RESEARCH ARTICLE OPEN ACCESS

The Constrained Method of Accessibility and Privacy Preserving Of Relational Database

Mr Rakesh Ramesh Tannu*, Prof. Sandip A. Kahate**
**(Second Year Master of Engineering, Department of Computer Engineering, SPCOE, Dumbarwadi, Otur, Tal-Junnar, Dist-Pune, Maharashtra, India)*
*** (Assistant Professor, Department of Computer Engineering, SPCOE, Dumbarwadi, Otur, Tal-Junnar, Dist-Pune, Maharashtra, India)*

ABSTRACT
Now in organizations or companies maximum information or data available and that data are related to tabular form means relational database. Sometimes organization wanted to distribute that particular information or data in within organization or other organization in daily basis. Here the thing is that the organization faces the some kind of problems of security related because they distributed that information for its purposes and here sometimes organization wanted that particular information will be modified or upgraded, Now they can used numbers of methods or technics for encryption and electronic signatures for given a security and protection of that particular data in during transmission network. In that protection of that protection used various different mechanisms and strong methods for accessing that specific that particular data or information. It is very well known that current or today the proper data must take as access control polices. Also some kind of methods for CIA towards database system must be adopted.

Keywords: Privacy Preserving Mechanism, Access Control Mechanism, Access Control, k-anonymity, Relational Database.

I. INTRODUCTION

Organizations often stored and collect consumer data or information for improved the maximum their services. Access Control Mechanisms (ACM) gives a surely used that only authenticated or authorized and proper data available to users. Whenever the sensitive or private data may be wrong used or sometimes misused by authorized users to manage the privacy of consumers. Now the privacy-preservation is to used for control policies or methods on sensitive data that protection against identity disclosure by using some kind of privacy requirements.

Now the private or sensitive information or data, also they can be removed of identifying attributes very easily linked attacks by the authorized or legal persons .The suppression and generalization of records to satisfy privacy requirements by using Anonymization algorithm with minimum distortion of micro or small data. The both security and protection on private or sensitive information used the particular Anonymity methods guarantee to us. Now a privacy achieved that of accuracy and imprecision are introduced in accurate or proper and authorized information under the control policy and some kind of methods.

II. LITERATURE SURVEY

Now in current time in various organizations those arrival data or information is a various format and increasingly size continuously in network. Sometimes the different organizations are now shifting their transactions and shopping and also their infrastructure through a web since end users. So everyone interacting to the world wide web and taking wanted his needs, due to this a large that is huge data comes at host in a network. The literature survey is an important part in this paper because its introduces past work or its regarding some functions of different authors which helpful while the whole paper.

Elisa Bertino et all [1] give us a perfect solution on data security and protection used following three points: To give a security on private or sensitive information or data against unauthorized disclosure, integrity is the prevention of unauthorized and not properly or correctly data modification and availability is prevention recovery from the hardware and software problems and other regarding from malicious data access denials make the database system unavailable.

Pierangela Samarati et all [2] has been defines or explains that the currently in Networking mostly demand that broadcasting and shearing the information/ data, Sometimes in past conditions released or distributed the particular information was many times in tabular and statistical format max conditions call the information on today release in particular small or micro data. To provide the protection or security on anonymity of the entities called as respondents that particular information or data refers, Now the data holders often remove or encrypting explicit identifiers like names, addresses

and phone numbers. Deidentifying data/information, However gives not guarantee of anonymity released or drop particular information often conditions another data like race, birthdate, sex and ZIP code that specific information or data to publicly available to reindentify respondents and inferring information or data was not intended for disclosure. They address problems or sometimes issues of drop or releasing micro data while safeguarding the anonymity of that the respondents to which the process of k-anonymity. A table providing k-anonymity if attempts to link explicitly finding/identified information or data to that its content map that information/data to minimum k-entites.

Ashwin Machanavajjhala et all [3] had been explain about two normal attacks or simple attacks that k anonymized data or information collection has some or minimum subtle but severe privacy or protection related problems are occurred. First, the attacker may be find the values of private or sensitive attributes/properties, that is a specific problem. Second, attackers often have background knowledge, and show that k-anonymity does not have guarantee against attackers using background knowledge. Now to provide a exactly analysis of these two attacks, and a novel and strong privacy criterion called l-diversity that can defend against like attacks.

Alexander Brodsky et all [4] defines or explains complex/sophisticated conditions/situations of inference channels that activated while database constraints are combined/together with non private/sensitive information to obtained that the particular private or sensitive information. Now here present an integrity security mechanism, called as the Disclosure Monitor, which guaranteed or confirm data private/sensitive or confidentiality by extending the standard must access control mechanism with a Disclosure Inference Engine. That particular Engines provides and gives us that all the data/information that is disclosed to a user based on the user's past and present queries and the mata data and database constraints, Now the particular engine are operated in two modes: data dependent mode when disclosure is established based on the real data values and data independent mode while only queries are utilizing to generated the disclosed data/information, that the particular disclosure interference algorithms are two modes to characterize by the properties of soundness (i.e. everything are is make by the algorithm) The technical base or core focus on the establishment of sound and complete that algorithms on both data dependent and data independent disclosures.

III. SYSTEM ARCHITECTURE

3.1 Existing System

- The privacy-preservation is that the particular protection/security on identity disclosure used some other kind of requirements.
- The private or sensitive information, after cancellation of identifying attributes, are untill get easily to link attacks by authorized/ legal users.
- Suppression & generalization of relational data used by PPM.

3.2 Limitation of Existing System

- To users no privacy used.
- All queries regarding aggregate imprecision is very lass or minimum.
- Micro data/small data sometimes are not known.
- To individual/single person, this method not good.

3.3 Proposed System

- PPM & ACM are used strongly for Relational database.
- Proper Formulation the accuracy and privacy constraints.
- All problems evaluation used the Heuristics process.

Now the PPM gives us the confirmation for the privacy and accuracy targets are met but firstly the private/sensitive data present. The selected predicates of QI attributes through the permission of access control policy or method. The imprecision bound for each and every permission query defined by the administrator policy, role-to-permission assignments and user-to-role assignments. The authorized data/information has been on desired level of the accuracy by the surely the function of the imprecision bound.

To users not shared/passed the imprecision bound data or information because knowing the imprecision bound in result in violating the particular privacy/sensitive requirements. The imprecision bound for each and every permission with PPM is wanted to meet privacy requirements. After the anonymization the particular proper tuples/records values in relation are replaced with the generalized values. In that cases, the access control enforcement over the generalization data/information need the properly explained, Now here two point discussed that Relaxed and Strict access control enforcement mechanisms over anonymized data/information. The access control enforcement by reference monitor are available two type as follows.

- To permission that the all partitions that are overlapped permissions.

- To permission that only particular partitions that is fully enclosed permission.

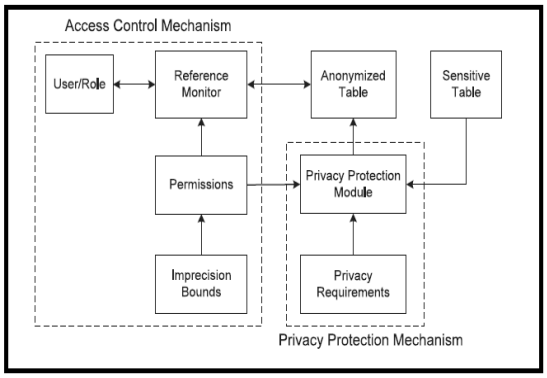


Fig. 1: Proposed Architecture

IV. IMPLEMENTATION DETAILS

Here completing all the process than used following two algorithms.

- TDH-(Top Down Heuristic Algorithm)
- TDH-1(Top Down Heuristic Algorithm 1)
- ECC-(Elliptic Curve Cryptography)

4.1 Algorithm: Top-Down Heuristic Algorithm

The TDH algorithm is mostly used the greedy and proper heuristics partitioning that divided list at median, Sometimes if the median again falls inside the specific query than again the splitting the specific partitions and when overlapped query still not occurred so the imprecision related query cannot change as both the new partitions. Now splitting the partition along the query cut and then selected the dimension/size at least along which the imprecision is for all that queries.

It works under the following stages

Input: T, K, Q, and BQ_j
Output: P

1 Initialize Set of Candidate Partitions(CP←T)
2 **for** (CP_i Ɛ CP) **do**
3 Find the set of quries QO that overlap CP_i such that ic^{Qo}_j and $ic_{CPi} > 0$
4 Sort queries QO in increasing order of BQ_j
5 **while**(Feasible cut is not found) **do**
6 Select query from QO
7 Create query cuts in each dimension
8 Select dimension and cut having least overall imprecision for all queries in Q
9 **if** (Feasible cut found) **then**
10 Create new partition and add to CP
11 **else**
12 Split CPi recursively along median till anonymity requirement satisfied
13 Compact new partition and add to P
14 return (P)

4.2 Algorithm: Top-Down Heuristic Algorithm 1

Now the particular partition is divided through a logical database and its regarding constituent elements in distinct independent parts.The particular Database partition MPA(manageability, performance and availability) that particular reasons are used. The comparison between the query bound and query imprecision through the definition o the query imprecision.This Algorithm is used for repartitioning procedures .

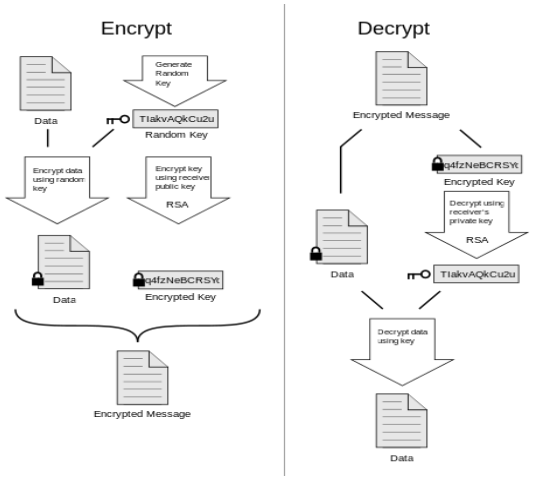
It works under the following stages

Input: T,K,Q, and BQ_j
Output: P

1 Initialize Set of Candidate Partitions(CP←T)
2 **for** (CPi Ɛ CP) **do**
//Depth-First (preorder) traversal
3 Find the set of quries QO that overlap CP_i such that ic^{Qo}_j and $ic_{CPi} > 0$
4 Sort quires QO in increasing order of BQ_j
5 Select query from QO with smallest BQ_j
6 Create query cuts in each dimension
7 Reject cuts with skewed partitions
8 Select dimension and cut having least overall imprecision for all queries in Q
9 **while**(Feasible cut is not found) **do**
10 Select query from QO
11 Create query cuts in each dimension
12 Select dimension and cut having least overall imprecision for all queries in Q
13 **if**(Feasible cut found) **then**
14 Create new partitions and add to CP_i
15 **else**
16 Split CP**i** recursively along median till anonymity requirement satisfied
17 Compact new partitions and add to P
18 Update BQ_j according to ic^{Qj} and ic_{Pi} , ∧ Q_j Ɛ Q
19 return(P)

4.3 Algorithm: Elliptic Curve Cryptography Algorithm

This Algorithm is used for strong Authentication, Security and Protection. Its used to construct the Public Key Cryptography System. Its used many times public key (Asymmetric) but here instead of Asymmetric key used Random key for Sender and Receiver for performing accordingly Encryption and Decryption



V. EXPERIMENTAL RESULT

The purposes of the experimental calculations are to check the impact of before and after partitions of table through tulpe wised.

Table 1 Sensitive

ID	AGE	ZIP CODE	DISEASE
1	17	22	FLU
2	26	32	FEVER
3	32	42	DIARREA
4	37	32	FLU
5	20	22	FEVER
6	40	42	DIARREA

Table 2 Anonymous

ID	AGE	ZIP CODE	DISEASE
1	0-20	10-30	FLU
2	0-20	10-30	FEVER
3	20-30	10-30	DIARREA
4	20-30	30-40	FLU
5	30-40	30-40	FEVER
6	30-40	30-40	DIARREA

Table 3 Partition Accuracy Id Variations

ID	Before Partition Selection	After Partition Selection
10	50%	60%
50	60%	70%
100	70%	80%

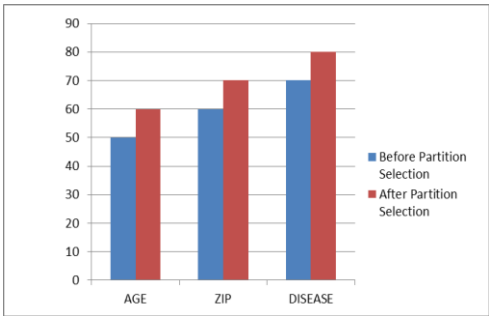


Fig 1: Partition Accuracy ID Variations

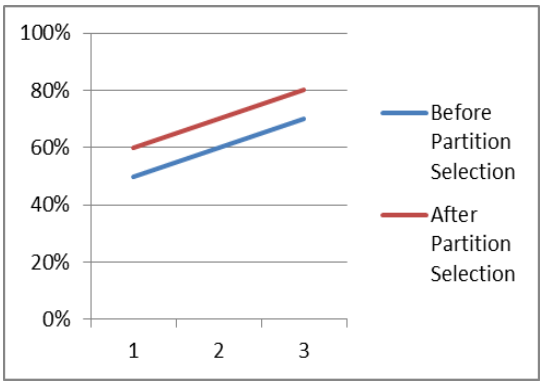


Fig 2: Partition Accuracy ID Variations

Where 1:- AGE
2:- ZIP
3:- DISEASE

VI. CONCLUSION AND FUTURE SCOPE

The ACM and PPM are together through the framework, The ACM gives the permissions only proper/authorized query predicates on private information. The PPM anonymizes to meet the sensitive requirements and the ACM are set to predicate imprecision constraints. Now due to above all predicates regarding terms the better security methods or technics when accessing and sharing large organizational crucial relational dataset.

ACKNOWLEDGMENT

I would like to thanks to my project guide Prof. Sandip Kahate they have been given me proper guidance for writing this paper.

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.

[5]. A Standard for Role-Based Access Control" IEEE Transactions on Industrial Informatics, Vol. 9, No. 1, Feb 2013.

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

[7]. 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.

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

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

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

[11]. 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.

[12]. 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.

[13]. K.Le Fevre,D.De Witt, and R. Ramkrishnan, "Mondrian Multidim mentional K-Anonymity," Proc.22nd Int'l Conf.Data Eng.,pp.25-25,2006.

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

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