DOI 10.29042/2019-4781-4790

Helix Vol. 9 (1): 4781- 4790

A Novel Approach of Association Rule Hiding Using DBCT (Distortion, Blocking and Cryptographic Technique)

*[1]P. R. S. Naidu, [2]B. Prasanth Kumar, [3]Dr. P. Sateesh, [4]Dr. B. Srinivas, [5]Chandra Sekhar Darapaneni
[1,3,4]Department of Computer Science Engineering, MVGR College of Engineering Andhra Pradesh, India
[2]Department of computer Science Engineering, Raghu Institute Of Technology Andhra Pradesh, India
[5]Scholar, Acharya Nagarjuna University Andhra Pradesh, India
Email: prsn1988@gmail.com,prasanthkumar.cst@gmail.com, satish@mvgrce.edu.in, srinio.b@mvgrce.edu.in, dsekhar1807@gmail.com

Received: 15th October 2018, Accepted: 29th January 2019, Published: 28th February 2019

Abstract
Associative rule hiding is a technique used in hiding sensitive data, during data processing to secure the sensitive association rules generated using association rule mining. Several methods were planned within the literature for hiding sensitive data items. Few apply distributed databases across various sites, few indulged data perturbation, and few utilized clustering and few of them employ data distortion technique. Algorithms supporting this method will follow either of the following two techniques. Hide a particular rule with the help of data alteration technique or hide the principles relying on the sensitivity of the items to be hidden. The proposed perspective dependent on data distortion technique which modifies the position of the sensitive items, yet its support is not at all altered and also used the ideology of representative results to shear the rules initially and then hides those sensitive rules. Experimental results exhibit that proposed method hides lot of rules at a minimum range of database scans in contrast to existing algorithms supporting data distortion technique.

Keywords
DBCT (Distortion, Blocking and Cryptographic Technique), Association Rule Hiding, Data Mining

Introduction

Machine learning is categorized into two types.

i) **Supervised learning** is a data mining task of surmising a function from **labeled training data**. The training data includes set of training examples. Each example in supervised learning has a set of input objects along with desired output values.
ii) While the complication of an **unsupervised learning** task is for discovering hidden structured data which is neither classified nor labeled. The algorithm has to act on that information without guidance..

A. Data Mining:

Data mining is the procedure used for sorting out the huge data sets so that to identify patterns and establish relationships by solving problems with the help of data analysis. Data need to be altered in order that information couldn't be identified by data mining techniques. Handling such sensitive data is the most important criteria from being accessed by the unauthorized activities. This has led to the disclosure of risks if the data is revealed to outside parties. This perspective has led to the research of hiding the sensitive information within database.

B. Privacy preserving data mining:

Privacy preserving is regarded as an important concern in association with data mining. This includes protecting independent data and the sensitive information without affecting the efficacy of the data. For preserving the privacy of information one should alter the original database in so that sensitive information shouldn't get involved in the mining result while the non-sensitive information was obtained. For securing sensitive association rules, privacy preserving data mining includes the concept named "association rule hiding". Before getting involved in this area, association rule mining technique has to be concerned.

Mining frequent patterns, associations and correlations:

Frequent patterns are those appearing continuously in data sets.

Eg: Light Cream + Chicken = Frequent Itemset

Frequent pattern mining looks for recursive relationships of a given dataset. Frequent item set mining guides to locate associations and correlations among items of large transactions or relational datasets.

"Finding hidden patterns play an crucial part in mining associations, correlations and decision making in Business which improves sales and Profits"

With immense volumes of information regularly gathered and stored, several companies are growing curious in mining those patterns present in their databases. Uncovering of interesting correlation relationships between vast accounts of business decision making process like customer shopping analysis.

 Helix E-ISSN: 2319-5592; P-ISSN: 2277-3495

Background and Related Work:

In 2004, Vassilios et al. [4] Proposed two fundamental approaches so that to safeguard sensitive rules from revelation. The initial proposal avoids rules from being obtained by concealing the frequent sets from that they're obtained. The other proposal minimize the significance of the rules of specifying their confidence below a user-specified threshold. Based on these approaches they have developed five-algorithms and evaluated so that to analyze time complexity and their influence on original database.

In 2012, Dhyanendra Jain et al. [5] has proposed to modify the database transactions for reducing the confidence of sensible rules *with no change in the support of the sensitive item,* that is in distinction with previously existing algorithms, that either decline or raises the aid of the sensitive item to change the database transactions.

In 2015, NeelkamalUpadhyay et al. [1] Has made a survey about association rule hiding approaches. Also included the merits and demerits of each technique involved in the association rule hiding process.

Kshitij Pathak et al. [2] Introduced a system for fast Privacy preserving association rule, including the idea of PC clusters for performing the task in parallel, in order to obtain improvised outcomes during execution time.

Sunil Kumar et al. [3] Suggested an algorithm for hiding association rules in data mining, thereby, reduced the number of modifications and hide more rules in less time. As well the effectiveness of the algorithm is compared with ISLF and DSRF approach.

Problem Definition

A. Spatial association rule mining:

Association rule mining is the efficient data mining technique for identifying hidden patterns from huge masses of data which was initially presented by R. Agarwal in 1993. For the fuller understanding of association rule mining, consider following example.

B. Market Basket Analysis:

This procedure studies client purchasing practices by discovering association among various item sets that customer places in their shopping baskets. Obtaining those item sets and associations thereby helping retailers to expand selling methods by gaining insight into matters that are often bought along by customers. Market Basket Analysis retailers do ***selective marketing*** and organize their shuffle space.

"Seeing the Customer Behavior which groups or lots of items are customers likely to purchase on a given trip to store?"

Market Basket Analysis might be conducted on retail data of customer transactions at the depot. Effects were used for planning, marketing/ advertising to design new catalogue.

Ex: Clients who buy PCs additionally tend to purchase the antivirus software simultaneously is represented in the association pattern. Association rule generates the highest number of rules and only a few are concerned. For solving this interested measurement problem minimum support and minimum confidence thresholds are used for each principle.

Two standards of rule interestingness:

1. Support

2. Confidence

Support is 2% of all the transactions under analysis exhibits PC and antivirus software are bought simultaneously while confidence is 60%, i.e., 60% of customers who purchased a PC also bought the software.

*"**Typically association rules are considered interesting if they satisfy both minimum support threshold and minimum confidence threshold."***

Consider I= {I1, I2,…… I'm} as set of items, D is a transactional database where each transaction T is a non-empty item set so that **T⊆I**. A unique identifier TID is associated with each transaction.

C. Association rule:

An association rule is of the form A =>B where A and B are subsets of item set in I. **A□ □I, B □ I, and A∩B=Ø.** In the rule, A => B, where A is called the antecedent (left-hand-side) and B is the consequent (right-hand-side). **Support** for a rule A => B, is denoted by **S (A=>B),** the percentage of transactions in D that contain A ∪ B i.e both the items sets A and B.

The probability is taken as **Support (A=>B) = P (A ∪ B)**. **Confidence** for a rule A => B, is denoted by C (A =>B), the percentage of transactions in D containing A that also contain B. The probability is taken as **C (A=>B) = P (B │A).**

P (B │A)= support(A ∪ B)/ support(A)

Rules that satisfy the minimum confidence threshold and minimum support threshold are called "**strong**"

The occurrence of the frequency of an item set:

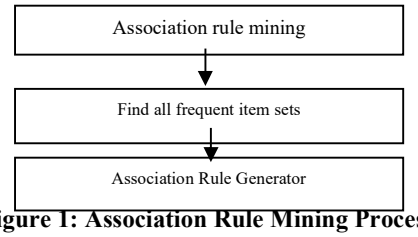


Figure 1: Association Rule Mining Process

  Helix E-ISSN: 2319-5592; P-ISSN: 2277-3495

There are various association rule mining algorithms namely ***Apriori algorithm***, ***Partition algorithm, Pincher search algorithm, Dynamic item set counting algorithm***.

Apriori algorithm proposed by R. Agarwal and R. Srikant in 1994 for mining frequent item sets of Boolean association rules. This algorithm employs prior knowledge of frequent item set properties. It uses an iterative approach called as a level-wise search, in which k-item lots are utilized to explore (k+1) item sets. The set of frequent 1-item sets is identified by scanning the database to accumulate the count of each point and collecting those items that satisfy minimum support. The derived set is denoted by L1. Next L1 is used to find L2 i.e., the set of frequent 2-item sets which are practised to find L3 and so on until no more frequent k-item sets are set up.

Apriori Property is used to cut down the search distance.

"All non-empty subsets of a frequent item set must also be frequent"

If an item sets I don't satisfy the minimum support threshold, min_sup, then I is not frequent, i.e., **p (I) <min_sup.** For suppose item set A is added to the item set I, then the resulting item sets **I∪A** can't occur more frequently than I.
Therefore, **I∪A**is not frequent either i.e.,

P (I∪A) <min_sup

"Anti-Monotonicity: If a set cannot pass a test, all of its supersets will fail the same examination as good"

A two-step procedure is adopted, containing join and prune.

Join Step:

Chicken ⋈ Chicken
Light cream Light cream
Pasta Pasta

Support:

Chicken, Light cream = 4/6 = 66.66%
Chicken, Pasta = 4/6 = 66.66%
Light cream, Pasta = 3/6 = 50 %
Chicken, Light Cream ⋈ Chicken, Light cream
Chicken, Pasta, Chicken, Pasta
Light cream, Pasta Light cream, Pasta

Support:

Chicken, Light cream, Pasta = 33/6 = 50%

PRUNING:

ITEMS: Chicken, Light cream, Pasta
Chicken (Light cream = 4/6 = 66.66%
Chicken (Pasta = 4/6 = 66.66%
Light cream (Chicken = 4/4 = 100%
Light cream (Pasta = ¾ = 75%
Pasta (Chicken = 4/4 = 100%
Pasta (Light cream = ¾ = 75%
Chicken (Light cream, Pasta = 3/6 = 50%
Light cream (Chicken, Pasta = ¾ =75%
Pasta (Chicken, Light cream = ¾ = 75%
Chicken, Light cream (Pasta = ¾ = 75%
Chicken, Pasta (Light cream = ¾ = 75%
Light cream, Pasta (Chicken = 3/3 = 100%

Frequent Item Sets:

Light cream (Chicken
Pasta (Chicken
Pasta, Light cream (Chicken

Proposed Approach

In that respect are different approaches for association rule hiding, where and which we mainly discuss and implement distortion and cryptographic method in this theme.

Association rule hiding for privacy-preserving data mining:

Association rule hiding is a latest updated procedure in data mining, that analyzes the matter of hiding sensitive association rules in the data, i.e. maintaining the privacy and security of item sets in traditional databases.
Association rule hiding must satisfy some conditions which are presented to a lower place:

i) Sensitive rule should not be generated from Sanitize database.
ii) Non of sensitive rule must be generated from Sanitized database.
iii) No new rule which is present in the database should be generated from Sanitized database.

D. Association rules hiding approaches:

  Helix E-ISSN: 2319-5592; P-ISSN: 2277-3495

These attacks are classified into five categories which are talked about infra.

1. Heuristic Based Approach: is further sorted into two types i) Data distortion technique ii) Data block technique.

i) Data Distortion Technique: In this method includes restoring 1-values to 0-values (delete items) or 0-values to 1-values (include items). Rule hiding in data distortion based system can be done by two methods. At first reducing the confidence of rules and second is lessening the support of the rules.

The regulations with minimum confidence threshold is 70%

	Confidence
Light Cream => Chicken	4/4 = 100%
Light Cream, Pasta => Chicken	3/3 = 100%
Chicken, Light cream => Pasta	3/4 = 75%

Table 1: Item-Sets Showing the Confidence %

Now we apply data distortion technique for hiding the following set of Association rules, If we want to hide the rule, **Light Cream => Chicken** we will consider the original dataset and then we hide the association rule using Data Distortion followed by Data Blocking and to enhance more privacy we then implement Cryptographic Technique.

Data distortion is classified into two categories inorder to hide sensitive association rules.

Category-1: Increase support of LHS

- Search for transaction which support

  Light Cream=Chicken=1

- Update the values of Light cream from 1 to 0 where Light cream = Chicken = 1.

Consider an example of traditional data,

Transaction ID	List of Items IDs
T_{100}	Chicken, Light Cream, Pasta
T_{200}	Chicken,LightCream,Pasta,Avacado
T_{300}	Chicken, Light Cream, Pasta
T_{400}	Chicken,LightCream
T_{500}	Chicken ,Shrimp
T_{600}	Chicken, Pasta

Table 2: Transactional Data showing List of Six Transactions happened on a Particular Day

Database D using specified notation:

Item Appears in the Transaction Record: **1**

Item does not appears: **0**

I1-Chicken, I2-Light Cream, I3-Pasta, I4,-Avocado I5-Shrimp

TID	Items	I_1, I_2, I_3, I_4, I_5	Size
T_{100}	I_1, I_2, I_3	11100	3
T_{200}	I_1, I_2, I_3, I_4	11110	4
T_{300}	I_1, I_2, I_3	11100	3
T_{400}	I_1, I_2	11000	2
T_{500}	I_1, I_5	10001	2
T_{600}	I_1, I_3	10100	2

Table 3: Transactional Data showing List of Six Transaction Records

Category-1: A transferred database D, where rules on LHS will be hidden.

Now we are trying to hide the rule, **Light Cream => Chicken**

Step-1: Search for transaction which support

Light Cream=Chicken=1

Step-2: Now update table, put 0 for Item Light Cream all the transaction where Light Cream=Chicken=1

Transactions which support Light Cream = Chicken=1 are

  Helix E-ISSN: 2319-5592; P-ISSN: 2277-3495

TID	Items	I_1, I_2, I_3, I_4, I_5	Size
T_{100}	I_1, I_2, I_3	11100	3
T_{200}	I_1, I_2, I_3, I_4	11110	4
T_{300}	I_1, I_2, I_3	11100	3
T_{400}	I_1, I_2	11000	2

Table 4: Transactional Data showing List of Four Transaction Records

Now applying step-2 on the two transactions.

We update the value of Light* Cream *from 1 to 0 and also set the updated basket size.

TID	Items	I_1, I_2, I_3, I_4, I_5	Size
T_{100}	I_1, I_2, I_3	10100	2
T_{200}	I_1, I_2, I_3, I_4	10110	3
T_{300}	I_1, I_2, I_3	10100	2
T_{400}	I_1, I_2	10000	1
T_{500}	I_1, I_5	10001	2
T_{600}	I_1, I_3	10100	2

Table 5: Updated Table after Hiding Item-2 (Category-1)

Category-2: A transformed database D', where rules containing item on RHS will be hidden.

For the same rule **Cream => Chicken**

if we want to hide the rule, we update the value from 1 to 0 on RHS.

For hiding the association rule, follow the following two steps:

Step-1:Search for transaction which has support for

from the original database D we have two transactions with Search for transaction which support

Light Cream=Chicken=1

Step-2: Now update the values from 1 to 0 on RHS part of the transaction and also set the updated basket size.

TID	Items	I_1, I_2, I_3, I_4, I_5	Size
T_{100}	I_1, I_2, I_3	01100	2
T_{200}	I_1, I_2, I_3, I_4	01110	3
T_{300}	I_1, I_2, I_3	01100	2
T_{400}	I_1, I_2	01000	1
T_{500}	I_1, I_5	10001	2
T_{600}	I_1, I_3	10100	2

Table 6: Updated Table after Hiding Item-5 (Category2)

Now if we calculate the confidence for the rule,

{I5} =>{ I1, I2}, the confidence is reduced from 100% to 0%. It means the rule is successfully hidden.

ii) Data blocking technique: is used to maximise or minimise the support of the items by substituting 0's or 1's by unknowns "?", such that it becomes troublesome for an adversary to understand the value behind "?" which is effective and allocates certain privacy. When hiding many of the rules at one time then they need less range of database scans and prune a lot of rules.

Category-1 from the Data Distortion Phase

TID	Items	I_1, I_2, I_3, I_4, I_5	Size
T_{100}	I_1, I_3	1?100	2
T_{200}	I_1, I_3, I_4	10110	3
T_{300}	I_1, I_3	?0100	1
T_{400}	-	??000	?
T_{500}	I_1, I_5	10001	2
T_{600}	I_1, I_3	10100	2

Category-2 from the Data Distortion Phase

 Helix E-ISSN: 2319-5592; P-ISSN: 2277-3495

TID	Items	I_1, I_2, I_3, I_4, I_5	Size
T_{100}	I_2, I_3	?1100	2
T_{200}	I_2, I_3, I_4	01110	3
T_{300}	I_2, I_3	01100	2
T_{400}	I_2	??000	?
T_{500}	I_1, I_5	10001	2
T_{600}	I_1, I_3	10100	2

Implement either Category-1 or Category-2 but not both as it will leads to inverse the operations performed so far.

3. Cryptography Based Approach is applied to perform multiparty computation on distributed databse over different sites. Various number of parties will be sharing their private data without disclosing any sensitive information. It is categorized as: (i) vertically partitioned distributed data and (ii) horizontally partitioned distributed data. In such perspective rather than falsifying the database, it encrypts actual database itself for sharing. The communication cost of this approach is extremely effective.

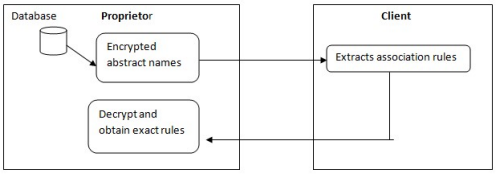


Figure 2:Cryptographic Technique for Association Rule Hiding

Implementation of Cryptographic Approach For Category-1 after performing Data Blocking

c1	c2	c3	c4	c5
Chicken	Light Cream	Pasta	Avocado	Shrimp
1	?	1	0	0
1	0	1	1	0
?	0	1	0	0
?	?	0	0	0
1	0	0	0	1
1	0	1	0	0

Step1: Vertical Partitioning of Data without changing the product names i.e attribute names.
To implement this step the admin has to maintain look ahead table

Original Dataset D	Modified Dataset D'
C1	C2
C2	C3
C3	C5
C4	C1
C5	C4

Chicken	Light Cream	Pasta	Avocado	Shrimp
0	1	?	0	1
1	1	0	0	1
0	?	0	0	1
0	?	?	0	0
0	1	0	1	0
0	1	0	0	1

Step2: Horizontal Partitioning of Data is applied to database obtained after performing Vertical Partitioning without changing the product names i.e. attribute names. R1- Row 1 and so on
To implement this step the admin has to maintain look ahead table

Original Dataset D	Modified Dataset D'
R1	R6
R2	R5
R3	R4
R4	R3
R5	R2
R6	R1

Chicken	Light Cream	Pasta	Avocado	Shrimp
0	1	0	0	1
0	1	0	1	0
0	?	0	0	1
0	?	0	0	1
1	1	0	0	1
0	1	?	0	1

Results and Analysis

We used market_basket.csv dataset which is having 7500 transaction records with 119 products.
Transactions as itemMatrix in sparse format with
7501 rows (elements/item sets/transactions) and
119 columns (items) and a density of 0.03288973
i.e 3 % are non zeros and 97 % are zeros

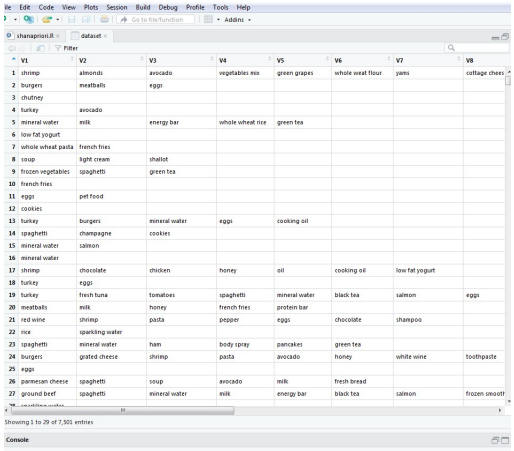


Figure 3: Market_Basket_Optimisation Dataset

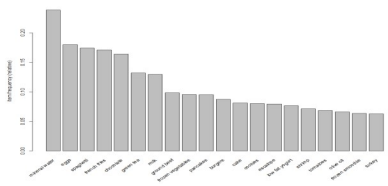
First we analyzed basket size(number of products per transaction by counting them)
There are total 1754 transactions that contain only one product, there is only one transaction that contains 20 products and on an average there are 4 products per transaction.

Basket Size	Count
1	1754
2	1358
3	1044
4	816
5	667
6	493
7	391
8	324
9	259
10	139
11	102
12	67
13	40
14	22
15	17
16	4
18	1
19	2
20	1

Min	1.000
1st Qu.	2.000
Median	3.000
Mean	3.914
3rd Qu.	5.000
Max	20.000

After Analyzing Basket size we found most frequent items

Most Frequent Items	Count
Mineral Water	1788
eggs	1348
spaghetti	1306
French fries	1282
chocolate	1229
Others	22405



X axis: Product
Y axis: Item Frequency (Relative)

Figure 4: Top 20 Products that are Most Frequently Brought (Individual)

While fixing **minimum support threshold (MST)** we assumed that a specific product brought 4 times a day and in a week 28 should be the count and calculating the relative frequency i.e **(28/7500)** i.e **0.037 i.e 0.04**

Minimum Confidence Threshold (MCT): 0.2

811 Association rules generated which satisfy both MST & MCT. We are interested in top 10

Which are sorted based on the LIFT value

set item appearances ...[0 item(s)] done [0.00s].
set transactions ...[119 item(s), 7501 transaction(s)] done [0.00s].
Sorting and recoding items ... [114 item(s)] done [0.00s].
Creating transaction tree ... done [0.00s].
Checking subsets of size 1 2 3 4 done [0.01s].
Writing ... [811 rule(s)] done [0.00s].

Parameter Specification:

Confidence -0.2	Max Time-5
Minval-0.1	Support- 0.04
Smax-1	MinLength-1
arem-none	MaxLength-10
aval-False	Target- Rules
original support- True	

Algorithmic Control:

Filter-0.1	Load- True
Tree-True	Sort-2
Heap-True	verbose-True
Memopt-False	

Top 10 Association Rules :

```
    lhs                                      rhs           support     confidence lift     count
[1] {light cream}                         => {chicken}     0.004532729 0.2905983  4.843951 34
[2] {pasta}                               => {escalope}    0.005865885 0.3728814  4.700812 44
[3] {pasta}                               => {shrimp}      0.005065991 0.3220339  4.506672 38
[4] {eggs,ground beef}                    => {herb & pepper} 0.004132782 0.2066667  4.178455 31
[5] {whole wheat pasta}                   => {olive oil}   0.007998933 0.2714932  4.122410 60
[6] {herb & pepper,spaghetti}             => {ground beef} 0.006399147 0.3934426  4.004360 48
[7] {herb & pepper,mineral water}         => {ground beef} 0.006665778 0.3906250  3.975683 50
[8] {tomato sauce}                        => {ground beef} 0.005332622 0.3773585  3.840659 40
[9] {mushroom cream sauce}                => {escalope}    0.005732569 0.3006993  3.790833 43
[10] {frozen vegetables,mineral water,spaghetti} => {ground beef} 0.004399413 0.3666667  3.731841 33
>
```

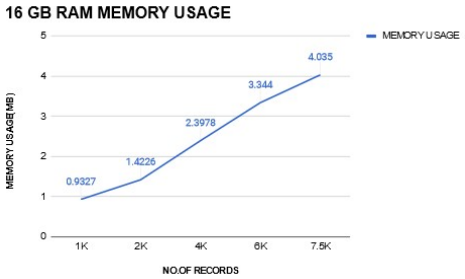
Figure 5: Association Rules with Lift value

Performance Evaluation

RAM: 16GB

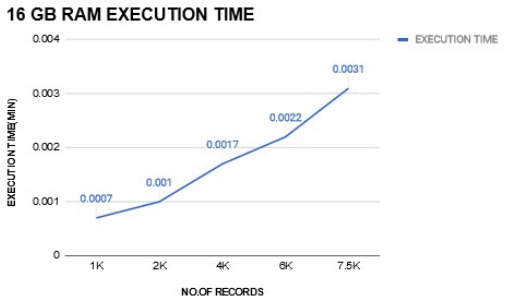
NO OF RECORDS	EXECUTION TIME		MEMORY USAGE	
	GENERATED (milliseconds)	SCALED(minutes)	GENERATED (bytes)	SCALED (megabytes)
1k	46	0.0007	932736	0.9327
2k	64	0.001	1422664	1.4226
3k	79	0.0013	1907160	1.9071
4k	106	0.0017	2397872	2.3978
5k	112	0.0018	2871016	2.871
6k	137	0.0022	3344216	3.344
7k	149	0.0024	3504776	3.504
7.5k	188	0.0031	4035384	4.035

Table 7: Performance Results on 16GB RAM Configuration System



Graph 1: CPU Performance w.r.t Memory for 16 GB RAM

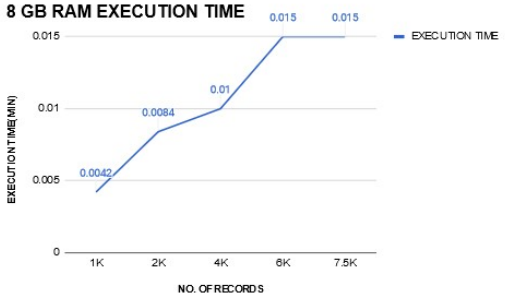
  Helix E-ISSN: 2319-5592; P-ISSN: 2277-3495



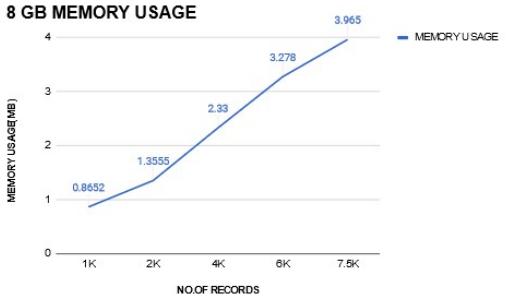
Graph 2: CPU Performance w.r.t Time for 16 GB RAM

NO OF RECORDS	EXECUTION TIME		MEMORY USAGE	
	GENERATED (milliseconds)	SCALED (minutes)	GENERATED (bytes)	SCALED (megabytes)
1k	254	0.0042	865264	0.8652
2k	509	0.0084	1355376	1.3555
3k	473	0.0078	1839488	1.8394
4k	637	0.01	2330640	2.33
5k	803	0.013	2803784	2.803
6k	913	0.015	3278072	3.278
7k	894	0.014	3738024	3.738
7.5k	908	0.015	3965216	3.965

Table 8: Performance Results on 8GB RAM Configuration System



Graph 3: CPU Performance w.r.t Time for 8 GB RAM

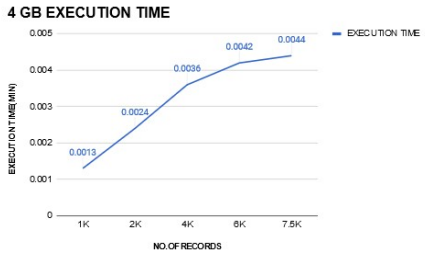


Graph 4: CPU Performance w.r.t Memory for 8GB RAM

RAM: 4GB

NO OF RECORDS	EXECUTION TIME		MEMORY USAGE	
	GENERATED (milliseconds)	SCALED (minutes)	GENERATED (bytes)	SCALED (megabytes)
1k	80	0.0013	716448	0.7164
2k	145	0.0024	1104568	1.1045
3k	163	0.0027	1486336	1.4863
4k	217	0.0036	1870904	1.8709
5k	212	0.0035	2246200	2.2462
6k	257	0.0042	834280	0.8342
7k	262	0.0043	786429	0.7864
7.5k	269	0.0044	753616	0.7536

Table 9: Performance Results on 4GB RAM Configuration System



Graph 5: CPU Performance w.r.t Time for 4 GB RAM

Conclusion

In this paper, we have discussed about how association rules are generated and a new approach to hide sensitive data i.e.(DBCT) a hybrid technique which applies data distortion followed by data Blocking and finally cryptographic technique which is being performed in different configuration machines and generated corresponding performance metrics i,e evaluated space and time complexities. On further work, we can implement some efficient association rule hiding techniques which might give better performance results than DBCT.

References

[1] NeelkamalUpadhyay, KuldeepTripathi& Prof. Ashish Mishra "A Survey of Association Rule Hiding Approaches" in IRACST - International Journal of Computer Science and Information Technology & Security(IJCSITS), ISSN: 2249-9555, Vol. 5, No1, February 2015

[2] Kshitij Pathak, Narendra S Chaudhari&Aruna Tiwari "Privacy Preserving Association Rule Mining by Introducing Concept of Impact Factor" in 2012 7th IEEE Conference on Industrial Electronics and Applications (ICIEA)

[3] Sunil Kumar, Mahaveer Singh & Nidhi Porwal "An Algorithm for Hiding Association Rules on Data Mining" in National Conference on Communication Technologies & its impact on Next Generation Computing CTNGC 2012 Proceedings published by International Journal of Computer Applications® (IJCA)

[4] Vassilios S. Verykios, Member, IEEE, Ahmed K. Elmagarmid, Senior Member, IEEE, Elisa Bertino, Fellow, IEEE, YucelSaygin, Member, IEEE, and Elena Dasseni "Association Rule Hiding" in IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, VOL. 16, NO. 4, APRIL 2004

[5] Dhyanendra Jain, Amit sinhal, Neetesh Gupta, PriushaNarwariya, DeepikaSaraswat& Amit Pandey "Hiding Sensitive Association Rules without Altering the Support of Sensitive Item(s)" in International Journal of Artificial Intelligence & Applications (IJAIA), Vol.3, No.2, March 2012

[6] M. Atallah, E. Bertino, A. Elmagarmid, M. Ibrahim, and V. S.Verykios "Disclosure limitation of sensitive rules."In Proc. of the 1999 IEEE Knowledge and Data Engineering Exchange Workshop (KDEX'99), pp. 45–52, 1999.

[7] S. Vijayarani, A. Tamilarasi and R. SeethaLakshmi, "Privacy Preserving Data Mining Based on Association Rule-A Survey". In Proc. of the International Conference on Communication and Computational Intelligence-2010, pp. 99-103.

[8] Sambhaji, Shintre Sonali, and P. Kalyankar Pravin. "Study of Mining and Hiding of Sensitive Association Rule."

[9] Zhang, Xiaoming, and Xi Qiao. "New Approach for Sensitive Association Rule Hiding." *Education Technology and Training, 2008. and 2008 International Workshop on Geoscience and Remote Sensing. ETT and GRS 2008. International Workshop on*. Vol. 2. IEEE, 2008.

[10] Chen, Shan-Tai, et al. "An Improved Algorithm for Completely Hiding Sensitive Association Rule Sets." *Computer Science and its Applications, 2009. CSA'09. 2nd International Conference on*. IEEE, 2009.

[11] Gulwani, Padam. "Association rule hiding by positions swapping of support and confidence." *Information Technology and Computer Science* 4 (2012): 54-61.

[12] SathiyaPriya, K., G. Sudha Sadasivam, and N. Celin. "A new method for preserving privacy in quantitative association rules using DSR approach with automated generation of membership function." *Information and Communication Technologies (WICT), 2011 World Congress on*. IEEE, 2011.

[13] Dubey, Sulakshana, and Arun Sen. "Data Mining Based on Association Rule Privacy Preserving." *Binary Journal of Data Mining & Networking* 5.1 (2015): 16-21.

[14] Priya, K. Sathiya, G. Sudha Sadasivam, and V. B. Karthikeyan. "A new method for preserving privacy in quantitative association rules using Genetic Algorithm." *International journal of computer Applications* 60.12 (2012).

[15] Rao, K. Srinivasa, CH Suresh Babu, and A. Damodaram. "Support and Confidence Based Algorithms for Hiding Sensitive Association Rules." (2014).

  Helix E-ISSN: 2319-5592; P-ISSN: 2277-3495