A Survey on Access Control and Privacy Preserving Mechanisms on Relational Database

Mr. Rakesh Ramesh Tannu[1], Prof. S. A. Kahate[2]

[1] *Student, Computer Engineering, Sharadchandra Pawar COE, Dumberwadi, Otur, Junnar, Pune, Maharashtra, India.*
[2] *Assistant Professor, Computer Engineering, Sharadchandra Pawar COE, Dumberwadi, Otur, Junnar, Pune, Maharashtra, India.*

ABSTRACT

In current days of information technology, the assessment of data from existing database that are connected in a network were carried out simply by applying protection to database at the time of access only. Since during access of such data the access or privacy protection will not be there, due to this release and leakage of data can occur in a network. While the Access protection mechanism provides protection to sensitive data and privacy protection mechanism avoid the assessment of data by unauthorized users. Here the introductory and literature survey has presented which help further to design efficient system by considering all terms and circumstances.

Keyword: - *Relational Database, Accessing Methods, Privacy Preserving Techniques*

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. 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 [2] [4].

Security breaches are typically categorized as unauthorized data observation, incorrect data modification, and data unavailability. Unauthorized data observation results in the disclosure of information to users not entitled to gain access to such information. All organizations, ranging from commercial organizations to social organizations, in a variety of domains such as healthcare and homeland protection, may suffer heavy losses from both financial and human points of view as a consequence of unauthorized data observation. Incorrect modifications of data, either intentional or unintentional, result in an incorrect database state. Any use of incorrect data may result in heavy losses for the organization. When data is unavailable, information crucial for the proper functioning of the organization is not readily available when needed [3] [5].

Early research efforts in the area of access control models and confidentiality for DBMSs focused on the development of two different classes of models, based on the discretionary access control policy and on the mandatory access control policy. This early research was cast in the framework of relational database systems. The relational data model, being a declarative high-level model specifying the logical structure of data, made the development of simple declarative languages for the specification of access control policies possible. These earlier

models and the discretionary models in particular, introduced some important principles that set apart access control models for database systems from access control models adopted by operating systems and file systems [8].

Content-based access control is an important requirement that any access control mechanism for use in a data management system should satisfy. Essentially, content based access control requires that access control decisions be based on data contents. Consider an example of a table recording information about employees of a company; a content-based access control policy would be the one stating that a manager can only access the employees that work in the project that he manages. Whenever a manager issues a query, the system has to filter the query result by returning only the tuples related to the employees that verify the condition of working in the project managed by this manager. Support for this type of access control has been made possible by the fact that SQL is a language for which most operations for data management, such as queries, are based on declarative conditions against data contents.

2. LITERATURE SURVEY

The literature survey introduces a wide conceptual concepts and terms related to actual topic which will used further to define an efficient method to solve the problem. Since here introduce the working of few professionals and their works similar to the same topic. The Elisa Bertino et all introduces Concepts, Approaches, and Challenges related to database security. As they are defined approaches as Access control mechanisms of current Database systems are based on discretionary policies governing the accesses of a subject to data based on the subject's identity and authorization rules. These mechanisms are discretionary in that they allow subjects to grant authorizations on the data to other subjects. Because of such flexibility, discretionary policies are adopted in many application environments and this is the reason that commercial Database systems adopt such policies [9].

An important aspect of discretionary access control is thus related to the authorization administration policy. Authorization administration refers to the function of granting and revoking authorizations. It is the function by which authorizations are entered into or removed from the access control mechanism. Common administration policies include centralized administration, by which only some privileged subjects may grant and revoke authorizations, and ownership administration, by which grant and revoke operations on data objects are entered by the creator (or owner) of the object. Ownership-based administration is often provided with features for administration delegation, allowing the owner of a data object to assign other subjects the right to grant and revoke authorizations. Delegation thus supports decentralized authorization administration. Most commercial Database systems adopt ownership-based administration with administration delegation. More sophisticated administration mechanisms can be devised such as joint administration, by which several subjects are jointly responsible for authorization administration [3].

Pierangela Samarati introduces Protecting Respondents' Identities in Microdata Release from the existing database. They had defined Today's globally networked society places great demand on the dissemination and sharing of information. While in the past released information was mostly in tabular and statistical form, many situations call today for the release of specific data (microdata). In order to protect the anonymity of the entities (called respondents) to which information refers, data holders often remove or encrypt explicit identifiers such as names, addresses, and phone numbers. Deidentifying data, however, provides no guarantee of anonymity. Released information often contains other data, such as race, birth date, sex, and ZIP code that can be linked to publicly available information to reidentify respondents and inferring information that was not intended for disclosure.

The approach is based on the definition of k-anonymity. A table provides k-anonymity if attempts to link explicitly identifying information to its content map the information to at least k entities. Here they were illustrate how k-anonymity can be provided without compromising the integrity (or truthfulness) of the information released by using generalization and suppression techniques. The concept of minimal generalization that captures the property of the release process not to distort the data more than needed to achieve k-anonymity, and present an algorithm for the

computation of such a generalization. Also the discussion had carried out of possible preference policies to choose among different minimal generalizations.

Surajit Chaudhuri Microsoft Corp. was explains the authorization in SQL is currently at the level of tables or columns. Many applications need a finer level of control. They was propose a model for fine-grained authorization based on adding predicates to authorization grants. The model supports predicated authorization to specific columns, cell-level authorization with nullification, authorization for function/procedure execution, and grants with grant option. The model also incorporates other novel features, such as query defined user groups, and authorization groups, which are designed to simplify administration of authorizations. A model is designed to be a strict generalization of the current SQL authorization mechanism [4].

Ashwin Machanavajjhala et all was defines two simple attacks that a k-anonymized dataset has some subtle but severe privacy problems. First, an attacker can discover the values of sensitive attributes when there is little diversity in those sensitive attributes. This is a known problem. Second, attackers often have background knowledge, and show that k-anonymity does not guarantee privacy against attackers using background knowledge. Give a detailed analysis of these two attacks, and propose a novel and powerful privacy criterion called l-diversity that can defend against such attacks [5] [12].

Alexander Brodsky et all defines the problem of inference channels that occur when database constraints are combined with non sensitive data to obtain sensitive information. Here present an integrated security mechanism, called the Disclosure Monitor, which guarantees data confidentiality by extending the standard mandatory access control mechanism with a Disclosure Inference Engine. The Disclosure Inference Engine generates all the information that can be disclosed to a user based on the user's past and present queries and the database and metadata constraints. The Disclosure Inference Engine operates in two modes: data-dependent mode, when disclosure is established based on the actual data items, and data-independent mode, when only queries are utilized to generate the disclosed information. The disclosure inference algorithms for both modes are characterized by the properties of soundness (i.e., everything that is generated by the algorithm is disclosed) and completeness (i.e., everything that can be disclosed is produced by the algorithm). The technical core of this paper concentrates on the development of sound and complete algorithms for both data dependent and data-independent disclosures [12].

Radu Sion defines the challenges and algorithms for Rights Protection for Categorical Data as new watermark embedding channels are discovered and associated novel watermark encoding algorithms are proposed. While preserving data quality requirements, the introduced solution is designed to survive important attacks, such as subset selection and random alterations. Mark detection is fully “blind” in that it doesn’t require the original data, an important characteristic, especially in the case of massive data. Various improvements and alternative encoding methods are proposed and validation experiments on real-life data are performed. Important theoretical bounds including mark vulnerability are analyzed [11].

3. PROPOSED WORK

According to Zahid Pervaiz et all proposed a framework for accuracy constrained privacy-preserving access control mechanism had defined to improve the security of database. 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 [1]. The specification of the imprecision bound ensures that the authorized data has the desired level of accuracy. 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.

4. CONCLUSIONS

The above conceptual terms defined by various authors states different views regarding the security of relational database such that while in a database that are connected to network should provide strong security while handling it. Here is the need of defining an efficient method to provide security by implementing statistical good access and privacy mechanisms.

ACKNOWLEDGEMENT

I would like to thank one and all those who had help me to write this paper. I would like to thank Prof S. A. Kahate for his valuable guidance and support.

REFERENCES

[1]. Zahid Pervaiz, Walid G. Aref, Senior Member, IEEE, Arif Ghafoor, Fellow, IEEE, and Nagabhushana Prabhu "Accuracy-Constrained Privacy-Preserving Access Control Mechanism for Relational Data" IEEE Transactions On Knowledge And Data Engineering, Vol. 26, No. 4, April 2014.

[2]. Elisa Bertino, Fellow, IEEE, and Ravi Sandhu, Fellow, IEEE "Database Security Concepts, Approaches, and Challenges" IEEE Transactions On Dependable And Secure Computing, Vol. 2, No. 1, January-March 2005.

[3]. Pierangela SamaratiProtecting Respondents' Identities in Microdata Release IEEE Transactions on Knowledge And Data Engineering, Vol. 13, No. 6, November/December 2001.

[4]. Surajit Chaudhuri "Fine Grained Authorization Through Predicated Grants" 2010 WASE International Conference on Information Engineering.

[5]. Ashwin Machanavajjhala, Daniel Kifer, Johannes Gehrke, and Muthuramakrishnan Venkit Asubramaniam "l-Diversity: Privacy Beyond k-Anonymity" IEEE Transactions on Industrial Electronics, Vol. 59, No. 1, January 2012.

[6]. S. Chaudhuri, T. Dutta, and S. Sudarshan Fine Grained Authorization through Predicated Grants IEEE 2012.

[7]. K. LeFevre, R. Agrawal, V. Ercegovac, R. Ramakrishnan, Y. Xu, and D. DeWitt Limiting Disclosure in Hippocratic Databases IEEE 2012.

[8]. D. Ferraiolo, R. Sandhu, S. Gavrila, D. Kuhn, and R. Chandramouli "NIST Standard for Role-Based Access Control" IEEE Transactions on Industrial Informatics, Vol. 9, No. 1, Feb 2013.

[9]. K. LeFevre, D. DeWitt, and R. Ramakrishnan Mondrian Multidimensional K-An onymity 7th International Conference for Internet Technology and Secured Transactions (ICITST- 2012).

[10]. J. Friedman, J. Bentley, and R. Finkel "An Algorithm for Finding Best Matches in Logarithmic Expected Time "IEEE 2012.

[11]. A. Meyerson and R. Williams "The Complexity of Optimal k-Anonymity"2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications.

[12]. G. Aggarwal, T. Feder, K. Kenthapadi, R. Motwani, R. Panigrahy, D. Thomas, and A. Zhu Approximation Algorithms for k-Anonymity computers and security 2013.