A Survey on Association Rule Hiding Methods

Khyati B. Jadav
Department of Computer Engineering
LJ Institute of Engineering & Technology, Ahmadabad, Gujarat, India-382210

Jignesh Vania
Department of Computer Engineering
LJ Institute of Engineering & Technology, Ahmadabad, Gujarat, India-382210

Dhiren R. Patel, Ph.D
Department of Computer Engineering
National Institute of Technology Surat, India

ABSTRACT
In recent years, the use of data mining techniques and related applications has increased a lot as it is used to extract important knowledge from large amount of data. This has increased the disclosure risks to sensitive information when the data is released to outside parties. Database containing sensitive knowledge must be protected against unauthorized access. Seeing this it has become necessary to hide sensitive knowledge in database. To address this problem, Privacy Preservation Data Mining (PPDM) include association rule hiding method to protect privacy of sensitive data against association rule mining. In this paper, we survey existing approaches to association rule hiding, along with some open challenges. We have also summarized few of the recent evolution.

General Terms
Data mining, Privacy preserving data mining

Keywords
Association rule hiding

1. INTRODUCTION
Data Mining is the process of extracting useful knowledge from large amounts of data. It is a knowledge discovery process which is useful to find patterns [26]. Discovered knowledge is expressed in terms of decision tree, clusters or association rules. Data mining has numerous applications in marketing, business, medical analysis, engineering design, bioinformatics, scientific exploration, etc. This has increased the disclosure risks when the data is released to outside parties. For example, consider Indian superstores like Food Bazaar and Reliance Fresh. Suppose shopkeeper of Reliance Fresh mines the association rules related to Food Bazaar, where he found that most of the customers who buy bread also buy milk. Seeing this, shopkeeper of Reliance Fresh exploits this information and puts some discount on the cost of bread. This is how customers of Food Bazaar will now move to Reliance. This scenario leads to the research of sensitive knowledge (or rule) hiding in database. Therefore, before releasing the dataset to the other party, each supermarket is willing to hide sensitive association rules of its own sensitive products. So, the sensitive information (or knowledge) will be protected. The problem of association rule hiding in the area of privacy preserving data mining was first proposed in 1999 by Atallah *et al.* [1].

Privacy preserving data mining (PPDM) is considered to maintain the privacy of data and knowledge extracted from data mining. It allows the extraction of relevant knowledge and information from large amount of data, while protecting sensitive data or information. To preserve data privacy in terms of knowledge, one can modify the original database in such a way that the sensitive knowledge is excluded from the mining result and non sensitive knowledge will be extracted. In order to protect the sensitive association rules (derived by association rule mining techniques), privacy preserving data mining include the area called "association rule hiding". The main aim of association rule hiding algorithms is to reduce the modification on original database in order to hide sensitive knowledge, deriving non sensitive knowledge and do not producing some other knowledge.

Rest of this paper is organized as follows: - In Section 2, discusses the association rule mining strategy. The concept of association rule hiding is given in section3. Section 4 presents the existing association rule hiding approaches by identifying open challenges. Section 5 summarizes the recent evolutions in sensitive association rule hiding. The metrics used for evaluating sensitive rule hiding approaches are given in section 6. Section 7 conclude our study by identifying future work with references at the end.

2. ASSOCIATION RULE MINING
Association rule mining [26] is the most effective data mining technique to discover hidden pattern from large volume of data. It was first introduced by R. Agarwal [2] in 1993. It works as follows:

Let I = {i1, i2, ... , im } be a set of items, D = {t1, t2 , ... , tn} be a set of transactions where ti $\subseteq$ I. A unique identifier, TID, is associated with each transaction. A transaction t supports X, a set of items I, if X $\subseteq$ t. For example, let take a sample database of transactions, as shown in "Table 1".

Table 1. Sample Transaction Table

TID	Transaction Items
T1	A,B,C
T2	A,B,C
T3	A,C
T4	A,E
T5	C,D

An association rule is in the form X => Y, where X and Y are the subsets of item set in I, X⊂I, Y⊂I, and X∩Y=Ø. In the rule X => Y, where X is called the antecedent (left-hand-side) and Y is the consequent (right-hand-side). Association rule mining generates high number of rules and only few of them are of interest. To solve interest measurement problem, minimum support and minimum confidence thresholds are

applied to each rule: Support for a rule $X => Y$, is denoted by $S(X=>Y)$, is the proportion of transaction in the data set which contain the item set and is defined as:

$$Support(X=>Y) = |X \cap Y| / |D|,$$

Where $|X \cap Y|$ is the number of transaction containing the itemset X and Y in the database, $|D|$ denotes the number of the transactions in the data.

Confidence for a rule $X => Y$, is denoted by $C(X =>Y)$, is the ratio of the support count of X U Y to that of the antecedent X defined as :

$$Confidence(X=>Y) = |X \cap Y| / |X|,$$

Where $|X|$ denotes the number of the transactions in the database D that contains itemset X. In other words, support describes how often the rule would appear in the database, while confidence measures the strength of the rule. A rule $X=>Y$ is strong if $support(X=>Y) \geq$ minimum support and $confidence(X=>Y) \geq$ minimum confidence.

As shown in Fig. 1, association rule mining works in two-step process:

i) First find all frequent item sets- itemset which occur at least as frequently as a pre-determined minimum support count.

ii) Generate strong association rules- based on user defined minimum support and minimum confidence.

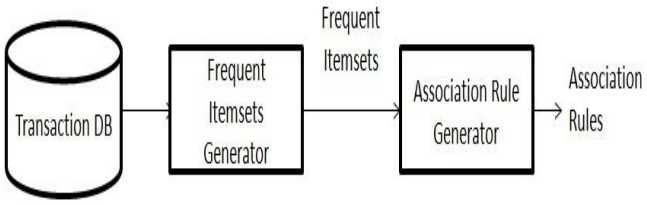

Figure 1: Association rule mining process [21]

Different types of association rule mining algorithms are available like Apriori algorithm, Partition algorithm, Pincher-search algorithm, Dynamic item set counting algorithm, FP-tree growth algorithm, etc [3]. Apriori algorithm is one of the most popular and best-known algorithm to mine association rule, proposed by Agrawal and Srikant [2]. It makes user of prior knowledge of frequent itemset properties, which is a two-step process: join step and prune step. It moves upward in the lattice starting from level1 till level k, where no candidate set remains after pruning. Apriori algorithm uses breadth first search strategy.

3. ASSOCIATION RULE HIDING

Association Rule hiding is the process of hiding strong association rules and creating sanitized database from the original database in order to prevent unauthorised party to generating frequent sensitive patterns. The general framework of sensitive association rule hiding is shown in Fig. 2.

The problem can be stated as follows: "Given a transactional database D, minimum confidence, minimum support and a set R of rules mined from database D. A subset RH of R is denoted as set of sensitive association rules which are to be hidden. The objective is to transform D into a database D' in

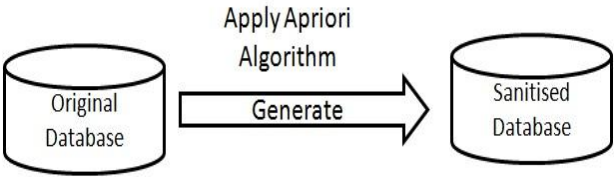

Figure 2: Framework of Sensitive Association Rule Hiding

such a way that no association rule in RH will be mined and all non sensitive rules in R could still be mined from D' [4]. The main purpose of the association rule hiding algorithms is to make the sensitive rules invisible which can be generated by association rule mining algorithms. M. Attallah et al. [1] have proved that finding an optimal solution of sanitization problem is NP-Hard.

Hiding a rule (e.g. X => Y), can be done either by decreasing the support of the itemset X and Y below minimum support threshold or decreasing the confidence of the itemset X and Y below minimum confidence threshold. Decreasing the confidence of a rule X => Y can be done by either increasing the support of X in transactions and not of Y or by decreasing the support of Y in transactions supporting both XY. Decreasing the support of a rule X => Y can be done by decreasing the support of the corresponding large itemset XY.

Association rule hiding must satisfy following conditions:

i) No sensitive rule should be generated from Sanitized database.

ii) Non sensitive rule must be generated from Sanitized database.

iii) No new rule, present in database should be generated from Sanitized database.

4. ASSOCIATION RULE HIDING APPROACHES

Sensitive association rule hiding is a subfield of Privacy Preserving Data Mining (PPDM). Privacy preserving data mining has been recently introduced to cope with privacy issues related to the data subjects in the course of mining of the data. Association Rule Hiding approaches can be classified into five classes: heuristic based approaches, border based approaches, exact approaches, reconstruction based approaches and cryptography based approaches.

4.1 Heuristic Based Approaches

This approach is further divided into two techniques: i) Data distortion technique and ii) Data Blocking Technique.

4.1.1 Data distortion Technique:

M. Attallah *et al.* [1] were the first to propose heuristic algorithm. They also proved that finding an optimal solution of sanitization problem is NP-Hard. In this technique we replace 1-values to 0-values (delete items) or 0-values to 1-values (add items). There are two basic approaches for rule hiding in data distortion based technique. First is reducing the confidence of rules and second is reducing the support of rules.

Verykios et al. [5] proposed five algorithms namely 1.a, 1.b, 2.a, 2.b, 2.c to hide sensitive knowledge of database by reducing support or confidence of sensitive rule. Algorithms 1.a, 1.b, and 2.a were aimed towards hiding association rules and algorithms 2.b, 2.c were related to hiding large itemsets.

But they produce undesirable side effects. Oliveira et al. [6] improved the balance between protection of sensitive knowledge and discovered pattern, which provided better privacy. Y-H Wu et al. [7] proposed a method that reduced the side effects on sanitized database. In this method it is found that if the sensitive item is on the LHS of the rule then the first algorithm increases its support. If the sensitive item is on the right of the rule then the second algorithm decreases its support. K.Duraiswamy et al. [27] proposed a clustering based approach that clusters the sensitive rules based on common item in R.H.S. of the sensitive rules and hides the R.H.S. items in each cluster by reducing support of it. This approach has high efficiency than others. But it hides the only rule which has single R.H.S. item.

4.1.2 Data Blocking Technique

Y. Saygin et al.[8][9] were the first to propose blocking technique in order to increase or decrease the support of the items by replacing 0's or 1's by unknowns "?", so that it become difficult for an adversary to know the value behind "?". This technique is effective and provides certain privacy. Wang and Jafari [10] proposed more efficient approaches then other approaches as in [8][9]. While hiding many rules at a time, they require less number of database scans and prune more number of rules. Now, consider the table shown in Table 2. For rule A⇒C, Support (A⇒C) = 80% and Confidence (A⇒C) = 100%. After fuzzifying the values, support and confidence becomes marginal. So in new database: 60% ≤ Confidence (A⇒C) ≤ 100% and 60% ≤ Support (A⇒C) ≤ 80%[4].

Table 2. Hiding A⇒C by blocking[4]

A	B	C	D
1	1	1	0
1	0	1	0
0	1	0	1
1	1	1	0
1	0	1	1

⇒

A	B	C	D
1	1	1	0
1	0	?	0
?	1	0	1
1	1	1	0
1	0	1	1

4.2 Border Based Approaches

Sun and Yu [11] were the first to propose border based approach. This approach hides sensitive association rule by modifying the borders in the lattice of the frequent and the infrequent itemsets of the original database. The itemsets which are at the position of the borderline separating the frequent and infrequent itemsets forms the borders. It uses the border of non-sensitive frequent item and computes the positive and negative borders in the itemset. Then minimal affected modification is selected. If modification is done by greedy selection then it leads to minimum side effects.

The authors in [28] use the revised positive and negative borders and try to remove all the sensitive itemsets belonging to negative border. They select positive border item with highest support and maximum distance from the border, which determines item through which the hiding of the itemset will incur. These approaches are more efficient than [7].

4.3 Exact Approaches

This approach is better than other approaches but requires high time complexity. In this approach minimally extends the original database by a synthetically generated database called extended database and formulates the construction of the extended database as a constraint satisfaction problem (CSP) which is then solved by using Binary Integer Programming (BIP) and the solution for association rule hiding is nothing but determining a sanitized database by satisfying constraints. This approach provides exact solution. Exact based approach can be considered as the descendent of border based approach. Gkoulalas and Verykios [12] proposed the exact border approach in which authors initially made use of border revision theory introduced by Sun and Yu [11] so as to achieve optimal solution as compared to previous approaches. They proposed an approach to find optimal solution for rule hiding problem which tries to minimize the distance between the original database and its sanitized version. Gkoulalas-Divanis and Verykios[24] introduced the first exact methodology to perform sensitive frequent itemset hiding based on the notion of a hybrid database generation.

4.4 Reconstruction Based Approach

This approach is implemented by perturbing the data first and reconstructing the distributions at an aggregate level in order to perform the association rules mining. Mielikainen [13] was the first analyzed the computational complexity of inverse frequent set mining and showed in many cases that the problems are computationally difficult. In this approach it first places the original data aside and start from knowledge base. To sanitize, it conceals the sensitive rules by sanitizing itemset lattice rather than sanitizing original dataset. Later Y. Guo[14] proposed a FP tree approach which is based on inverse frequent set mining algorithm. The proposed model has three phases, first phase generates frequent item sets from the original database, second phase performs sanitization algorithm over frequent item sets by selecting hiding strategy and identifying sensitive frequent items sets according to sensitive association rules. The third phase generates sanitized database by using inverse frequent item set mining algorithm and then releases this database.

In reconstruction based approaches, first frequent sets are generated, as shown in Fig. 3. From the non sensitive frequent set, new dataset is generated which preserves the privacy of sensitive information.

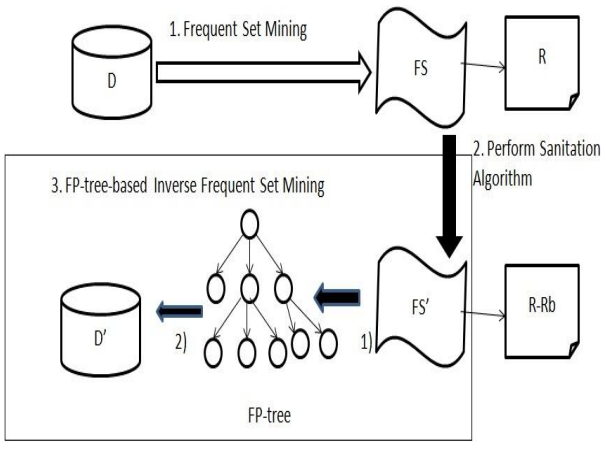

Figure 3: Framework of Reconstruction Based Approach [14]

4.5 Cryptography Based Approaches

These approaches are used for multiparty computation, when database is distributed among several sites. Multiple parties may wish to share their private data, without leaking any

sensitive information at their end. This approach is categorised as: vertically partitioned distributed data and horizontally partitioned distributed data.

In these approaches instead of distorting the database, it encrypts original database itself for sharing. Vaidya and Clifton [15] proposed a secure approach for sharing association rules when data are vertically partitioned. In terms of communication cost this approach is very effective, but it is very expensive for large amount of datasets. The authors in [16] addressed the secure mining of association rules over horizontal partitioned data. This approach mines association rules securely with reasonable communication cost and computation cost.

The advantages and limitations of the above presented association rule hiding approaches are given in table 3.

Table 3. Summary of association rule hiding approaches

Advantages	Limitations
Heuristic Based Approaches (Distortion technique)	
Efficiency, scalability and quick responses due to which it is getting focus by majority of the researchers. Totally takes best decision	Produce undesirable side effects in new database (i.e. Lost rules and new rules).
Heuristic Based Approaches (Blocking technique)	
Maintains truthfulness of the underlying data. Minimizes side effects.	Difficult to reproduce original dataset.
Border Based Approaches	
Maintains data quality by greedily selecting the modification with minimal side effects. Improvement over pure heuristic approach.	Unable to identify optimal hiding solution But still dependent on heuristic to decide upon the item modification.
Exact Approaches	
Guarantees quality for hiding sensitive information than other approaches.	But requires very high time complexity due to integer programming
Reconstruction Approaches	
Create privacy aware database by exacting sensitive characteristic from the original database. Lesser side effects in database than heuristic approach.	The open problem is to restrict the number of trans-actions in the new database.
Cryptographic Approaches	
Secure mining of association rule over partitioned database.	Do not protect the output of a computation. Falls short of providing a complete answer to the problem of privacy preserving data mining. Communication and computation cost should be low.

5. RECENT EVOLUTIONS

Many algorithms have been proposed in recent years to hide sensitive association rule in databases. Recent evaluations are as follows:

C N Modi et al. [17] proposed a heuristic algorithm named DSRRC (Decrease Support of R.H.S. item of Rule Clusters) which was able to hide many sensitive association rule at a time. They have analyzed experimental results for DSRRC, which show that performance of the DSRRC algorithm is better than other existing heuristic approaches. They have achieved improvement in misses cost, artifactual patterns, dissimilarity and maintain data quality in comparison to Algo 1b of [5]. This approach was able to hide only the rules that contain single item on R.H.S. of the rule.

Nikunj et al. [18] introduced a heuristic based algorithm named MDSRRC(Modified Decrease Support of R.H.S. item of Rule Clusters) to hide sensitive association rules with multiple items on L.H.S and R.H.S. This algorithm is the improved version of DSRRC [17]. This algorithm does modification on minimum number of transaction in database in order to hide maximum sensitive rules and also to maintain data quality. They have also showed the performance comparison between DSRRC and MDSRRC.

K. Pathak et al. [19] proposed an approach that is based on concept of pc cluster (improve performance by running operations in parallel), impact factor (of a transaction is equal to number of itemsets that are present in those itemsets which represents sensitive association rule) and hybrid algorithm (which is a combination of ISL (Increase support of LHS) and DSR (Decrease support of RHS). This approach is able to reduce the execution time and maintain data quality.

Shyue-Liang Wang et al. [20] have proposed a novel algorithm for hiding sensitive association rules on multi-relational databases which are stored in data warehouses. The proposed approach is based on "mining-then-joining", which means first mining of sensitive association rules from each database and then joining all dimension tables for hiding purpose. They have also discussed two important issues to deal with multi-table association rule hiding. The first issue is how to calculate supports of itemsets efficiently and the second issue is how to reduce the confidence of an association rule by minimal modification of dimension tables.

Le et al. [21] proposed a heuristic algorithm which relies on three heuristic steps to hide a set of sensitive association rules using distortion technique. HCSRIL (Heuristic for Confidence and Support Reduction based on Intersection Lattice) algorithm which is based on intersection lattice of frequent itemset. This algorithm was able to minimize the side effects as they specified victim item and minimum number of transactions. They also showed that the performance of the HCSRIL algorithm in the average case of the experiment for lost rules, ghost rules, false rules, accuracy and CPU time is better than the performance of MaxMin2 [25]. This algorithm was then also applied to retailer's data and found that the result was outstanding, which concluded that this approach can also be useful in today's enterprises.

6. EVALUATION METRICS

Following metrics are used to evaluating association rule hiding algorithms [22][23].

1) ***Efficiency***- It is measured in terms of CPU-time, space requirements and communication required for hiding. In short, good performance in terms of resources allocated.

2) ***Scalability***- It is measured in terms of good performance for increasing sizes of input datasets.

3) ***Data quality***- Data quality parameters are accuracy measure, completeness, consistency which are in

relationship to preservation of original data values and of data mining results.

4) ***Hiding failure***- It is the percentage of the portion of information that fails to be hidden. It is derived by, HF = |Rs(D')| / |Rs(D)| where, |Rs(D')| are the number of sensitive rules appearing in the sanitized database and |Rs(D)| are the number of sensitive rules in the original database.

5) ***Privacy level***- It measures the degree of uncertainty according to which the protected information can still be predicted.

6) ***Lost Rules cost***- It measures the number of nonsensitive association rules found in the original database but not in sanitized database.

7) ***Ghost Rules***- It measures the percentages of rules that are not present in the original database but can be derived from sanitized database.

8) ***Dissimilarity***- It quantifies difference between original database and sanitized database.

7. CONCLUSION

Association rule hiding is an important concept in the area of privacy preserving data mining. It protects the privacy of sensitive information in databases against the association rule mining approaches. In this paper, we surveyed methods of hiding sensitive association rules by identifying some open challenges that will be useful to research community in this area. It is found that finding an optimal solution for sanitizing database (to protect privacy of sensitive information) is NP-Hard. Existing approaches provide only the approximate solution to hide sensitive knowledge. There is need of finding exact solution to the privacy problem in database disclosure.

In future, hybrid technique can be found to reduce the side effects and increase the efficiency by reducing the modifications on database, while hiding the association rules. Parallel algorithm can be developed to hide sensitive rules and also improve the performance of the algorithms for large database. An algorithm for incremental environment can also be developed, as most of the current frequent hiding algorithms are designed for static database.

8. REFERENCES

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

[2] R. Agrawal, T. Imielinski, and A. Swami, "Mining association rules between sets of items in large databases". In Proceedings of the 1993 ACM SIGMOD International Conference on Management of Data, Washington, DC, May 26-28 1993, pp. 207-216.

[3] 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.

[4] K. Shah, A. Thakkar and A. Ganatra, "A Study on Association Rule Hiding Approaches". (IJEAT)International Journal of Engineering and Advanced Technology, vol 3, issue-3, February 2012, pp. 72-76.

[5] V.S. Verykios, A. Elmagarmid, E. Bertino, Y. Saygin, and E. Dasseni, "Association rule hiding," IEEE Transactions on Knowledge and Data Engineering, Vol. 16, No.4, 434–447, 2004.

[6] S. Oliveira, O. Zaïane, and Y. Saygın, "Secure Association Rule Sharing," In: Dai, H., Srikant, R., Zhang, C. (eds.) PAKDD 2004. LNCS (LNAI), Vol. 3056, pp. 74–85. Springer, Heidelberg, 2004.

[7] Y. H. Wu, C.M. Chiang and A.L.P. Chen, "Hiding Sensitive Association Rules with Limited Side Effects", IEEE Transactions on Knowledge and Data Engineering, Vol.19, No. 1, Jan. 2007, pp. 29-42.

[8] Y. Saygin, V. Verykios, and C. Clifton, "Using Unknowns to Prevent Discovery of Association Rules" ACM SIGMOD, Vol. 30, No. 4, pp. 45–54, 2001.

[9] Y. Saygin, V. Verykios, and A. Elmagarmid, "Privacy preserving association rule mining," In: Proc. Int'l. Workshop on Research Issues in Data Engineering (RIDE 2002), pp.151–163, 2002.

[10] S. Wang, and A. Jafari, "Using unknowns for hiding sensitive predictive association rules," In: Proc. IEEE Int'l. Conf. Information Reuse and Integration (IRI 2005), pp. 223–228, 2005.

[11] X. Sun, and P. Yu, "A Border-Based Approach for Hiding Sensitive Frequent Itemsets," In: Proc. Fifth IEEE Int'l. Conf. Data Mining (ICDM 2005), pp. 426–433, 2005.

[12] A. Gkoulalas-Divanis, V. Verykios, "An Integer Programming Approach for Frequent Itemset Hiding," In: Proc. ACM Conf. Information and Knowledge Management (CIKM 2006), pp. 748–757 2006.

[13] T. Mielikainen, "On inverse frequent set mining", In Proc. of 3rd IEEE ICDM Workshop on Privacy Preserving Data Mining. IEEE Computer Society, 2003, pp.18-23.

[14] Y. Guo, "Reconstruction-Based Association Rule Hiding" In Proc. of SIGMOD2007 Ph.D. Workshop on Innovative Database Research 2007(IDAR2007), June 2007, pp.51-56.

[15] J. Vaidya, and C. Clifton, "Privacy preserving association rule mining in vertically partitioned data," In proc. Int'l Conf. Knowledge Discovery and Data Mining, pp. 639–644, July 2002.

[16] M. Kantarcioglu, and C. Clifton, "Privacy-preserving distributed mining of association rules on horizontally partitioned data," IEEE Transactions on Knowledge and Data Engineering, Vol. 16, No. 9, pp. 1026-1037, Sept. 2004.

[17] C. N. Modi, U. P. Rao, and D. R. Patel, "Maintaining privacy and data quality in privacy preserving association rule mining," 2010 Second International conference on Computing, Communication and Networking Technologies, pp. 1–6, Jul. 2010.

[18] N Domadiya and U. P. Rao, "Hiding Sensitive Association Rules to Maintain Privacy and Data Quality in Database" 2013 3rd IEEE International Advance Computing Conference (IACC), pp. 1306-1310, 2013.

[19] K. Pathak, N. S. Chaudgari and A. Tiwari, "Privacy Preserving Association Rule Mining by Introducing

Concept of Impact Factor" 2012 7th IEEE Conference on Industrial Electronics and Application(ICIEA), pp. 1458-1461, 2012.

[20] S-L Wang, T Hong, Y-C Tsai, and H-Y Kao, "Hiding Sensitive Association Rules on Stars" 2010 IEEE International Conference on Granular Computing, pp 505-508, 2010.

[21] H. Q. Le, "Association rule hiding in risk management for retail supply chain collaboration" 2013 Elsevier on Computers in Industry 64, pp. 776-784, 2013.

[22] V. S. Verkios, "Association rule hiding methods" 2013 John Wiley & Sons, Inc, Vol. 3, January/February 2013, pp. 28-38.

[23] C. Modi, U.P. Rao and D.R.Patel, "A Survey on Preserving Privacy for Sensitive Association Rules in Databases" Springer-Verlag Berlin Heidelberg 2010, pp. 538-544.

[24] A. Gkoulalas-Divanis, and V. S. Verykios, " Exact knowledge hiding through database extension" IEEE Trans Knowledge Data Eng 2009, pp. 699–713.

[25] G. Tuncel, and G. Alpan, "Risk assessment and management for supply chain networks": a case study, Computers in Industry 61 (2010), pp. 250–259, 2010.

[26] J. Han, and M. Kamber, Data Mining: Concepts and Techniques, pp. 227–245. Morgan Kaufmann Publishers, San Francisco, 2001.

[27] K. Duraiswamy, and D. Manjula, "Advanced approach in sensitive rule hiding," Modern Ap-plied Science," Vol.3, No. 2, 2009.

[28] G. V. Moustakides, and V. S. Verykios, "A Max-Min Approach for Hiding Frequent Itemsets," In: Proc. Sixth IEEE Int'l. Conf. Data Mining (ICDM 2006), pp. 502–506.