ISSN: 0976-3031

Available Online at http://www.recentscientific.com

CODEN: IJRSFP (USA)

International Journal of Recent Scientific Research
Vol. 9, Issue, 4(B), pp. 25656-25659, April, 2018

International Journal of Recent Scientific Research

DOI: 10.24327/IJRSR

Research Article

ACCESS CONTROL WITH PRIVACY MECHANISMS FOR RELATIONAL DATA SUPPORTING MULTI-ROLE

Vijaya Bhaskar S. Ch., Chandra Sekhar K., Devaki K and Karthik P

Department of IT, MVSR Engineering College

DOI: http://dx.doi.org/10.24327/ijrsr.2018.0904.1902

ARTICLE INFO

Article History:

Received 8th January, 2018
Received in revised form 21st February, 2018
Accepted 05th March, 2018
Published online 28th April, 2018

Key Words:

Authentication; authorization; access control; anonymization; k-anonymity; l-diversity; precision; privacy preservation

ABSTRACT

In the present advanced world, with the expansion of utilizing web, individual information is gathered with online exercises for examination or for observation. So there is a need of giving protection to the individual information. In numerous associations the touchy information is imparted to approved access, yet there is still revelation of personality of people. So protection is a noteworthy concern. Protection for the delicate information can be accomplished through anonymization calculations and ought to fulfill the properties like k-namelessness or l-assorted variety. The subject of the work is to give protection and least accuracy level to the information.
In this paper, a structure is created which puts an extra component of access control with protection systems for numerous part. At the point when the entrance control and anonymization calculations for information are incorporated, they cooperate as an organization for an application as a configurable security assurance for get to control structure.

INTRODUCTION

Each consortium or organization keeps a game plan of databases to keep up the data and there is a need to impart that data to others. As we are living in the quickly developing world, where web is fundamental and web based business has empowered individuals to complete day by day exercises on the web, for instance, e-managing an account, web based shopping and notwithstanding counselling an expert over the Internet. Such online exercises construe enormous measure of information is created and accumulated constantly. Such accumulated information speak to an essential resource today as they could be utilized for different purposes going from logical research to statistic slant examination or showcasing purposes or in disorder reconnaissance and so forth the aggregation and usage of this individual information is acknowledged as a typical business rehearse today. In any case, this pattern moves to a noteworthy worry for data security. Clients are worried that their own information may fall into various hands and be misused without wanting to. Thus Information privacy needed for personal information. The Confidentiality, Availability and Integrity are designed to empower the Information security within the Organizations. They are weighed to be the necessary components of the security. To guarantee only approved data is to be available to the users, access control mechanism is implemented in the databases. However there is a possibility to misuse of sensitive information by the authorized users. To improve the protection against the identity disclosure and accomplishing the privacy policies, the idea of privacy preservation of sensitive data introduced by fulfilling some privacy prerequisites [2].

The paper deals with the privacy preservation in the anonymity aspects. Sensitive information is an important part of every database and even if we are implementing the privacy protection mechanisms [2] there may have the chances of linkage attacks [4] by the authorized users even though the removal of identifying attributes. This problem has talked about in micro data publishing [3] and protection definitions like k-anonymity [2], l-diversity [5] etc.

Imprecision is an issue in getting the information. An idea of imprecision bound is introduced in order to take care of the issue of imprecision where an insignificant level of tolerance or a threshold is characterized for every permission [1]. The imprecision added to every permission/query and aggregate imprecision for all queries got minimized in the work load anonymization techniques [5], [6]. The protection of XML information also examined in [15] and spatial database[16]. The topic which consists satisfying accuracy constraints for the individual permissions in the idea of workload aware

Corresponding author:* **Vijaya Bhaskar S. Ch
Department of IT, MVSR Engineering College

anonymization had not discussed yet. The accuracy constrained privacy preserving access control mechanism introduced is relevant in the workload aware anonymizations [1]. The point which discusses the continuous data publishing anonymization is presented in [4]. A static relational table is utilized as a part of this paper where the table is anonymized just once. A concept like accuracy constraints for permissions applied to any privacy preserving security policy in role based access control also discussed.

Normally the anonymization techniques are used to ensure the privacy for the data. In many of the works generalization is used [1] which is one of the anonymization technique. In order to preserve the confidentiality of the data, the access control mechanisms are essential for providing authentications whereas the privacy preservation is also important because it prevents the micro data or the sensitive information not to disclose with a third party user.

To enhance the proficiency of the security methods, a privacy preservation module and an accuracy preserving module is joined [1]. The proposed system deals with the access control and data anonymization techniques integrated with multi-role.

The rest of this paper proceeds as follows. In section 2 related work is discussed. The section 3 discusses the previous work. Section 4 discusses proposed work. Implementation and results of privacy protection access control framework is discussed in section 5. Section 6 concludes the paper.

Related Work

Given a relation T = {A1, A2, A3……..An}, where Ai is a property, T* is the anonymized version of the relation R. We accept that T is a static relational table. The properties can be of the following types:

Identifier. Attributes, like name, Id which can uniquely identify an individual. In anonymized relation these characteristics are completely removed.

Quasi-identifier (QI). Attributes, like postal district, gender, date of birth that conceivably distinguishes an individual in view of other data accessible to a foe. QI attributes are summed up to fulfil the secrecy prerequisites.

Sensitive attribute. Attributes, like salary or disease, that if related to one of a kind individual will bring about a privacy beach.

Access control mechanism for relational databases

To characterize tuple-level authorizations fine-grained access control like Oracle VPD [8] and SQL [9] are presented in relational databases. Truman model [10] is introduced for evaluating user queries. A user inquiry is altered by the access control mechanism and just approved tuples are returned in this model. Column level access control permits questions to execute on the approved segment of the relational data [8], [11] Cell level access control mechanisms permit queries by supplanting the unauthorized cell values by NULL values.

For defining permissions on objects based on roles in an association a Role-based Access Control (RBAC) was presented. A RBAC approach setup incorporates an arrangement of Users (U), an arrangement of Roles (R), and a set of Permissions (P). We expect that the selected predicates on the QI attributes characterize a permission for the relational RBAC model, [11]. UA is a user-to-role(U _ R) connection and PA is a role to-permission (R _ P) assignment relation.

Privacy definitions

Here, privacy definitions identified with anonymity are presented.

Definition 1 (Equivalence Class (EC)). An equivalence class is an arrangement of tuples having the same QI attribute values.

Definition 2 (k-anonymity Property). A table T* fulfils the k-anonymity property if every equivalence class has k or more tuples [2].

Previous Work

Access control mechanisms for databases are an imperative idea that permits queries on the approved portion of the database [8], [10]. Later a client approval is constrained to predefined predicates in a Predicate based fine-grained access system [11]. Many techniques introduced for the enforcement of access control and privacy policies, they got discussed in [11]. The interaction between the access control mechanisms and the privacy protection mechanisms was missing in those studies.

Recently, Chaudhuri *et al*. have concentrated on access control with privacy mechanisms [12]. Irregular noise was added to original query in differential security and the outcomes which fulfil protection imperatives. Be that as it may, they don't consider the precision limitations for authorizations. Li *et al*. [5] characterized protection as far as K-anonymity where subsequent to sampling; k-anonymity offers comparable privacy ensures as those of differential privacy.

The accuracy-constrained privacy preserving access control framework [1] allows the access control administrator to indicate imprecision limitations that the privacy protection mechanism is required to meet along the privacy requirements. Both privacy-aware access control and issue of workload-aware anonymization are comparable.

We allude the overview of paper [3] for k-anonymity procedures and algorithms. LeFevre *et al*. [5] in his work the workload aware anonymization methods discussed for the first time, they proposed an algorithm named Selection Mondrian algorithm, it is an alteration to the greedy multidimensional partitioning algorithm Mondrian [10]. In their algorithm, the greedy splitting heuristic minimizes the aggregate of imprecision for all queries on the premise of given query workload. A R+ tree based anonymization algorithm was presented by Iwuchukwu and Naughton in [7].

The anonymized information utilizing biased R+ tree in light of the given inquiry workload is more accurate for queries. Taking into account space, filling curves for k-anonymity and l-diversity Ghinita *et al*. have proposed a few algorithms [13]. They likewise present the issue of accuracy-constrained anonymization for a given bound of satisfactory data loss for every equivalence class [13].

Thus, Xiao *et al*. [14] propose to add noise to queries as per the size of the queries in an offered workload to fulfil differential privacy. In any of these works limits for question imprecision have not been considered. The current literature on workload-

aware anonymization has a centre to minimize the general imprecision for a given arrangement of queries, however the anonymization with imprecision requirements for individual inquiries has not been talked about some time recently. We follow the imprecision meaning of LeFevre *et al*. [6] and present the requirement of imprecision bound for every query in a given query workload.

Proposed Work

Traditionally, research in the database community in the zone of information security can be extensively grouped into two - access control research and information protection research. The idea of access control is to approve a client to get to just a subset of the information. This approval is upheld by expressly revising queries to confine access to the approved subset. The primary limitation of conventional access control system in supporting information security is that it is "black and white" [7]. That is, the access control mechanism offers only two choices: release no aggregate information thereby protecting privacy at the expense of utility, or release accurate aggregates thus risking privacy breaches for utility. Thus, a hybrid system is needed that combines a set of authorization predicates restricting access per user to a subset of data and privacy protection mechanism.

In the proposed system, a relational table, containing sensitive information, is taken. This table is anonymized. The database contains incremental data, with the administrator having the permission to add data into the table. The table has to be anonymized each time data is added into the database. Role based access control is being utilized here. The idea of role based access control (RBAC) started with multi-user and multi-application on-line frameworks. The focal idea of RBAC is that consents are connected with roles and users are allotted to suitable roles. This greatly simplifies administration of authorizations. Roles are made for the different job functions in an association and users are allocated roles in view of their responsibilities and capabilities. Users can be effortlessly reassigned starting with one part then onto the next [18]. The access control approaches characterize choice predicates accessible to parts while the privacy requirement is to satisfy the k-anonymity or ℓ-diversity [7]. Another limitation that ought to be satisfied by the privacy protection mechanism is the imprecision destined for every determination predicate. Query imprecision is defined as the distinction between the quantity of tuples returned by an inquiry assessed on an anonymized relation R* and the quantity of tuples for the same query on the original relation R [1]. The imprecision bound for every permission characterize a threshold on the measure of imprecision that can be endured. If imprecision bound is not satisfied, at that point false alarms are created because of high rate of false positives. The imprecision bound is preset by the administrator and this data is not imparted to the users on the grounds that knowing the imprecision bound can bring about violating the privacy requirement. The imprecision bound will be different for the different roles that exist within the organization. So, in a nutshell, it can be said that the privacy protection module anonymizes the data to meet the privacy requirement along with the imprecision destined for every authorization. The frame work of access control with privacy mechanisms for relational data supporting multi-role is shown in below figure1.

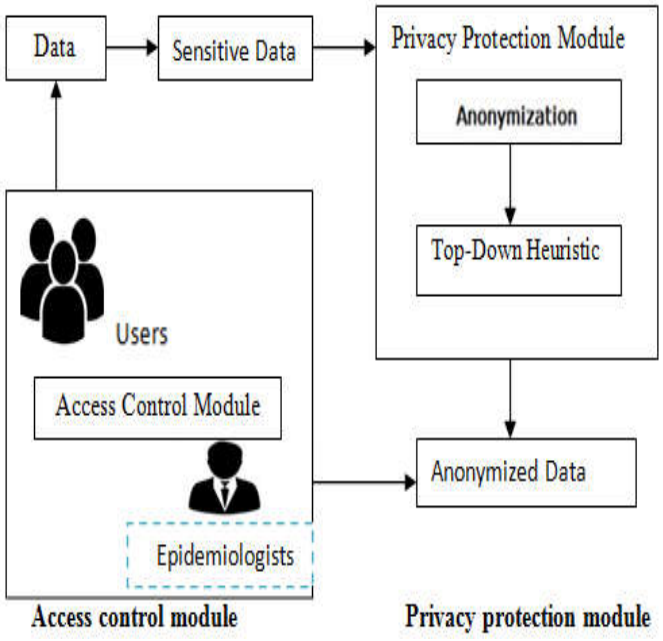

Fig 1 Framework of access control privacy mechanisms for relational data with multi-role

Implementation

The system is implemented in Dreamweaver with JSP support. Tomcat server is used as application server and mySQL as backend database. A medical dataset is taken for the privacy preserving access control model. This medical dataset or relational table is generated based on user/patient registration information. Table1 shows the sample relational table.

Table 1 Consisting of sensitive information

P.Id	Name	Email	Zip	Gender	Age	Disease	Blood Group	Belongs to
Pid1	Teja	Teja@gmail.com	500038	Male	26	Back Pain	A+	CE1
Pid2	Bhavya	bhavya@yahoo.com	504231	Female	40	Cold	A+	CE1
Pid3	Naresh	Navya654@rediff.com	504231	Female	44	Fever	O+	CE2
Pid4	Robert	Jessy876@yahoo.com	500038	Female	34	Fever	A-	CE1
Pid5	John	John.jina@gmail.com	500038	Male	26	Head ach	B+	CE2
Pid6	Meichel	Meichel@hotmail.com	504231	Male	60	Cancer	AB+	CE1
Pid7	Tina	Tina4you@gmail.com	500097	Female	23	Calf	AB+	CE1
Pid8	Miya	miyakit@yahoo.com	500042	Female	45	Dengue	B+	CE2
Pid9	Tabasum	Tabasum7@gmail.com	598765	Female	70	Swine flue	A+	CE1

In this table Patient Id is an Identity attribute. Email, Zip and Gender are Quasi-Identity attributes. Disease is sensitive attribute. Relational table has to be anonimized to different roles to make privacy of sensitive information. Privacy protection can be achieved by using anonimization algorithm called Top- Down Heuristic. In Top-Down Heuristic algorithm, the partitions are spilt along the median cut. Initially the whole tuple space (T) is added to the candidate partitions (CP). If the feasibility cut found from the selected query in while loop, candidate partition (CP) overlaps on QO and resulting partitions are added to CP. Otherwise the Candidate partition is checked for median cut. A feasible cut means that each partition resulting from spilt should satisfy the privacy requirement. Merge the tuples and new partitions are added to resulting table. When anonimization algorithm Top-Down heuristic applies to the relational table, results anonymized table. This anonymized table is viewed by various

Epidemiologists (Table2. and Table3) who have the role based access permission. Thus the privacy for the sensitive information is achieved.

Table 2 Anonimized Table of Country Epidemiologist 1

Zip	Gender	Age	Disease	RBAC
500038-1; 500097-1; 504231-1;	Female-2; Male-1;	1-30	Back Pain	CE1
500038-1; 500097-1; 504231-1;	Female-2; Male-1;	1-30	Cold	CE1
500038-1; 504231-1;	Female-1; Male-1;	31-60	Fever	CE1
500038-1; 504231-1;	Female-1; Male-1;	31-60	Cancer	CE1
500038-1; 500097-1; 504231-1;	Female-2; Male-1;	1-30	Cough	CE1
595765-1;	Female-1;	61-90	Swine Flue	CE1

Top-Down Heuristic Algorithm
Input: R, CP, QO
Output: R^*

Initialize set of candidate partitions(CP←T)
Initialize set of queries with dimensions
While (next)

Select query from QO If(feasibility cut found)

Overlap CP_ion QO_j QO^*= QO^*+QO_j
For (QO_j€QO^*)
Based on CP_i (median)

Merge tuples and found count, for all quasi sets compact new partitions and add to R^* return R^*

Table 3 Anonimized Table of Country Epidemiologist 2

Zip	Gender	Age	Disease	RBAC
500038-1; 504231-1;	Female-1; Male-1;	1-30	Fever	CE2
500038-1; 504231-1;	Female-1; Male-1;	1-30	Head Ach	CE2
500042-1;	Female-1;	31-60	Dengue	CE2

CONCLUSION

The access control and privacy preserving modules are combined in order to provide better results. Here the sensitive information in original database will only be available to the access control modules after providing some privacy to data. The privacy protection mechanism that is being used is called data anonymization. It is used to anonymize the data to meet privacy requirements and the imprecision bound. The system is accuracy constrained because some amount of imprecision is added when the database is updated. Imprecision constraints are introduced on the predicates set by the access control mechanism. The database is incremental in nature with the administrator having the authority to add data into the database. So anonymization has to be applied each time the database is updated. The combined use of access control mechanism and data anonymization ensures both privacy and security of the sensitive information.

References

1. Zahid Pervaiz, Walid G.Aref, Arif Gafoor, Nagabhushana Prabhu "Accuracy constrained privacy preserving access control mechanism for relational data" IEEE Transaction on Knowledge Engineering, vol.26, No.4, April 2014, pp.795-807
2. E. Bertino and R. Sandhu, "Database Security-Concepts, Approaches, and Challenges," IEEE Trans. Dependable and Secure Computing, vol. 2, no. 1, pp. 2-19, Jan.-Mar. 2005.
3. P. Samarati, "Protecting Respondents' Identities in Microdata Release," IEEE Trans. Knowledge and Data Eng., vol. 13, no. 6, pp. 1010-1027, Nov. 2001
4. B. Fung, K. Wang, R. Chen, and P. Yu, "Privacy-Preserving Data Publishing: A Survey of Recent Developments," ACM Computing Surveys, vol. 42, no. 4, article 14, 2010
5. A. Machanavajjhala, D. Kifer, J. Gehrke, and M.Venkitasubramaniam, "L-Diversity: Privacy Beyond k-anonymity"
6. 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.
7. 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.
8. K. Browder and M. Davidson, "The Virtual Private Database in oracle9ir2," Oracle Technical White Paper, vol. 500, 2002
9. S. Rizvi, A. Mendelzon, S. Sudarshan, and P. Roy, "Extending Query Rewriting Techniques for Fine-Grained Access Control," Proc. ACM SIGMOD Int'l Conf. Management of Data, pp. 551-562, 2004.
10. S. Chaudhuri, T. Dutta, and S. Sudarshan, "Fine Grained Authorization through Predicated Grants," Proc. IEEE 23rd Int'l Conf. Data Eng., pp. 1174-1183, 2007.
11. K. LeFevre, D. DeWitt, and R. Ramakrishnan, "Mondrian Multidimensional K-Anonymity," Proc. 22nd Int'l Conf. Data Eng., pp. 25- 25, 2006.
12. N. Li, W. Qardaji, and D. Su, "Provably Private Data Anonymization: Or, k-Anonymity Meets Differential Privacy," Arxiv preprint arXiv: 1101.2604, 2011.
13. G. Ghinita, P. Karras, P. Kalnis, and N. Mamoulis, "Fast Data Anonymization with Low Information Loss," Proc. 33rd Int'l Conf. Very Large Data Bases, pp. 758-769, 2007.
14. G. Ghinita, P. Karras, P. Kalnis, and N. Mamoulis, "A Framework for Efficient Data
15. Anonymization Under Privacy and Accuracy Constraints," ACM Trans. Database Systems, vol. 34, no. 2, article 9, 2009.
16. E. Bertino, S. Castano, and E. Ferrari "Securing XML Documents with Author-X", IEEE Internet Computing, vol. 5, no. 3, pp. 21-30, 2001.

****