Volume 6, Issue 6, June 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

The Survey on Access Controlling Method and Privacy Preserving Mechanisms on Relational Databases

[1]R. R. Tannu, [2]S. A. Kahate
[1] Second Year Master of Engineering, [2] Assistant Professor
[1, 2] Department of Computer Engineering, SPCOE, Dumbarwadi, Otur, Tal:-Junnar, Dist:- Pune, Maharashtra, India

Abstract: ***Now in current days of information or data technology, the particular data or information from existing database that is connected in the network but the thing is that to simply applying protection on databases, Now in during access that particular not provided privacy protection so that times our database can leakage in network. When the ACM provides protection to private or sensitive data and PPM avoid the assessment of data by unauthorized users. Here to the available a introductory and literature survey has presented that help to design efficient system by considering all terms and circumstances.***

Keywords: Access Control Mechanisms, Privacy Preserving, Relational Databases.

I. INTRODUCTION

As organizations developed their system and distributed, information or data systems for daily business, they want to become maximum security breaches even as they gain productivity and advantages of efficiency. Now organizations used some security likes encryption and electronic signatures, are used available to protect or security on data or information when transmitted in sites, a truly that data protection must include mechanisms for controlling the policies based on data or information contents, subject qualifications and characteristics, and other related contextual information or data, such as that time. It is well known that when semantics of data or information must be taken into account in order to specify effective access control policies. Also, methods of CIA specifically tailored to database systems must be adopted [2][4].

Security/protections are specially categorized as unauthorized or wrong data observation, wrong data modification, and data unavailability. Unauthorized data/information observation results in that disclosure of information to users not entitled to gain access to that information. Maximum all organizations, ranging from commercial organizations to social organizations, in a various domains like as healthcare and homeland protection, may suffer heavy losses from both financial and human points of view and its intentions as a consequences of unauthorized data observation. Wrong/not proper data or information modifications of either intentional or unintentional, result in an wrong database state. Now may used of wrong data or information may result in heavy losses for the organization. When data is unavailable or not present, data crucial for the proper functioning of the organization is not readily available when needed [3][5].

Now researching or identifying efforts in that the area of accessing the control models and confidentiality/privacy for DBMSs concentrate on the establishment of two various classes of models, its based that on discretionary access control policy or technics and on the mandatory access control policy or technics. This early research was cast in that framework of relational database systems. The relational data model, being a declarative high-level model specifying the logical structured and its formatting of data/information, made the establishment of simple declarative languages for that specifications of access control policies will possible. These earlier models and the discretionary models in specific, introduced some important ethics that set apart access control models for database systems from access control models adopted by the operating systems and file systems [8].

Content-based access control is an very important requirement that any access control mechanism for use in data management system should be satisfied. Now, content based access control requires that access control decisions are based on data contents. Consider an example of a table recording information or data about employees of a company; a content-based access control policy are manager can only access or manages the employees regarding a company project. Now, When a manager issues sometimes query, the system has to filtering technics used for a query result by returning only the tuples related to the employees that verify the condition of working in the project managed by the manager. Support of SQL is a language for which most operations for data management, like queries, are based on declarative conditions against data contents.

II. LITERATURE SURVEY

The literature survey introduces a huge conceptual concepts and some topics regarding to real topic which will used further that defined to solve the problems. Now here the contributed the some professionals and their works similar to the same topic. The Elisa Bertinoet all declares the some Concepts or procedures, Approaches, and Challenges regarding to database security. They are defined approaches the ACM 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. The mechanisms are discretionary allow subjects to grant authorizations on the data to other subjects. Reasons in that of such flexibility, discretionary policies or technics are adopted in many applications environments and the reason that commercial Database systems adopt such policies or technics [9].

Its important side of discretionary access control are regarding to the authorization administration policy. Authorization or Authentication administration refering that the function of granting and revoking authorizations. Its a functions of the which authorizations are entered or inserted and removed from the access control mechanism. Common policies or technics included 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 will supported or helped decentralized authorization administration. Most commercial Database systems adopt ownership-based with administration delegation. Most complex or sophisticated administration mechanisms may be devised such as joint administration, by which several subjects are jointly responsible for authorization administration [3].

PierangelaSamarati introduces Protecting Respondents' Identities in Micro data or small data Release from the existing database. They defined Today's globally networked society places great or most demand on the dissemination and sharing of information or data. When the past released information was mostly in tabular and statistical form, mostly conditions called today for the release of specific data or information (micro data). In ordered to secured or protect the anonymity of the entities (called respondents) to which information or data refers, data holders always remove or encrypt explicit identifiers likes names, addresses, and contact numbers. Deidentifying data, however, provides no surety of anonymity. Released information or data always contains other data or information like 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.

Now the main point is based on that conceptually and practically represents of k-anonymity. A particular table provides and give us k-anonymity if attempted to link explicitly identifying/finding information or data to that contents map the information/data to at least k entities or k related tuples/records.Here they were showing how to k-anonymity may be provided without any compromising that integrity of information droped used through generalization and suppression technics or its regarding methods.The procedure of minimal generalization that catches the property of the release procedure is not to vanishing the data more than needed to achieve k-anonymity,and present a particular algorithm for the computation of like as a generalization. Also the discussion had carried out of possible preference policies to select among various minimal generalizations.

SurajitChaudhuri Microsoft Corp. had been discussed the authorization or authentication that SQL is currently at the level of tables or regarding columns. Maximum applications need a finer level of control. They were proposed or explanations a model for fine-grained authorization based on the adding predicates to authorization grants. The model helped/supported predicated authorization to specific columns, cell-level authorization or authentication for features or process execution, and grants with the particular option. The model also incorporates other novel features, like query defined user groups, and authorization groups, which are designed to simplify administration of authorizations. A model is designed that the strict generalization of the current SQL authorization mechanism [4].

AshwinMachanavajjhalaet all had been explains two simple attacks that a k-anonymized dataset has some subtle but sometimes seever privacy problems. First, an attacker may be finding the values of sensitive attributes when there is small diversity in that private or sensitive attributes. This is called as problem. Now the Second, attackers always the background knowledge, and show that k-anonymity does not guarantee privacy or sensitive against attackers used some kind background knowledge. Now given a exactly analysis of that two attacks, and propose or explanations a novel and strongly privacy criterion known as the l-diversity that can defend against that particular attacks [5][12].

Alexander Brodsky et all explains the problem of inference channels that can occur when particular database constraints are combined with non sensitive or private data or information to obtain that particular private information. Here available an integrated security mechanism, known as the Disclosure Monitor, which sure data confidentiality by extending the standard mandatory access control mechanism with a Disclosure Inference Engine. Now this Engine generates all the information or data that may be disclosed to a user based on the user's past and present queries and that particular database and metadata constraints. Now that particular Engine operates in two modes: data-dependent mode, when disclosure is developed based on the real data items, and data-independent mode, when only queries are utilized to generate the disclosed information or data. The disclosure inference algorithms for both modes are characterized by the properties or attributes of soundness (i.e. all regarding that is generated by the algorithm is disclosed) and completeness (i.e., all things that may be disclosed is produced by the algorithm). The technical core of this paper focusing on the development of sound and complete algorithms for both data dependent and data-independent disclosures [2].

RaduSion had been discussed that the challenges and algorithms for Rights Protection for Categorical Data as new watermark embedding channels are finding and associated novel watermark encoding algorithms are proposed. When privacy preserving data quality requirements, the introduced solution is designed to survive main thing is that attacks, like subset selection and random alterations. Mark detection is fully "blind" into that is doesn't require the original data, an important characteristic, especially in the case of massive data. different improvements and alternative particular encoding methods are proposed or established and validation experiments on real-life data are performed. Important theoretical bounds including mark vulnerability are analyzed [1].

III. PROPOSED WORK

According to the ZahidPervaizet all proposed a framework for accuracy constrained privacy preserving access control mechanisms had been defined/explains to improved the security of that database. The PPM ensures or guarantee that the privacy or sensitive accuracy goals are met before the sensitive or private data or information is present to the ACM. The authentication and permissions in the access control policy or technics are based on selective predicates on that QI attributes. The policy administrator defines and the explains the permission along with the imprecision bound for each permission user-to-role assignments and role to permission assignments [1]. The specification of the imprecision bound ensures that the authorized data or information has designed level of accuracy. The particular imprecision bound information is not shared with users because that knowing the imprecision bound may possible result in violating the privacy requirement along with imprecision bound for each permission.

IV. CONCLUSION

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

ACKOWLEDGEMENT

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

REFERENCES

[1] 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.

[2] Pierangela Samarati, "Database Security Concepts, Approaches, and Challenges," IEEE Transactions on Knowledge And Data Engineering, Vol. 13, No. 6, November/December 2001. Grants" WASE International Conference on Information Engineering.

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

[4] S. Chaudhuri, T. Dutta, and S. Sudarshan, "Fine Grained Authorization through Predicated Grants," IEEE Transactions On Dependable And Secure Computing, Vol. 2, No. 1, January-March 2012. A Standard for Role-Based Access Control" IEEE Transactions on Industrial Informatics, Vol. 9, No. 1, Feb 2013.

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

[6] G. Aggarwal, T. Feder, K. Kenthapadi, R. Motwani, R. Panigrahy, D. Thomas,and A. Zhu, "Approximation Algorithms for k-Anonymity computers and security," IEEE Transactions On Dependable And Secure Computing, Vol. 1, No. 1, January-March 2013.

[7] Li Liu,Murat Kantarcioglu and Bhavani Thuraisingham "Privacy Preserving Decision Tree Mining from Perturbed Data" International Conference on System Sciences, 2009.

[8] Rezwan Ahmed, George Karypis "Algorithms for Mining the Evolution of Conserved Relational States in Dynamic Networks" IEEE International conference on Big Data, 2014.

[9] K. Browder and M.Davidson, "The Virtual Private Database in oracle9ir2" Oracle Technical White Paper ,vol.500,2002

[10] A Rask , D.Rubin and B Neumann , "Implementing Row-and Cell-Level Security in Classified Database Using SQL Server 2005," MS SQL Server Technical Center ,2005.

[11] K.LeFevre , R. Agrawal, V, Ercegovac , R.Ramkrishnan , Y.Xu,and D.Dewitt,"Limiting Disclousre in Hipppocratic Dtabases ," Proc.30th Int Conf.Very Large Databases ,pp.108-119,2004.

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

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

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

