objective class of workloads, consisting of one or more data processing tasks and selection predicates. The benefit of anonymity is resisting the attacker's inference attacks. Access control mechanism for relational data is made with the privacy preservation based model. Role Based Access Control

(RBAC) idea protects the sensitive data with minimum imprecision values. K-Anonymity model is integrated with minimum imprecision based data access control mechanism. Privacy preserved data access control mechanism is improved with incremental mining model and cell level access control. The proposed approach reduces the imprecision rate in query processing. Access control mechanism is personalized for incremental mining model. Time complexity is reduced in the proposed approach. The planned approach provides the dynamic policy management mechanism.

A).Table Level Access Control Mechanism

- *Tuple*: while evaluating user queries, suppose a model called Truman [10]. During this model, a user query is customized by the access control mechanism and exclusively the approved tuples are returned.
- *Column*: It permits queries to execute on the authorized column of the relational data only [11], [7].
- *Cell:* It is enforced by substituting the unauthorized cell values by NULL values [9].

B).Role Based Access Control

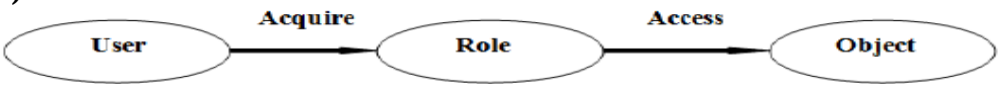

Fig 2: Role based access control

The permissions on objects based on roles in an organization.

- U = user1, user2, user3 where U is a set of Users.
- R = role1, role2, role3 where R is a set of Roles.
- P = permission1, permission2, permission3 where P is a set of Permission.

V. IMPLEMENATION

Access control mechanism for relational data is made with the privacy preservation based model. Role Based Access Control (RBAC) idea protects the sensitive data with minimum imprecision values. K-Anonymity model is integrated with minimum imprecision based data access control mechanism. Privacy preserved data access control mechanism is improved with incremental mining model and cell level access control. The proposed approach reduces the imprecision rate in query processing.

A).The Access Control Mechanism

The Access control mechanism permits only licensed query predicates on sensitive data.

- *User/Role:* It permits process permissions on objects primarily based on roles in a company. An RBAC is composed of a collection of Users, a collection of Roles, and a collection of Permissions. Assume that the selection predicates on the QI attributes define permission [7]. UA may be user-to-role assignment relation and PA may be role to permission assignment relation. When a user allotted to a task executes a query, the tuples that are used fulfilling the combination of the query predicate and the permission are returned.
- *Permissions:* It is mainly based selection predicates on the QI attributes. The imprecision bound for every query, user-to-role assignments, and role-to permission assignments.
- *Imprecision Bound:* It makes sure that the licensed data has the required level of accuracy. The imprecision bound certain will be accustomed meet the privacy requirements. The privacy protection mechanism is mandatory to fulfil the privacy requirement according to the imprecision bound for every permission [8].

B).Partitioning Algorithm

In this heuristic, we have a tendency to split the partition on the query cut and then select the dimension on that imprecision is minimum for the entire queries. If several queries overlap a partition, at that time the query to be used for the cut needs to be hand-picked. The queries having imprecision greater than zero for the partitions are sorted based on the imprecision bound as well as

the query with least amount imprecision bound is chosen. The intuition behind this call is that the queries with minor bounds include lower tolerance for error and such a partition split ensures the decrease in imprecision for the query with the least imprecision bound.

C).Privacy Protection Mechanism

PPM ensures that the privacy plus accuracy goals are met before the sensitive data is out there to the access control mechanism.

- Privacy Protection Module: It anonymizes the info to satisfy privacy necessities and imprecision constraints on predicates set by the access control mechanism.
- Sensitive Table.

Table 1: Sensitive table

	QI_1	QI_2	S_1
ID	Age	Zip	Disease
1	5	15	Flu
2	15	25	Fever
3	28	28	Diarrhea
4	25	15	Fever
5	22	28	Flu
6	32	35	Fever
7	38	32	Flu
8	35	25	Diarrhea

The Table 1 does not satisfy k-anonymity as a result of knowing the age and postal code of a person i.e. quasi identifier allows associating a disease to that person.

- Anonymous Table

Table 2: Anonymous table

	QI1	QI2	S1
ID	Age	Zip	Disease
1	0-20	10-30	Flu
2	0-20	10-30	Fever
3	20-30	10-30	Diarrhea
4	20-30	10-30	Fever
5	20-30	10-30	Flu
6	30-40	20-40	Fever
7	30-40	20-40	Flu
8	30-40	20-40	Diarrhea

The projected approach gets information in an exceedingly anonymous version of sensitive table. The ID attribute is removed within the anonymized table and is shown just for recognition of tuples. Here, for any combination of selection predicates on the postal code and age attributes, there are minimum of two tuples in each EC.

VI. CONCLUSION

The approach design is a combination of access control mechanism and privacy protection Mechanism. New approach offer information access control to user it suggests that we forestall anonymous user to access private data. If any consumer desires to access information that is secure then he/she wants to lift up the request to the responsible consumer next this consumer send you the key which is used to access his/her data. It strictly forestall anonymous user to access authorized data. The projected approach implemented table level, row level, and cell level access control mechanism. Query set is to access the data and this sets appointed to user for roles and authorization purpose. The access control mechanism permits only authorized query predicates on sensitive information. The privacy preserving module anonymizes the info to get privacy needs. Imprecision bound assessment is optimized. The approach projected privacy-preserving access control to progressive data and dynamic access control. This mechanism reduces the time complexity. The benefit of anonymity is defending against the attacker's inference attacks. For future work we plan to extend the proposed privacy-preserving mechanism for dynamic data.

REFERENCES

1. 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.
2. P. Samarati, "Protecting Respondents' Identities in Microdata Release," IEEE Trans. Knowledge and Data Eng., vol. 13, no. 6, pp. 1010-1027, Nov. 2001.
3. K. LeFevre, D. DeWitt, and R. Ramakrishnan, "Workload-Aware Anonymization Techniques for Large-Scale Datasets," ACM Trans. Database Systems, vol. 33, no. 3, pp. 1-47, 2008.
4. 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.
5. 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.
6. R. Sandhu and Q. Munawer, "The Arbac99 Model for Administration of Roles," Proc. 15th Ann. Computer Security Applications Conf., pp. 229-238, 1999.
7. S. Chaudhuri, T. Dutta, and S. Sudarshan, "Fine Grained Authorization through Predicated Grants", Proc. IEEE 23rd Intl Conf. Data Eng., pp. 1174-1183, 2007.
8. Zahid Pervaiz, Walid G. Aref, Senior Member, IEEE, Arif Ghafoor, Fellow, IEEE, and Nagabhushana Prabhu, Accuracy-Constrained Privacy-Preserving Access Control Mechanism for Relational Data, IEEE Tran. knowledge and Data Eng.,vol.26,n0.4,April 2014.
9. K. LeFevre, R. Agrawal, V. Ercegovac, R. Ramakrishnan, Y. Xu, and D. DeWitt," Limiting Disclosure in Hippocratic Databases", Proc. 30th Intl Conf. Very Large Data Bases, pp. 108-119, 2004.
10. S. Rizvi, A. Mendelzon, S. Sudarshan, and P. Roy, "Extending Query Rewriting Techniques for Fine-Grained Access Control," Proc. ACM SIGMOD Int'l Conf. Management of Data, pp. 551-562, 2004
11. K. Browder and M. Davidson, "The Virtual Private Database in oracle9ir2," Oracle TechnicalWhite Paper, vol. 500, 2002.

