Journal of Information Technology and Telecommunications
Received: Nov 05, 2015, Accepted: Dec 18, 2015, Published: Dec 21, 2015
J Inform Technol Telecomm, Volume 1, Issue 1
http://crescopublications.org/pdf/JITT/JITT-1-R003.pdf
Article Number: JITT-1-R003

Review Article Open Access

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

Ch V Raju

Department of Information Technology, TKR College of Engineering and Technology, Meerpet, Telangana, India

Citation: Ch V Raju (2015) Access Control Mechanism of Accuracy-Constrained Privacy-Preserving for Relational Data. J Inform Technol Telecomm 1: R003.

Abstract

Access control mechanisms protect sensitive information from unauthorized users. However, when sensitive information is shared and a Privacy Protection Mechanism (PPM) is not in place, an authorized user can still compromise the privacy of a person leading to identity disclosure. A PPM can use suppression and generalization of relational data to anonymize and satisfy privacy requirements, e.g., k-anonymity and l-diversity, against identity and attribute disclosure. However, privacy is achieved at the cost of precision of authorized information. In this paper, we propose an accuracy-constrained privacy-preserving access control framework. The access control policies define selection predicates available to roles while the privacy requirement is to satisfy the k-anonymity or l-diversity. An additional constraint that needs to be satisfied by the PPM is the imprecision bound for each selection predicate. The techniques for workload-aware anonymization for selection predicates have been discussed in the literature. However, to the best of our knowledge, the problem of satisfying the accuracy constraints for multiple roles has not been studied before. In our formulation of the aforementioned problem, we propose heuristics for anonymization algorithms and show empirically that the proposed approach satisfies imprecision bounds for more permissions and has lower total imprecision than the current state of the art.

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 anonymityaspect. 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.

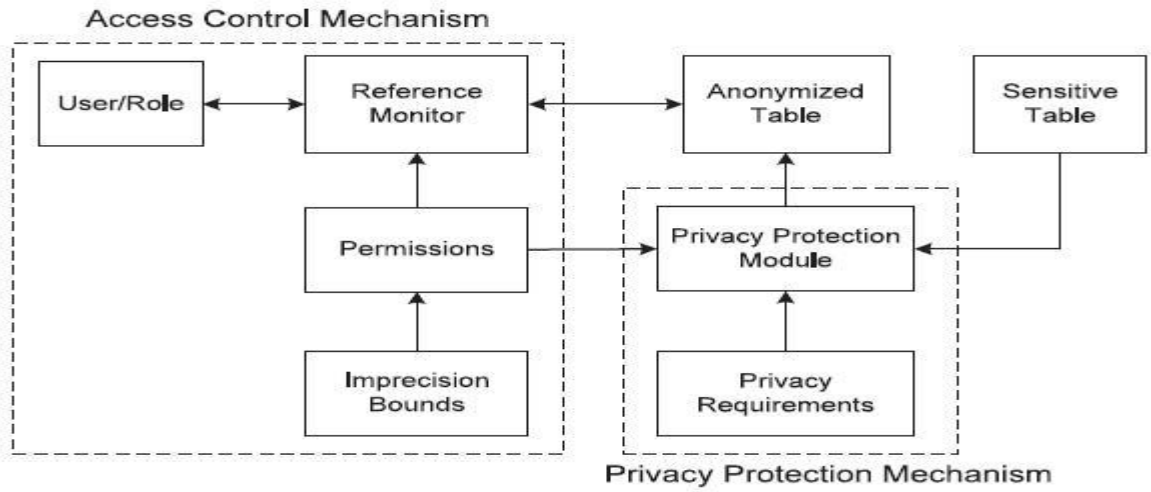
Proposed System

- 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.

System Architecture



System Requirements

Hardware Requirements

- System : Pentium IV 2.4 GHz.
- Hard Disk : 40 GB.
- Floppy Drive : 1.44 Mb.
- Monitor : 15 VGA Colour.
- Mouse : Logitech.
- Ram : 512 Mb.

Software Requirements

- Operating system : Windows XP/7.
- Coding Language : JAVA/J2EE
- IDE : Netbeans 7.4
- Database : MYSQL

Reference

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