ISSN No. 0976-5697

Volume 7, No. 4, July-August 2016

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

SWARM OPTIMIZER BASED ON THE SENSITIVE RULE HIDING WITH THE CONSTRAINTS MINIMIZATION FOR THE DATA PUBLISHING

P.Tamil Selvan
Research Scholar
Department of Computer Science
Karpagam University,Coimbatore, India

Dr.S.Veni
Research Supervisor
Department of Computer Science
Karpagam University.Coimbatore ,India

Abstract: Recently, motivating the demand for the privacy and secure data mining research is the expansion of techniques that include the privacy and security along with the effective data publishing. Most of the research work is developed for the data distribution with the privacy. However, the protocols used in the homomorphic encryption which increased the computational costs and communication. In order to overcome the limitations, a Swarm optimization and Iterative Privacy Rule Preservation (SIPRP) method is designed in the paper to improve the efficiency of the privacy preserving association rule mining with the constraint minimization. Initially, SIPRP method generates the association rules for the privacy preserving distribution database based on the support and confidence threshold. Then, the sensitive rules associated with the optimal sensitive items which are hidden are evaluated. After that, the sensitive rules are subjected to the Particle Swarm Optimization (PSO) for hiding and preserving highly confidential privacy rules. The constraints arise on preserving the high confidential privacy rules which are minimized by the iterative generation rules for the different sensitive sets of items. Finally, the SIPRP method obtains the sensitive sets of items for generating the specific sensitive. It is hidden with the less effect on the privacy being exposed during the data distribution across the multiple users. The Proposed SIPRP method uses adult data sets from the University of California's Irvine data repository for conducting the experimental work. Experimental evaluation of the SIPRP method is done with the performance metrics such as the number of sensitive rules, processing time, number of hidden rules, and the rate of privacy. Experimental analysis shows that the SIPRP method is able to improve the privacy rate by 10.5% and also increases the number of hidden rule generated by 26.5 % when compared to the state-of-the-art works.

Keywords: computational cost, association rule mining, sensitive item sets, sensitive rules, principle component analysis

I. INTRODUCTION

Most of the research work is developed in the Privacy Preserving Data Mining (PPDM) for hiding the private, confidential, or secure information. Protocol to the secure mining of the association rule was developed in [1] for providing the secured mining association rules using two secure multi-party algorithms. However, the method increased the computational costs. Corporate privacy preserving framework was designed in [2] that introduced an Encrypt/Decrypt (E/D) module to change the client data before it delivered to the server and improves the true patterns with their correct support. However, E/D module assumes that the attacker does not possess knowledge on the hiding aspect and relaxation may break the vulnerabilities encryption scheme and bring privacy. It is ambiguous in providing the corporate privacy preserving association rule mining.

Homomorphic matching technique was introduced in [3] the privacy preservation for improving the privacy level. The secrecy views and null based virtual updates was illustrated [4] for achieving data privacy for reducing the computation cost. The Direct and indirect discrimination was performed [5] using the legitimate classification rules while preserving data quality which results in the improved privacy level at the cost of accuracy.

A privacy preserving mining scheme was presented [6] for achieving privacy and scalability in a large scale. Efficient clustering was designed [7] with the aim of improving the computational performance and reducing the computational cost through the Fractional Calculus. Hierarchical K-Means Clustering [8] was applied on the horizontally partitioned data with the objective to improve the communication cost.

A heuristic algorithm was introduced [9] for enhancing the privacy sensitive knowledge as the item sets avoid more inference channels. The method does not provide better privacy rate. The architecture of the SensorSafe is a software-based framework, which was designed [10] to permit privacy-aware data sharing. It preserves both the provider privacy and consumer utility. A practical data publishing method was introduced [11] for producing masked version of data that protects the individual privacy and the information usefulness for the cluster analysis.

In [12], a simple Anonymization technique is presented using sub-clustering to achieve the privacy and high data utility with less execution time. The method is not appropriate for data streams. A novel heuristic algorithm was developed [13] to hide from the view and a set of sensitive association rules that using the distortion technique reduces the side effects. The Privacy preserving data mining methods for hiding fuzzy association rules [14] was designed for balancing the level of privacy.

Hiding-missing-artificial utility (HMAU) algorithm was introduced [15] for hiding sensitive sets of items in the data sanitization process by reducing the side effects. A Compact prelarge GA-based (cpGA2DT) algorithm was illustrated [16] for hiding sensitive sets of items that minimize the side effects of PPDM. Data Privacy Preservation using different Perturbation Techniques was developed [17] to provide higher privacy and also the data utility. The survey of the different privacy preservation techniques using the association rule hiding to achieve

minimal side effects with higher data utility was presented in [18]. A novel noise addition techniques was designed in [19] for protecting individual privacy.

In the paper, Swarm optimization and Iterative Privacy Rule Preservation (SIPRP) method is designed for enhancing the efficiency of the privacy preserving association rule mining with constraint minimization. In SIPRP method, sensitive rules are subjected to the Particle Swarm Optimization (PSO) for hiding and preserving highly confidential privacy rules. The SIPRP method hides the sensitive rules with aiming at the privacy preserving distribution database.

The paper is designed with five sections The Section 2 describes the design of the SIPRP method using Particle Swarm Optimization technique for hiding the sensitive rules. The section 3 introduces the different experimental setting which is studied in the work. The section 4 presents the experimental results and discusses their significance. Finally, the paper concludes in the section 5.

II. DESIGN OF SWARM OPTIMIZATION AND ITERATIVE PRIVACY RULE PRESERVATION (SIPRP) METHOD

The design of Swarm optimization and Iterative Privacy Rule Preservation (SIPRP) method is described in a detail manner this section. The main goal of the SIPRP method is to hide the sensitive rules form the public aiming at improving the privacy rate. Initially, the SIPRP method generates the association rule based on their support and confidence threshold. The sensitive rules associated with the optimal sensitive item is hidden and then they are estimated for hiding sensitive rules.SIPRP method hides the sensitive rules using the Particle Swarm Optimization (PSO) mechanism with the objective of preserving highly confidential privacy rules. The SIPRP method reduces the constraints occur while preserving the high confidential privacy rules through the iterative generations rules for diverse sensitive sets of items. Finally, the SIPRP method ensures the sensitive rules to be hided with less effect on the privacy which is exposed during the data distribution across multiple users. The architecture diagram of the SIPRP method for hiding sensitive rule is shown in the below Figure 1.

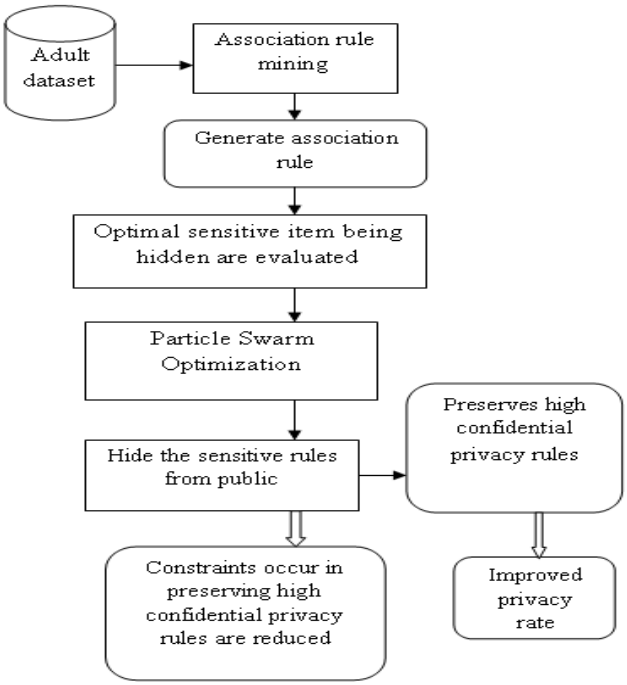

Figure 1 Architecture diagram of SIPRP technique for sensitive rule hiding

As shown in Figure 1, SIPRP method initially takes the adult data set as an input, then applies the association rule mining for generating the association rule based on the support and confidence value. After generating the association rule, sensitive rule related with the optimal sensitive item is concealed and evaluated with the objective for improving the privacy rate. Next, the SIPRP method hides the sensitive rules form the public with the help of particle swarm optimization. The PSO mechanism preserves the high confidential privacy rules for reducing the constraints occur which in turn improves the privacy rate of sensitive rules.

A. *Association rule mining for generating sensitive rules*

SIPRP method generates the sensitive rules with the association rule mining technique. The Association rule mining technique in the SIPRP method protects the sensitive data items by hiding the sensitive rules from the data miners and discloses all the non-sensitive rules to the public. The Association rule mining technique generates the association rule based on the support and confidence threshold value and then evaluation is made. The sensitive rules associated with the optimal sensitive items are hidden to preserve the privacy rate. The task of Association rule mining technique in the SIPRP method is illustrated in the below Figure 2.

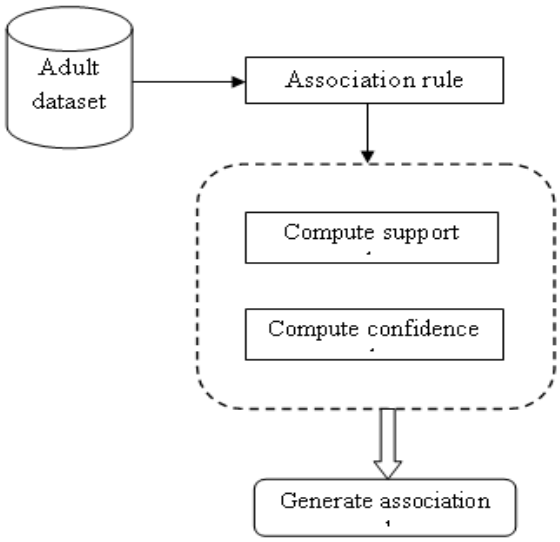

Figure 2 task of Association rule mining technique in SIPRP method

After performing the association rule, the SIPRP method calculates the sensitive rules associated with the optimal sensitive items. It is hidden for providing high confidential privacy rules.

Let us Consider, 'D' is a Database that consists a set of transactions $D = \{T1, T2, \dots, Tn\}$ and each transaction contains a set of items $I = \{I1, I2, \dots, Im\}$. The Association Rule Mining technique recognizes all association rules $X \Rightarrow Y$ with a minimum support and confidence value. The support value of an item $X \in I$ in the database D is the count of transactions contains X and represented as $Sup\ count(X)$. Support value of X is denoted as $Sup(X)$ which is mathematically formulated as,

$$Sup(X) = \frac{Sup\ count(X)}{n} * 100 \ \dots\dots\dots (1)$$

From (1), n is the number if transaction is D. Item set X is termed as a frequent item set when it satisfies the following condition

$$Sup\ (X) > SUPmin \ \dots\dots\dots (2)$$

Where $SUPmin$ indicates the Minimum Support Threshold (i.e. predefined threshold). The Confidence measure for rule $X \rightarrow Y$ in dataset D is mathematically formulated as below,

$$Confidence(X \rightarrow Y) = \frac{Sup(XY*100)}{Sup(X)} \ \dots\dots\dots (3)$$

SIPRP method using the rule generation algorithm for generating the association rule is the algorithmic process is described as follows,

Input: Database 'D', set of items '$I = \{I1, I2, \dots, Im\}$', Support Value: $Sup(X)$, Confidence Threshold Value: $Confidence(X \rightarrow Y)$
Output: generate sensitive rules
Step 1: **Begin** Step 2: **For** each Database 'D' Step 3: **For** each Items 'X Step 4: measure the support value using (1) Step 5: measure confidence value using (3) Step 6:generate the association rule based on support and confidence threshold value Step 7 **End for** Step 9: **End for** Step 10: **End**

Figure 3 Rule Generation algorithm for generating sensitive rule

As shown in the Figure 3, the rule generation algorithm initially measures the support and confidence value in each item and the database. And then generates the sensitive rules based on the support and confidence values evaluated. After that, SIPRP method evaluates the sensitive rule associated with the optimal sensitive item being concealed to hide the sensitive rules.

B. *Particle Swarm Optimization for hiding the sensitive rules*

SIPRP method used Particle Swarm Optimization (PSO) mechanism to hide the sensitive rules from the data miners with the objective of improving the privacy rate. In SIPRP method, PSO mechanism obtains the highly confidential privacy rules based on the two primary operations such as 'Velocity update' and 'Position update'. SIPRP method hides the sensitive rules form the public during the data distribution with the help of PSO mechanism.

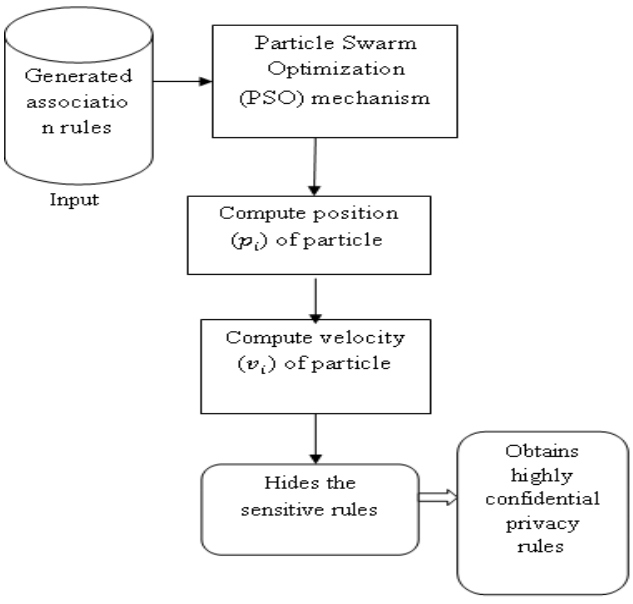

Figure 4 Sensitive Rule Hiding using the Particle Swarm Optimization

As shown in the Figure 4, Initially Particle Swarm Optimization mechanism takes the Generated associated rules in the input. Then, the PSO mechanism computes the position and velocity of the each particle with the aim of hiding the sensitive rules from the public. Based on the computed position and velocity, the PSO mechanism significantly hides the sensitive rules which result in preserving the highly confidential rule and enhancing the privacy rate.

Each particle in the PSO mechanism has a 'position' and a 'velocity' where position is represented as a solution suggested by the particle. Velocity is the rate of changes in the next position with respect to the current position. The position and velocity values are randomly initialized in the SIPRP method. PSO mechanism contains collection of random particles. During the each iteration, all particles are updated by using $pbest$ and $gbest$ values. $pbest$ refers the best solution it has attained so far. Another best value is the $gbest$ so far acquired with any particle in the population. After that, the particle updates its velocity using the below equation,

$$v_i = v_i + c1 * rand() * (pbest[] - p_i) + c2 * rand() * (gbest[] - p_i) \ldots (4)$$

For each iteration, the particle updates its position using the following equation

$$p_i = p_i + v_i \ \ldots\ldots\ldots (5)$$

From (4), (5), i represents a particles number i.e.$i = 1, .., N$, whereas N refers the number of particles in the swarm. v_i indicates the particle velocity, p_i is the position of current particle and rand () refers a random number between (0, 1). c1, c2 are the learning factors generally which are assigned as c1 = c2 = 2.

For each particle, Fitness function is determined by considering the each transaction as a particle which mathematically formulated as,

$$f(tran_i) = \sum_{j=1}^{m} \left(\frac{tran_i(A_j)}{sup(A_j)} \right) \ldots\ldots\ldots\ldots (6)$$

Where $sup(A_j) = \sum_{i=1}^{n} tran_i(A_j)$ …… (7)

From eqn (6), (7), m refers the number of attributes, n is the number of transactions, $f(tran_i)$ fitness for a transaction $tran_i$ whereas $sup(A_j)$ is a support of attribute A_j.The PSO algorithm for hiding the sensitive rule is described as:

// PSO algorithm for hiding sensitive rules
Input: Sensitive rules identified and the corresponding attributes involved in the rules
Begin
Initialize particle with the random position and velocities
Do
For each particle
Calculate the fitness value using (6)
If the fitness value is better than the best fitness value ($pBest$)
set current value as the new $pBest$
End for
Choose the particle with the best fitness value of all the particles as the $gBest$
For each particle
Calculate the particle velocity using (4)
Update particle position using (5)
End for
While maximum iterations or minimum error criteria is not attained
End while
End
Output: obtains highly confidential privacy rules

Figure 5 PSO algorithm for hiding the sensitive rules

Form the Figure 5, the PSO algorithm initially takes the Sensitive rules generated as input. Then, PSO algorithm computes the fitness function in each particle by means of considering the each transaction as a particle. After that, PSO algorithm computes the velocity and position of particle, then update the position of particle using the equation (5). Based on the updated position value, SIPRP method hides the sensitive rule which results in improved privacy rate and reduced constraints occur.

III. EXPERIMENTAL SETTING

The Swarm optimization and Iterative Privacy Rule Preservation (SIPRP) method is developed to improve the efficiency of privacy preserving the association rule mining with the constraint minimization. SIPRP method is implemented using the java language. The SIPRP method uses the Adult data set from the University of California Irvine data repository which contains the information about the individuals such as age, level of education and current employment type.

The adult dataset consists of forty nine thousand records and also binomial label that represents the salary of less or greater than fifty thousand US dollars, referred to as <50K or >50K in SIPRP method. The adult dataset has been divided into a training dataset and test dataset for conducting the experimental work. Training dataset comprises of thirty two thousand records and a test dataset comprises of sixteen thousand records. There are fourteen attributes consisting of seven polynomials, one binomial and six continuous attributes and are used in the SIPRP method to preserve the privacy of certain attributes including the salary, relationship and marital status. The employment class attribute denotes the employer type (i.e. self employed or federal) and occupation refers to the employment type (i.e. farming or managerial). The education attribute include of

high school graduate or doctorate. The relationship attribute includes the information related to unmarried or married.

The final nominal attributes are country of residence, gender and race. The continuous attributes are age, hours worked per week, education number, capital gain and loss and a survey weight attribute assigned to an individual depends on the information such as area of residence and type of employment. The performance of the SIPRP method is evaluated with the metrics such as number of sensitive rules, processing time, number of hidden rules, rate of privacy.

IV. DISCUSSION

In this section, the result analysis of SIPRP method is evaluated. The performance of SIPRP method is compared with the exiting two methods namely, protocol for secure mining of association rule [1], corporate privacy-preserving framework [2]. The performance of TFVODT framework is evaluated along with the following metrics.

A. Impact of number of sensitive rules

In SIPRP method, the number of sensitive rule describes the ratio in the number of association rules generated to the given set of items which measured in terms of percentage (%) and mathematically formulated as,

$$\text{Number of sensitive rule} = \frac{\text{number of association rule generated}}{\text{set of items}} * 100 \ldots\ldots (8)$$

When higher the number of association rule generated, the method is said to be more efficient.

Table 1 Tabulation for the Number of sensitive rule

Number of items	Number of sensitive rules (%)		
	SIPRP method	protocol for securing the mining of association rule	corporate privacy-preserving framework
1	76	61	54
2	79	64	57
3	82	67	60
4	85	70	63
5	88	73	67
6	91	76	70
7	93	79	73

Table 1 represents the ratio in the number of sensitive rule generated with respect to the different number of items and the comparison is made with the two existing methods, namely protocol for secure mining of association rule [1], corporate privacy-preserving framework [2]. From the table value, it is clear that the proposed SIPRP method increases the number of sensitive rule generated than the other state-of-art methods.

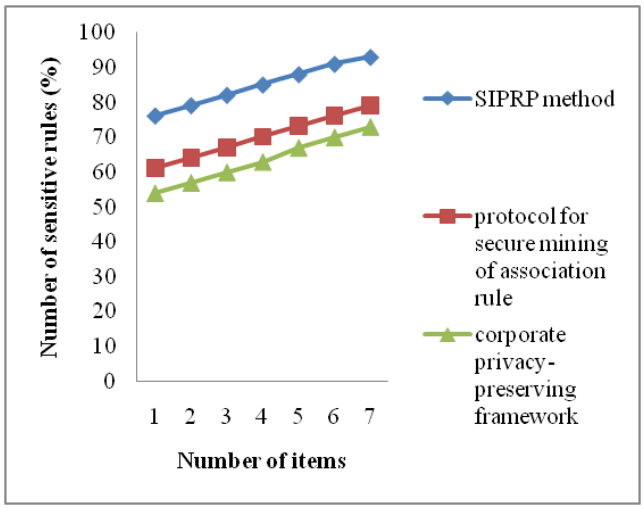

Figure 6 Measure of the Number of sensitive rules

Figure 6 shows the impact of the number of sensitive rule generated with respect to varying number of items in the range of 1 to 7 using the SIPRP method, protocol for secure mining of the association rule [1], corporate privacy-preserving framework [2]. As illustrated in the Figure, the proposed SIPRP method performs relatively well when compared to the two other existing methods. This is because of the application of the Association rule mining technique in SIPRP method that generates the association rule based on their support and confidence threshold value. Then, SIPRP method evaluates the sensitive rules associated with the optimal sensitive items being hidden for preserving the privacy rate. Therefore, the number of sensitive rule generated using the SIPRP method is improved by 18% as compared to the protocol for securing the mining of association rule [1] and 25% as compared to the corporate privacy-preserving framework [2] respectively.

B. Impact of the number of hidden rules

In SIPRP method, number of hidden rules is defined as the ratio in number of sensitive rules hidden without any side effects to the total number of sensitive rules given which are mathematically formulated as,

$$\text{Number of the hidden rules} = \frac{\text{number of sensitive rules hidden without any side effects}}{\text{total number of sensitive rules}} * 100 \ldots\ldots (9)$$

The number of hidden rules is measured in the term of percentage (%). When the numbers of hidden rules are higher, the method is said to be more efficient.

Table 2 Tabulation for the Number of hidden rules

Number of sensitive rules	Number of hidden rules (%)		
	SIPRP method	protocol for securing the mining of association rule	corporate privacy-preserving framework
10	71	57	44
20	73	59	46
30	75	61	48

40	77	63	50
50	79	65	52
60	81	67	54
70	83	69	56

The number of hidden rules using the SIPRP method is elaborated in the table 2. We consider the framework with the different number of sensitive rules in the range of 10 to 70 for the experimental purpose using the java language. The performance of the proposed SIPRP method is compared with the existing two methods namely, protocol for secure mining of association rule [1], corporate privacy-preserving framework [2]

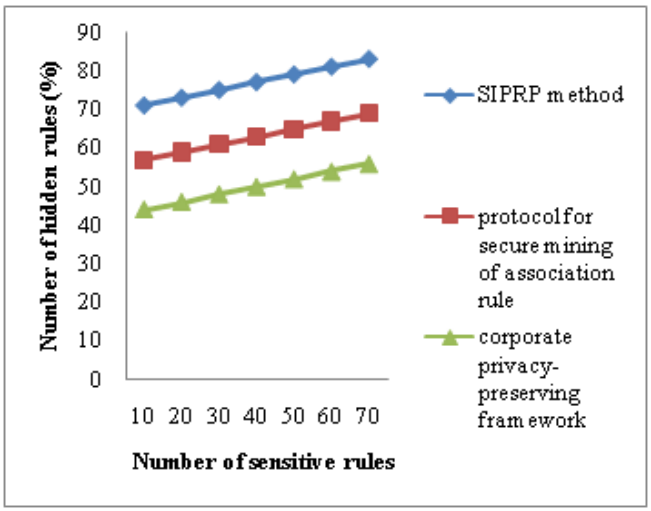

Figure 7 Measuring the Number of hidden rules

Figure 7 demonstrates the Number of hidden rules versus different number of sensitive rule input using the three different methods. As illustrated in the Figure, the proposed SIPRP method performs well when compared to the two other methods protocol to secure the mining of association rule [1], corporate privacy-preserving framework [2]. This is because of the application of the Particle Swarm Optimization mechanism in the SIPRP method. With the help of PSO mechanism, SIPRP method computes the position and velocity of each particle with the aim of hiding the sensitive rules from the public. Based on the computed value such as position and velocity, SIPRP method significantly hides the sensitive rules from the public. As a result, Number of hidden rules using SIPRP method is improved by 18% as compared to the protocol for secure mining of association rule [1] and 35% as compared to corporate privacy-preserving framework [2] respectively.

C. Impact of processing time

In SIPRP method, the processing time is described as the amount of time taken to hide the sensitive rules from the public with minimum side effects. Processing time is measured in the term of milliseconds (ms).When the time is lower for hiding the sensitive rule with minimum constraints, more efficient the method is said to be.

Table 3 Tabulation for the processing time

Number of sensitive rules	Processing time (ms)		
	SIPRP method	protocol for securing the mining of association rule	corporate privacy-preserving framework
10	13	19	23
20	25	31	35
30	35	43	47
40	47	55	58
50	59	67	71
60	71	79	83
70	83	91	95

To determine the performance of the SIPRP method, comparison is made with two other existing methods protocol to secure mining of the association rule and [1], corporate privacy-preserving framework [2]. Table 3 represents the time taken for hiding the sensitive rules with minimum side effects. From the table, it is illustrative that the processing time using the proposed SIPRP method is reduced when compared with the existing methods.

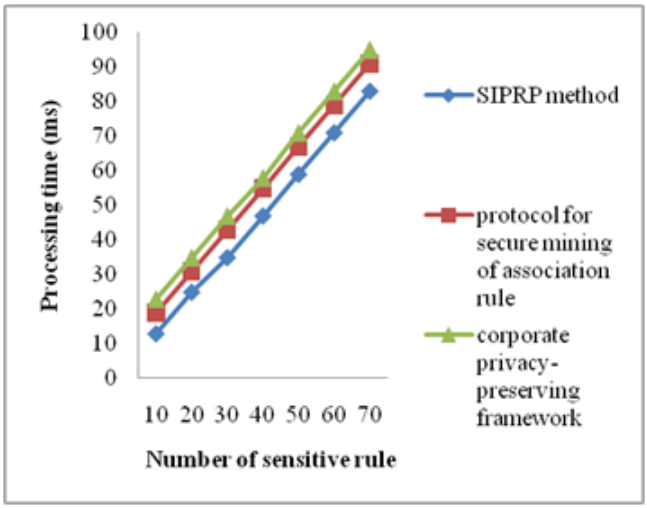

Figure 8 Measure of processing time

Figure 8 illustrates the impact of the processing time with respect to the different sensitive rule in the range of 10 to 70. As illustrated in the Figure, the proposed SIPRP method mechanism consumes minimum time for hiding sensitive rules when compared with the other two methods, the protocol to secure mining of association rule [1], corporate privacy-preserving framework [2]. It is because the application of the association rule mining and the PSO mechanisms in the SIPRP method efficiently hides the sensitive rules without any side effects with less processing time and preserves the high confidential privacy rule. Therefore, the processing time for hiding sensitive rules using the SIPRP method is reduced by 21% as compared to the protocol to secure mining of the association rule [1] and 32% as compared to the corporate privacy-preserving framework [2] respectively.

D. Impact of privacy rate

The privacy rate using the SIPRP method is defined as the rate at which the sensitive rule is privately

transacted to the corresponding user without showing to the public user. The privacy rate is measured in the terms of percentage (%).

Table 4 Tabulation for Privacy rate

Number of sensitive rules	Privacy rate (%)		
	SIPRP method	Protocol for securing the mining of association rule	Corporate privacy-preserving framework
10	82	76	64
20	84	78	66
30	83	77	65
40	86	80	68
50	88	82	70
60	90	84	72
70	92	86	74

The privacy rate for preserving highly confidential rule using the SIPRP method is elaborated in the table 4 and comparison is made with the other two methods [1], [2] respectively. It is consider that the method with the different sensitive rules in the range of 10-70 for the experimental purpose using the java language. From the table value, it is clear that the proposed the SIPRP method improves the privacy rate for preserving highly confidential sensitive rule than the other state-of-art methods.

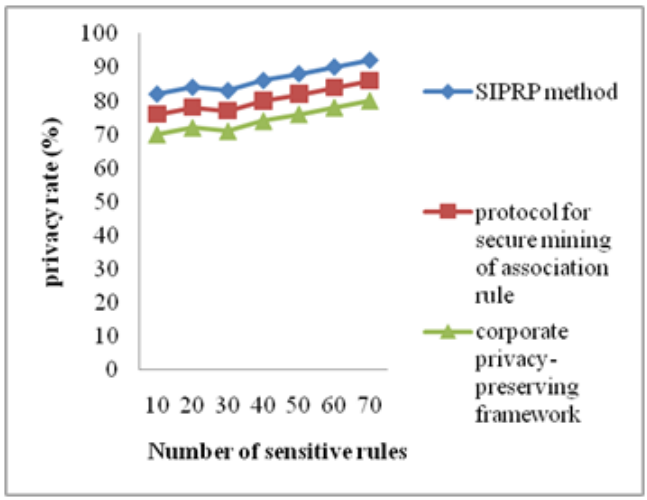

Figure 9 Measure of Privacy rate

The Figure 9 presents the privacy rate for preserving highly confidential rule using the SIPRP method with respect to the different sensitive rule in the range of 10 to 70. As illustrated in the Figure, the proposed SIPRP method mechanism provides higher privacy rate when compared with the other two methods, protocol to secure mining of association rule [1], corporate privacy-preserving framework [2]. It is because the application of the PSO mechanisms in the SIPRP method significantly hides the sensitive rules from the public with minimum constraints and preserves the high confidential privacy rule. Therefore, privacy rate for hiding sensitive rules using the SIPRP method is improved by 7% as compared with the protocol to secure mining of association rule [1] and 14% as compared to corporate privacy-preserving framework [2] respectively.

V. CONCLUSION

In the paper, an effective novel framework is designed. It is called as Swarm optimization and Iterative Privacy Rule Preservation (SIPRP) method. SIPRP method is developed to improve the efficiency of the privacy preserving association rule mining with the constraint minimization. The SIPRP method improves the privacy preservation for the distributed data mining and significantly hides the sensitive rules from the public using the PSO mechanism. SIPRP method preserves the highly confidential privacy rules by means of hiding the sensitive rules which in turn improves the privacy rate. Proposed SIPRP method reduces the constraints arise in preserving the high confidential privacy rules through the iterative generations of the rules for different sensitive sets of items. Experimental evaluation of SIPRP method is conducted with the Adult Data Set extracted from the UCI repository to provide the high quality privacy preservation of sensitive rules which significantly contributes to the relevance The experiments conducted for the SIPRP method, it is observed that, the number of hidden rules generated for the different item set provides the more accurate results as compared to the existing methods. The results show that the SIPRP method provides the better performance with an improvement of privacy rate by 10.5% and improvement of number of hidden rules generated by 26.5 % when compared to the state of the art works.

VI. REFERENCES

[1] Tamir Tassa, "Secure Mining of Association Rules in Horizontally Distributed Databases", IEEE Transactions on Knowledge and Data Engineering, Vol. 26, No. 4, APRIL 2014

[2] 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

[3] Dimitrios Karapiperis and Vassilios S. Verykios, "An LSH-Based Blocking Approach with a Homomorphic Matching Technique for Privacy-Preserving Record Linkage", IEEE Transactions on Knowledge and Data Engineering, Volume 27, Issue 4, April 2015, Pages 909-921.

[4] Leopoldo Bertossi and Lechen Li, "Achieving Data Privacy through Secrecy Views and Null-Based Virtual Updates", IEEE Transactions on Knowledge and Data Engineering, Volume 25, Issue 5, May 2013, Pages 987-1000.

[5] Sara Hajian and Josep Domingo-Ferrer, "A Methodology for Direct and Indirect Discrimination Prevention in Data Mining", IEEE Transactions on Knowledge and Data Engineering, Volume 25, Issue 7, July 2013, Pages 1445-1459.

[6] Fosca Giannotti, Laks V. S. Lakshmanan, Anna Monreale, DiIssue Pedreschi and Hui (Wendy) Wang, "Privacy-Preserving Mining of Association Rules From Outsourced Transaction Databases", IEEE Systems Journal, Volume 7, Issue 3, September 2013, Pages 385-395.

[7] Pawan R. Bhaladhare and Devesh C. Jinwala, "A Clustering Approach for the □-Diversity Model in Privacy Preserving Data Mining Using Fractional Calculus-Bacterial Foraging Optimization Algorithm", Advances in Computer Engineering, September 2014 , Pages 1-13.

[8] Anrong Xue, Dongjie Jiang, Shiguang Ju, Weihe Chen, and Handa Ma , "Privacy-Preserving Hierarchical-k-means Clustering on Horizontally Partitioned Data", International

Journal of Distributed Sensor Networks, Volume 5, Issue 1, 2009, Pages 81 – 82.

[9] Arpit Agrawal, "Security based Efficient Privacy Preserving Data Mining", International Journal of Application or Innovation in Engineering & Management (IJAIEM), Volume 2, Issue 7, July 2013

[10] Supriyo Chakraborty, Zainul Charbiwala , Haksoo Choi , Kasturi Rangan Raghavan , Mani B. Srivastava, "Balancing behavioral privacy and information utility in sensory data flows", Pervasive and Mobile Computing, Elsevier journal, Vol. 8, No. 3, , Pages 331–345, June 2012

[11] Benjamin C.M. Funga, Ke Wangb, Lingyu Wanga, Patrick C.K. Hungc, "Privacy-preserving data publishing for cluster analysis", Data & Knowledge Engineering, Elsevier journal, Vol. 68, No. 6, Pages 552–575, June 2009

[12] V. Rajalakshmi, G. S. Anandha Mala, "Anonymization by Data Relocation using Sub-clustering for Privacy Preserving Data Mining", Indian Journal of Science and Technology, Vol. 7(7), pp. 975-980, July 2014

[13] Maulesh R. Chhatrapati , Shilpa Sherasiya ," Privacy Preserving Data Mining Using Heuristic Approach " ,International Journal for Innovative Research in Science & Technology, Volume 1 , Issue 10 , 2349-6010, March 2015

[14] K. SATHIYAPRIYA , G. SUDHASADASIVAM , C. J. P. SUGANYA ," Hiding Sensitive Fuzzy Association Rules Using Weighted Item Grouping and Rank Based Correlated Rule Hiding Algorithm ",Wseas Transactions On Computers , Volume 13, 2014

[15] Chun-Wei Lin, Tzung-Pei Hong, and Hung-Chuan Hsu, "Reducing Side Effects of Hiding Sensitive Itemsets in Privacy Preserving Data Mining", Hindawi Publishing Corporation, The Scientific World Journal, Vol. 2014, Article ID 235837, 12 pages

[16] Chun-Wei Lin, Binbin Zhang, Kuo-Tung Yang, and Tzung-Pei Hong, "Efficiently Hiding Sensitive Itemsets with Transaction Deletion Based on Genetic Algorithms" Hindawi Publishing Corporation, The Scientific World Journal, Vol. 2014, Article ID 398269, 13 pages

[17] Kavitha S, Raja vadhana P, "Data Privacy Preservation Using Various Perturbation Techniques", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 3, Issue 2, February 2015

[18] Gayathiri P, B Poorna, "Association Rule Hiding Techniques for Privacy Preserving Data Mining: A Study", International Journal of Advanced Computer Science and Applications (IJACSA), Vol. 6, No. 12, 2015

[19] Md Zahidul Islama, Ljiljana Brankovicb**, "**Privacy preserving data mining: A noise addition framework using a novel clustering technique, Knowledge-Based Systems, Elsevier journal, Volume 24, Issue 8, December 2011, Pages 1214–1223

Tamil Selvan P. completed his M.Phil in Computer Science from Karpagam University in 2009. He is working as Assistant Professor in Department of Computer Science, Karpagam University, Coimbatore. His experience is 7 yrs. He has presented a paper in International Conference. His research interests are Data mining and warehousing.

Dr.S.Veni completed her Ph.D in Computer Science from Bharathiar University in 2014. she is working as Associate Professor in Department of Computer Science, Karpagam University, Coimbatore. Her experience is 12 yrs. she has presented various papers in National and International Conference. Her research interests are Computer Networks.