International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 04 Issue: 08 | Aug -2017 www.irjet.net p-ISSN: 2395-0072

Privacy Preservation Using Partition Technique

Swati Abhimanyu Nase

Master of Engineering, Computer Science & Engineering ,CSMSS CHH , Shahu College Of Engineering , Aurangabad, Maharashtra ,India

---

Abstract – Privacy preserving data mining applied to privacy violating applications. Sensitive information, confidential information are only access certain authorized person. Randomization, k-anonymity privacy preserving methods used for privacy preserving data mining. Medical database mining is one of application of privacy preserving data mining. This paper represents heuristic strategy for privacy preserving data mining.

Keywords : Access, Randomization, k-anonymity, Heuristic, Privacy preserving data mining

I . INTRODUCTION

When too much time or memory required direct search techniques not applied. Heuristic solve problem more quickly and find approximate solution for solving a problem. Whether to use heuristic for solving problem includes criteria optimality, completeness , accuracy and precision, execution time. Consider algorithm approach for driving some one house. It gives direct instruction like take west hill mall exit, drive 250 miles down to hill, turn left take first right. The large while colour house at north. Heuristic approach for getting someone house. Find the last letter i mailed you .Drive to the town, ask someone where our house is, somebody glad to help you. If you can't find someone call me on phone and i will come to get you. Objective of heuristic is produce solution in reasonable time frame for solving problem in Hand.

II. LITERATURE SURVEY

To anonymized data generalization and suppression techniques applied. Access control policy defined where authorized person having permission to access particular record. Concept of identifier attribute, quasi identifier attribute, sensitive attribute defined. Heuristic for partition implemented by using different heuristic algorithm [1]. Fine Grained Authorization through Predicated Grants paper present generalization of SQL authorization mechanism. Authorization at level of tables and column. Fine grained control restricts access to only information in some rows in table further certain column in rows required in practical database application. Example employee can see some columns of rows corresponding to their employee's data. Current SQL authorization models course grained which access all rows of table or not at all. Fine grained authorization can be implemented in current SQL language definition by using views or table valued function with built in function such as user id which provide user specific parameter values .User id provides identity of application user. Predicted grant statement authorized access only rows that satisfies grant predicate. Suppose department head access to information of employee. Other authorization on same object valid through revoke grant permission to column. Grant with nullify is specified on column queries can access column but value return for row will be NULL. Salesperson can see the aggregate of sale aggregate is used .Example select region sum(units) from sales. Authorization group is granted to user group or role. predicate call to user defined function enabling full power of programming language to be used when required[2].

III. EXPERIMENTAL RESULTS

Main focus on how many record to fetch using top down heuristic based on selection predicate whether it is Quasi identifier attribute, Sensitive attribute, role identifier attribute .Performance measurement depends on time in millisecond vs. no of record to fetch. Successful login for user test case. Graphs based on time in millisecond vs. no of tuple fetch drawn based on predicate selection condition.

Table1-Series1.

Role identifier attribute	YES
Quasi identifier attribute	NO
Sensitive attribute	NO

Table1 series1 contains information where role identifier attribute set value YES, Quasi identifier attribute set value NO and sensitive attribute set value NO

Table2-Series2.

Role identifier attribute	YES
Quasi identifier attribute	YES
Sensitive attribute	NO

Table2 series2 contains information where role identifier attribute set value YES, Quasi identifier attribute set value YES and sensitive attribute set value NO.

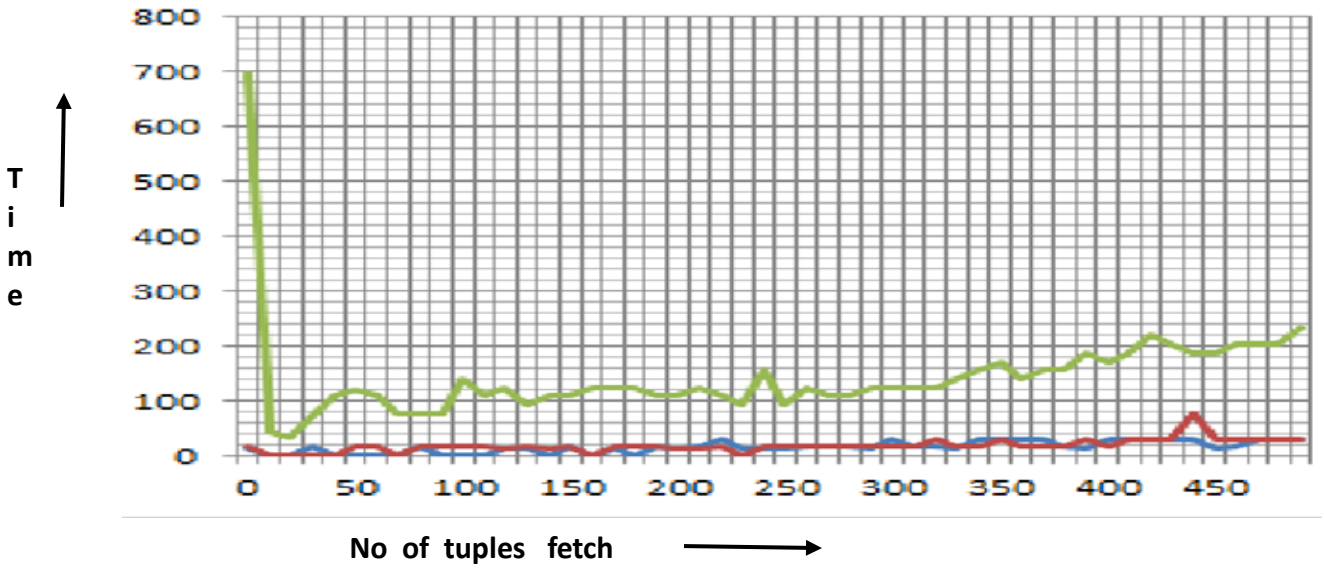
Table3-Series3

Role identifier attribute	YES
Quasi identifier attribute	YES
Sensitive attribute	YES

Table3 series3 contains information where role identifier attribute set value YES, Quasi identifier attribute set value YES and sensitive attribute set value YES. How much time required fetching record from database based on top down heuristic algorithm, role identifier, quasi identifier, sensitive attribute and imprecision bound on that performance analysis depends. Following fig1 give line graph representation based on number of tuple fetch VS time in millisecond.

Fig 1. Line graph representation

Performance parameter : Number of tuple fetch VS time in millisecond .



Series1 in table1 indicated by blue line, series 2 in table2 indicated by red line, series3 in table3 indicated by green line. Time required for series1 is less, series2 is more and series3 is most.

IV CONCLUSION

Implementation of heuristic technique for partition to fetch record from database based on series1,series2, series3 condition described in table1,table2, table3. Graph based on predicates selection condition VS time is drawn for performance measurement.

REFERENCES

[1] IEEE TRANSACTION ON KNOWLEDGE AND DATA ENGINEERING VOL.26,NO 4,APRIL 2014 Accuracy-Constrained Privacy Preserving Access Control Mechanism for relational data by Zahid Pervaiz, senior Member, IEEE, Arif Ghafoor, Fellow,IEEE and Nagbhushana Prabhu.

[2] 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.