An Enhance Encryption Scheme For Privacy-Preserving Mining Association Rules In Outsourced Database

P. Sowjanya* and B. Venkatesh #

Student of M.Tech, Global College Of Engineering and Technology, Andhra Pradesh, India

 # Department of CSE, Global College Of Engineering and Technology, Andhra Pradesh, India

***Abstract*— Data mining techniques are used to discover hidden information from large databases. Among many data mining techniques, association rule mining is receiving more attention to the researchers to find correlations between items or items sets efficiently. In distributed database environment, the way the data is distributed plays an important role in the problem definition. The data may be distributed horizontally or vertically or in hybrid mode among different sites. There is an increasing demand for computing global association rules for the databases belongs to different sites in a way that private data is not revealed and site owner knows the global findings and their individual data only. In this paper a model is proposed which adopts a sign based secure sum cryptography technique to find global association rules with trusted party by preserving the privacy of the individual's data when the data is distributed horizontally among different sites.**

***Keywords*— Data Mining, Distributed Database, Privacy Preserving Association Rule Mining, Cryptography Technique.**

Manuscript received Mar, 2014. ***P. Sowjanya****, Student of M.Tech, Global College Of Engineering and Technology, Kadapa, Andhra Pradesh, India.* ***Email: sowji.gcet@gmail.com***

B. Venkatesh*, Assistant Professor Department of CSE, Global College Of Engineering and Technology, Kadapa, Andhra Pradesh, India.*

I. INTRODUCTION

Data mining has been viewed as a threat to privacy because of the widespread proliferation of electronic data maintained by corporations. This has lead to increased concerns about the privacy of the underlying data. Data mining techniques find hidden information from large database while secret data is preserved safely when data is allowed to access by single person. Now a days many people want to access data or hidden information using data mining technique even they are not fully authorized to access. For getting mutual benefits, many organizations wish to share their data to many legitimate people but without revealing their secret data. In large applications the whole data may be in single place called centralized or multiple sites called distributed database. Methodologies are proposed by many authors for both centralized as well as distributed database to protect private data. This paper deals with privacy preserving in distributed database environment while sharing discovered knowledge/hidden information to many legitimate people. In distributed environment, database is a collection of multiple, logically interrelated databases distributed over a computer network and are distributed among number of sites. As the database is distributed, different users can access it without interfering with one another.

In distributed environment, database is partitioned into disjoint fragments and each site consists of only one fragment. Data can be partitioned in different ways such as horizontal, vertical and mixed. In horizontal partitioning of data, each fragment consists of a subset of the records of a relation R where as vertical partitioning of data, each fragment consists of a subset of attributes of a relation R. The another partitioning method is mixed fragmentation where data is partitioned horizontally and then each partitioned fragment is further partitioned into vertical fragments and vice versa [1]. Figure 1.a shows a method for mixed partitioned in which data is first partitioned vertically and then horizontally. Figure 1.b shows another mixed method in which data is partitioned horizontally and then vertically partitioned.

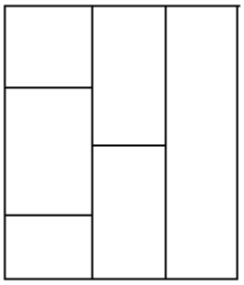

Figure1.a: Vertically partitioned database is further partitioned into horizontal

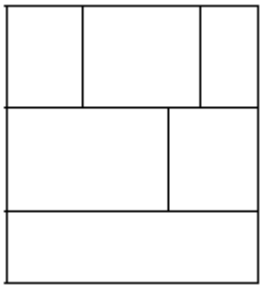

Figure1.b: Horizontally partitioned database is further Partitioned into vertical.

In data mining, association rule mining is a popular and well researched method for discovering interesting relations between variables in large databases. When data is distributed among different sites, finding the global association rules is a challenging task as the privacy of the individual site's data is to be preserved.

In this paper, a model is proposed to find global association rules by preserving the privacy of individual sites data when the data is partitioned horizontally among n number of sites.

II. LITERATURE SURVEY

The following have been analysed and studied in order to delegate.

2.1 M tamer Ozsu Patrick Valduriez,: Distributed database system (DDBS) technology is the union of what appear to be two diametrically opposed approaches to data processing: database system and computer network technologies. Database systems have taken us from a paradigm of data processing in which each application defined and maintained its own data (Figure 1.1) to one in which the data are defined and administered centrally (Figure 1.2). This new orientation results in data independence, whereby the application programs are immune to changes in the logical or physical organization of the data, and vice versa. One of the major motivations behind the use of database systems is the desire to integrate the operational data of an enterprise and to provide centralized, thus controlled access to that data. The technology of computer networks, on the other hand, promotes a mode of work that goes against all centralization efforts. At first glance it might be difficult to understand how these two contrasting approaches can possibly be synthesized to produce a technology that is more powerful and more promising than either one alone. The key to this understanding is the realization. that the most important objective of the database technology is integration, not centralization. It is important to realize that either one of these terms does not necessarily imply the other. It is possible to achieve integration without centralization,

and that is exactly what the distributed database technology attempts to achieve. In this chapter we define the fundamental concepts and set the framework for discussing distributed databases. We start by examining distributed systems in general in order to clarify the role of database technology within distributed data processing, and then move on to topics that are more directly related to DDBS.

2.2 R Agarwal, T Imielinski and A Swamy,: We are given a large database of customer transactions. Each transaction consists of items purchased by a customer in a visit. We present an efficient algorithm that generates all significant association rules between items in the database. The algorithm incorporates buffer management and novel estimation and pruning techniques. We also present results of applying this algorithm to sales data obtained from a large retailing company, which shows the effectiveness of the algorithm.

2.3 Verykios, V.S., Bertino, E., Nai Fovino, I., Parasiliti, L., Saygin, Y., and Theodoridis, Y. 2004: We provide here an overview of the new and rapidly emerging research area of privacy preserving data mining. We also propose a classification hierarchy that sets the basis for analyzing the work which has been performed in this context. A detailed review of the work accomplished in this area is also given, along with the coordinates of each work to the classification hierarchy. A brief evaluation is performed, and some initial conclusions are made.

2.4 Y. Lindell and B. Pinkas,: In this paper, we survey the basic paradigms and notions of secure multiparty computation and discuss their relevance to the field of privacy-preserving data mining. In addition to reviewing definitions and constructions for secure multiparty computation, we discuss the issue of efficiency and demonstrate the difficulties involved in constructing highly efficient protocols. We also present common errors that are prevalent in the literature when secure multiparty computation techniques are applied to privacy-preserving data mining. Finally, we discuss the relationship between secure multiparty computation and privacy-preserving data mining, and show which problems it solves and which problems it does not.

2.5 Elisa Bertino , Igor Nai Fovino Loredana Parasiliti Provenza: Recently, a new class of data mining methods, known as privacy preserving data mining (PPDM) algorithms, has been developed by the research community working on security and knowledge discovery. The aim of these algorithms is the extraction of relevant knowledge from large amount of data, while protecting at the same time sensitive information. Several data mining techniques, incorporating privacy protection mechanisms, have been developed that allow one to hide sensitive item sets or patterns, before the data mining process is executed. Privacy preserving classification methods, instead, prevent a miner from building a classifier which is able to predict sensitive data. Additionally, privacy preserving clustering techniques have been recently proposed, which distort sensitive numerical attributes, while preserving general features for clustering analysis. A crucial issue is to determine which ones among these privacy-preserving techniques better protect sensitive information. However, this is not the only criteria with respect to which these algorithms can be evaluated. It is also important to assess the quality of the data resulting from the modifications applied by each algorithm, as well as the performance of the algorithms. There is thus the need of identifying a comprehensive set of criteria with respect to which to assess the existing PPDM algorithms and determine which algorithm meets specific requirements. In this paper, we present a first evaluation

framework for estimating and comparing different kinds of PPDM algorithms. Then, we apply our criteria to a specific set of algorithms and discuss the evaluation results we obtain. Finally, some considerations about future work and promising directions in the context of privacy preservation in data mining are discussed.

2.6 M. Kantarcioglu and C. Clifto: Data mining can extract important knowledge from large data collections but sometimes these collections are split among various parties. Privacy concerns may prevent the parties from directly sharing the data, and some types of information about the data. This paper 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.

2.7 Chin-Chen Chang, Jieh-Shan Yeh, and Yu-Chiang Li: Data mining can extract important knowledge from large data collections—but sometimes these collections are split among various parties. Privacy concerns may prevent the parties from directly sharing the data and some types of information about the data.
This paper 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.

2.8 Mahmoud Hussein, Ashraf El-Sisi,and Nabil Ismail. The advancement in data mining techniques plays an important role in many applications. In context of privacy and security issues, the problems caused by association rule mining technique are investigated by many research scholars. It is proved that the misuse of this technique may reveal the database owner's sensitive and private information to others. Many researchers have put their effort to preserve privacy in Association Rule Mining. In this paper, we have presented the survey about the techniques and algorithms used for preserving privacy in association rule mining with horizontally partitioned database.

2.9 Lalanthika Vasudevan , S.E. Deepa Sukanya, N. Aarthi: In our era, Knowledge is not "just" information anymore, it is an asset. Data mining is thus extensively used for knowledge discovery from large databases. The problem with data mining is that with the availability of non-sensitive information, one is able to infer sensitive information that is not to be disclosed. Thus privacy is becoming an increasingly important issue in many data mining applications. This has led to the development of privacy preserving data mining. Two main approaches to privacy preserving data mining have emerged in recent years. The first approach protects the privacy of the data by using an extended role based access control approach where sensitive objects identification is used to protect an individual's privacy. The second approach uses cryptographic techniques. We propose a new solution by integrating the advantages of both these techniques with the view of minimizing information loss and privacy loss. By making use of cryptographic techniques to store sensitive data and providing access to the stored data based on an individual's role, we ensure that the data is safe from privacy breaches.

2.10 Vaidya, J. and Clifton, C. 2002. Privacy considerations often constrain data mining projects. This paper addresses the problem of association rule mining where transactions are distributed across sources. Each site holds some attributes of each transaction, and the sites wish to collaborate to identify globally valid association rules. However, the sites must not reveal individual transaction data. We present a two-party algorithm for efficiently discovering frequent item sets with minimum support levels, without either site revealing individual transaction values.

III. PROPOSED SYSTEM

The proposed model is illustrated by using three horizontally partitioned distributed databases for finding privacy preserving association rule mining. In this sample model, the horizontally partitioned databases called fragments such as DB1, DB2 and DB3 are placed in Site1,Site2 and Site3 respectively. Apart from these three sites, there exist a special site called Trusted Party site. Sample databases at Site1, Site2and Site3 are given below.

TABLE II.A DATABASE DB1, AT SITE$_1$

T-Id \Item	A_1	A_2	A_3	A_4	A_5
Site$_1$ has the following database					
T_1	1	0	0	1	0
T_2	1	1	0	1	1
T_3	0	1	1	0	1
T_4	0	0	1	1	1
T_5	1	1	0	1	1

TABLE II.B DATABASE DB2 AT SITE$_2$

T-Id \Item	A1	A_2	A_3	A_4	A_5
Site$_2$ has the following database					
T_1	0	1	1	1	1
T_2	0	0	1	1	1
T_3	1	1	1	1	0
T_4	1	1	0	1	1
T_5	1	1	0	0	1

TABLE II.C DATABASE, DB3 AT SITE$_3$

T-Id \Item	A_1	A_2	A_3	A_4	A_5
Site$_3$ has the following database					
T_1	1	0	0	1	1
T_2	1	1	1	0	1
T_3	1	0	1	1	1
T_4	1	0	1	1	0
T_5	1	0	1	1	1

TP request three sites to send encrypted form of local frequent item sets by sending two values such as minimum support threshold and public key. Each site computes local frequent item sets for their database by using minimum support threshold value 40% which is sent by the TP. The local frequent item sets (LF) of sites Site1, Site2and Site3, are given below.

Local frequent item sets at Site1

LF_1= { A_1 ,A_2,A_3 ,A_4,A_5,(A_1,A_2),(A_1,A_4),(A_1,A_5), (A_2,A_4),(A_2,A_5),(A_3,A_5),(A_4,A_5),(A_1,A_2,A_4), (A_1,A_2,A_5),(A_1,A_4,A_5),(A_2,A_4,A_5),(A_1,A_2,A_4,A_5)}

Local frequent item sets at Site$_2$

LF_2= { A_1 ,A_2 ,A_3 ,A_4 ,A_5,(A_1,A_2),(A_1,A_4), (A_1,A_5), (A_2,A_3), (A_2,A_4), (A_2,A_5), (A_3,A_4), (A_3,A_5),(A_4,A_5),(A_1,A_2,A_4),(A_1,A_2,A_5),(A_2,A_3,A_4) (A2,A_4,A_5),(A_3,A_4,A_5)}

Local frequent item sets at Site$_3$

LF_3= {A_1 ,A_3 ,A_4 ,A_5,(A_1,A_3),(A_1,A_4), (A_1,A_5), (A_3,A_4), (A_3,A_5),(A_4,A_5),(A_1,A_3,A_4,A_5) }

After receiving the encrypted form of local frequent item sets from the sites, TP prepares a merged frequent item list after eliminating duplicates. The merged list is as follows.

{A_1,A_2,A_3,A_4,A_5,(A_1,A_2),(A_1,A_3),(A_1,A_4),(A_1,A_5), (A_2,A_3),(A_2,A_4),(A_2,A_5),(A_3,A_4),(A_3,A_5),(A_4,A_5), (A_1,A_3,A_4),(A_1,A_3,A_5),(A_1,A_4,A_5),(A_1,A_2,A_4), (A_1,A_2,A_5),(A_2,A_3,A_4)(A_2,A_4,A_5),(A_3,A_4,A_5), (A_1,A_2,A_4,A_5),(A_1,A_3,A_4,A_5)}

The following are the random numbers and signs sent by TP along with merged list to the three sites.

Site1 received RN1 = 20, Sign1 = ('+').

Site2 received RN2 = 39, Sign2 = ('-').

Site3 received RN3 = 41, Sign3 = ('-').

Each site computes partial support and broadcast to all other sites in order to find the total partial supports. All three sites broadcast total partial supports for all the item sets in the merged list. TP finally declares global frequent item sets by comparing global excess support (GES) of an item set with zero where GESi is computed by subtracting SignSumRN from TotalPSi. The following steps illustrate the process of finding whether

the two item sets in the merged list are globally frequent or not. Consider the two item sets {(A3, A5), (A3, A4, A5)} from the merged list.

Let X1= (A3, A5) and X2 = (A3, A4, A5)

From the tables 2.1, 2.2 & 2.3, length of databases at three sites are given below

| DB1 | = 5, | DB2 | = 5, | DB3 | = 5 Global database size is | DB | = | | 3 1 I DBi = 15

TP computes SignSumRN by adding three random numbers along with signs using the formula SignSumRN = (+) 20 + (-) 39 + (-) 41 = - 60

Partial supports for X1 at different sites are computed as follows.

At Site1

PS11= X1.Sup – 40% of DB1 + (Sign1) RN1

PS11 = 2 – 2 + 20 = 20

At Site2

PS21 = X1 .sup – 40% of DB2 + (Sign2) RN2

PS21 = 2 - 2 - 39 = - 39

At Site3

PS31 = X1.sup – 40% of DB3 + (Sign3) RN3

PS31 = 3 -2 - 41 = - 40

Site1 broadcasts 20 to Site2 and Site3, Site2 broadcasts 39 to Site1 and Site3, and Site3 broadcasts -40 to Site1 and Site2. TotalPSij are computed at all sites.

TotalPS11 = PS11 + PS21 + PS31 =20 +(- 39 -40)

= -59

TotalPS21 = PS21 + (PS11 + PS31) = - 39 + (20 -40)

= -59

TotalPS31 = PS31 + (PS11 + PS21) = -40 + (20 - 39)

= -59

TP receives -59 as total support of an item set X1 from three sites which ensures the computations performed by all sites is correct. TP then calculates Global Excess Support (GES1) by subtracting SignSumRN from TotalPS11.

GES1= TotalPS11 - SignSumRN

= -59 - (-60) = 1

The value of GES1 is 1 which is greater than or equal to 0, so (A3,A5) is declared as globally frequent by TP and actual support(AS1) of X1 is computed by adding minimum support of the total database to GES1.

AS1 = GES1 + MinSup * |DB| = 1 + 6 = 7 where |DB| = 15.

Hence, the global frequent item set (A3,A5) support is 7.

Let us find whether the item set X2 is globally frequent or not. Partial support for X2 at three sites are computed as follows.

At Site1

PS12 = X2.Sup – 40% of DB1 +(Sign1) RN1

= 1 – 2 + 20 = 19

At Site2

PS22 = X2 .sup – 40% of DB2 +(Sign2) RN2

= 2 - 2 - 39 = -39

At Site3

PS32 = X2.sup – 40% of DB3 + (Sign3) RN3

= 2 -2 - 41 = -41

Site1 broadcasts 19 to Site2 and Site3, Site2 broadcasts 39 to Site1 and Site3, and Site3 broadcasts -41 to Site1 and Site2. TotalPSi2 are computed at all sites and as follows

TotalPS12 = PS12 + PS22 + PS32 =19 +(- 39 -41)

= - 61

TotalPS12 = TotalPS22 = TotalPS32 = - 61

Each site sends its computed TotalPSi2 (total support of X2) to TP. TP then finds GES2.

GES2 = TotalPS12 - SignSumRN

= 59 - (-60)

= -1

The value of GES2 is -1 which is lower than zero, so (A3, A4, A5) is declared as globally infrequent by TP even though it is frequent at Site2 and Site3. The above procedure is repeated for all the item sets in the merged

list to find whether they are globally frequent or not. Finally TP prepares a list which consists of global frequent item sets and their support values, TP then broadcast this list to three sites. This information is given in the following table.

TABLE III GLOBAL FREQUENT ITEM SETS AND SUPPORTS

Item Set	Sup	Item Set	Sup	Item Set	Sup
A_1	11	(A_1,A_2)	6	(A_4,A_5)	9
A_2	8	(A_1,A_4)	9	(A_3,A_4)	7
A_3	9	(A_3,A_5)	7	(A_1,A_4,A_5)	6
A_4	12	(A_1,A_5)	8		
A_5	12	(A_2,A_5)	7		

Even though the merged list consists of 25 item sets only 13 item sets are globally frequent. Each site can generate global association rules for each global frequent item set based on the specified minimum confidence threshold. The following computations illustrates that how a rule can be declared as strong or weak rule based on the user specified minimum confidence threshold value (65%).

For the item set (A1, A4, A5), the various rules that can be generated are {A1 → (A4, A5), A4 → (A1, A5), A5 → (A1, A4), (A1, A4) →A5, (A1, A5) →A4, (A4, A5) →A1}.

All these rules need not be strong rules. A rule can be declared as strong only when the confidence of the rule is greater than minimum confidence threshold value.

For the rule A1 → (A4, A5)

Confidence of this rule is

Sup (A1, A4, A5) / Sup(A1)

= 6/11 = 54%

The rule, A1 → (A4,A5) is a weak rule since rule's confidence is lower than minimum confidence value of 65%.

For the rule (A1, A4) → A5 Confidence of this rule is

Sup (A1, A4, A5) / Sup(A1, A4)

= 6/9 = 66%

Hence, (A1,A4) → A5 is a strong rule as its confidence is greater than minimum confidence.

For the rule (A4, A5) → A1 Confidence of this rule is

Sup (A1, A4, A5) / Sup(A4, A5)

= 6/9 = 66% M ≥ MinConf

Hence, (A4, A5) → A1 is a strong rule as its confidence is greater than minimum confidence

For the rule (A1, A5) → A4 Confidence of this rule is

Sup(A1, A4, A5) / sup(A1,A5)

= 6/8 = 75 %

The rule, (A1,A5) → A4 is a strong rule as its confidence is greater than minimum confidence.

V. PRIVACY PRESERVATION IN THE PROPOSED MODEL

A new model is proposed in this paper to find efficiently privacy preserving association rule mining in horizontally partitioned databases. The proposed model can be applied to any number of sites and for any number of transactions in the databases of the sites. Many tasks such as findings of locally frequent item sets, partial supports and total supports for each item set in the merged list are performed independently at different sites. Hence the computation time of the proposed model is less. The efficiency of the proposed method in terms of privacy and communication is discussed as follows.

Privacy is ensured by using encryption and decryption techniques at the time of transferring the frequent item sets from different sites to trusted party. From this, trusted party can know only local frequent item sets of each site but he does not know the supports of any item and cannot predict any thing related to sites database.

At the time of calculation of Partial Supports of an item set at each Sitei, MinSup * DBi is subtracted and the value of sign * random number is added to the supports of the item at that site. So Partial Supports are in disguised form and broadcast to the sites securely. Each site is not having any idea about the sign, random number which are assigned by trusted party to other sites

and the database size of other sites is also not known. So from the Partial Supports, no site can predict other sites data/information. In this way, partial supports of item sets can be broadcast to all other sites by preserving privacy of individual data. Hence, the sign based secure sum concept which is used in the computation of partial supports enhances the privacy.

Trusted party receives total partial support of each item set from all sites in order to find the global frequent item sets. By having these total supports, trusted party cannot find sites data/information since the database size of any site and local supports of any item at any site is not known by trusted party. Although trusted party assigned random numbers, signs to all sites and total database size is known, he cannot predict any site's private data.

Finally results that are global frequent item sets and their supports are broadcasted by trusted party to all sites. With these results, no site owner can predict local support of any global frequent item sets, as global frequent item sets may not be frequent in all sites and any site owner can not predict the contribution of other sites database which makes the item set globally frequent.

In distributed environment, the cost of communication is measured in terms of the number of communications for data transfer among all the sites and trusted party which are involved in the process of finding global association rules.

The efficiency of an algorithm is assessed in terms of the communication costs incurred during information exchange. The proposed model minimizes the number of data transfers by allowing the transfer of bulk of data at a time from one site to another site and trusted party to sites. For example each site sends local frequent item sets of their database in a single data transfer to trusted party and even the sites sends its partial support for each item to other sites in a single transfer instead of sending one item set's partial support in one transfer to other sites. Hence the proposed model needs less communications.

Trusted party also broadcast all the global frequent item sets for all sites in a single transfer. Hence the proposed model is more economy in terms of communication cost as it utilizes bulk data transfers.

The above discussion clearly specifies that the proposed model is efficient for finding global association rules by satisfying privacy constraints.

IV. CONCLUSIONS

The main threat in finding association rule mining in distributed database environment is privacy that is no site owner wish to provide database or local frequent item sets or support value to any one. However every owner wishes to access mined result by participating indirectly in the mining process by providing partial results in disguised form. The problem of preserving privacy in association rule mining when the database is distributed horizontally among n ($n > 2$) number of sites with a trusted party is considered. A model is proposed in this paper which adopts a sign based secure sum cryptography technique to find the global association rules without disclosing individual's private data/information. The trusted party initiates the process and prepares the merged list. All the sites computes the partial supports and total supports for all the item sets in the merged list using the sign based secure sum cryptography technique and based on these results finally trusted party finds global frequent item sets. The functionality of the proposed model is illustrated with an example. The performance of the proposed model in terms of privacy and communication is presented and it indicates that this model efficiently preserves the privacy of individual sites in the process of finding global frequent item sets and global association rules with minimum number of communications.

REFERENCES

[1] M tamer Ozsu Patrick Valduriez, Principles of Distributed Database Systems ,3rd Edition.

[2] R Agarwal, T Imielinski and A Swamy, Mining Association Rules between Sets of Items in Large Databases, Proceedings of the 1993 ACM SIGMOD International Conference on Management of Data, page 207-210, 1993.

[3] Verykios, V.S., Bertino, E., Nai Fovino, I., Parasiliti, L., Saygin, Y., and Theodoridis, Y. 2004. State-of-the-art in privacy preserving data mining. SIGMOD Record, 33(1):50–57.

[4] Y. Lindell and B. Pinkas, Secure Multiparty Computation for Privacy-Preserving Data Mining, The Journal of Privacy and Confidentiality (2009), 1, Number 1, pp. 59-98.

[5] Elisa Bertino , Igor Nai Fovino Loredana Parasiliti Provenza ,A Framework for Evaluating Privacy Preserving Data Mining Algorithms, Data Mining and Knowledge Discovery, 2005, 11, 121–154.

[6] M. Kantarcioglu and C. Clifto. Privacy-preserving distributed mining of association rules on horizontally partitioned data. In IEEETransactions on Knowledge and Data Engineering Journal, volume 16(9), pages 1026–1037.

[7] Chin-Chen Chang, Jieh-Shan Yeh, and Yu-Chiang Li, Privacy- Preserving Mining of Association Rules on DistributedDatabases, IJCSNS International Journal of Computer Science and Network Security, VOL.6 No.11, November 2006.

[8] Mahmoud Hussein, Ashraf El-Sisi,and Nabil Ismail, Fast Cryptographic Privacy Preserving Association Rules Mining on Distributed Homogenous Data Base, I. Lovrek, R.J. Howlett, and L.C. Jain (Eds.): KES 2008, Part II, LNAI 5178, pp. 607– 616, 2008.© Springer-Verlag Berlin Heidelberg 2008.

[9] Lalanthika Vasudevan , S.E. Deepa Sukanya, N. Aarthi ,Privacy Preserving Data Mining Using Cryptographic Role Based Access Control Approach, Proceedings of the International MultiConference of Engineers and Computer Scientists 2008 Vol I, IMECS 2008.

[10] Vaidya, J. and Clifton, C. 2002. Privacy preserving association rule mining in vertically partitioned data, 8th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, ACM Press, pp. 639–644.

[11] A.C. Yao. Protocols for secure computations. In Proceedings of the 23rd Annual IEEE Symposium on Foundations of Computer Science, 1982

AUTHOR BIOGRAPHY

P. Sowjanya, Student of M.Tech, Global College Of Engineering and Technology, Kadapa, Andhra Pradesh, India. **Email:** sowji.gcet@gmail.com

B. Venkatesh, Assistant Professor Department of CSE, Global College Of Engineering and Technology, Kadapa, Andhra Pradesh, India.