ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

An Effective Privacy-Preserving Access Control Method for Relational Data

D. Chandra Sekhar,
M.Tech Student
Department of CSE,
CREC, Tirupathi, JNTU-Anathapuram, A.P, India.

R. Suresh
Associate Professor & HoD
Department of CSE,
CREC, Tirupathi, JNTU-Anathapuram, A.P, India.

ABSTRACT

To prevent the misuse of sensitive data by the authorized users and provide both 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 protect the data from unauthorized or third party user. When there is a lack in privacy preserving mechanism (PPM) and data is shared with others, the authorized user may need to compromise the privacy of data or Information. The privacy preservation can be achieved through anonymization techniques like generalization or suppression. Along with privacy the precision of the authorized data is important. The aim of the work is to provide better security and minimum level of precision to the retrieved data, for that in this paper an accuracy constrained privacy preserving access control mechanism is implemented with additional constraint on each selection predicate called imprecision bounds. New approach plan to extend the proposed privacy-preserving cell level access control .Today's fast growing world, the malicious intent or hacking purpose also increasing. So there is a need to provide a better security to our system.

Keywords— Access control, privacy, k-anonymity, query evaluation

1. INTRODUCTION

Many organizations collect and analyze consumer data to improve their services. Access Control Mechanisms (ACM) are 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 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. In this paper, we investigate privacy-preservation from the anonymity aspect. The sensitive information, even after the removal of identifying attributes, is still susceptible to linking attacks by the authorized users. This problem has been studied extensively in the area of micro data publishing and privacy definitions, e.g., k-anonymity, l-diversity, and variance diversity. Anonymization algorithms use suppression and generalization of records to satisfy privacy requirements with minimal distortion of micro data. The anonymity techniques can be used with an access control mechanism to ensure both security 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 every permission to define a threshold on the amount of imprecision that can be tolerated. Existing workload aware anonymization techniques minimize the imprecision aggregate for all queries and the imprecision added to each permission/query in the anonymized micro data is not known. Making the privacy requirement more stringent (e.g., increasing the value of k or l) results in additional imprecision for queries. However, the problem of satisfying accuracy constraints for individual permissions in a policy/workload has not been studied before. The heuristics proposed in this paper for accuracy-constrained privacy-preserving access control are also relevant in the context of workload-aware anonymization. The anonymization for continuous data publishing has been studied in literature. In this paper the focus is on a static relational table that is anonymized only once. To exemplify our approach, role-based access control is assumed. However, the concept of accuracy constraints for permissions can be applied to any privacy-preserving security policy, e.g., discretionary access control.

2. EXISTING SYSTEM

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. Investigate privacy-preservation from the anonymity aspect. The sensitive information, even after the removal of identifying attributes, is still susceptible to linking attacks by the authorized users.

DISADVANTAGES OF EXISTING SYSTEM:

- Minimize the imprecision aggregate for all queries.
- The imprecision added to each permission/query in the anonymized micro data is not known.
- Not satisfying accuracy constraints for individual permissions in a policy/workload.

3. PROPOSED SYSTEM

The heuristics proposed in this paper for accuracy constrained privacy-preserving access control are also relevant in the context of workload-aware anonymization. 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.

ADVANTAGES OF PROPOSED SYSTEM:

- Formulate the accuracy and privacy constraints.
- Concept of accuracy-constrained privacy-preserving access control for relational data.
- Approximate the solution of the k-PIB problem and conduct empirical evaluation.

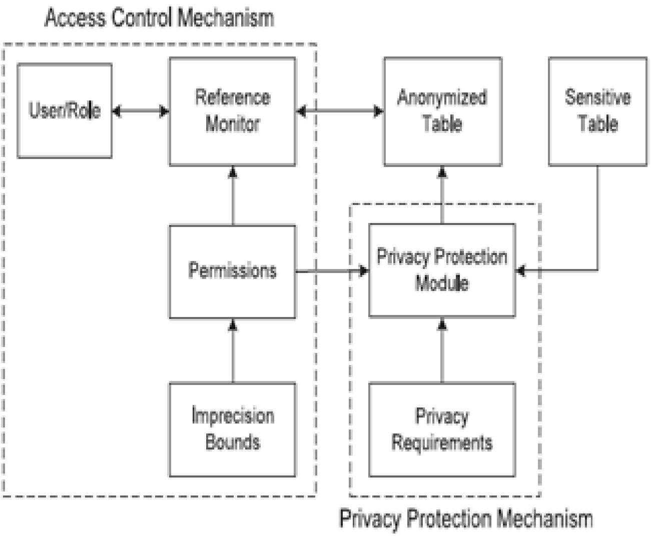

Fig 1: System Architecture.

4. IMPLEMENTATION

An accuracy-constrained privacy-preserving cell level access control mechanism is a combination of access control and privacy protection mechanisms. Individual sensitive is easily inferred by an attacker. Protecting data privacy is an important problem, in micro-data distribution. Anonymization is to protect individual privacy, with minimal impact on the quality of the resulting data. The system produce an anonymous view based on a target class of workloads, consisting of one or more data mining tasks and selection predicates. The advantage of anonymity is resisting the attacker's inference attacks. Access control mechanism for relational data is constructed with the privacy preservation based model. Role Based Access Control (RBAC) scheme 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 system reduces the imprecision rate in query processing. Access control mechanism is adapted for incremental mining model. Time complexity is reduced in the proposed system. The proposed system provides the dynamic policy management mechanism.

A. ACCESS CONTROL MECHANISM

The Access control mechanism allows only authorized query predicates on sensitive data.

1) User/Role: It allows defining permissions on objects based on roles in an organization. An RBAC is composed of a set of users, a set of roles, and a set of Permissions. Assume that the selection predicates on the QI attributes define permission.UA is a user-to-role assignment relation and PA is a role to permission assignment relation. When a user assigned to a role executes a query, the tuples that are used satisfying the conjunction of the query predicate and the permission are returned.

2) Permissions: It based on selection predicates on the QI attributes. The imprecision bound for each query, user-to-role assignments, and role-to permission assignments.

3) Imprecision Bound: It ensures that the authorized data has the desired level of accuracy. The imprecision bound can be used to meet the privacy requirement. The privacy protection mechanism is required to meet the privacy requirement according to the imprecision bound for each permission.

B. PRIVACY PROTECTION MECHANISM

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

1) Privacy Protection Module: It anonymizes the data to meet privacy requirements and imprecision constraints on predicates set by the access control mechanism

2) Sensitive Table.

3) Anonymous Table.

The proposed system gets information in a anonymous version of sensitive table. The ID attribute is removed in the anonymized table and is shown only for identification of tuples. Here, for any combination of selection predicates on the zip code and age attributes, there are at least two tuples in each equivalence class.

5 CONCLUSIONS

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. We formulate this interaction as the problem of k-anonymous Partitioning with Imprecision Bounds (k-PIB). We give hardness results for the k-PIB problem and present heuristics for partitioning the data to the satisfy the privacy constraints and the imprecision bounds. In the current work, static access control and relational data model has been assumed. For future work, we plan to extend the proposed privacy-preserving access control to incremental data and cell level access control.

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] 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.

[4] 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.

[5] 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.

[6] 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.

[7] J. Buehler, A. Sonricker, M. Paladini, P. Soper, and F. Mostashari, “Syndromic Surveillance Practice in the United States: Findings from a Survey of State, Territorial, and Selected Local Health Departments,” Advances in Disease Surveillance, vol. 6, no. 3, pp. 1-20, 2008.

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

[9] A. Rask, D. Rubin, and B. Neumann, “Implementing Row-and Cell-Level Security in Classified Databases Using SQL Server 2005,” MS SQL Server Technical Center, 2005.

[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] 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.

[12] 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.
[13] D. Ferraiolo, R. Sandhu, S. Gavrila, D. Kuhn, and R. Chandramouli, “Proposed NIST Standard for Role-Based Access Control,” ACM Trans. Information and System Security, vol. 4, no. 3, pp. 224- 274, 2001.

[14] K. LeFevre, D. DeWitt, and R. Ramakrishnan, “Mondrian Multidimensional K-Anonymity,” Proc. 22nd Int’l Conf. Data Eng., pp. 25- 25, 2006.

[15] J. Friedman, J. Bentley, and R. Finkel, “An Algorithm for Finding Best Matches in Logarithmic Expected Time,” ACM Trans. Mathematical Software, vol. 3, no. 3, pp. 209-226, 1977.

[16] A. Meyerson and R. Williams, “On The Complexity of Optimal k-Anonymity,” Proc. 23rd ACM SIGMOD-SIGACT-SIGART Symp. Principles of Database Systems, pp. 223-228, 2004.

[17] G. Aggarwal, T. Feder, K. Kenthapadi, R. Motwani, R. Panigrahy, D. Thomas, and A. Zhu, “Approximation Algorithms for k-Anonymity,” J. Privacy Technology, vol. 2005112001, pp. 1-18, 2005.

[18] R. Sandhu and Q. Munawer, “The Arbac99 Model for Administration of Roles,” Proc. 15th Ann. Computer Security Applications Conf., pp. 229-238, 1999.