A Survey on Security and Accuracy Constrained Privacy Preserving Task Based Access Control Mechanism for Relational Data

Pratik Bhingardeve[1], D. H. Kulkarni[2]

[1, 2] Pune University, Smt. Kashibai Navale College of Engineering, Vadgaon (BK), Pune-411041, India

Abstract: ***Data privacy problems square measure more and more turning into vital for several applications. Access management mechanisms give protection to our sensitive business information from unwanted user. Resource and information sharing is additional and crucial part of our daily life and business. Essentially analysis within the data processing or information mining with sub space of information security is loosely classified into access management analysis and data privacy analysis. Each plays vital role in information security thence we've integrated these methodologies to boost our security on relative information. Mistreatment privacy protective mechanism we will generalize and suppress our relative information to anonymize and satisfy privacy needs against identity and attribute speech act. We've not solely collective these methodologies however we've conjointly provided further security by mistreatment encryption that wasn't gift in previous system.***

Keywords: Workload aware anonymization, Access control, privacy, l-diversity.

1. Introduction

Data privacy problems are getting progressively vital for our society. This can be proved by the very fact that the accountable management of sensitive knowledge is expressly being mandated through laws like the Sarbanes-Oaxley Act and therefore the insurance movability and answerability Act (HIPAA) [3]. Protective individual privacy is a crucial downside. Access management mechanisms area unit accustomed make sure that solely approved data is obtainable to users. However, sensitive data will still be ill-used by approved users to compromise the privacy of shoppers. Databases within the globe area unit typically massive and sophisticated. The challenge of querying such infuse in a very timely fashion has been studied by the database, data processing and knowledge retrieval communities, however seldom studied within the security and privacy domain. We have a tendency to have an interest within the downside of protective access privacy for users once querying massive databases of many lots of or thousands of gigabytes of knowledge. This can be a more durable downside than in alternative domains as a result of the matter contents of queries area unit themselves protected against the info server [5].

The concept of privacy-preservation for sensitive data can require the enforcement of privacy policiesor the protection against identity disclosure by satisfying some privacy requirements. We investigate privacy-preservation from the anonymity aspect. 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 [1].

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 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. But it has some disadvantages such as User's doesn't have efficient privacy and accurate constraints. System not able to retrieve data in customized way. 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 [7].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.

Licensed Under Creative Commons Attribution CC BY

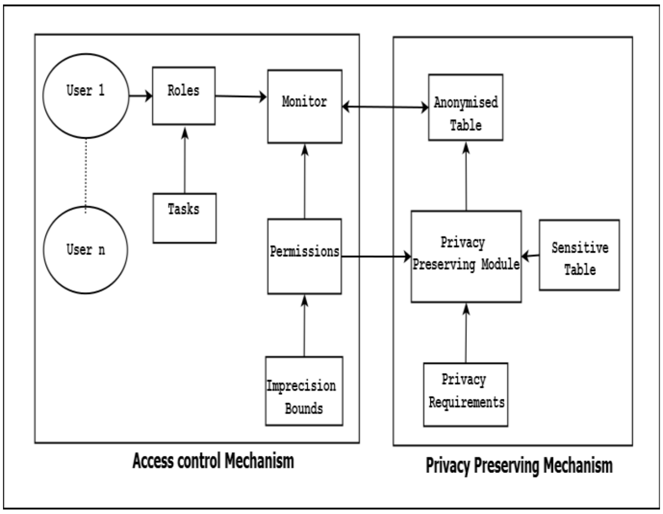

Figure: Proposed System Architecture with ACM and PPM [1]

To overcome the disadvantages of existing system we proposed a system that provides more security by adding encryption to data. Data can be retrieved in a customized way that will make users to access in a more flexible way which will reduce user efforts. And access control concentrates on anomaly users to avoid privacy issues. The advantages of proposed system are we are able to formulate the accuracy and privacy constraints. As previously done we also can keep concept of accuracy-constrained privacy-preserving access control for relational data. Due to use of encryption system will provide security and privacy to users.

2. Literature Review

We have referred various papers for our research regarding access control mechanism, privacy preserving, k-anonymity, and for workload aware anonymity concepts. In this we came across the paper which proposed studying the interaction between the access control mechanisms and the privacy protection mechanisms was discussed by Chaudhuri et al. [3] have studied 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. They further also stated that how we can implement noisy views based on differentially private algorithms. 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, we show that it is a principled way to integrate differential privacy primitives with privacy guarantees [3].

Further Vaidya et al. [8] demonstrated that general and efficient distributed privacy preserving knowledge discovery is truly feasible. We have considered the security and privacy implications when dealing with distributed data that is partitioned either horizontally or vertically across multiple sites, and the challenges of performing data mining tasks on such data. SinceRDTs can be used to generate equivalent, accurate and sometimes better models with much smaller cost, we haveproposed distributed privacy-preserving RDTs. Our approach leverages the fact that randomness in structure can provide strong privacy with less computation. The experiments show that the privacy preserving version of the RDT algorithm scales linearly with data set size, and requires significantly less time than alternative cryptographic approaches. In the future, we plan to develop general solutions that can work for arbitrarily partitioned data.

In Li et al. [4] they have define the privacy requirement in terms of k-anonymity 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 challenges of privacy-aware access control are similar to the problem of workload-aware anonymization. In our analysis of the related work, we focus on query-aware anonymization. They also introduce the problem of accuracy-constrained anonymization for a given bound of acceptable information loss for each equivalence class [9]. Similarly, Xiao et al. [10]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. [5]and introduce the constraint of imprecision bound for each query in a given query workload. In which further they concluded 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, we developed a suite of techniques for incorporating a family of tasks (comprised of queries, classification, and regression models) directly into the anonymization procedure.

In another paper by Hwai-Jung Hsu and Feng-Jian Wang. "A Delegation Framework for Task-Role Based Access Control in WFMS [11] they focused on Access management is very important for shielding data integrity in work flow management system (WFMS). Compared to traditional access management technology like discretionary, mandatory, and role based mostly access management models, task-role-based access management (TRBAC) model, AN access management model supported each tasks and roles, meets additional needs for contemporary enterprise environments. However, few discussions on delegation mechanisms for TRBAC area unit created. Within the framework, the methodology for delegations requested from each users and WFMS is mentioned. The constraints for delegate choice like delegation loop and separation of duty (SOD) area unit self-addressed. With the framework, a sequence of algorithms for delegation and revocation of tasks area unit created bit by bit

Licensed Under Creative Commons Attribution CC BY

3. Conclusion

The planned additive approach of access management and privacy protection mechanisms in our system provides a lot of security by adding cryptography to information 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.

References

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

[2] 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.

[3] 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.

[4] N. Li, W. Qardaji, and D. Su, "Provably Private Data Anonymization: Or, k-Anonymity Meets Differential Privacy," Arxiv preprint arXiv:1101.2604, 2011.

[5] Femi Olumofin and Ian Goldberg "Preserving Access Privacy Over Large Databases", University of Waterloo Waterloo, Ontario, Canada N2L 3G1, 2012

[6] Yung-Wang Lin, Li-Cheng Yang, Luon-Chang Lin, and Yeong-Chin Chen "Preserving Privacy in Outsourced Database", International Journal of Computer and Communication Engineering, Vol. 3, No. 5, September 2014.

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

[8] JaideepVaidya, BasitShafiq, Wei Fan,DanishMehmood, and David Lorenzi "A Random Decision Tree Framework for Privacy-Preserving Data Mining",IEEE transactions on dependable and secure computing, vol. 11, no. 5, september/october 2014

[9] 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.

[10] 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.

[11] Hwai-Jung Hsu And Feng-Jian Wang, "A Delegation Framework for Task-Role Based Access Control in Wfms", Journal Of Information Science And Engineering 27, 1011-1028 (2011)

Licensed Under Creative Commons Attribution CC BY