DUAL ENCRYPTION MECHANISM IN OUTSOURCED TRANSACTION DATABASE

DHAVAL R. PATEL
DEPARTMENT OF COMPUTER ENGINEERING
HASMUKH GOSWAMI COLLEGE OF ENGINEERING
VAHELAL,AHMEDABAD

ABSTRACT

In my research paper there are used a dual security in many other research I see that there are security at client side server side some other but I observe there is some problem I there so I think that security provide at all side because some time provider or database administrator also see our data. So here I implement such security which are protect our database from client side as well as service provider side. In our system actual data can change using fact entry and using key and hashing function we can get actual data.

INTRODUCTION

Many researchers have found several approaches for outsourced transaction database. So several methods such Access control based approach, Attribute based approach, Fake tuple insertion based approach, Hardware-level encryption based approach, Secret share distribution based approach, Order preserving encryption based approach, Authenticated data structure based approach, Fragmentation based approach, Combined fragmentation and encryption based approach, Insert prototype in oracle based approach and Secret sharing and fake-tuple insertion based approach come into existence to maintain privacy in outsourced transaction database. Here we discussed benefits and drawbacks of all these techniques. I implement such security which are protect our database from client side as well as service provider side. In our system actual data can change using fact entry and using key and hashing function we can get actual data.

KEEYWORD Encryption, Hash Faction, Decryption

IDENTIFY, RESEARCH AND COLLECT IDEA

I study below research paper for getting ideas

1.Order Preserving Encryption Based Approach : Getting idea about encryption and hash function technique.

2.Secret Share Distribution based approach : Getting idea about dual security.

3.Fragmentation based approach : Getting idea about data base fragment and apply encryption on fragment data base

4.Fake Tuple Insertion Based Approach : Getting idea about add fact tuple to hide actual value

WRITE DOWN YOUR STUDIES AND FINDINGS

Encryption of Original TDB:-
Input: -Original TDB D Output: -Encrypted TDB D*
Steps:-

1. First apply 1-1 substitution method to hide original item's name, so convert original TDB D as cipher transaction database D^*.

2. After applying substitution method arrange all the cipher items in tabular form with respectto their support values (number of occurrences of item in original TDB).
3. Arrange all the items in the decreasing order of support and apply rob frugal k-grouping methodto divide items in group. The grouping algorithm given below:-
   Gfrug definition:- Assume e1, e2, . . . , en is the list of cipher items in descending order of support (with respect to D), the groups created by Frugal are {e1, . . . ,ek}, {ek+1, . . . , e2k},

and so on. The last group, if less than k in size, is merged with its previous group. They denote the grouping obtained using the above definition as Gfrug. Given a TDB D and its Frugal grouping Gfrug = (G1, ...,Gm), the grouping method Rob Frugal consists in modifying the groups of Gfrug by repeating the following operations, until no group of items is supported in D:

1) Select the smallest j ≥ 1 such that suppD(Gj) >0;

2) find the most frequent item i∈Gjsuch that, for the least frequent item I of GjThey have: suppD(Gj\ {i} ∪ {i}) = 0; and

3) swap Iwithi’ in the grouping.

4. Adding fake transaction in following way
   a. Put “0” value of the noise column in which item has maximum support in the group.
   b. Find noise value corresponding to item with maximum support in group in table.
   c. Count noise value for every items using equation N(ei) =Max support of Item – Support of (ei).
   d. Discard all rows whose noise value are “0” and arrange all rows in decreasing order of their noise values.
   e. Create hash table to store value of noise or frequency of occurrence of fakely occurred in TDB with <ei, Timesi, occursi> where, ei = Num of item in TDB, timesirepresents the number of times that the fake transaction {e1, e2, . . . , ei} occurs in the set of fake transactions, and occiis the number of times that eioccurs altogether in the future fake transactions after the transaction {e1, e2, . . . , ei}, the ith entry of a hash table HT containing the item eihastimesi= N(ei) − N(ei+1)occursi= where g is the number of items in the current group.
   f. Do these all steps till added all fake transaction in all group.

5. Then finally add these fake-transactions in the original database and sends to the third party service-provider.
   END

<u>Decryption (True Pattern-Mining Task):-</u>

Input: - Query Output: -True Pattern Mining Result

Steps:-

1. Data-owner fire query or give minimum threshold value of support for mining particular pattern.
2. Servers mining result from the encrypted pattern and send mined result to the data-owner.
3. Then after data-owner removes fake transaction with the help of below equation

Support(S) = Supp D*(E) – (Supp D*(E) - Supp D (E))

Where, for every item set S and its corresponding cipher item set E, we have that suppD(S) ≤ suppD∗ (E).

S = support of item set in TDB

D*(E) = Encrypted TDB with fake support

D (E) = Encrypted pattern with original support

4. Finally Data-owner get true pattern from fake-transaction.

END

TDB and its support table. (a) TDB. (b) Item support table.

(a)

TDB	
Bread	
Milk	Bread
Bread	Milk
Water	Milk
Bread	Beer
Bread	Eggs
Water	

(b)

ITEM	SUPPORT
Bread	5
Milk	3
Water	2
Beer	1
Eggs	1

Step 1 Apply 1-1 substitution method in order of alphabetically of every items.

Encrypted TDB

Items	Support
e1	1
e2	5
e3	1
e4	3
e5	2

Step 2 Arrange tables of items in decreasing order of support.

.Encrypted TDB in decreasing order of support

Items	Support
e2	5
e4	3
e5	2
e1	1
e3	1

Step 3 Do grouping using Rob frugal grouping method (Grouping with k=2).
Grouping of encrypted TDB D*

Items	Support
e2	5
e5	2
e4	3
e1	1
e3	1

Here k=2 means in one group minimum items elements are 2 so G1= {e2, e5} and G2= {e4, e1, e3}
Step 4 Adding fake transactions

A. Find noise value corresponding maximum support of an item in particular group.

Noise table of TDB

Items	Support	Noise
e2	5	0
e5	2	3
e4	3	0
e1	1	2
e3	1	2

B. Discard the row which has noise value is “0”
Noise table after discarded rows of “0” value

Items	Support	Noise
e5	2	3
e1	1	2
e3	1	2

C. Arrange the rows in decreasing order of noise
Noise table of decreasing order of noise

Items	Support	Noise
e5	2	3
e1	1	2
e3	1	2

D. Create Hash table to store the value of noise or frequency of occurrence of fakely in original TDB using <Ei, Timei, Occursi> In general, the ith entry of a hash table HT containing the item eihastimesi= N(ei) − N(ei+1)

occuri= $\sum_{j=i+1}^{g} N(ej)$ where g is the number of items in the current group.

Here, i=5 N(e5)=3 times3=N(e5) – N(e1)
= 3 – 2=1
Occurs of e5 = 2

Hash Table

Hash Table
< e5,1, 2 >
< e1, 0, 2 >
< e3, 2, 0 >

ei, timesi, occi, where timesirepresents the numberof times that the fake transaction {e1, e2,.,ei} occurs inthe set of fake transactions, and occursiis the number of timesthateioccurs altogether in the future fake transactions after the transaction {e1, e2, . . . , ei}.
So, in this way data-owner send the encrypted TDB D* with adding fake transaction to the server.

CONCLUSION

We have studied the problem of corporate privacy-preserving mining of frequent patterns on an outsourced TDB. We have proposed an encryption scheme in which grouping done by using columnar transposition methodand finally adding fake transaction. The fake transactions are efficiently increases by our novel grouping method and grouping execution time is less as compare to base work.

Additionally we have proposed encryption with RSA to encrypt mine result with data-owner’s public key so here provides two layer securities. This approach allows to a data owner, like a supermarket, to give its data in outsourcing to a service provider and to obtain query service from it, without disclosing important information, like customer’s behaviour. So in this way we can say that by our proposed approach privacy is preserved in outsourcing TDB as well as in mining pattern.

REFERENCES

[1] www.oracle.com/technetwork/topics/.../oes-refarch-dbaas 508111.pdf
[2] http://dbaas.wordpress.com/2008/05/14/whatexactly-is-database-as-a-service/
[3] https://451research.com/reportshort?entityId=78105&referrer =marketing
[4] E. Mykletun, M. Narasimha, and G. Tsudik, “Authentication and integrity in outsourced databases”, In Proc. of ACM Trans. On Storage, vol. 2, 2006, pp. 107-138.

[5] M. Xie, H. Wang, J. Yin, and X. Meng, "Integrity auditing of outsourced data,"VLDB 2007, pp. 782-793.

[6] Zheng-Fei Wang, Ai-Guo Tang, "Implementation of Encrypted Data for Outsourced Database", In Proc. of Second International Conference on Computational Intelligence and Natural Computing (CINC), IEEE, 2010, pp. 150-153.

[7] Li Feifei, Marios H, George K, "Dynamic Authenticated Index Structures for Outsourced Database", In Proc. of ACM SIGMOD'06. Chicago, Illinois, 2006, pp. 121-132

[8] SomchartFugkeaw, "Achieving Privacy and Security in Multi- Owner Data Outsourcing", In Proc. of IEEE Transactions 2012, pp.239-244.