

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

Association Rule Mining for Frequent Itemset on Encoded Cloud Data

Mansi Mehta¹, M Sindhuja², T C Nivetha³, N. R. Rejin Paul⁴

Student, Department of Computer Science and Engineering, Velammal Institute of Technology, Chennai,
Tamil Nadu, India^{1,2,3}

Assistant Professor, Department of Computer Science and Engineering, Velammal Institute of Technology, Chennai,
Tamil Nadu, India⁴

ABSTRACT: Association rule mining is an important data mining method that has been studied extensively by the academic community and has been applied in practice. In the context of association rule mining, the state-of-the-art in privacy preserving data mining provides solutions for categorical and Boolean association rules but not for quantitative association rules[2]. In this paper, the results show high efficiency, privacy and accuracy of rules for small to moderate updates in large volumes of data. It is trusted that the framework that is developed is therefore applicable and valuable for securely mining big data. In this paper, by forcing a few constraints on the source areas; with the goal that the focal target area tracks and privatizes changes and an outsider mines the information incrementally. The outcomes demonstrate high effectiveness, protection and exactness of principles for little to direct updates in extensive volumes of information. It is trusted that the system that is created in this way is pertinent and profitable for mining huge information.

KEYWORDS: Privacy-Preserving, cloud computing, frequent itemset mining, encryption algorithm.

I. INTRODUCTION

Protecting privacy is an important element in many database applications. Many countries set up privacy laws to clearly protect privacy, For instance, medical records and personal information of patients in a hospital should not be disclosed. There are new approaches to handle the privacy-preserving data mining problems. One approach is to modify the database randomly so that other parties can fully access the modified data. However, data mining algorithms can then produce only approximate results using the modified data. Another approach is to develop new algorithm applying cryptographic techniques so that accurate results can be obtained without direct access to the source data [1]. The protection of the confidentiality of this information has been a long-term goal for the database security research community and for the government statistical agencies. Recent advances in data mining and machine learning algorithms have increased the disclosure risks that one may encounter when releasing data to outside parties[17]. Data products (macrodata or tabular data and micro-data or raw data records), are designed to inform public or business policy, and research or public information. Securing these products against unauthorized accesses has been a long-term goal of the database security research community and the government statistical agencies. Solutions to this problem require combining several techniques and mechanisms. Recent advances in data mining and machine learning algorithms have, however, increased the security risks[13]. This paper deals with the problem of limiting disclosure of sensitive rules. In particular it is attempted to selectively hide some frequent itemsets from large databases with as little as possible impact on other non-sensitive frequent itemsets. Frequent itemsets are sets of items that appear in the database "frequently enough" and identifying them is usually the first step toward association/correlation rule or sequential pattern mining. Experimental results are presented along with some theoretical issues related to this problem[13-14]. Incrementality is a major challenge in the mining of dynamic databases. A number of incremental strategies have been proposed earlier with several limitations. A serious limitation is the need to examine the entire

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

family of closed itemsets, whenever there are insertions or deletions in the database. The proposed strategy relies on an efficient and selective update of the closed itemsets using an indexed trie structure. The framework emphasizes on certain fundamental and structural properties of Galois Lattice theory to overcome the limitations of the earlier approaches. Apart from facilitating a selective update, the indexed structure removes the necessity of working with a wholly memory resident [22]. We consider an uncommon case in affiliation control mining where mining is directed by an outsider over information situated at a focal area that is refreshed from a few source areas. The information at the focal area is very still while that streaming in through source areas is in movement. In this paper, we force a few constraints on the source areas; with the goal that the focal target area tracks and privatizes changes and an outsider mines the information incrementally. Our outcomes demonstrate high effectiveness, protection and exactness of principles for little to direct updates in extensive volumes of information. We trust that the system we create is in this way pertinent and profitable for mining huge information.

II. LITERATURE SURVEY

In 2014, VikramGarg, Anju Singh, Divakar Singh, Published a paper on “A Survey of Association Rule hiding Algorithms” In this paper we will provide a comparative theoretical analysis of Algorithms that have been developed for Association Rule Hiding.

In 2006, Xiao-Bai Li and SumitSankar, Published a paper on “A Tree-Based Data Perturbation Approach for Privacy-Preserving Data Mining” proposed a kd-tree based perturbation method, which recursively partitions a data set into smaller subsets such that data records within each subset are more homogeneous after each partition. The confidential data in each final subset are then perturbed using the subset average. An experimental study is conducted to show the effectiveness of the proposed method

In 2004, Matthew Eric Otey, SrinivasanParthasarathy, Chao Wang, Adriano Veloso, and Wagner Meira, Jr, Published a paper on “Parallel and Distributed Methods for Incremental Frequent Item set Mining” shows how to parallelize this incremental algorithm. We also propose a distributed asynchronous algorithm, which imposes minimal communication overhead for mining distributed dynamic datasets.

In 2004, Murat Kantarcioglu and Chris Clifton, Published a paper on “Privacy- Preserving Distributed Mining of Association Rule on Horizontally Partitioned Data” addresses secure mining of association rules over horizontally partitioned data. The methods incorporate cryptographic techniques to minimize the information shared, while adding little overhead to the mining task.

In 2003, Stanley R.M.oliveira, OsmarR.Zaiane, Published a paper on “Protecting Sensitive Knowledge by Data Sanitization” addressing the problem on protecting actionable knowledge for strategic decisions, but at the same time not losing the great benefit of association rule mining. To accomplish that, we introduce a new, efficient one-scan algorithm that meets privacy protection and accuracy in association rule mining, without putting at risk the effectiveness of the data mining.

III. PROPOSED SYSTEM

❖ SYSTEM DESIGN

In this paper, privacy-preserving framework for secure frequent item set mining on encrypted data is proposed, where only one aided server is needed besides the Cloud Service Provider (CSP). There are n users $\{U_1, \dots, U_n\}$, a data miner, a Cloud Service Provider (CSP), and an Evaluator. Each user uploads a transaction (or multiple transactions) to the CSP. The CSP maintains a transaction database, which includes a massive number of transactions contributed from different users. The data miner can submit frequent item set mining queries to the CSP, and as to leverage, an Evaluator to assist

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

the CSP to perform frequent item set mining efficiently on the transaction database. At the end of the executions, the CSP will return a Boolean result (e.g., frequent or not) of a mining query to the data miner.

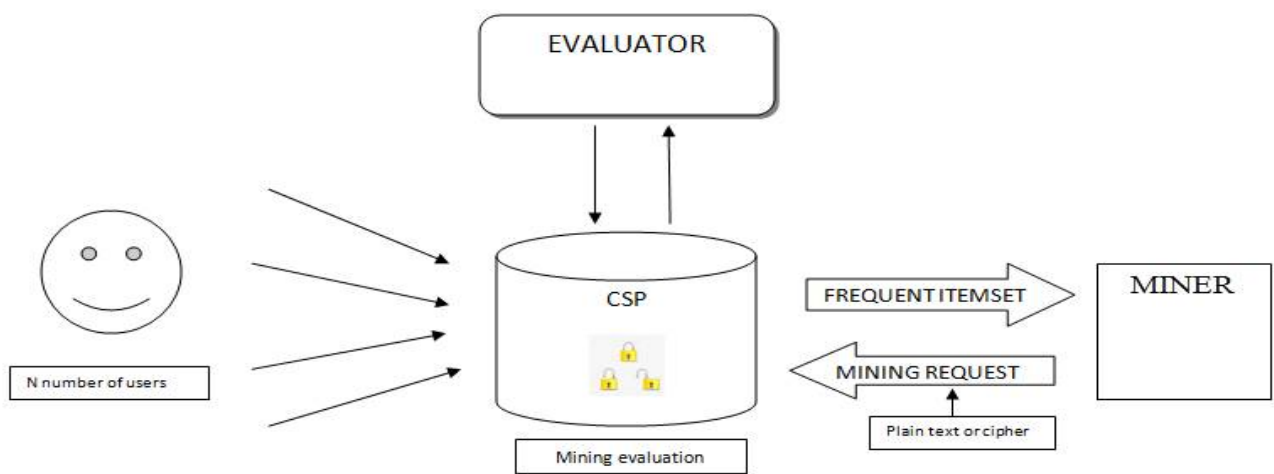


Figure 1.0 represents the design of the system architecture

A. CSP (CLOUD SERVICE PROVIDER):

The CSP collects encrypted transactions and maintains an encrypted transaction database, and the Evaluator assists the CSP to carry mining on encrypted data. Based on this framework, we design three protocols, where the first protocol is better in terms of mining time and the second protocol is stronger in the aspect of privacy protection. To achieve a better efficiency of Protocol, we introduce the third protocol via sacrificing little privacy. Due to the leverage of this only one aided server, our protocols outperform the previous work mentioned above in the aspect of running time with a similar privacy level in practice

B. EVALUATOR:

The Evaluator assists the CSP to carry mining on encrypted. To assist the CSP to perform frequent item set mining efficiently on the transaction database. At the end of the executions, the CSP will return a Boolean result (e.g., frequent or not) of a mining query to the data miner. An encryption algorithm is used here to encrypt all the data items before storing it in the CSP, this is to ensure privacy between various admins and to protect the details from different admins. The algorithm used here is an AES algorithm standard, which stands for The Advanced Encryption Standard.

AES ENCRYPTION

AES is a block cipher with a block length of 128 bits. AES allows for three different key lengths: 128, 192, or 256 bits. Most of our discussion will assume that the key length is 128 bits. Encryption consists of 10 rounds of processing for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys. Except for the last round in each case, all other rounds are identical. Each round of processing includes one single-byte based substitution step, a row-wise permutation step, a column-wise mixing. The order in which these four steps are executed is different for encryption and decryption. To appreciate the processing steps used in a single round, it is best to think of a 128-bit block as consisting of a 4×4 array of bytes, arranged as follows:

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

$$\begin{bmatrix} \text{byte}_0 & \text{byte}_4 & \text{byte}_8 & \text{byte}_{12} \\ \text{byte}_1 & \text{byte}_5 & \text{byte}_9 & \text{byte}_{13} \\ \text{byte}_2 & \text{byte}_6 & \text{byte}_{10} & \text{byte}_{14} \\ \text{byte}_3 & \text{byte}_7 & \text{byte}_{11} & \text{byte}_{15} \end{bmatrix}$$

Notice that the first four bytes of a 128-bit input block occupy the first column in the 4×4 array of bytes. The next four bytes occupy the second column, and so on.

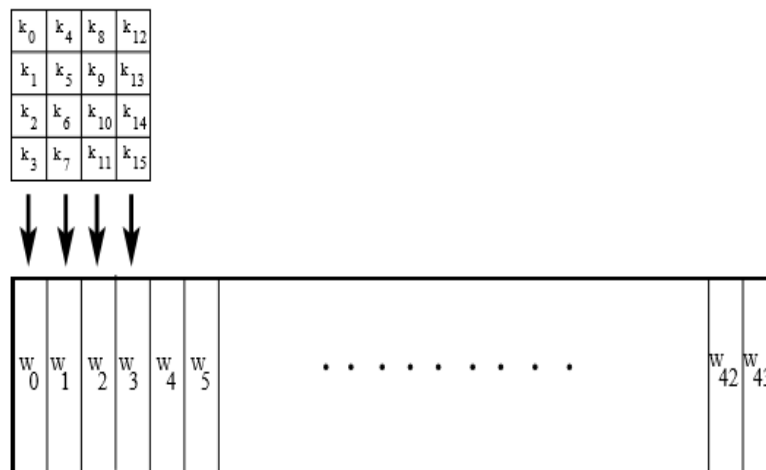


Figure 1.1 shows the four words of the original 128-bit key being expanded into a key schedule consisting of 44 words.

For encryption, each round consists of the following four steps: 1) Substitute bytes, 2) Shift rows, 3) Mix columns, and 4) Add round key. The last step consists of XORing the output of the previous three steps with four words from the key schedule. For decryption, each round consists of the following four steps: 1) Inverse shift rows, 2) Inverse substitute bytes, 3) Add round key, and 4) Inverse mix columns. The third step consists of XORing the output of the previous two steps with four words from the key schedule. Note the differences between the order in which substitution and shifting operations are carried out in a decryption round vis-a-vis the order in which similar operations are carried out in an encryption round. The last round for encryption does not involve the “Mix columns” step. The last round for decryption does not involve the “Inverse mix columns” step.

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

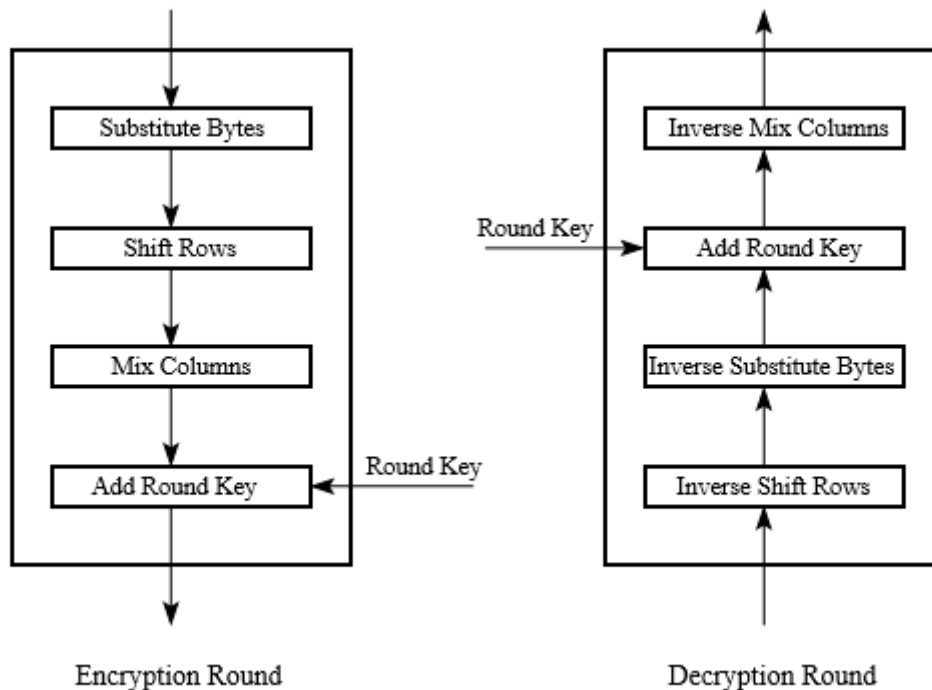


Figure 1.2 denotes the one round of encryption is shown at left and one round of decryption at right.

STEP 1: Substitute bytes called SubBytes for byte-by-byte substitution during the forward process. (The corresponding substitution step used during decryption is called InvSubBytes). This step consists of using a 16×16 lookup table to find a replacement byte for a given byte in the input state array. The entries in the lookup table are created by using the notions of multiplicative inverses in $GF(28)$ and bit scrambling to destroy the bit-level correlations inside each byte.

STEP 2: ShiftRows step is for shifting the rows of the state array during the forward process. (The corresponding transformation during decryption is denoted InvShiftRows for Inverse ShiftRow Transformation). The goal of this transformation is to scramble the byte order inside each 128-bit block.

STEP 3: MixColumns is for mixing up of the bytes in each column separately during the forward process. (The corresponding transformation during decryption is denoted InvMixColumns and stands for inverse mix column transformation.) The goal is here is to further scramble up the 128-bit input block. The shift-rows step along with the mix-column step causes each bit of the ciphertext to depend on every bit of the plaintext after 10 rounds of processing. In DES, one bit of plaintext affected roughly 31 bits of ciphertext. But now we want each bit of the plaintext to affect every bit position of the ciphertext block of 128 bits.

STEP 4: AddRoundKey is for adding the round key to the output of the previous step during the forward process. (The corresponding step during decryption is denoted InvAddRoundKey for inverse add round key transformation.)

C. MINER:

The miner requests for frequent itemset that are carried out in the CSP from the user, which is being evaluated from the evaluator. The mining request is a plain text or a cipher text. The data miner can submit frequent item set mining queries to the CSP, and we leverage an Evaluator to assist the CSP to perform frequent item set mining efficiently on

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

the transaction database. At the end of the executions, the CSP will return a Boolean result (e.g., frequent or not) of a mining query to the data miner.

❖ SUB-SYSTEM

1. Data Loading
2. Calculating count value
3. Finding Min and Max threshold value
4. Removing redundant data
5. Frequent item set

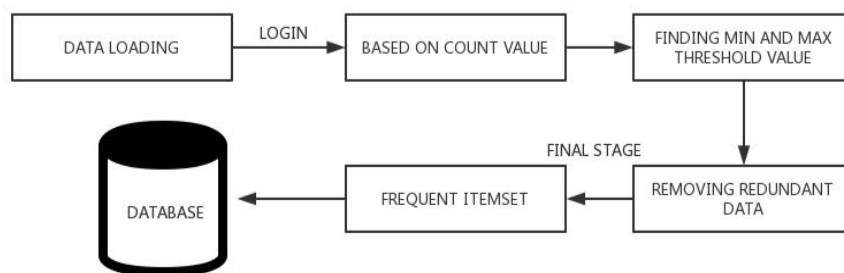


Figure 1.3 represents the systematic flow of the sub-systems

DATA LOADING

All the data will be uploaded into the database which is here is a Cloud Service Provider. Then the Admin will upload all the itemsets into the database. Those set of items are represented in a table format. The table holds the TRANS_ID, Items sets. Transaction id is customer id and itemset are the set of items which are listed as products. By this format all the data will be loaded.

CALCULATING COUNT VALUE

The count value is based on the total number of items and their related items sold. The frequent item, frequent pair item and least sold item based on the association rule mining algorithm. Association rule learning is a **rule-based machine learning** method for discovering interesting relations between variables in large databases. It is intended to identify strong rule discovered in databases using some measures of interest.

Pseudocode for calculating count value

```

for each transaction t=d
{
Ct=subset(ck,t);
for each candidate c=ctc.count++;
}
Lk{c=ck|c.count>min_sup};
If(k>=2)
{
delete_datavalue(d,lk,lk-1);
}
  
```

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

FINDING MIN AND MAX THRESHOLD VALUE

This sub system is used to determine the minimum and maximum threshold values of the items based on the attribute, characteristics and parameters. The threshold value is calculated based items selling ratings. If the threshold value is lesser than the count value then that particular item must be removed.

Pseudocode finding min and max threshold value

```
For(K=2;Lk-1=0;k++)
{
CK=apriori_gen(LK-1,min_sup); For each transaction t=d
{
Ct=subset(CK,t);
LK={c=CK|c.count>min_supp};
Return L=UkLk;
}
```

REMOVING REDUNDANT DATA

The additional data can simply be a complete copy of the actual data, or only select pieces of data that allow [detection of errorsreconstruction](#) of lost or damaged data up to a certain level. There will be lots of redundant items, so we must remove all the redundant items and also the infrequent items. By finding the frequent item set there will be no redundant data in the item set.

Pseudocode for removing redundant data

```
For each transaction t=d
{
For each data value
{
If(data value!=null and data value!=0)
{
Datarow.count++;
}
}
```

FREQUENT ITEMSET

Admin uploads their items into the database. After uploading the item, the uploaded item can be viewed as stored data. Finding frequently sold items that means which product is frequently bought by the customer. Also, Find frequent co-occurring items. That means, the items that are sold frequently together. The frequent items will be found in the single record.

Pseudocode for finding frequent itemset

```
For each itemset I1=LK-1
{
For each itemset I2=LK-1
{
If(I1[1]=I2[1])^(I1[2]=I2[2])^...^(I1[K-2]=I2[K-2])^(I1[K-1]<I2[K-1])
Then
{
Delete datarow;
}
}
```


International Journal of Innovative Research in Science, Engineering and Technology

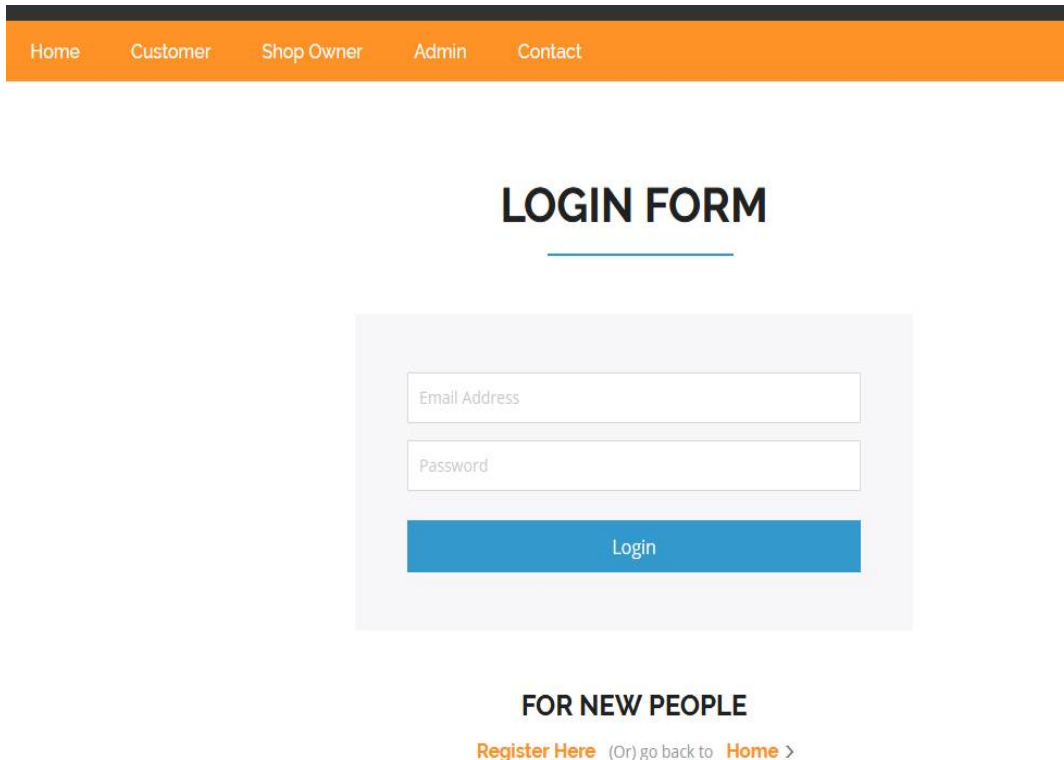
(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

IV. RESULTS

In this paper, three practical privacy-preserving frequent itemset mining protocols on encrypted cloud data is proposed. The Protocol 1 achieves an extremely higher mining performance while Protocol 2 provides a stronger privacy guarantee. Towards more practical efficiency, to optimize the performance of the second protocol by leveraging a minor leakage of privacy to achieve Protocol 3. Experimental results show that the protocols are much more efficient than previous work with the same security levels. In future work, is to focus on further improving the efficiency of frequent itemset mining on larger scale database. Furthermore, due to the special properties of streaming data (realtime and continuous) and its extensively practical application, focusing on the study of the efficient privacy-preserving frequent itemset mining algorithm on stream data.



Home Customer Shop Owner Admin Contact

LOGIN FORM

Email Address

Password

Login

FOR NEW PEOPLE

[Register Here](#) (Or) go back to [Home](#) >

Figure 1.4 represents customer login page, existing users can log in to the website using mail id provided to the server and the new users will have to register as a new user. The user cannot give unauthorized mail address because the redundant data will be evaluated by the admin.

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018



Customer Details

Name	ContactNumber	MailID	City	RegisterDate	RegisterStatus
Vicky	9876543210	vicky@gmail.com	Chennai	23/01/2018	Accept
Vicknesh	9864753664	Vicknesh@gmail.com	Chennai	15/02/2018	Accept
Kumar	9887767554	vicky123@gmail.com	Chennai	22/02/2018	Accept

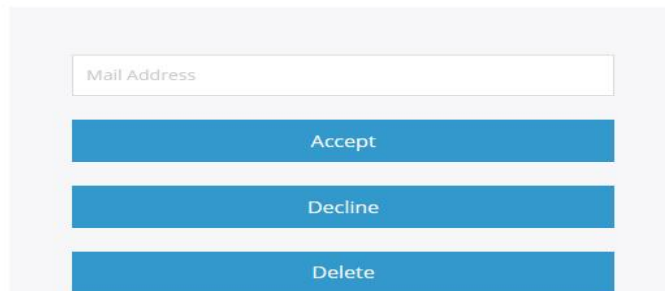


Figure 1.5 represents customer details, the admin has a control over the customer details given by the customers.

The admin duty is to accept or decline user's log in into the system for further shopping.



Product Details

Name	TotalQuantity	RemainingQuantity	SoldQuantity	PricePerUnit
Horlicks	400	385	15	15
Soap	0	0	0	0
Chocolate	344	344	0	50
Ice Cream	55	50	5	15
Abcde	78	75	3	22

Figure 1.6 represents product details, which are added into the system by the Admin.

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

WELCOME !!!

ADD PRODUCT NAME

ADD

PRODUCT NAME

Horlicks

QUANTITY

PRICE PER UNIT

Rs.

ADD

Figure 1.7 represents owner's product details, consists of each product's price and a new product can also be added into the system by the Admin.

[Home](#) [My Profile](#) [Shopping Site](#) [Purchase Details](#) [Log Out](#)

WELCOME !!!

ProductName	Quantity	PricePerUnit	TotalPrice	PurchaseDate
Horlicks	4	135	540	28/01/2018
Horlicks	4	135	540	28/01/2018
Horlicks	3	135	405	28/01/2018
Abcde	3	22	66	24/02/2018

Figure 1.8 represents minimum and maximum transactions taken place by all the customers. It shows the over all purchase details.

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

V. CONCLUSION

Previous work on privacy preserving quantitative association rule mining using discrete wavelet transform has been set in an environment where the collection of data is not transient and not subject to change. Since data is seldom static and at rest, that approach has little practical significance. We propose a solution to incrementally mine quantitative association rules securely in a dynamic environment where the detection of change in the original data is initiated and controlled by a database other than the one in which changes originate. Tests show 90% -100% accuracy of the rules for most datasets even when 50% of the original data undergoes a change. Comparisons indicate that the proposed TB-PIRU algorithm outperforms other approaches in preserving both data privacy and rules and is very efficient for 10% of changes in the original data, when this data is large in size. We provide a heuristic analysis of privacy for numeric data. A future study is required to conduct a formal analysis of privacy.

REFERENCES

- [1] W. K. Wong, D. W. Cheung, E. Hung, and H. Liu, "Protecting privacy in incremental maintenance for distributed association rule mining," PAKDD'08: Proceedings of the 12th Pacific-Asia conference on Advances in knowledge discovery and datamining, 2008.
- [2] M. Ahluwalia, A. Gangopadhyay, and Z. Chen, "Preserving Privacy in Mining Quantitative Association Rules," International Journal of Information Security and Privacy, 2010.
- [3] M. Ahluwalia, R. Gupta, A. Gangopadhyay, Y. Yesha, and M. McAllister, "Target-Based Database Synchronization," present-ed at the 25th ACM Symposium on Applied Computing, Sierre, Switzerland, 2010
- [4] M. Ahluwalia, A. Gangopadhyay, Z. Chen, and Y. Yesha, "Target-Based Privacy Preserving Association Rule Mining," presented at 26th ACM Symposium on Applied Computing, Tai-Chung, Taiwan, 2011.
- [5] D. W. Cheung, S. D. Lee, and B. Kao, "A general incremental technique for maintaining discovered association rules," Proc. 5th Int. Conf. Database Systems Advanced Applications, pp. 1-4, 1997.
- [6] A. Evfimevski, R. Srikant, R. Agrawal, and J. Gehrke, "Privacy preserving mining of association rules," 8th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD'02), pp. 217 -228, 2002.
- [7] J.-L. Lin and J. Y.-C. Liu, "Privacy preserving itemset mining through fake transactions," in Proceedings of the 2007 ACM symposium on Applied computing. Seoul, Korea: ACM Press, 2007, pp. 375-379.
- [8] S. Rizvi and J. R. Haritsa, "Maintaining Data Privacy in Association Rule Mining," VLDB, pp. 682-693, 2002.
- [9] Z.-Y. Chen and G.-H. Liu, "Quantitative Association Rules Mining Methods with Privacy-preserving," Sixth International Conference on Parallel and Distributed Computing, Applications and Technologies, 2005. PDCAT 2005., pp. 910-912, 2005.
- [10] J. S. Vaidya and C. Clifton, "Privacy preserving association rule mining in vertically partitioned data," 8th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, pp. 639 -644, 2002.
- [11] 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, pp. 1026-1037, 2004.
- [12] C. C. Aggarwal and P. S. Yu, "A Condensation Approach to Privacy Preserving Data Mining," 9th International Conference on Extending Database Technology, pp. 183-199, 2004.
- [13] S. R. M. Oliveira and O. R. Zaïane, "Protecting Sensitive Knowledge by Data Sanitization," In proc. of the 3rd IEEE International Conference on Data Mining, pp. 613-616, 2003.
- [14] M. J. Atallah, A. K. Elmagarmid, M. Ibrahim, and V. S. Verykios, "Disclosure Limitation of Sensitive Rules," presented at IEEE Knowledge and Data Engineering Workshop, 1999.
- [15] S. Menon, S. Sarkar, S., "Minimizing Information Loss and Pre-serving Privacy," Management Science, vol. 53, pp. 101-116, 2007.
- [16] Y. Saygin, V. S. Verykios, and C. Clifton, "Using Unknowns to Prevent Discovery of Association Rules," ACM SIGMOD Rec-ord, vol. 30, pp. 45-54, 2001.
- [17] V. S. Verykios, A. K. Elmagarmid, B. Elisa, Y. Saygin, and D. Elena, "Association Rule Hiding," IEEE Transactions on Knowledge and Data Engineering, vol. 16, pp. 434-447, 2004.
- [18] E. Dasseni, Verykios, V., Elmagarmid, A. and Bertino, E., "Hiding Association Rules by Using Confidence and Support," Proc. of 4th Intl. Information Hiding Workshop (IHW), 2001.
- [19] Y. Saygin, Verykios, V. and Elmagarmid, A., "Privacy Preserving Association Rule Mining," Proc. of 12th Intl. Workshop on Research Issues in Data Engineering (RIDE), 2002.
- [20] 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, pp. 1026-1037, September 2004.
- [21] J. S. Vaidya and C. Clifton, "Privacy preserving association rule mining in vertically partitioned data," presented at 8th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, Edmonton, Canada, July 2002.
- [22] B. Kalpana, R. Nadarajan, and J. S. Babu, "A Galois Lattice framework to handle updates in the mining of closed itemsets in dynamic databases," in Proceedings of the 1st Bangalore annual Computer conference. Bangalore, India: ACM, 2008, pp. 1-6.
- [23] W. Cheung and O. R. Zaïane, "Incremental Mining of Frequent Patterns without Candidate Generation or Support Constraint," In Proceedings of the Seventh International Database Engineering and Applications Symposium (IDEAS'03), pp. 111-116, 2003.

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

- [24] M. E. Otey, S. Parthasarathy, C. Wang, A. Veloso, and W. Meira, Jr., "Parallel and distributed methods for incremental frequent item set mining," *Systems, Man, and Cybernetics, Part B: Cybernetics*, IEEE Transactions on, vol. 34, pp. 2439-2450, 2004.
- [25] A. Veloso, W. M. Jr, M. B. d. Carvalho, B. Póssas, S. Parthasarathy, and M. Zaki, "Mining frequent item sets in evolving data-bases," *Proc. 2nd SIAM Int. Conf. Data Mining* Arlington, TX, pp. 494-510, 2002.
- [26] V. Ganti, J. Gehrke, and R. Ramakrishnan, "DEMON: Mining and monitoring evolving data," *Proc. 16th Int. Conf. Data Engineering*, San Diego, CA, pp. 439-448, 2000.
- [27] F. A. Chowdhury, K. T. Syed, J. Byeong-Soo, and L. Young-Koo, "Mining high utility patterns in incremental databases," *Proceedings of the 3rd International Conference on Ubiquitous Information Management and Communication*, pp. 656-663, 2009.
- [28] S. Lee and D. Cheung, "Maintenance of discovered association rules: When to update?," *SIGMOD Workshop Research Issues Data Mining Knowledge Discovery*, 1997.
- [29] D. Cheung, J. Han, V. Ng, and C. Y. Wong, "Maintenance of discovered association rules in large databases: An incremental updating technique," *Proc. 12th Int. Conf. Data Engineering*, pp. 106-114, 1996.
- [30] M. Ahluwalia and A. Gangopadhyay, "Privacy Preserving Data Mining –Taxonomy of Existing Techniques," in *Computer Security, Privacy and Politics: Current Issues, Challenges and Solutions*, R. Subramanian, Ed.: IGI Global, 2008.