CHAPTER 6

REINFORCED SOCIAL ANT AND DISCRETE SWARM OPTIMIZATION FOR
SENSITIVE ITEM AND RULE HIDING

6.1 INTRODUCTION

Privacy Preservation Data Mining (PPDM) is significant to preserve the secret information from the unauthorized access for effective data publishing. The privacy preservation is very useful to hide the sensitive information with minimal side effects from the original database. Privacy preservation of data publishing preserves the privacy of individual in database while hiding the sensitive items without the disclosure of sensitive data. But the PPDM ensures the sensitive information and rule is not identified. Therefore, hiding the sensitive items and rules are required to be addressed for improving the privacy preservation efficiency during the data publishing. The Swarm optimization and Iterative Privacy Rule Preservation (SIPRP) method was developed in the previous chapter to improve the efficiency of privacy preserving association rule mining with constraint minimization.

In recent years, with the objective of hiding the sensitive data and rule has been researched with difference persons. Multilevel trust in the privacy preserving data mining technique was designed to enable the perturbed copies of data without the possibility of accessing the information by third parties and hence ensuring the improved trust level. But, the security aspects using the multilevel trust in privacy preserving data mining method were not considered. In order to improve the security and privacy, the protocol for secure
mining of association rule was introduced with the aid of two secure multi-party algorithms in horizontally distributed databases. Though, the protocol provides lesser sensitivity rule to hide the data while preserving the privacy for data publishing.

An integrated framework called, the Reinforced Social Ant and Discrete Swarm Optimization (RSA-DSO) model is proposed to solve the multi-objective factors including data and rule hiding for the data publishing. In RSA-DSO model, the sensitive data items and sensitive rules is designed to preserve the privacy of transactional database and therefore ensuring the smooth data publishing. Initially, the Reinforced Social Ant model ensures the data hiding which is involved during the optimal sensitive data item occur only once. Next, the Discrete Swarm Optimization (DSO) model ensures the optimized rule hiding which resulting in improving the accuracy of privacy preservation during the data publishing. Therefore, the performance of the proposed, RSA-DSO model provides the security for preserving the privacy of data mining and thus attains the higher privacy preservation accuracy with the minimum optimal hiding time for data publishing.

6.2 REINFORCED SOCIAL ANT AND DISCRETE SWARM OPTIMIZATION (RSA-DSO) MODEL

An integrated reinforced social ant and discrete swarm optimization (RSA-DSO) model is implemented with the objective of hiding the sensitive data item and sensitive rules for data publishing. During the proposed RSA-DSO model, the convergence characteristics for data item hiding is strictly performed once and also achieved the data item hiding without any redundancy. In order to hide the efficient sensitive rules, the RSA-DSO model is obtained based on the performance of attaining the sigmoid function instead
of traditional support-confidence values. That helps to calculate the better solutions with the discrete database which resulting in optimize the sensitive rule for data publishing.

Tamir Tassa et al. (2014) intended the protocol for secure the mining of association rule in PPDM to improve the privacy and efficiency using two secure multi-party algorithms. The protocol provides the enhanced security and more efficient for data publishing during horizontally distributed databases. Although, the protocol contains minimum sensitivity rule to hide the data while preserving the privacy for data publishing.

In order to overcome such limitations, the proposed RSA-DSO model is introduced to solve the problem of hiding the sensitive data items and rules during the data publishing. For preserving the privacy of an individual or organization, the sensitive data items and sensitive rules are detected in the transactional database with the aim of providing the essential rules which in turns hiding the sensitive data items. In addition, the Reinforced Social Ant model for the sensitive data item hiding and Discrete Optimization model for sensitive rule hiding is designed using proposed RSA-DSO model which is discussed in the following section.

Rahat Ali Shah and Sohail Asghar (2014) described the genetic algorithm to hide the sensitive rules while implementing some modifications in the transaction database through which the sensitive items being measured. However, the privacy preservation genetic algorithm requires huge amount of time to hide the sensitive data item. Therefore, the proposed RSA-DSO model is established to minimize the time while hiding the sensitive data item using the reinforced social ant sensitive using when compared to the genetic algorithm.
6.2.1 Reinforced Social Ant Sensitive Data Item Hiding

The data hiding technique is called Reinforced Social Ant Sensitive (RSA-S) model which is designed to investigate lesser cost path while attaining the optimal path using proposed RSA-DSO model. That helps to identify the balance between the searching optimal sensitive item and given dataset for sensitive data hiding with minimum time interval in an efficient manner. With the help of RSA-DSO model, the figure 5.1 demonstrates the Reinforced Social Ant Sensitive Data Item Hiding model is given below.

As shown in the figure 6.1, the Reinforced Social Ant Sensitive (RSA-S) data item hiding involves two steps. Initially, the RSA-S method takes the transaction database (i.e. Adult dataset) as input. After performing the transaction database, the optimal frequent data and sensitive data identification is performed based on reinforcement model which resulting in hiding the sensitive data with better efficient.

Let us consider the database ‘$D$’ that is involved during the set of transactions $D = t_1, t_2, ..., t_n$ and set of items $I = i_1, i_2, ..., i_n$ for every transaction. The minimum support threshold value is referred as ‘$mint$’, where the support value of an items along with the frequent item in the database ‘$D$ ’ which is mathematically expressed as follows.
From the equations (6.1) and (6.2), the support value of an item is symbolized by \( \sup(i_p) \) and the frequent item indicates as \( \freq(i_p) \) respectively. Then the optimal (i.e. sensitive item) path using social ant is very essential to attain the convergent result of cooperation between ants (i.e. transactions) within the colony (i.e. database). Though, it is highly necessary that the traversal includes the sensitive data items more than once. Hence, the RSA-S method is introduced to detect the minimum cost involved during the sensitive data item and also extract the sensitive data item only once. With the design of RSA-S technique consists of two steps, the sensitive data item is obtained by means of hiding the sensitive data item and reinforcement learning technique.

Arpit Agrawal (2013) planned heuristic algorithm for increasing the privacy of sensitive data items in PPDM based on the privacy support threshold. Though, the sensitive items should not be hidden by using the heuristic algorithm. To address this problem, the proposed RSA-DSO model is designed to attain the better sensitive data and is being hided when compared to the heuristic algorithm.

Let us consider \( r(Cost_a, Cost_b) \) denotes the measure of cost which is performed with the sensitive data item from transaction \( T_a \) to \( T_b \). Followed by this, the total cost is required to accomplish \( n \) number of sensitive data item from different transactions \( t_1, t_2, ..., t_n \) respectively which is mathematically formulated as given below.
From the equation (6.3), the Reinforced Social Ant Sensitive algorithm is utilized to discover the optimal sensitive data from a given database ‘\(D\)’ of ‘\(n\)’ transaction with a local heuristic \(\beta_{pq} = \frac{1}{r} (p,q)\), and ‘\(\alpha\)’ indicates the mathematical representation for pheromone formation. After that, the probability that an item ‘\(k\)’ within the transaction ‘\(p\)’ present in ‘\(q\)’ is expressed as follows.

\[
\text{Prob}^k_{pq}(t) = \frac{[\beta_{pq}][\alpha_{pq}(t)]}{[\beta_{pn}][\alpha_{pn}(t)]}
\]  
(6.4)

From the equation (6.4), the shorter edges with large amount of pheromone (i.e. frequent data item) are selected by means of multiplying the pheromone on edge ‘\(p,q\)’ with the equivalent heuristic value ‘\(\beta(p,q)\)’. This is similar to reinforce model where the optimal frequent items are reinforced and identification of sensitive data hiding are being selected. Based on the obtained frequent data item, the sensitive data item is performed through ‘\(Dfactor\)’, which is mathematically written as follows.

\[
Dfactor = \left[ \frac{\text{Max} \left( \text{Sup}(i_p) \right) - \text{Min} \left( \text{Sup}(i_p) \right)}{1 - \text{Min} \left( \text{Sup}(i_p) \right)} \right] \cdot |\text{DI}|
\]  
(6.5)

From the equation (6.5), ‘\(Dfactor\)’ is represented as optimal sensitive data item which is measured based on the difference between maximum support count ‘\(\text{Max} \left( \text{Sup}(i_p) \right)\)’ and minimum support count ‘\(\text{Min} \left( \text{Sup}(i_p) \right)\)’ among every sensitive data items that helps to improve the privacy preservation efficiency. Figure 6.2 shows that
the algorithmic description of reinforcement model based sensitive data item using RSA-DSO model is given below.

| **Input** | Database ‘D’, Transaction \{t_1, t_2, ..., t_n\}, minimum support threshold ‘mint’, |
| **Output** | Optimized sensitive data hiding |

**Step 1:** Begin

**Step 2:** For each database ‘D’

**Step 3:** For every transaction ‘t_1, t_2, ..., t_n’

**Step 4:** Measure support count using (5.1)

**Step 5:** Measure frequent item using (5.2)

**Step 6:** Obtain sensitive data item using (5.5)

**Step 7:** End for

**Step 8:** End for

**Step 9:** End

**Figure 6.2 Reinforcement-based Sensitive Data hiding algorithm**

As shown in the figure 6.2, the reinforcement-based Sensitive Data Hiding algorithm is introduced to discover the optimal sensitive data to be hidden (with the probability take place the sensitive data item should be once) from the given database ‘D’ and for every transaction ‘t_1, t_2, ..., t_n’. Based on this, the support count is measured and then the optimal frequent items are obtained which resulting in improving the exact privacy preservation. After measuring the optimized frequent data items, the reinforcement model is evaluated to improve the identification of sensitive data items and data hiding using the ‘D_factor’ with in the minimum time.
6.2.2 Discrete Swarm Optimized Sensitive Rule Hiding

After performing the reinforcement-based sensitive data hiding, the Discrete Swarm Optimization (DSO) model is designed based on the performance of hiding the sensitive rule using RSA-DSO model. The Discrete Swarm Optimized Sensitive Rule Hiding technique is to combine the traditional Particle Swarm Optimization (PSO) model which aims to achieve the sigmoid function for identifying the sensitive rules. In order to attain the sensitive rules, DSO model detects the association rule to be hided for enhancing the privacy preservation accuracy among various users.

Peng Cheng et al. (2015) designed Evolutionary Multi-Objective (EMO) technique detects the suitable transaction dataset in which they hide the sensitive rules with minimal side effects. EMO utilize the fitness value of each individual to be evaluated with the help of support and confidence value while preserving the privacy. But, the accuracy to hide the sensitive rules using EMO method gets reduced. Hence, the RSA-DSO model is proposed to improve the accuracy while preserving the privacy rate when compared to EMO approach. Figure 6.3 demonstrates the flow chart of Discrete Swarm Optimization (DSO) model using RSA-DSO model is given below.
The above figure shows that the DSO model, the particles (i.e. transactions) indicates the problem solution where every particle has a velocity and iterative evolution method is performed. With the design of DSO model, each iteration’s and each particle is updated based on its personal best value ‘pbest’ and global best value ‘gbest’ by means
of fitness function for computing the association rule. At first, the ‘\( p_{\text{best}} \)’ value denotes the personal best solution of transactions with the help of fitness function so far. Next, the ‘\( g_{\text{best}} \)’ value represents the best solution between every ‘\( p_{\text{best}} \)’ values in the population (i.e. database). Therefore, the transactions and corresponding velocities are updated using ‘\( p_{\text{best}} \)’ and ‘\( p_{\text{best}} \)’ values in a database which is expressed as given below.

\[
V_a(n + a) = V_a(n) + p_{\text{cons}} \left( p_{\text{best}} - p_i(n) \right) + g_{\text{cons}} \left( g_{\text{best}} - p_i(n) \right)
\] (6.6)

From the equation (6.6), ‘\( V_a \)’ indicates the velocity of ‘\( a_{\text{th}} \)’ particle (i.e. transaction) in a population (i.e. database), where ‘\( p_{\text{cons}} \)’ and ‘\( g_{\text{cons}} \)’ are constants which is measured using personal best and global best solutions. Then the fitness function is subjected with the sum of ratio of the transaction based on the support of frequent item sets is given below.

\[
\text{Min} \ F(x) = [f_1(x), f_2(x), \ldots, f_n(x)], \quad \text{where} \ x = x_1, x_2, \ldots, x_n
\] (6.7)

From the equation (6.7), Function ‘\( F(x) \)’ symbolize the fitness function with ‘\( f_i(x) \)’ denotes the fitness value and ‘\( x \)’ represents the vector for ‘\( n \)’ decision variables. During the obtained ‘\( p_{\text{best}} \)’ and ‘\( g_{\text{best}} \)’ values, the DSO model evaluates the sensitive rules instead of using the traditional support and confidence factors by means of sigmoid function is formulated as given below.

\[
\text{Sig} \ V_{ab}(t + 1) = \frac{1}{1 + e^{-V_{ab}(t+1)}}
\] (6.8)

From the equation (6.8), ‘\( V_{ab}(t + 1) \)’ represents the velocity of ‘\( a_{\text{th}} \)’ and ‘\( b_{\text{th}} \)’ particle with respect to the time interval ‘\((t + 1)\)’. While the function gets updated (from equation 6.6), then the random number ‘\( \text{rnd} \)’ is lying between the ‘\( 0 \)’ and ‘\( 1 \)’. When the
random number is less than \( 'Sig V_{ab}^t(t + 1)' \), then the identified rule called sensitive rule. On the other hand, when the random number is greater than \( 'Sig V_{ab}^t(t + 1)' \), then the identified rule called not sensitive rule and the process repeats with another transactions during the database. As a result, the DSO model provides transactions and their corresponding velocities based on the random number which in turns improves the privacy preservation accuracy with better efficient.

R.J. Kuo et al. (2011) intended association rule mining technique for improving the accuracy and automatically verifies the appropriate threshold values. Then the particle swarm optimization algorithm investigates the optimal fitness value of every particle and detects the lesser threshold values while the information to be transformed. However, the association rule mining is improved to hide the sensitive rule. Therefore, the proposed RSA-DSO model is described to attain the optimized rule hiding when compared to the association rule mining. Figure 6.4 illustrates the algorithmic process of Discrete Swarm Optimization (DSO) algorithm using RSA-DSO model for identifying the sensitive rule and hiding the discrete model as follows.

<table>
<thead>
<tr>
<th>Input:</th>
<th>database ‘( D )’, Transaction ( {t_1, t_2, \ldots, t_n} ), minimum support threshold ‘( mint )’, random number ‘( rnd )’</th>
</tr>
</thead>
<tbody>
<tr>
<td>Output:</td>
<td>Optimized rule hiding</td>
</tr>
<tr>
<td>Step 1: Begin</td>
<td></td>
</tr>
<tr>
<td>Step 2:</td>
<td>For each database ‘( D )’</td>
</tr>
<tr>
<td>Step 3:</td>
<td>For every transaction ‘( t_1, t_2, \ldots, t_n )’</td>
</tr>
</tbody>
</table>
Step 4: Generate association rule using (6.6)
Step 5: Measure fitness function using (6.7)
Step 6: Extract sensitive rules using (6.8)
Step 7: Generate random number between ‘0’ and ‘1’
Step 8: If ‘rnd’ < ‘$\text{Sig} V_{ab}(t + 1)$’
Step 9: Then ‘$V_{ab}(t + 1)$’ = 1
Step 10: Sensitive rule identified
Step 11: Perform rule hiding
Step 12: End if
Step 13: If ‘rnd’ > ‘$\text{Sig} V_{ab}(t + 1)$’
Step 14: Then ‘$V_{ab}(t + 1)$’ = 0
Step 15: Not a sensitive rule
Step 16: End if
Step 17: End for
Step 18: End for
Step 19: End

Figure 6.4 Discrete Swarm Optimization Algorithm

Figure 6.4 shows that the Discrete Swarm Optimization (DSO) algorithm for hiding the sensitive rule using RSA-DSO model. At first, for every database and transaction, the association rule is generated and then measures the fitness function for extracting the sensitive rules. After that, every possible rule is being extracted from the equation (6.8). As a result, the RSA-DSO model employs sigmoid function for identifying the solution due to
the discrete optimization problem which results in detecting the optimized sensitive rules with better efficient.

Yaping Li et al. (2012) introduced the multilevel trust in the privacy preserving data mining technique for allowing the perturbed copies of data exclusive the possibility of accessing the information by third parties, hence it ensures the improved trust level. But, the security aspects using multilevel trust in privacy preserving data mining method were not considered. In order to overcome this issue, the RSA-DSO model is proposed to improve the security level while preserving the privacy when compared to the multilevel trust in PPDM technique.

6.3 EXPERIMENTAL SETTINGS

In order to measure the effectiveness of the proposed framework, the integrated Reinforced Social Ant and Discrete Swarm Optimization (RSA-DSO) model is implemented with the help of JAVA language. The RSA-DSO model employs the adult data set from the University of California Irvine data repository that contains the information regarding age, level and current employment type. The last nominal attributes known as country of residence, gender and race.

During RSA-DSO model, the continuous attributes consists of age, hours worked per week, education number, capital gain and loss and survey weight attribute assigned to an individual based on the information like area of residence and type of employment.

6.4 RESULTS AND DISCUSSION

In this section, the result analysis of the proposed Reinforced Social Ant And Discrete Swarm Optimization (RSA-DSO) model is compared with the existing technique namely Multilevel Trust in Privacy Preserving Data Mining (MLT-PPDM) developed by Yaping Li
et al.(2012) and Protocol for secure mining of association rule developed by Tamir Tassa (2014). Then the performance of the proposed RSA-DSO model is analyzed with following metrics including privacy preservation accuracy, time for optimal data hiding and number of sensitive rules.

6.2.1 Measure of Privacy Preservation Accuracy

Privacy preservation accuracy is defined as the ratio of the number of privacy preserved perturbed copies to the total number of perturbed copies taken for the data publishing. The privacy preservation accuracy is mathematically formulated as given below.

\[ PPA = \left( \frac{\text{Number of privacy preserved perturbed copies}}{n} \right) \times 100 \]  

(6.9)

From the equation (6.9.), where \( PPA \) is denoted as privacy preservation accuracy which is analyzed with respect to the number of perturbed copies \( n \). The privacy preservation accuracy is measured in terms of percentage (%). When the privacy preservation accuracy is higher, the method is said to be more efficient.

**Table 6.1 Tabulation of Privacy Preservation Accuracy**

<table>
<thead>
<tr>
<th>Age (Number of perturbed copies)</th>
<th>Privacy Preservation Accuracy (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Proposed RSA-DSO</td>
</tr>
<tr>
<td>10</td>
<td>77.28</td>
</tr>
<tr>
<td>20</td>
<td>81.52</td>
</tr>
</tbody>
</table>
Table 6.1 demonstrates the privacy preservation accuracy on the basis of proposed RSA-DSO model and existing system including MLT-PPDM method by Yaping Li et al. (2012) and protocol for secure mining of association rule by Tamir Tassa (2014). Number of perturbed copies are varied from the range of 10 to 100 for the experimental evaluation. For increasing the number of perturbed copies, the privacy preservation accuracy is also increased using all the techniques shown in the table 6.1. However, the proposed RSA-DSO model significantly measured by means of improving the privacy preservation accuracy when compared to the existing method.

Figure 6.5 explains the privacy preservation accuracy using the proposed RSA-DSO model and comparison is made with the existing method namely MLT-PPDM method by Yaping Li et al. (2012) and protocol for secure mining of association rule by Tamir Tassa (2014). From the figure 5.5, the proposed RSA-DSO model is proficiently maximizing the privacy preservation accuracy when compared to the existing methods.
In order to detect the problem of discrete optimization, the DSO algorithm utilizes the fitness function for extracting the sensitive rule in a significant manner using RSA-DSO model. Therefore, the privacy preservation accuracy is improved using the proposed RSA-DSO model by 14% when compared to the existing MLT-PPDM method by Yaping Li et al. (2012) and 30% when compared to the existing protocol for secure mining of association rule by Tamir Tassa (2014) respectively.

6.4.2 Measure of Time for Optimal Hiding

Time for optimal hiding for the proposed RSA-DSO model is measured as the amount of time taken to require single transaction to the total number of transactions. Time for optimal hiding is measured in terms of milliseconds (ms). The time for optimal hiding is mathematically formulated as given below.

\[
Time = Total\ number\ of\ transcation \cdot Time\ ( single\ transaction) \quad (6.10)
\]
From the equation (6.10), the time for optimal hiding is represented as ‘\( \text{Time} \)’ that is evaluated based on the total number of transactions. If the time for optimal hiding gets lower, then the technique is significantly more efficient.

Table 6.2 Tabulation of Time for Optimal Hiding

<table>
<thead>
<tr>
<th>Total number of transactions</th>
<th>Proposed RSA-DSO</th>
<th>Existing MLT-PPDM</th>
<th>Existing protocol for secure mining of association rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>2.22</td>
<td>3.62</td>
<td>5.43</td>
</tr>
<tr>
<td>10</td>
<td>3.85</td>
<td>5.21</td>
<td>6.66</td>
</tr>
<tr>
<td>15</td>
<td>5.55</td>
<td>6.55</td>
<td>8.42</td>
</tr>
<tr>
<td>20</td>
<td>6.67</td>
<td>7.67</td>
<td>9.67</td>
</tr>
<tr>
<td>25</td>
<td>6.89</td>
<td>7.98</td>
<td>9.59</td>
</tr>
<tr>
<td>30</td>
<td>8.9</td>
<td>10.32</td>
<td>12.42</td>
</tr>
<tr>
<td>35</td>
<td>10.8</td>
<td>12.31</td>
<td>14.01</td>
</tr>
<tr>
<td>40</td>
<td>12.95</td>
<td>14.36</td>
<td>16.34</td>
</tr>
<tr>
<td>45</td>
<td>14.32</td>
<td>15.53</td>
<td>17.13</td>
</tr>
<tr>
<td>50</td>
<td>15.3</td>
<td>16.64</td>
<td>18.31</td>
</tr>
</tbody>
</table>

Table 6.2 explains the time for optimal hiding with respect to the proposed RSA-DSO model and existing method includes MLT-PPDM method by Yaping Li et al. (2012) and protocol for the secure mining of association rule by Tamir Tassa (2014). Total number of transactions is taken from the range of 5 to 50 for conducting test. From the table 6.2, increasing the total number of transactions, the time for optimal hiding is also increased.
using all the techniques. However, the proposed RSA-DSO model generates minimal time to hide the sensitive items when compared to the existing method.

**Figure 6.6 Measure of Time for Optimal Hiding**

Figure 6.6 illustrates the time for optimal hiding using proposed RSA-DSO model which is compared with the existing system namely MLT-PPDM method by Yaping Li et al. (2012) and protocol for secure mining of association rule by Tamir Tassa (2014). The proposed RSA-DSO model is efficiently reduces the optimal hiding time when compared to the existing methods as shown in the figure 6.6. With the integration of reinforcement model is addressed for hiding the data item that is mainly based on the probability to occur the sensitive data item is evaluated only once. In addition, RSA-DSO model separates the sensitive data items where the optimal frequent items are reinforced using ‘Dfactor’ are being measured which in turns reducing the time for optimal hiding. Therefore, the RSA-DSO model minimize the time for optimal hiding by 16% when compared to the existing
MLT-PPDM method by Yaping Li et al. (2012) and 30% when compared to the existing protocol for secure mining of association rule by Tamir Tassa (2014) respectively.

6.4.3 Measure of Number of Sensitive Rules

The number of sensitive rules are defined as the ratio of the number of associative rule generated to the given number of items using RSA-DSO model. The number of hidden rules are mathematically represented as follows,

\[
\text{Number of hidden rules} = \frac{\text{number of associative rule generated}}{\text{number of items}} \times 100
\]  

(6.11)

From the equation (6.11), the number of hidden rules are measured in term of percentage (%). While the number of hidden rules gets lower, thus the technique is efficiently more efficient.

Table 6.3 Tabulation of the Number of Sensitive Rules

<table>
<thead>
<tr>
<th>Number of items</th>
<th>Number of Sensitive Rules (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Proposed RSA-DSO</td>
</tr>
<tr>
<td>1</td>
<td>79</td>
</tr>
<tr>
<td>2</td>
<td>82</td>
</tr>
<tr>
<td>3</td>
<td>85</td>
</tr>
<tr>
<td>4</td>
<td>84</td>
</tr>
<tr>
<td>5</td>
<td>86</td>
</tr>
<tr>
<td>6</td>
<td>88</td>
</tr>
<tr>
<td>7</td>
<td>86</td>
</tr>
</tbody>
</table>
Table 6.3 shows the number of sensitive rules for the proposed RSA-DSO model and the existing method including MLT-PPDM method by Yaping Li et al. (2012) and protocol for secure mining of association rule by Tamir Tassa (2014). Number of items is taken as input which is varied from the range of 1 to 10 for the experimental purpose. For all method, table 6.3 illustrate the number of sensitive rules are generated with respect to the increasing of number of items. However, the proposed RSA-DSO model provides better performance in terms of reducing the number of sensitive rules when compared to the existing method.

<table>
<thead>
<tr>
<th></th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>87</td>
<td>89</td>
<td>91</td>
</tr>
<tr>
<td>72</td>
<td>66</td>
<td>70</td>
<td></td>
</tr>
<tr>
<td>68</td>
<td>74</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

![Figure 6.7 Measure of Number of Sensitive Rules](image-url)
Figure 6.7 describes the number of sensitive rules using the proposed RSA-DSO model and compared with the existing system namely MLT-PPDM method by Yaping Li et al. (2012) and protocol for secure mining of association rule by Tamir Tassa (2014). From the figure 6.7, the proposed RSA-DSO model comparatively minimizes the number of sensitive rules when compared to the existing methods. This is due to the incorporation of RSA-DSO model provides the optimal number of sensitive data items occurs only once and discretization of rule generation which resulting in minimizing the number of sensitive rules to be generated. Therefore, the number of sensitive rules are reduced using the proposed RSA-DSO model by 22% when compared to the existing MLT-PPDM method by Yaping Li et al. (2012) and 34% when compared to the existing protocol for secure mining of association rule by Tamir Tassa (2014) respectively.

6.5 SUMMARY

A proposed Reinforced Social Ant and Discrete Swarm Optimization (RSA-DSO) model is introduced for solving the multi-objective factors including the data and rule hiding with the help of reinforcement and discrete optimization model. Initially, the RSA-S model ensures the sensitive data item with the objective of reducing the optimal sensitive data time and increasing the privacy preservation accuracy for data publishing. Next, the DSO model guarantees the sensitive rule hiding with respect to the sigmoid function for evaluating the sensitive rules instead of using traditional support and confidence values which resulting in decreasing the sensitive rule generation. Finally, the proposed RSA-DSO model is very efficient to improve the privacy preservation accuracy with minimal time for optimal hiding, hence the optimizing the generation of sensitive rules for data publishing. In addition, the simulation results illustrate that the RSA-DSO model provides better
performance with the improvements of privacy preservation accuracy by 22% and reduction of optimal hiding time by 23% when compared to the state-of-the-art works.