International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 3 Issue: 4 1931 - 1933

Security Management Methods in Relational Data

Suhasini Gurappa .Metri
PG Student, CSE Dept
Cambridge institute of technology ,Bangalore ,India .
Email:suhasini.m1990@gmail.com

Dr. D. R. Shashi Kumar
HOD of CSE
Cambridge Institute of Technology Bangalore,India.
Email:shashikumar.cse@citech.edu.in

Abstract: The paper demonstrate on accuracy constrained privacy-preserving access control mechanism for relation data framework with multilevel anonymization techniaues. Access control policy which define selection predicate on sensitive data and privacy requirement deals with anonymity. As privacy protection mechanism (PPM) provides less privacy protection and the data is shared so the user should compromise the with the privacy of dada.The goal of the paper is to provide more security to the sensitive data along with minimal level of precision. An imprecision bound constraint is introduced on each selection predicate. Accuracy constraints for multiple roles also has been satisfied. Along with the multiple anonymity we can also do encryption of the anonymized data it provid more security.

Keywords: *Access control, Anonymity, privacy preservation*

*****

I. Introduction

Every organization maintain a database for there customer information that information should be secured,some times there is a possibility of misuse of sensitive information from authorized users, so we have to protect sensitive information from the misuse. Privacy preserving mechanism used to protect sensitive data. Organizations implement access control mechanism to assure that only sensitive information is available to authorized users. Sometimes confidential information is misused by authorized users to adjust the privacy of the customer. Organizations collect and analyze the data to improve the services .In this paper going to preserve the privacy by anonymity aspect. After removing the primary keys from the database of particular users ,the sensitive data may suffer from linking attacks from authorized users [6]. To improve the protection against identity discloser and support the privacy policy ,the concept of privacy preservation of sensitive data is introduced by satisfying some privacy requirements [5].In this paper we crosscheck privacy-preservation by anonymity aspect. Every database have to maintain the sensitive information from privacy mechanisms, then also there is possibility that they suffer from linking attacks from authorized users. This problem has been studied in micro data publishing and privacy definitions like k-anonymity[6], l-diversity[3], variance diversity[2]. Anonymization algorithm uses suppression or generalization of records to satisfy the privacy requirement with minimal distortion of micro data.

While Accessing information from database ,the concept of imprecision bound is introduced in every access from database to solve the problem of where minimal level of tolerance is defined for each access query. Present workload aware anonymization methods minimize the imprecision aggregate for all query/permission.

The concept of satisfying the accuracy constraint for individual permissions in a policy or workload has not been studied before. Accuracy constrained privacy preserving access control mechanism relevant in the workload–aware anonymization. The concept of continuous data publishing has been also discussed. Many access control mechanisms are there to deal with relational database. Role-based Access Control that allows defining permission on object based on roles in an organization.

II. Literature Survey

While access data from database it is important to implement few access control mechanisms. It allows only authorized users can have the access to database. Along with the access control mechanism there is an imprecision bound for each permission/query, it guarantees that only sensitive data will be available to users.

Anonymization techniques are used to maintain the privacy of information/data. Some of privacy terms as follows

Equivalence Class(EC): An equivalence class is a set of tuples having the same Quasi-identifiers(QI) attribute values.

k-anonymity Property: A table T* satisfies the k-anonymity property if each equivalence class has k or more tuples[6].

k-anonymity is above to homogeneity attacks when all tuples in an equivalence class is having the same sensitive value. To overcome this problem *l*-diversity has been proposed [3] there should be at least *l* distinct values of the sensitive attributes in an each equivalence class T*. For sensitive numeric attributes an l-diverse equivalence class can still leak information if the numeric values are close to each other [2]. To overcome this problem variance diversity

 ISSN: 2321-8169
1931 - 1933

has been proposed. In this variance of each equivalence class to be greater than a given variance diversity parameter.

We may access Relation Data in many ways ,fine grained access control for relational data eg., SQL [7], For evaluating users queries, most concepts attain a Truman model [4]. Cell level access control for Relational dada [9].

Role-based access control (RBAC) allow addressing permissions/query on objects based on roles in an company/organization. In role based access control many can have the same role. Structure of role based access control as follows it consist of set of roles(R),set of users(U),set of permissions/query(P) [8] .

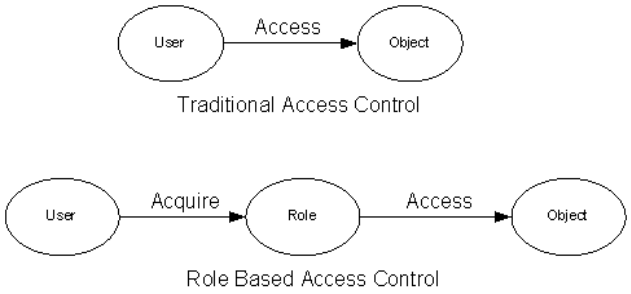

Figure. 1 .Framework of RBAC

We know how privacy preserving access control mechanism works [1] this framework is a combination of access control mechanism and privacy preserving mechanism. Access control mechanism assures that only authorized user have access permission on sensitive data and it provide the confidentiality of the data. Privacy preserving module anonymizes the sensitive data based on imprecision bound and conditions from access control mechanism. It has some disadvantage that is system not able to retrieve data in a customized way. Also in privacy preserving uses only one anonymization technique [1].

Accuracy constrained privacy preserving access control mechanism, illustrated in figure. 2 (arrow represent the direction of information flow), is proposed. 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 the selection predicate on Quasi-identifier (QI) attributes. The policy administrator defines the permissions along with the imprecision bound for each permission/query, user-to-role assignment, and role to permission assignment [8]. The imprecision bound information is not shared with the users because knowing the imprecision bound can result in violating the privacy requirement. the privacy protection mechanism is required to meet the privacy requirement along with the imprecision bound for each permission.

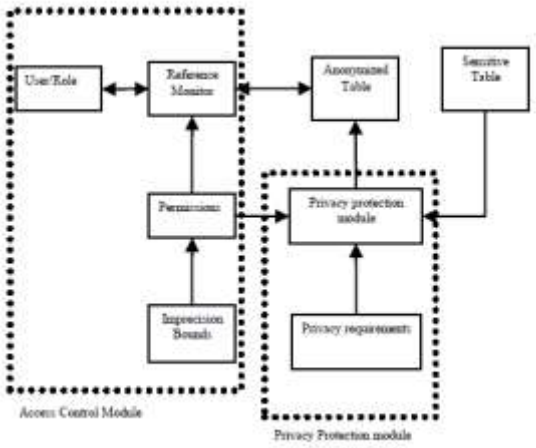

Figure. 2. Accuracy constrained privacy- preserving access control mechanism

III. Proposed System

To overcome the disadvantage of existing system and provide more security to data while accessing d that is done by encypting the data. Accuracy control module and privacy-preserving module is combined [1] this framework improve the efficiency of the security system. The proposed system deal with multilevel anonymization techniques. In the proposed approach instead of using single anonymization technique like generalization or suppression, a combined form of anonymization technique introduced like both generalization and suppression.

We know how accuracy constrained privacy –preserving access control mechanism works and its configuration is the combination of two modules [1]

Generalization anonymization technique was used in accuracy constrained privacy preserving access control mechanism.

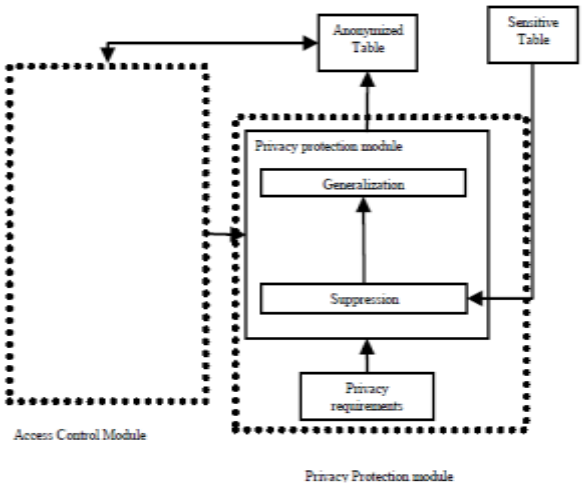

Figure. 3. Accuracy constrained privacy-preserving access control mechanism with multilevel

Anonymization techniques replaces the data in the table with the some other values that is cannot be identified by the users. In generalization method individual values or attributes are replaced by some broader category (for example the value '19' of the attribute 'age' may be replaced by in the range 15-25 etc.) In this framework anonymization is applied only once to the data values for security. In the proposed system multilevel anonymization is performed to improve the efficiency of the security system. Here suppression is also performed with the generalization, in suppression certain values of the attribute are replaced by an asterisk '*'(for example zip code of ram be 812372 after suppression it becomes 8123**,812***,etc).

Here Suppressed information of original table is used in the first level of anonymization , a generalized value is used in second level of anonymization. This also provide the minimum level of preference to the data along with that the sensitive information will get protected. The proposed system illustrated in figure 3.

IV. Conclusion

The paper discuss about the how to improve the efficiency of the security system. Anonymization techniques are used to maintain the privacy. Access control policy which define selection predicates on sensitive data. Multilevel anonymization technique is introduced to improve the efficiency of accuracy constrained privacy preserving access control mechanism for relational data.

REFERENCE

[1] Zahid Pervaiz, Walid G.Aref, Arif Gafoor, "Accuracy constrained privacy preserving access control mechanism for relational databases" IEEE Transaction on Knowledge Engineering, vol.26, No.4, April 2014, pp.795-807 .

[2] K. LeFevre, D. DeWitt, and R. Ramakrishnan, "Workload Anonymization Techniques for Large-Scale Datasets," ACMTrans. Database Systems, vol. 33, no. 3, pp. 1-47, 2008.

[3] A. Machanavajjhala, D. kifer, j. Gehrke, and M. Venkitasubramaniam,"L-Diversity: Privacy Beyond k-anonymity," ACM Trans.Knowledge Discovery from Data, vol. 1, no. 1, article 3, 2007.

[4] S. Rizvi, A. Mendelzon, S. Sudarshan, and P. Roy, "ExtendingQuery Rewriting Techniques for Fine-Grained Access Control,"Proc. ACM SIGMOD Int'l Conf. Management of Data, pp. 551-562,2004.

[5] 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.

[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. Rask, D. Rubin, and B. Neumann, "Implementing Row-andCell-Level Security in Classified Databases Using SQL Server2005," MS SQL Server Technical Center, 2005.

[8] Dipmala Salunke, Anilkumar Upadhyay1, Amol Sarwade2, Vaibhav Marde3, Sachin Kandekar 4 "A survey paper on Role Based Access Control," International Journal of Advanced Research in Computer and Communication EngineeringVol. 2, Issue 3, March 2013.

[9] K. LeFevre, R. Agrawal, V. Ercegovac, R. Ramakrishnan, Y. Xu,and D. DeWitt, "Limiting Disclosure in Hippocratic Databases,"Proc. 30th Int'l Conf. Very Large Data Bases, pp. 108-119, 2004.