Volume 5, Issue 3, March 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Survey on Accuracy Constrained Privacy-Preserving Access Control Mechanism for Relational Data

Sahithi B[1], K. S. Vijaya Lakshmi[2]
Department of Computer Science and Engg.,
V.R.Siddhartha Engineering College (Autonomous)
Affiliated to JNTUK, Vijayawada, Andhra Pradesh, India

Abstract- While Sensitive information is being shared, an authorized user has to compromise with his privacy leading to identity disclosure. But Privacy Protection Mechanism (PPM) with its suppression and generalization of relational data anonymizes and satisfies privacy requirements using k-anonymity and l-diversity, against identity and attribute disclosure. Thus access control mechanism helps in protecting sensitive information from unauthorized users. Usually privacy is achieved at the cost of precision of authorized information. The present project focuses on an accuracy-constrained privacy-preserving access control framework. While satisfying the privacy requirement, k-anonymity or l-diversity, the access control policies define selection predicates available to rolls. The PPM needs to satisfy an additional constraint namely the Imprecision Bound for each selection predicate. The literature survey might provide techniques for workload-aware anonymization for selection predicates, as the problem of satisfying the accuracy constraints for multiple roles has not been studied before. The purpose of the present project is to propose heuristics for anonymization algorithms and to show the viability of the proposed approach for empirically satisfying the imprecision bounds for more permission.

Key words: Access control, Privacy, k-anonymity, Precision, Imprecision, l-diversity.

I. INTRODUCTION

Organizations collect and analyze consumer data to improve their services. Access Control Mechanisms (ACM) is used to ensure that only authorized information is available to the users. However, sensitive information can still be misused by authorized users compromising 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.

The anonymity techniques can be used with an access control mechanism [1] 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.

An integrated framework of achieving both privacy and security is proposed though the integration of Access Control Mechanism with Privacy Preservation [1] Technique to prevent the authorized user from misusing the sensitive information. The enforcement of privacy policies or the protection against identity disclosure satisfying some privacy requirements are the pre-requisites for privacy-preservation of sensitive data. Even after removal of identifying attributes, the sensitive information is susceptible to liking attacks by the authorized users. So the present investigation is proposed to study the area of micro data publishing and privacy definitions such as k-anonymity [2], l-diversity [3] and variance diversity.

The privacy requirements with minimal distortion of micro data can be satisfied by using suppression and generalization of anonymization algorithms. In a way to ensure security and privacy of sensitive information, the anonymity techniques can be used. To define a threshold on the amount of imprecision that can be tolerated for each permission, the concept of imprecision bound is to be used. A role based access [4][5] control is assumed in a way to focus on a static relational table that is anonymized only once.

In existing system [1] 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 concept of privacy-preservation for sensitive data requires the enforcement of privacy policies or the protection against identity disclosure by satisfying some privacy requirements by investigating 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. But it has some disadvantages such as – User doesn't have efficient privacy and accurate constraints. System fails to retrieve data in customized way. It minimizes the imprecision aggregate for all queries. The imprecision added to each permission/query in the anonymized micro data is not known, thus, not satisfying accuracy constraints for individual permissions in a policy/workload. System doesn't provide security for data which motivated me to work on this.

An accuracy-constrained privacy-preserving access control mechanism, illustrated in Fig.[1] (Arrows 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 selection predicates on the QI attributes. The policy administrator defines the permissions along with the imprecision bound for each permission/query, user-to-role assignments, and role-to permission assignments [6].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.

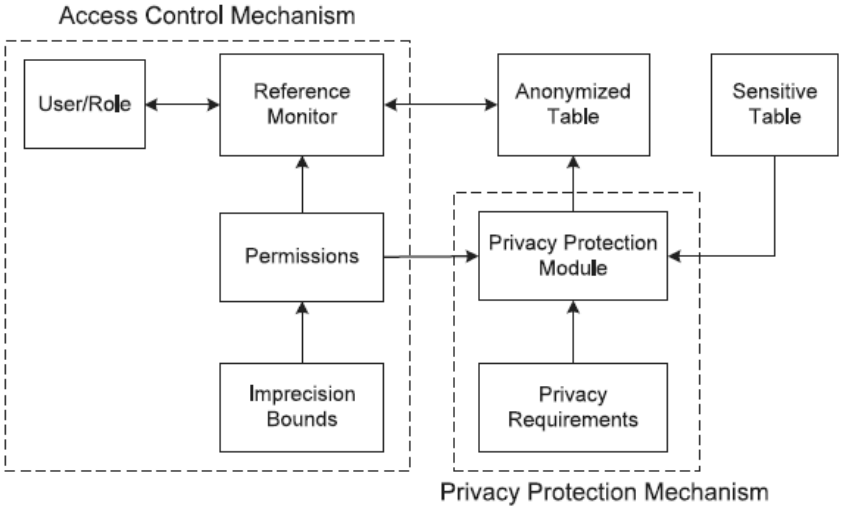

Fig 1: Accuracy-constrained privacy-preserving access control mechanism.

To overcome the disadvantages of existing 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 and the advantages of proposed system are - formulate the accuracy and privacy constraints. Concept of accuracy-constrained privacy-preserving access control for relational data was studied and the solution of the k-PIB problem was approximated and empirical evaluation was conducted.

II. LITERATURE REVIEW

Various papers were referred for the present research regarding access control mechanism, privacy preserving, k-anonymity, and for workload aware anonymity concepts. In this, the Private Data Anonymization was proposed or, k-Anonymity Meets Differential Privacy was discussed by Li et al [7], they defined the privacy requirement in terms of k-anonymity that after sampling, k-anonymity offers similar privacy guarantees as those of differential privacy. In this paper the privacy requirement were defined in terms of k-anonymity [2] that after sampling, k-anonymity offers similar privacy guarantees as those of differential privacy. The proposed accuracy-constrained privacy preserving access control framework allows the access control administrator to specify imprecision constraints that the privacy protection mechanism is required to meet along with the privacy requirements. The proposed accuracy-constrained privacy preserving access control framework allows the access control administrator to specify imprecision constraints that the privacy protection mechanism is required to meet along with the privacy requirements. The challenges of privacy-aware access control are similar to the problem of workload-aware anonymization. In our analysis of the related work, query-aware anonymization was focused. The problem of accuracy-constrained anonymization for a given bound of acceptable information loss for each equivalence class was proposed [8]. Similarly, Xiao et al. [9] proposed to add noise to queries according to the size of the queries in a given workload to satisfy differential privacy. However, bounds for query imprecision have not been considered. The existing literature on workload-aware anonymization has a focus to minimize the overall imprecision for a given set of queries. However, anonymization with imprecision constraints for individual queries has not been studied before. For the present study, the imprecision definition of Lefebvre et al. is followed[10] and the constraint of imprecision bound for each query in a given query workload is introduced. In which they concluded the problem of measuring the quality of anonymized data. The most direct way of measuring quality is with respect to the purpose for which the data will be used. For this reason, a suite of techniques for incorporating a family of tasks (comprised of queries, classification, and regression models) were introduced directly into the anonymization procedure.

The interaction between the access control mechanisms and the privacy protection mechanisms was discussed by Chaudhuri et al. [11]. Access control with privacy mechanisms in which they concluded with the sketch of an architecture for a hybrid system that enhances an authorization policy with the abstraction of noisy views that encapsulate previously proposed privacy mechanisms. Accessing data through a set of views is natural for users of database systems and thus the noisy views abstraction represents a natural progression of the concept of authorization views. It was also stated how noisy views based on differentially private algorithms could be implemented. A key advantage of the proposed hybrid system is its flexibility. It can support queries that refer to both the base tables and the differentially

private views thus resulting in a system that is more powerful than using access control techniques or differential privacy techniques in isolation. While combining authorizations and differentially private views in this manner seems ad-hoc, it is shown to be a principled way to integrate differential privacy primitives with privacy guarantees [11]. The definition of differential privacy was used [12] whereby random noise is added to original query which results to satisfy privacy constraints. However, the accuracy constraints for permissions were not considered. But the present study defines the privacy requirement in terms of k-anonymity.

Workload-aware anonymization is first studied by LeFevre et al. [10]. They have proposed the Selection Mondrian algorithm, which is a modification to the greedy multidimensional partitioning algorithm Mondrian [13]. In their algorithm, based on the given query-workload, the greedy splitting heuristic minimizes the sum of imprecision for all queries. The present study has considered the problem of measuring the quality of anonymized data. It is our position that the most direct way of measuring quality is with respect to the purpose for which the data will be used. For this reason, a suite of techniques were developed for incorporating a family of tasks (comprised of queries, classification, and regression models) directly into the anonymization procedure. An extensive empirical study indicates that this typically leads to high-quality data. Further, the quality of the data with respect to a particular workload is not necessarily correlated with simple general-purpose measures that have been proposed in the previous literature. In the second half of the article, the problem of scalability is introduced. Two techniques were developed that allow our anonymization algorithms to be applied to datasets much larger than main memory. The first technique is based on ideas from scalable decision trees [Gehrke et al. 1998], and the second is based on sampling. An experimental evaluation and analytical study indicate that these techniques work very well in practice. Iwuchukwu and Naughton have proposed an R+-tree based anonymization algorithm [14]. The authors illustrated by experiments that anonymized data using biased R+-tree based on the given query workload is more accurate for those queries than for an unbiased algorithm.

Further Ghinita et al. have proposed algorithms based on space filling curves for k-anonymity and l-diversity [3]. They also introduce the problem of accuracy-constrained anonymization for a given bound of acceptable information loss for each equivalence class [15]. Similarly, Xiao et al. [9] propose to add noise to queries according to the size of the queries in a given workload to satisfy differential privacy. However, bounds for query imprecision have not been considered. The existing literature on workload-aware anonymization has a focus to minimize the overall imprecision for a given set of queries. However, anonymization with imprecision constraints for individual queries has not been studied before. We follow the imprecision definition of LeFevre et al. [10] and introduced the constraint of imprecision bound for each query in a given query workload.

III. CONCLUSION

An accuracy-constrained privacy-preserving access control framework for relational data has been proposed. The planned additive approach of access management and privacy protection mechanisms in our system provides a lot of security and information is retrieved during a custom-made approach which will build users to access during as lot of versatile approach. Any access management concentrates on anomaly users to avoid privacy problems security .The ACM allows solely licensed user predicates on sensitive information and PPM anonymizes the information to satisfy privacy necessities and inexactness constraints on predicates set by the access management mechanism. 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. This interaction is formulated as the problem of k-anonymous Partitioning with Imprecision Bounds (k-PIB). Hardness results are given for the k-PIB problem and the heuristics for partitioning the data are presented to satisfy the privacy constraints and the imprecision bounds. In the current work, static access control and relational data model has been assumed. The proposed privacy-preserving access is extended to control incremental data and cell level access control.

REFERENCES

[1] ZahidPervaiz, Walid G. Aref, ArifGhafoor, and NagabhushanaPrabhu "Accuracy-Constrained Privacy-Preserving Access Control Mechanism for Relational Data" IEEE Trans. On Knowledge and Data Engineering, Vol. 26, No. 4, April 2014.

[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] 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. Chaudhuri, R. Kaushik, and R. Ramamurthy, "Database Access Control & Privacy: Is There a Common Ground?" Proc. Fifth Biennial Conf. Innovative Data Systems Research (CIDR), pp. 96-103, 2011.

[5] 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.

[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] N. Li, W. Qardaji, and D. Su, "Provably Private Data Anonymization: Or, k-Anonymity Meets Differential Privacy," Arxiv preprint arXiv: 1101. 2604, 2011.

[8] G. Ghinita, P. Karras, P. Kalnis, and N. Mamoulis, "A Framework for Efficient Data Anonymization Under Privacy and Accuracy Constraints," ACM Trans. Database Systems, vol. 34, no. 2, article 9, 2009.

[9] X. Xiao, G. Bender, M. Hay, and J. Gehrke, "Ireduct: Differential Privacy with Reduced Relative Errors," Proc. ACM SIGMOD Int'l Conf. Management of Data, 2011.

[10] K. LeFevre, D. DeWitt, and R. Ramakrishna, "Workload-Aware Anonymization Techniques for Large-Scale Datasets," ACM Trans. Database Systems, vol. 33, no. 3, pp. 1-47, 2008.

[11] S. Chaudhuri, R. Kaushik, and R. Ramamurthy, "Database Access Control & Privacy: Is There a Common Ground?" Proc. Fifth Biennial Conf. Innovative Data Systems Research (CIDR), pp. 96-103, 2011.

[12] C. Dwork, "Differential Privacy," Proc. 33rd Int'l Colloquium Automata, Languages and Programming, pp. 1-12, 2006.

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

[14] 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.

[15] G. Ghinita, P. Karras, P. Kalnis, and N. Mamoulis, "A Framework for Efficient Data Anonymization Under Privacy and Accuracy Constraints," ACM Trans. Database Systems, vol. 34, no. 2, article 9, 2009.

