Survey On Dynamic Privacy Policy Inference For User-uploaded File With Access Control Mechanism On Group User Data

Miss. Vinee Gemnani[1], Prof. Garima Singh Makhija[2]

[1] [2] Department of Computer Science and Engineering, RTMNU University , W.C.E.M., Nagpur, Maharashtra, India.

---***---

Abstract: ***Data protection is extremely important for all companies, large and small. There are some situations when sensitive information has to be shared to authorized person for some authentication, verification or authorization purpose. A set of Access Control Mechanism (ACM) protects sensitive information from unauthorized users. 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 which is Dynamic Privacy-Protection Mechanism (DPPM) which is Dynamic Privacy Policy Interface from the anonymity aspect. Thus the project deals with building of such mechanism which can be dynamically use for the protection of the data in flexible manner.***

Keywords: ACM, DPPM, k-anonymity, l-diversity.

1. INTRODUCTION

As organizations increase their reliance on, possibly distributed, information systems for daily business, they become more vulnerable to security breaches even as they gain productivity and efficiency advantages. Privacy preserving data mining is a novel research direction in data mining and statistical databases, where data mining algorithms are analyzed for the side-effects they suffer in data privacy. Though a number of techniques, such as encryption and electronic signatures, are currently available to protect data when transmitted across sites, a truly comprehensive approach for data protection must also include mechanisms for enforcing access control policies based on data contents, subject qualifications and characteristics, and other relevant contextual information, such as time. It is well understood today that the semantics of data must be taken into account in order to specify effective access control policies. Also, techniques for data integrity and availability specifically tailored to database systems must be adopted. Information is today probably the most important and demanded resource. We live in an internet worked society that relies on the dissemination and sharing of information in the private as well as in the public and governmental sectors. Governmental, public, and private institutions are increasingly required to make their data electronically available.

In existing system [1] the heuristics proposed in this paper for accuracy constrained privacy-preserving access control for relational data. 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 limitations 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.

Organization collects and analyzes consumer data to improve their services. Access Control Mechanisms (ACM)are used to ensure that only authorized information is available to users.[1] However, sensitive information may still be misused by authorized users to compromise the privacy of consumers. Keeping all the objective to privacy and prevention of data, the project introduce to design the new Dynamic Privacy Protection mechanism (DPPM) which can be use for protection of data and also for the privacy of data. In general we have been observed that when user using some application environment on which he/she storing the data can be also authenticate by authorized user who providing the permission to access those data. And hence there should be some authentication should be developed for the user so that data cannot be misused even by the authorizer who providing the service for the user. Considering this aspect the this project is developing the environment as a mechanism for the user so that they can provide safety for the particular data belong to them. Also data can be any raw data on which this mechanism will able to protect it, this real time mechanism will be user friendly for the user so that protection and privacy can be achieved in well manner.

2. Review Of Literature:

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 Zahid Pervaiz et. Al. [1] focus on the accuracy-constrained privacy-preserving access control framework for relational data has been proposed. They 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.

In another paper 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 provide that how we can implement noisy views based on differentially private algorithms. A main 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 combine 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. Since RDTs can be used to generate equivalent, accurate and sometimes good models with much less cost, we have proposed distributed privacy-preserving RDTs. Our can provide strong privacy with less computation.

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. 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.

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.

3. Proposed Scheme:

The phases of proposed method are shown by following flow diagram.

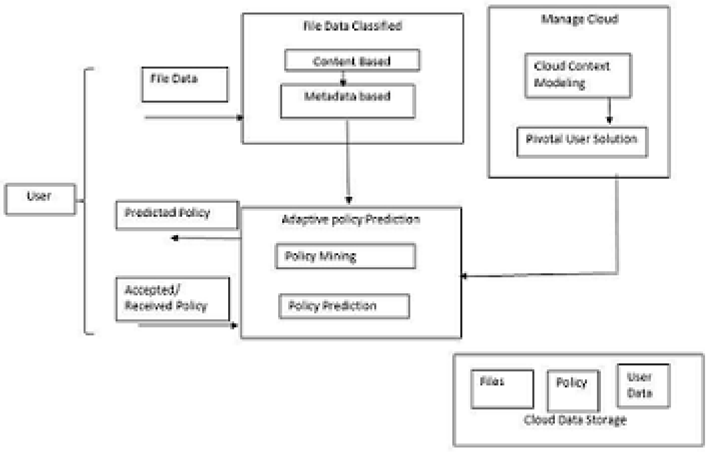

Figure.1. Proposed System Architecture

To overcome the disadvantages of existing system we proposed a system in which user can dynamically create the privacy policies to provide more security for their data. Presently available privacy protection mechanism includes protection on specific data like text data but not on any data or raw data. By overcoming this limitation, user can access any type of data. Making real time system will provide the efficient and convenient environment to user. This in turn will give us eminent and secure practical application to be use. Instead of making too critical structure this project will going to provide strong, sophisticated system structure for the user with less vulnerabilities. This ultimately impact on reducing the attacks by the attackers.

4. Conclusion:

This paper has introduced the real time system which will provide the efficient and convenient environment to user. The new dynamic privacy protection mechanism (DPPM) will allow to create dynamic protection policies to user this will helps to protect the sensitive data of user and Access Control Mechanism provides a protection of sensitive information from unauthorized users. This will be user friendly approach so that protection and privacy can be achieved in well manner.

References

[1] Zahid Pervaiz, 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).

Biographies:

Miss. Vinee Gemnani working as lecturer in Acharya Shrimanarayan Polytechnic College,Pipri,Wardha , Maharashtra , India .

Prof. Garima Singh Makhija working as HOD in CSE dept. Wainganga College of Engineering & Management Nagpur , Maharashtra , India.