International Journal of Advance Engineering and Research Development
Scientific Journal of Impact Factor (SJIF): 4.72
Special Issue SIEICON-2017,April -2017
e-ISSN : 2348-4470 p-ISSN : 2348-6406

Accuracy-Constrained Privacy-Preserving Row Level Access Control Mechanism for Relational Data Using TDH Algorithm

Romil Patel[1],Jignesh Tilva[2]

[1]Asst. Prof. Department of Information Technology, Sigma Institute of Engineering
[2] Asst. Prof. Department of Information Technology, Sigma Institute of Engineering

Abstract *- This particular system is used to protect the sensitive data of an organization that they are maintaining in their day to day life. In paper we use TDH algorithm for privacy preserving and also MD5 for key generation. Before this system is introduced, Access Control Mechanisms is used that assures only that the authorized information is accessed by the user, However, Confidential information can still be misused by authorized users to compromise the privacy of consumers. This concept of privacy-preservation for sensitive data requires the enforcement of several privacy policies and/or the protection against identity disclosure by satisfying some privacy requirements.*

Keywords: Access control, privacy, k-anonymity, query evaluation, Anonymization, Privacy preservation

I. INTRODUCTION

An accuracy-constrained privacy-preserving access control mechanism, illustrated in Fig.1, 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.

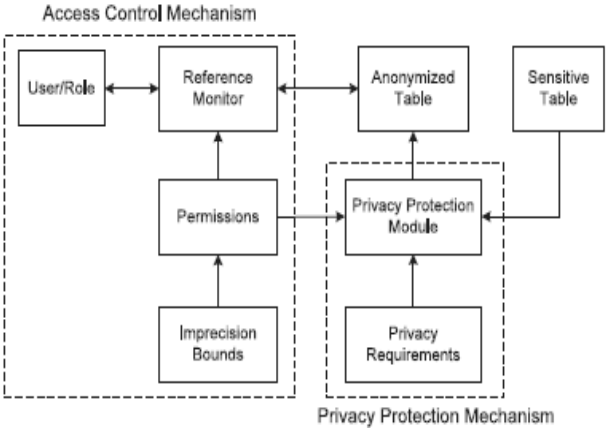

Figure 1 system architecture

II. ACCESS CONTROL FOR RELATIONAL DATA

A. Table level Access Control Mechanism

1) Tuple Level: When evaluating user queries, assume a model called Truman. In this model, a user query is modified by the access control mechanism and only the authorized tuples are returned.
2) Column level: It allows queries to execute on the authorized column of the relational data only
3) Cell level: It is implemented by replacing the unauthorized cell values by NULL values [3].

B. Role-based Access Control

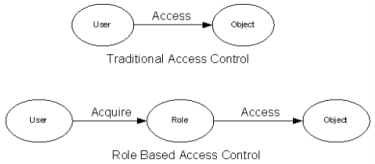

Figure 2 *Role Based Access Control [9]*

The permissions on objects based on roles in an organization [11].
1) U = user1, user2, user3 where U is a set of Users.
2) R = role1, role2, role3 where R is a set of Roles.
3) P = permission1, permission2, permission3 where P is a set of Permission [3].

C.Attributes

1) Identifier: Attributes which is uniquely identify an individual. These attributes are completely removed from the anonymized relation[1][11].
2) Quasi-identifier(QI): Attributes, that can potentially identify an individual based on other information available to an adversary. QI attributes are generalized to satisfy the anonymity requirements[3].
3) Sensitive attribute: Attributes, that if associated to a unique individual will cause a privacy breach[1].

D.Anoymity Definitions

1) Equivalence Class (EC): It is a set of tuples having the same QI attribute values[3].
2) k-anonymity Property: A anonymized table satisfies the k-anonymity property if each equivalence class has k or more tuples [3].
3) Query Imprecision: Difference between the number of tuples returned by a query evaluated on an anonymized relation and the number of tuples for the same query on the original relation [3].
4) Query Imprecision Bound: It is the total imprecision acceptable for a query predicate and is preset by the access control administrator.
5) Query Cut: The splitting of a partition along the query interval values[11]. For a query cut using Query, both the start of the query interval and the end of the query interval are considered to split a partition along the dimension [1].
Select randomly queries and store it into Query Cut set and divide it into an equal interval which is called Uniform Query set [3].

III. PRIVACY PROTECTION MECHANISM

PPM ensures that the privacy and accuracy goals are met before the sensitive data is available to the access control mechanism.

Privacy Protection Module: It anonymizes the data to meet privacy requirements and imprecision constraints on predicates set by the access control mechanism [1].

L-diversity: it is a form of group based anonymization that is used to preserve privacy in data sets by reducing the granularity of a data representation. This reduction is a trade-off that results in some loss of effectiveness of data management or mining algorithms in order to gain some privacy [2].

K-anonymity: A table T_ satisfies the k-anonymity property if each equivalence class has k or more tuples [1].

IV. PURPOSE

This particular system is used to protect the sensitive data of an organization that they are maintaining in their day to day life, so this system prevents the misuse of confidential data from authorized user. This system is useful for the organization which works on Database and primary need is to provide the role based security on database. Also provides privacy preservation on confidential data of organization.

V. PROPOSED SYSTEM

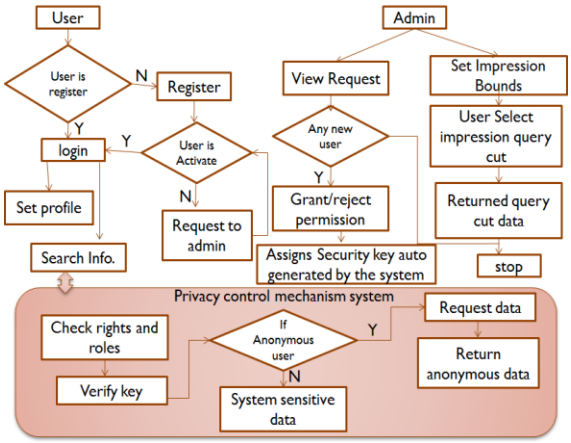

Figure 3 *System flow*

User: First of all the users within the organization register themselves in the system and the registration request goes to admin.
Login: Only after the admin grant the permission user will be able to login into the system.
Set Profile and Search Information: After logging into the system users can set their profile or search for the information.
Check Rights and roles: At the time when user requests for information the system check rights and role of that user if he/she has rights to access the requested information
Verify Key and Sensitive Data: The key will be verified and based on that the system will give an access to either sensitive information or an anonymous data within their imprecision bound. This key will be auto generated by the system when admin grants the permission.
Anonymous data: In case if the key is not verified or its invalid or wrong then anonymous data will be return rather than sensitive data.

View Request: An admin can see the pending user request and can grant for further login or reject the request.
Assigns security key auto generated by the system: After user has successfully logged in into the system, he/she will make a request for data. If admin allow the user to access the information he/she will send the key into mail account. This key is auto generated by the system so that its unique for all records.
Grant/Reject permission: Admin can grant or reject the permissions, sets role and their permissions and set the user imprecision bound that only within this the particular role can access the sensitive information.
Set imprecision bound: Query Imprecision is defined as the difference between the number of tuples returned by a query evaluated on an anonymized relation T and the number of tuples for the same query on the original relation T.
User Select impression query cut: A Query cut is defined as the splitting of a partition along the query interval values. For a query cut using Query Qi, both the start of the query interval and the end of the query interval are considered to split a partition along the jth dimension.

Registration	User_Id	User_Name	User_Password	Blood_Group
3	111	maruti	maruti	O+
4	454	sanket	sanket	O+
5	3435	abhi	abhi	O+
7	656	kantilal	kanti	O+
8	7634	MRT	mrt	O+
9	4355	ashvini	aa	B+
10	kunti	kunti	kunti	o+ve
11	madhuri	madhuri	madhuri	b+ve
12	mayur	mayur	mayur	a
13	az73646	zadeabhi	123456	A+
14	1234	Mahavir	mahi	B+
15	11	madhuri11	madhuri11	0
16	AGLambe123	AshishL	Ayush123@	0-
17	ML	mayurl	mayurl	A
18	55	madhuri55	madhuri55	0
19	11	11	11	o
20	mm	mm	mm	0

Returned query cut data:

7	656	kantilal	kanti	O+
8	7634	MRT	mrt	O+
9	4355	ashvini	aa	B+
10	kunti	kunti	kunti	o+ve
11	madhuri	madhuri	madhuri	b+ve
12	mayur	mayur	mayur	a
13	az73646	zadeabhi	123456	A+

VII. ALGORITHEM STEPS

Proposed Updated TDH Algorithm

Input: Dataset D, Query, BQ, T, K

Output: Partition (p)

Step 1: input dataset D

Step 2: initialization set of candidate partitions.

Step 3: for (CPi ϵ CP) do

Step 4: search the set of queries that overlap candidate partitions.

Step 5: if (feasible cut found)

Step 6: if (check with user secured attributes)

Add it into cp

Else

Do recursively

util anonymity requirement is not satisfy

Step 7: add into result set

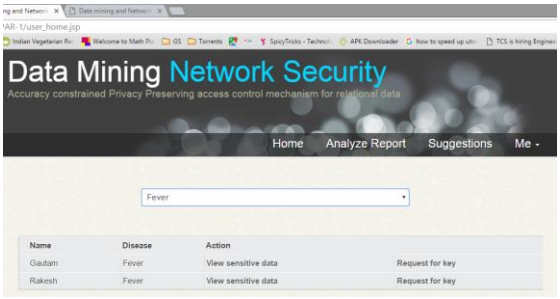

Figure 4 *User Data*

Figure 5 *anonyms data of user*

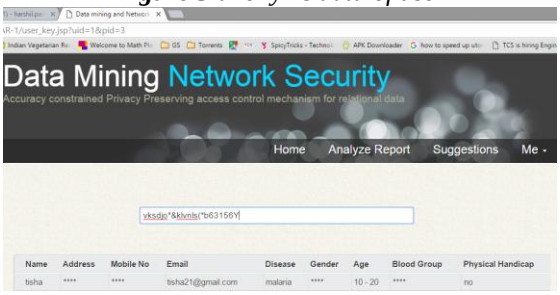

Figure 6 *wrong key Sensitive data*

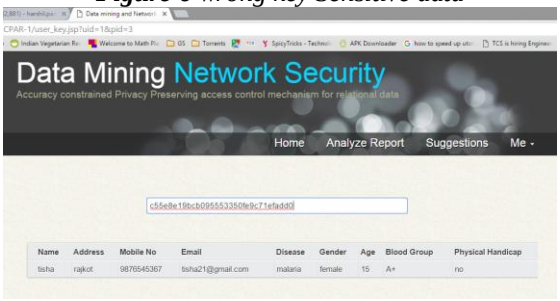

Figure 7 *Right Key Sensitive Data*

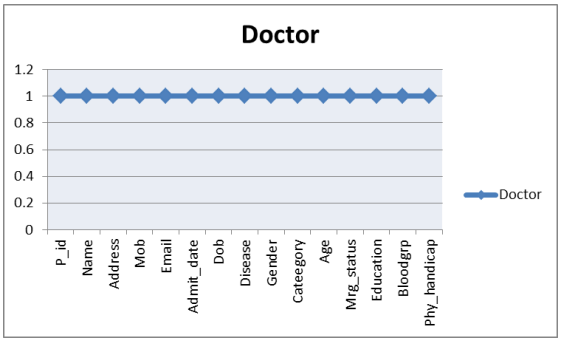

Figure 8 *without privacy preserve for doctor*

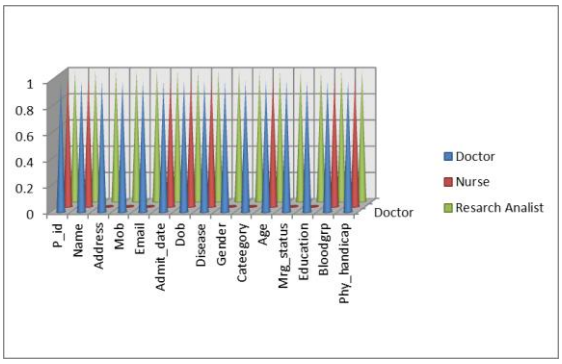

Figure 9 *with privacy preserve for all*

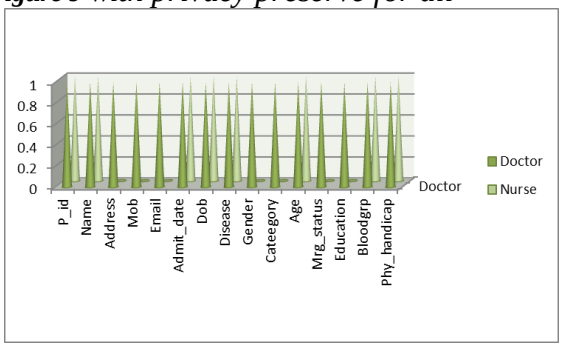

Figure 10 *role base access for doctor and Nurse*

VI. CONCLUSION

This system is useful for the organization which works on Database and primary need is to provide the role based security on database. Also provides privacy preservation on confidential data of organization. In the current work, static access control and relational data model has been assumed. For future work, we plan to extend the proposed privacy-preserving access control to incremental data and cell level access control.

REFERENCES

[1] . Zahid Pervaiz, Walid G. Aref, Senior Member, Arif Ghafoor, Fellow, and Nagabhushana Prabhu,"Accuracy-Constrained Privacy-Preserving Access Control Mechanism for Relational Data", IEEE TRANSACTIONS, VOL. 26, NO. 4, APRIL 2014.

[2] . Ankitha.N.Kulkarni, Ashwini.S, Vidhyashree.S, Chandrashekar. "K.TAccuracy-Constrained Privacy-Preserving Access Control Mechanism for Health Care Systems",IJARCCE *Vol. 4, Issue 5, May 2015*

[3] . Madhuri S. Lambe, Vrunda K. Bhusari," Accuracy-Constrained Privacy-Preserving Cell Level Access Control Mechanism for Relational Data", Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

[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] . Machanavajjhala, D. Kifer, J. Gehrke, and M. Venkitasubrama- niam, "L -Diversity: Privacy Beyond k-anonymity," *ACM Trans. Knowledge Discovery from Data*, vol. 1, no. 1, article 3, 2007.

[6] . P. Samarati, "Protecting Respondents' Identities in Microdata Release," *IEEE Trans. Knowledge and Data Eng.*, vol. 13, no. 6, pp. 1010-1027, Nov. 2001.

[7] . 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.

[8] . 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.

[9] . Suhasini Gurappa .Metri, Dr. D. R. Shashi Kumar, "Security Management Methods in Relational Data", International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169 Volume: 3 Issue: 4

[10] .Elisa Bertino, Ravi Sandhu, "Database Security—Concepts, Approaches, and Challenges", IEEE Transactions on Dependable and Secure computing, vol. 2, no. 1, january-march 2005

[11] .Bhoomi Desai, Vidhi Rathod, Kalyani Adawadkar "Accuracy-Constrained Privacy-Preserving Row Level Access Control Mechanism for Relational Data" ISSN (online): 2321-0613

