Outsourced Association Rule Mining for Partitioned Database using Encryption

Mr. Rajesh R. Kshirsagar[1] **Mr.H.A.Tirmare**[2]
[1,2]Department of Computer Science & Technology
[1,2]Department of Technology, Shivaji University, Kolhapur, India

Abstract— Data analysis techniques that is Association rule mining and Frequent item set mining are two widely used for various applications. The traditional system focused separately on vertically partitioned database and horizontally partitioned databases on the basis of this introducing a system which focus on both horizontally and vertically partitioned databases collaboratively with privacy-preserving mechanism. Data owners need to know the frequent item sets or association rules from a collective data set and disclose or reveal as few information about their unprocessed data as possible to other data owners and third parties. To guarantee data privacy a Symmetric Encryption Technique is used to get better result. Cloud aided frequent item set mining solution used to demonstrate an association rule mining solution. The resultant solutions are designed for outsourced databases that permit various data owners to efficiently share their data securely without compromising on data privacy. Data security is one of the key processes in outsourcing data to various outside users. Traditionally Fast Distribution Mining algorithm was proposed for securing distributed data. This work addresses a problem by secure association rules over partitioned data in both horizontal and vertical. A Frequent item sets algorithm and Distributed association rule mining algorithm is utilized for doing above procedure effectively in partitioned data, which includes services of the data in outsourcing process for distributed databases. This work maintains efficient security over vertical and horizontal view of representation in secure mining applications.

Key words: Association Rule Mining, Frequent Itemset Mining, Privacy-Preserving Data Mining, Partitioned Data

I. INTRODUCTION

Frequent item set mining and association rule mining, two widely used data analysis techniques, are generally used for discovering frequently co-occurring data items and interesting association relationships between data items respectively in large transaction databases. These two techniques have been employed in applications such as market basket analysis, health care, web usage mining, bioinformatics and prediction. A transaction database is a set of transactions, and each transaction is a set of data items with a unique TID (Transaction ID). An item set Z is regarded frequent if and only if Supp (Z) ≥ Ts, where Ts is a threshold specified by the data miner. Supp (Z) is Z's support, which is defined as Z's occurrence count in the database. An association rule is expressed using X ⇒ Y, where X and Y are two disjoint item sets. X ⇒ Y indicates that X's occurrence implies Y's occurrence in the same transaction with a certain confidence. A supermarket's transaction database as an example, where a transaction is some customer's shopping list. A customer buying "bread" and "butter" will also buy "milk". Then {bread, butter} ⇒ milk is a possible association rule. X ⇒ Y is meaningful and useful if the confidence is high and X ∪ Y is frequent. More specifically, X ⇒ Y is regarded as an association rule if and only if Supp(X ∪ Y) ≥ Ts and Conf (X ⇒ Y) ≥ Tc. Conf (X ⇒ Y) as the confidence of X ⇒ Y. The latter is the probability of Y's occurrence given X's occurrence (i.e. Conf (X ⇒ Y) = Supp(X ∪ Y)/Supp(X)). Tc denotes the threshold specified by the data miner. The values of Ts and Tc are generally configured based on the type of transactions, the usage of the mining result, the size of database, etc. It is easy to mine association rules after mining frequent item sets and obtaining their supports. Most association rule mining algorithms are built based on frequent item set mining algorithms.

If each data owner has one or more rows (i.e. transactions) in the joint database, we say that the database is horizontally partitioned. If each data owner has one or more columns in the joint database, the database is considered vertically partitioned. This work focuses on both vertically partitioned databases and horizontally partitioned database. In this work, proposing a cloud-aided privacy-preserving frequent item set mining solution for partitioned databases, which is then used to build a privacy-preserving association rule mining solution. Both solutions are designed for applications where data owners have a high level of privacy requirement. The solutions are also suitable for data owners looking to outsource data storage i.e. data owners can outsource their encrypted data and mining task to a semi-trusted (i.e. curious but honest) cloud in a privacy preserving manner. To the best of our knowledge, this is the first work on outsourced association rule mining and frequent item set mining for vertically and horizontally partitioned databases. The key underlying techniques in these solutions are an efficient enhanced secure encryption scheme and a secure outsourced comparison scheme.

The contributions of this paper are as follows:

- Proposing and designing privacy-preserving mining solutions for high privacy requirements. The proposed solutions are uniquely located in the design space.
- This work proposes an efficient secure encryption scheme and a secure outsourced comparison scheme. To avoid the disclosure of supports/confidences, design an efficient encryption scheme to facilitate secure outsourced computation of supports/ confidences, as well as a secure outsourced comparison scheme for comparing supports/confidences with thresholds.
- The proposed encryption scheme is tailored for the proposed comparison.
- This work proposes a cipher text tag approach for canceling out fictitious data's effect on mining result.

II. RELATED WORK

In [2], the principal work to identify and address privacy issues in vertically partitioned databases, a safe scalar product protocol is presented and used to construct a privacy-preserving frequent itemset mining solution. Association rules can then be found given frequent itemsets and their supports. Since the publication of this seminal work, a number of privacy preserving association rule mining or frequent itemset mining solutions have been published in the literature (see [3], [4], [25], [26], [27], [28], [29]).

The most relevant work is the privacy-preserving association rule mining solution presented in [3]. In this solution, a data owner known as the master is responsible for the mining. The other data owners (known as slaves) insert fictitious transactions to their respective datasets, and send the datasets to the master. Each data owner will also send his set of real transactions' IDs to a semi-trusted third-party server. The third-party server is assumed not to be colluding with any data owner, but it cannot be trusted to hold the raw data. The master generates association rule candidates from the joint database containing fictitious data. For each rule candidate $X \Rightarrow Y$, the master sends the ID lists of the transactions containing $X \cup Y$ and the transactions containing X to the third-party server. The server verifies if the rule is qualified or not. Similar to our solutions, a semi-trusted third-party is utilized for the mining. However, unlike our solutions, a data owner (i.e. the master) does the majority of the computational work. Therefore, we can hardly say that such a solution is an outsourced mining solution. Though fictitious data are added in datasets to lower data usability, the master is able to learn significant information about other data owners' raw data from the received datasets. In contrast, our solutions do not leak such information as we do not rely on one particular data owner to undertake the computations and we also encrypt the datasets.

Our solutions do not expose exact supports or confidences to data owners. Different from existing solutions based on encryption, we use symmetric encryption instead of asymmetric homomorphic encryption, and the manner in which we use symmetric encryption also differs from existing solutions. In our approach, we use encryption to create ERVs and build our secure outsourced comparison scheme.

Privacy-preserving Outsourced Association Rule Mining and Frequent Itemset Mining. Privacy-preserving outsourced frequent itemset mining and association rule mining have been considered in the setting of a single data owner [6], [23], [24], [5]. In existing solutions, the data owner outsources their data and the mining task to the cloud, but at the same time, wish to keep the raw data secret from the cloud. Generally, data items in the database are encrypted using a symmetric encryption prior to outsourcing. However, a later work [23] demonstrated that [6]'s solution is not secure. Giannotti et al. proposed a solution based on k-anonymity frequency [24], [5]. To counter frequency analysis attack, the data owner inserts fictitious transactions in the encrypted database to conceal the item frequency. After inserting the fictitious transactions, any item in the encrypted database will share the same frequency with at least k−1 other items. The data owner sends the encrypted database of both the real and fictitious transactions to the cloud. The cloud runs a classic frequent itemset mining algorithm, and returns the result (frequent itemsets and their supports) to the data owner. The data owner revises these itemsets' supports by subtracting them with these itemsets' corresponding occurrence counts in the fictitious transactions respectively. Finally, the data owner decrypts the received itemsets with the revised supports higher than the frequency threshold, and generates association rules based on found frequent itemsets. Our solutions use their techniques to conceal the raw data from the cloud and mitigate frequency analysis attack that can be undertaken by the cloud. Using these techniques alone, however, is not sufficient to protect data privacy in the vertically and horizontally partitioned database setting. To cancel out fictitious transactions, both [24], [5] require the data owner to count itemset occurrences in fictitious transactions.

In the vertically and horizontally partitioned database setting, data owners are unable to perform such calculation using the techniques described in [24], [5]. In our solutions, the cloud rather than the data owners cancels out fictitious transactions in a privacy preserving manner, and the underlying techniques are our symmetric encryption, secure comparison and ciphertext tag schemes.

III. System Architecture

The system model is comprised of two or more data owners and a cloud. Each data owner has a private database, and the data owners encrypt their private databases prior to outsourcing the encrypted databases to the cloud. Data owners can also request the cloud to mine association rules or frequent itemsets from the joint database on their behalf. The cloud is tasked with the compiling and storing of databases received from different data owners, the mining of association rules or frequent itemsets for data owners, and the sending of the mining result to relevant data owners.

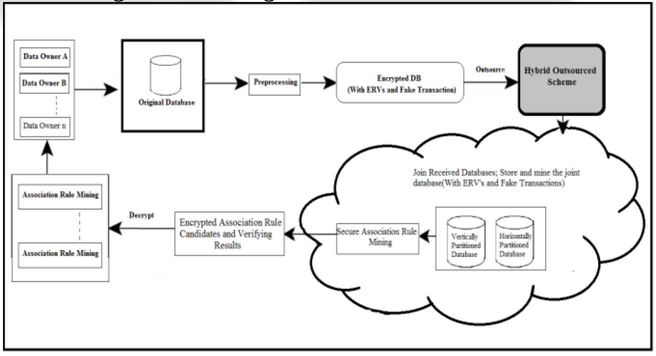

Data Owner A
Data Owner B
Data Owner n
Original Database
Preprocessing
Encrypted DB (With ERVs and Fake Transaction)
Outsource
Hybrid Outsourced Scheme
Join Received Databases; Store and mine the joint database(With ERV's and Fake Transactions)
Association Rule Mining
Association Rule Mining
Decrypt
Encrypted Association Rule Candidates and Verifying Results
Secure Association Rule Mining
Vertically Partitioned Database
Horizontally Partioned Database

Fig. 1: System architecture.

The proposed system consists of following processes

A. *Pre-processing Stage-*

In the preprocessing stage, data owners and the cloud collaborate to generate an encrypted joint database at the cloud's end and some auxiliary data for privacy-preserving mining. Each data owner inserts fictitious transactions to his private database, and encrypts items in the database with a Symmetric Encryption technique or substitution cipher. The fictitious transactions are used to mitigate frequency analysis attacks. Once the databases have been encrypted, they are outsourced to the cloud as part of the joint database maintained by the cloud. To allow the cloud to accurately mine the database (which has fictitious transactions), data owners tag each transaction in their outsourced databases and joint database with an encrypted realness value (ERV) using our customized encryption scheme. A realness value (RV for short) is either 0 or 1, which indicates that the transaction is fictitious or real, correspondingly. All ERVs are sent to the cloud. Please note that the cloud is still unable to determine whether a transaction is fictitious or not, even having ERVs.

B. Mining Stage-

In the mining stage, the cloud mines association rules for data owners in a privacy-preserving manner. The cloud mines association rule candidates from the encrypted joint database. Because of the existence of fictitious transactions, some candidates will be "false positives". To allow data owners detecting false positives, the cloud verifies candidates in a privacy-preserving manner. The cloud computes each candidate's encrypted verifying result from the ERVs, utilizing encryption and secure comparison schemes. The cloud returns all candidates and their encrypted verifying results to the data owners. Finally, data owners decrypt the encrypted verifying results and association rule candidates to recover the real association rules. The main idea of our frequent itemset mining solution is similar, and the only differences are in the mining stage. In the mining stage, the cloud mines frequent itemset candidates (i.e. the seemingly frequent itemsets are defined later) instead of association rule candidates. The data owners then decrypt the encrypted verifying results and frequent itemset candidates to recover the real frequent itemsets.

C. Hybrid Outsourced Scheme-

The proposed secure Hybrid Outsourced Scheme is based on the encryption scheme.

1) Verifiable Outsourcing Scheme

Users can verify the correctness of the honest cloud server output with great probability, and can also verify the incorrectness of the dishonest cloud server output with great probability.

2) Outsourced Comparable Scheme

In privacy-preserving data mining solutions, data owners require the cloud to compare supports/ confidences with thresholds. However, both supports and confidences must be kept secret from the cloud and data owners, while the comparison results must be kept secret from the cloud we also choose database partitioning strategies by using comparable scheme considering Fuzzy based approach.

3) Distributed Association Rule Mining-

Distributed Association Rule Mining algorithm is used to compute confidence and support of a given candidate itemset. By considering values of the attributes finding whether a particular itemset is frequent, Considering number of records (count) where the values for all the attributes in the itemset are not null, then the candidate itemset is declared as the frequent itemset.

a) Over Vertical Data Partitioned Database

Vertical association rules in partitioned data items based on support count of the item set depiction. This vertical partitioning can be developed using the following example there are some data sets from hospital and then some data sets from super market but there is a relative from people verification from two data sets. By taking good association rule mining in their prescribed data, for example we will find a rule {beef meat, sugar} =>{Diabetes} that means most people who consume beef, meat, sugar undergo diabetes in this case we have vertical partitioned data. Because each site's dataset is dissimilar with others, but they have a relational field that join their data together.

b) Over Horizontal Data Partitioned Database

In horizontal distributed data sets, all the transactions distributing among number of item sets. In that we are scheming global item set is equal to sum of local item sets. An itemset X is globally supported if the global support count of X is bigger than s% of the total transaction database size. A k-itemset is called a globally large k-itemset if it is globally supported. In this way we proceed to develop proficient progression in commercial data set representation in data outsourcing.

4) Frequent itemset mining-

For calculation of frequent items based on their support, mining algorithms like Apriori, Eclat and FP-growth. identifies all items 'c' such that their support $|\mathrm{sids}(c)|/|S| \geq \mathrm{MinSup}$. Those items having support greater than minsup will be considered as frequent items. Those items having support less than minsup are rejected.

5) Rule generation-

For generation of association rules Apriori rule generation algorithm is used which first starts the scanning of transaction database to get the support and then from that support calculate a candidate generation key and from that the support is compared with it and according to that the frequent itmsets are generated. The process is repeated until the final frequent itemsets are generated. By comparing confidence % (percent) with min confidence and generates the final rule i.e. the output of apriori is association rules.

6) Useful Concepts

To select appealing rules from the set of all feasible rules, constraints on various measures of significance and interest can be used. The best-known constraints are bare minimum thresholds on support and confidence.

7) Support

The support supp(X) of an itemset X is defined as the proportion of transactions in the data set which contain the itemset.

supp(X)= no. of transactions which contain the itemset X/total no. of transactions

8) Confidence

The confidence of a rule is defined:

$$\mathrm{Conf}(X \rightarrow Y) = \mathrm{Supp}(X \cup Y) / \mathrm{supp}(X)$$

IV. APRIORI ALGORITHM

Algorithm 1. Steps of Apriori algorithm.

V. ASSOCIATION RULE GENERATION WITH APRIORI ALGORITHM

Association rule generation is generally divided up into two steps:

1) First, minimum support is applied to find all frequent itemsets in a database.
2) Second, these frequent itemsets and the bare minimum confidence constraint are used to construct rules.

While the second step is straight frontward, the first step needs more awareness.

Finding all frequent itemsets in a database is difficult since it involves searching all possible itemsets (item combinations). The set of possible itemsets is the power set over I and has size 2n − 1 (excluding the empty set which is not a valid itemset). Although the size of the power set grows exponentially in the number of items n in I, proficient search is possible using the downward-closure property of support (also called anti-monotonicity) which guarantees that for a frequent itemset, all its subsets are also frequent and thus for an infrequent itemset, all its supersets must also be infrequent. Exploiting this property, efficient algorithms (e.g., Apriori and Eclat) can find all frequent itemsets.

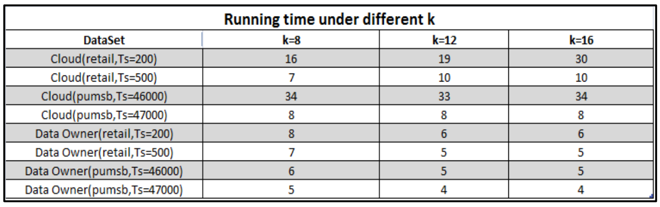
```
Apriori (T, minSupport) { //T is the database and
    minSupport is the minimum support
L1= {frequent items};
for (k= 2; $L_{k-1}$ !=∅; k++) {
    $C_k$= candidates generated from $L_{k-1}$
    //that iscartesian product $L_{k-1}$ x $L_{k-1}$ and eliminating
any k-1 size itemset that is not
    //frequent
    for each transaction t in database do{
        #increment the count of all candidates in $C_k$ that
are contained in t
        $L_k$ = candidates in $C_k$ with minSupport
    }//end for each
```

VI. ALGORITHMS (E.G., ECLAT AND FP-GROWTH) CAN FIND ALL FREQUENT ITEMSETS. EXPERIMENTS AND RESULTS

A. *Experimental Setup*

To evaluate performance of this system we compared their performance with existing algorithms. Experiments were performed on a standalone machine with a 2.53 GHz Intel Core 3 processor running Windows 7 and 1 GB of free RAM. To measure the performance we have taken retail dataset which contains retail market basket data. The dataset contains the no. of transactions. The events are partitioned by each data owner on their different kind of attributes. The attributes are defines the transaction ID, Name, date, etc.

B. *Result Analysis*



Running time under different k

DataSet	k=8	k=12	k=16
Cloud(retail,Ts=200)	16	19	30
Cloud(retail,Ts=500)	7	10	10
Cloud(pumsb,Ts=46000)	34	33	34
Cloud(pumsb,Ts=47000)	8	8	8
Data Owner(retail,Ts=200)	8	6	6
Data Owner(retail,Ts=500)	7	5	5
Data Owner(pumsb,Ts=46000)	6	5	5
Data Owner(pumsb,Ts=47000)	5	4	4

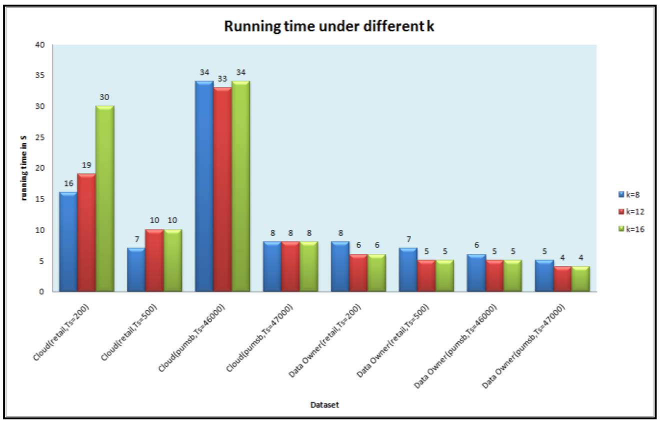
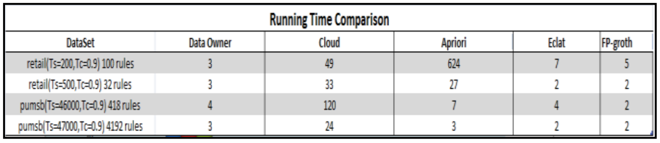


Fig. 2: Running time with different infrastructure

First experiment is carried out on transaction process dataset to find out execution time required to generate the rules. Fig. 2. shows graph of execution time(seconds) vs. cloud and different data owners by using different datasets.The above graph shows time required to generate rules.



Running Time Comparison

DataSet	Data Owner	Cloud	Apriori	Eclat	FP-groth
retail(Ts=200,Tc=0.9) 100 rules	3	49	624	7	5
retail(Ts=500,Tc=0.9) 32 rules	3	33	27	2	2
pumsb(Ts=46000,Tc=0.9) 418 rules	4	120	7	4	2
pumsb(Ts=47000,Tc=0.9) 4192 rules	3	24	3	2	2

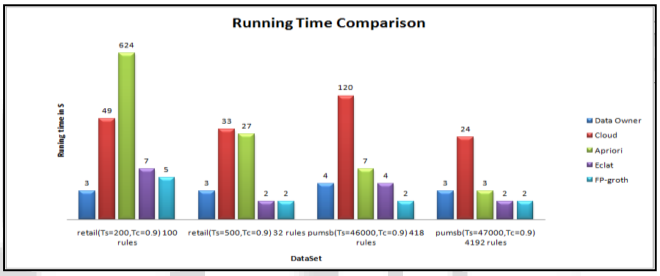
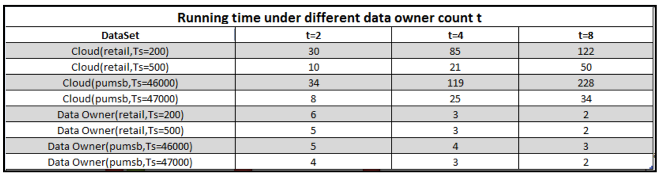


Fig. 3: Running time under different techniques

Second experiment is carried out to compare the running time of proposed system with the different algorithms, data owners and cloud on different kind of datasets. Fig. 3 shows datasets vs. different algorithms, owners and clouds.



Running time under different data owner count t

DataSet	t=2	t=4	t=8
Cloud(retail,Ts=200)	30	85	122
Cloud(retail,Ts=500)	10	21	50
Cloud(pumsb,Ts=46000)	34	119	228
Cloud(pumsb,Ts=47000)	8	25	34
Data Owner(retail,Ts=200)	6	3	2
Data Owner(retail,Ts=500)	5	3	2
Data Owner(pumsb,Ts=46000)	5	4	3
Data Owner(pumsb,Ts=47000)	4	3	2

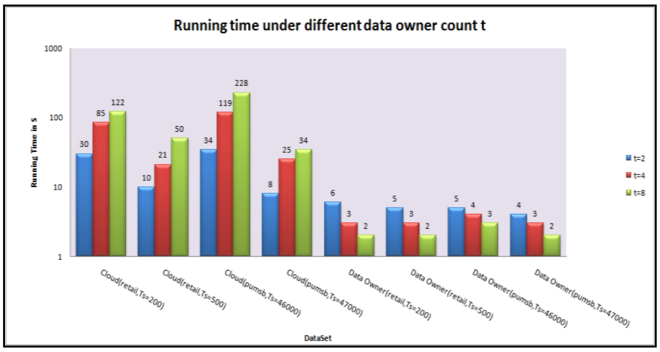


Fig. 4: Running Time Under different Data Owner Count

Fig.4 shows Running Time Under different Data Owner Count. The running time is calculated with different data owners and cloud on different kind of transaction database.

VII. Conclusion

Privacy Preservation techniques are gaining more importance now a days, because there is lot of information on the internet but user wants specific information and data owner also wants a privacy for their data, which can be provided by using privacy preservation techniques with an rule mining techniques. Here, we designed model- based privacy preservation technique i.e. privacy preserving outsourced association rule mining for partitioned database (PPOARMD). In PPOARMD, we observed that the system allows data owners to outsource mining chore on their joint data in the privacy preserving manner. When outsourcing the data we provide a best encryption scheme to avoid the leakage of data and to maintain privacy.

In the next phase, the items which are not purchased by users and the items which are not visited by the user are considered while giving recommendations to the user. This can be done by using a different rule mining method. Also we will implement hybrid outsourced scheme which is the combination of two techniques, which provides the best way for data owners to outsource their data on partitioned databases with a smaller amount data leakage and high level of privacy without compromising performance. The system is more scalable and efficient than previous systems.

References

[1] Lichun Li, Rongxing Lu, Kim-Kwang Raymond Choo, Anwitaman Datta, and Jun Shao, "Privacy Preserving-Outsourced Association Rule Mining on Vertically Partitioned Databases" IEEE Transactions on Information Forensics and Security, Vol. 11, No. 8, August 2016.

[2] J. Vaidya and C. Clifton, "Privacy preserving association rule mining in vertically partitioned data," in Proc. SIGKDD, 2002, pp. 639–644.

[3] B. Rozenberg and E. Gudes, "Association rules mining in vertically partitioned databases," Data Knowl. Eng., vol. 59, no. 2, pp. 378–396.

[4] S. Zhong, "Privacy-preserving algorithms for distributed mining of frequent itemsets," Inf. Sci., vol. 177, no. 2, pp. 490–503.

[5] F. Giannotti, L. V. S. Lakshmanan, A. Monreale, D. Pedreschi, and H. Wang, "Privacy-preserving mining of association rules from outsourced transaction databases," IEEE Syst. J., vol. 7, no. 3, pp. 385–395,Sep. 2013.

[6] W. K. Wong, D. W. Cheung, E. Hung, B. Kao, and N. Mamoulis,"Security in outsourcing of association rule mining," in Proc. VLDB,2007, pp. 111–122.

[7] J. Lai, Y. Li, R. H. Deng, J. Weng, C. Guan, and Q. Yan, "Towards semantically secure outsourcing of association rule mining on categorical data," Inf. Sci., vol. 267, pp. 267–286, May 2014.

[8] 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.

[9] O. Goldreich, "Encryption schemes", working draft, (2003) March.

[10] H. Grosskreutz, B. Lemmen and S. Rüping, "Secure Distributed Subgroup Discovery in Horizontally Partitioned Data", Transactions on Data Privacy, vol. 4 no. 3, (2011), pp. 147-165.

[11] Can Xiang, Chunming Tang "Efficient outsourcing schemes of modular exponentiations with checkability for untrusted cloud server" J Ambient Intell Human Comput (2015) 6:131–139.

[12] Xinjing Ge, Li Yan, Jianming Zhu, Wenjie Shi "Privacy-Preserving Distributed Association Rule Mining Based on the Secret Sharing Technique".

[13] Xuan Canh Nguyen, Hoai Bac Le, Tung Anh Cao "An enhanced scheme for privacy-preserving association rules mining on horizontally distributed databases" 978-1-4673-0309-5/12, 2012 IEEE

[14] Rui Xia, Feng Xu, Chengqing Zong, Qianmu Li, Yong Qi and Tao Li, "Dual Sentiment Analysis: Considering Two Sides of One Review" IEEE Trans. Knowl. Data Eng.,vol. 27, No. 8, August 2016, pp. 2120-2133.

[15] Boxiang Dong, Ruilin Liu, and Hui (Wendy) Wang "Trust-but-Verify: Verifying Result Correctness of Outsourced Frequent Itemset Mining in Data-Mining-As-a-Service Paradigm" IEEE Transactions On Services Computing, Vol. 9, No. 1, January/February 2016.

[16] P. Fournier-Viger. Real-life Datasets in SPMF Format, accessed on Apr. 6, 2016. [Online].Available:http://www.philippefournierviger.com/spmf/index.php?link=datasets.php.

[17] Sen Su, Shengzhi Xu, Xiang Cheng, Zhengyi Li, and Fangchun Yang, "Differentially Private Frequent Itemset Mining via Transaction Splitting" IEEE Transactions On Knowledge And Data Engineering, Vol. 27, No. 7, July 2015.

[18] Sumeet Bajaj and Radu Sion"TrustedDB: A Trusted Hardware-Based Database with Privacy and Data Confidentiality" IEEE Transactions on Knowledge and Data Engineering, Vol. 26, No. 3, March 2014.

[19] Fosca Giannotti, Laks V. S. Lakshmanan, Anna Monreale, Dino Pedreschi, and Hui (Wendy) Wang "Privacy-Preserving Mining of Association Rules From Outsourced Transaction Databases" IEEE SYSTEMS JOURNAL, VOL. 7, NO. 3, SEPTEMBER 2013.

[20] Tamir Tassa "Secure Mining of Association Rules in Horizontally Distributed Databases" IEEE Transactions on Knowledge and Data Engineering, 2013.

[21] Xuan Canh Nguyen, Hoai Bac Le, Tung Anh Cao, "An Enhanced Scheme For Privacy-Preserving Association Rules Mining On Horizontally Distributed Databases," In 2012 IEEE.

[22] Bogdan Carbunar and Radu Sion, "Toward Private Joins on Outsourced Data" IEEE Transactions On Knowledge And Data Engineering, Vol. 24, No. 9, September 2012.

I. Molloy, N. Li, and T. Li, "On the (in) security and (im) practicality of outsourcing precise association rule mining," in ICDM 2009..

[23] F. Giannotti, L. V. Lakshmanan, A. Monreale, D. Pedreschi, and H. W. Wang, "Privacy-preserving data mining from outsourced databases," in CPDP 2011.

[24] J. Vaidya and C. Clifton, "Secure set intersection cardinality with application to association rule mining,"

Journal of Computer Security,vol. 13, no. 4, pp.593–622, 2005.

[25] X. Ge, L. Yan, J. Zhu, and W. Shi, “Privacy-preserving distributed association rule mining based on the secret sharing technique,” in SEDM 2010.

[26] R. Kharat, M. Kumbhar, and P. Bhamre, “Efficient privacy preserving distributed association rule mining protocol based on random number,” in Intelligent Computing, Networking, and Informatics. Springer, 2014,pp. 827–836.

[27] C. Dong and L. Chen, “A fast secure dot product protocol with application to privacy preserving association rule mining,” in Advances in Knowledge Discovery and Data Mining - 18th Pacific-Asia Conference, PAKDD 2014, Tainan, Taiwan, May 13-16, 2014. Proceedings, Part I, 2014, pp. 606–617. [Online]. Available: http://dx.doi.org/10.1007/978-3-319-06608-0 50.

[28] J. Zhan, S. Matwin, and L. Chang, “Privacy-preserving collaborative association rule mining,” in DBSEC 2005.