



Privacy Preserving Data Mining Using Additive Perturbation on Relational Streaming Data

Ashish E. Mane, Prof. Pankaj Agarkar

Student, Department of Computer Engineering, Dr. D.Y. Patil School of Engineering, Lohegaon, Savitribai Phule Pune
University, Pune, Maharashtra, India¹

Assistant Professor, Department of Computer Engineering, Dr. D. Y. Patil School of Engineering, Lohegaon, Savitribai
Phule Pune University, Pune, Maharashtra, India²

ABSTRACT: Data mining concerns with extracting the required important data from the database and ignoring the rest. With the success of data mining, privacy preservation has also acquired the great importance. The new concept privacy preserving data mining PPDM, concerns with preserving the privacy of sensitive individuals data. In this paper, privacy of sensitive attribute data concerned with individual user or data miner is preserved. For preserving the privacy additive perturbation method is used, in which random noise are added to the sensitive attribute values from the require data set and perturb copies are generated. A new concept multilevel trust MLT-PPDM approach is used, in which we generate multiple perturb copies of same data for the data miners at different trust level. For perturb copies generation, group generation algorithm is used, in which for a given original data, multiple perturbed copies of same data will be generated. We are using relational streaming database which means records in the database are updated continuously and at the same time for each updated records perturb copies will be generated successfully, which is the new contribution to the proposed work.

KEYWORDS: Data mining; Privacy preservation data mining (PPDM); Additive perturbation; Group generation algorithm; Relational Streaming data.

I. INTRODUCTION

Data Mining deals with the extraction of knowledge from large set of data. It is a process of discovering the relevant and useful knowledge from the extensive amount of data stored in database, data warehouse or other data repositories. The obtained knowledge can be used for making various different types of decisions, information management, and query processing. But the matter of privacy of extracted data comes forward, because if this information goes in the hands of unauthorized person, there are severe chances of this information being misused by the data miner.

The data which is extracted can be sensitive or less important data, data for example- name, date of birth, sex, education qualification may not become harmful to the individual user but, the attribute data such or an individual bank account number, user id, telephone number and such related sensitive attribute data can become harmful to that user if this data is acquired by the unauthorized or malicious data miner. Hence the privacy of sensitive attribute data which is to be extracted by the data miner whether it is authorized or malicious becomes important. The important issue to be taken into consideration is, even non sensitive data also contains the sensitive information including personnel information and facts. So the concept Privacy Preserving Data Mining (PPDM) becomes important.

Privacy preserving data mining (PPDM) [8] deals with privacy of sensitive attribute data by not violating the integrity of that data. PPDM has various interesting approaches to preserve the privacy of sensitive information such as data perturbation, Cryptographic technique, Condensation approach, Hybrid approach. Data perturbation [1], [2], [8] is



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

a most popular approach for preserving the privacy of original data. There are also various classes of the data perturbation which includes additive perturbation, K-anonymity, matrix multiplicative, Data swapping etc. Among all this techniques, additive perturbation is most popular technique to perturb the data.

We are using additive perturbation approach [1] to perturb the relational attribute data values. This attribute data values are sensitive to the individual data miner. Previous data mining approach assumes single level trust on the data miner. In single level trust approach only one perturbed copy of original data is constructed by the data owner which is uncertain. Single level trust approach fails, where the organizations trust data miners at different levels. Due to this factor we are using a new concept known as Multilevel Trust Privacy preserving approach (MLT-PPDM) [1]. In this approach data owner trust the data miner at different trust levels and for each trust level multiple different perturbed copies of same original sensitive attribute value are generated. We have defined five trust levels for determining the trust level of data miner this are Very high, high, medium, low, very low. If the trust level is high then, less perturbed copies will be generated, perturbation will be less, if the trust level is low more amount of perturbation will be done in the perturbed copies.

Here Group generation algorithm is used to generate the perturbed copies of original data. For each trust level, multiple different perturbed copies of same data will be generated by the group generation algorithm. Malicious data miners can combine the different perturbed copies generated for each trust level and try to obtain the original data, this is known as diversity attack. The proposed system application generates the perturbed copies in such a way that, the data miner will find it hard to reconstruct and obtain the original information.

We are using the relational streaming database, in which records are updated periodically, for each newly added record, instantly new perturbed copies for newly added records are generated and data miner need not have to worry about the updated records. This is new contribution to the proposed work.

The implemented software application can be used in such organizations which store their large amount of data in the form of relational database and want to protect their sensitive data by unauthorized user.

II. RELATED WORK

Concept of privacy preserving data mining has given an attention by various researchers and lot of work is being carried out on it. For preserving the privacy of sensitive information and other data, various researchers have proposed different approaches of privacy preserving data mining (PPDM). One of the privacy preserving technique is data perturbation [1], It is an most popular technique which has various different classes such as additive perturbation, matrix multiplicative, data swapping, K-anonymity, Micro aggregation, etc. Among all this perturbation classes additive perturbation is most popular perturbation technique which is used in the proposed work.

Yaping Li, Minghua Chen, Qiwei Li, Wei Zhang, propose the mechanism of preserving the privacy of sensitive data by the additive perturbation technique. Previous data mining applications were assuming the single level trust, in which only one perturbed copies of original information were built, in this paper authors have extended the concept of single level trust to multilevel trust scenario. In the MLT-PPDM approach they have defined the high, medium and low trust levels for different data miners. For each trust level multiple different perturbed copies of same original data are generated. They have also proposed that their solution is robust against the diversity attacks [1].

Privacy preservation data mining was first proposed by the authors R. Agarwal and R. Shrikant [5]. In this, authors have discussed the technique to build the decision tree classifier from the training data in which individual record values are perturbed.

Shweta Taneja, Shashank Khanna, Sughanda Tilwalia, Ankita have discussed and compared various privacy preserving data mining techniques on which different authors have carried their work successfully [2]. They have presented the tabular comparison of different work carried out by the researchers.

Authors A.C. Yao in [3] and O. Goldreich in [4], [5] have discussed the Secure Multiparty Computation SMC techniques. The Secure Multi-party Computation (SMC) approach concerns the problem of calculating a function of



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

two or more parties secret inputs, in such a way that, each party finally gets the required designated function output and nothing else is revealed, except what is implied by the party's own inputs and outputs. This technique provides strongest level of privacy. Algorithms used by this technique are more complex and not practical for real use. Also the input consists of large amount of datasets. Due to this reasons the SMC is not used in practical applications. Due to these drawbacks of SMC another approaches were discovered and used. Author Y. Lindell and B.Pinkas in [6] has focused on Secure Multiparty Computation based privacy preserving data mining schemes.

Data perturbation [1], [7], [8], [9], [10], [11] is one of the privacy preservation PPDM approach which contains various classes such as additive perturbation, Matrix multiplicative perturbation, Data swapping, k-anonymity. In this approach there are various techniques such additive perturbation [1], [7], [8], [10], [11]. This approach is used in the proposed system to generate the perturb copies by adding the random noise to the original attribute data values. This is a very popular data perturbation technique.

Another data perturbation approach which is known as data swapping approach is discussed [2], the sensitive values are transformed by replacing the values of records.

The Authors in [9], [12] have proposed Matrix multiplicative approach which is other class of data perturbation, in this technique inter record distances are preserved approximately and ultimately transformed records can be used with many types of data mining applications.

The authors in [13], [14] proposed the technique of K-anonymity. This technique has two methods Generalization and Suppression. In generalization, the attribute values are generalized into the range so that the granularity of the representation is reduced. For example, date of birth of an individual can be generalized to year of birth, whereas in the suppression method the attribute value is removed completely.

III. BASIC CONCEPTS

A. Additive Perturbation:

Data perturbation is one of the privacy preserving data mining PPDM technique which has multiple classes such as K-anonymity, Matrix multiplicative, Additive perturbation, data swapping etc. Among all this classes additive perturbation is most important and popular data perturbation technique.

In the additive perturbation technique, some random noise R is added to the original data Q and perturbed copy P is generated.

$$P = Q + R$$

The noises are added randomly. There are various advantages of additive perturbation such as

- The noise can be added separately and independently to each attribute record value separately at any position.
- It is easy technique and has low cost.
- This technique can be used at web and corporate sector.

B. Multilevel Trust Approach MLT-PPDM:

In the multilevel trust approach data miner are trusted at different trust level and for each trust level, multiple different perturbed copies of same attribute data are constructed. We have defined five trust levels as very high, high, medium, low, very low. The magnitude of addition of noise to the original data depends on the trust level of the data miner. If the trust level is very high or high, then less amount of perturbation is done. If it is low or very low, more amount of perturbation is done to the perturb copies.

IV. PROPOSED ALGORITHM

A. Group Generation Algorithm:

The group generation algorithm generates the multiple perturbed copies for an original attribute data. There is one condition of this algorithm, that the trust level of the data miner for which the perturbed copies are to be generated should be known in advance. The trust level is determined during the role determination phase. It generates N number of multiple perturbed copies.



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

Basically, there are two types of this algorithm, parallel generation and sequential generation algorithm. The steps of these both algorithms are given below.

Algorithm 1: Parallel Generation:

```
{  
  
Input: Q, K  
Output: P  
  
Construct KR  $\leftarrow$  KQ  
  
Generate R  $\leftarrow$  KR  
  
Generate P  $\leftarrow$  HQ + R  
  
Output  $\leftarrow$  P  
}
```

The above algorithm then generates PP as HQ + RR and outputs the result. Above algorithm acts as the base algorithm for next algorithm that is Sequential Generation.

Algorithm 2: Sequential Generation

The parallel generation algorithm requires large amount of memory. So, an individual will prefer to use the algorithm which achieves task of efficient memory utilization. Instead of parallel generation algorithm one can sequentially start generating noise R1 to RM. We have used Sequential generation algorithm.

Sequential Generation:

```
{  
  
Input: Q, K  
Output: Pm  
  
Construct R  $\leftarrow$  N (0...KQ)  
  
Generate Pi  $\leftarrow$  Q + R1  
  
For i=2 to M do  
Create Noise  
  
Generate P  $\leftarrow$  Pi 1 + E  
  
Output  $\leftarrow$  Pi  
}
```

Where Q is original data,
R is noise,
P is perturbed copy.

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

V. BASIC SYSTEM ARCHITECTURE

A. System Architecture:

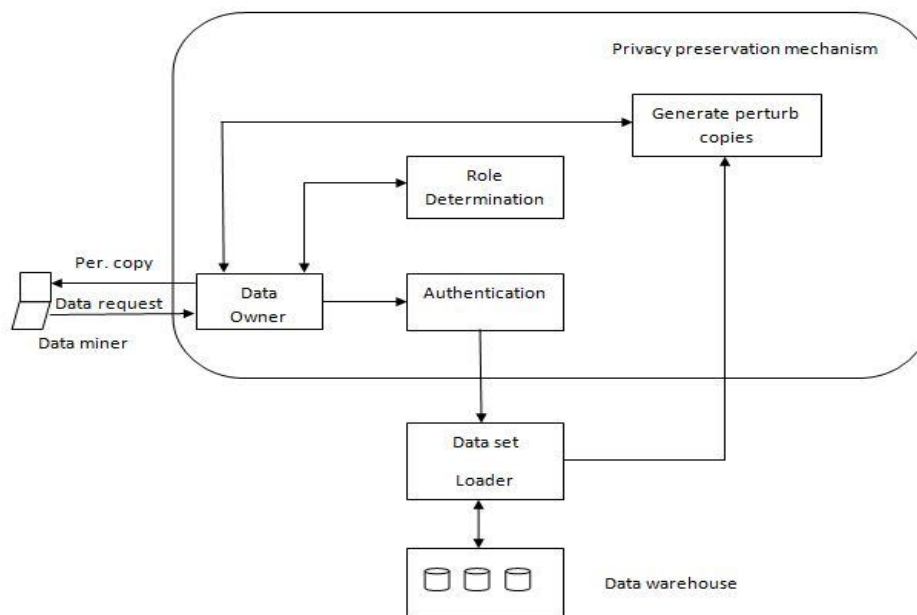


Fig. 1 Proposed System Architecture

Our proposed system takes the data input request from the data miner, for the attribute data values stored in the relational streaming database, determines the trust level of data miner by registering the details and generates the multiple perturbed copies for data miner at that trust level.

Also when the relational database is updated and the new records are added to the database, at the same time perturbed copies for that new added record are generated. Data miner need not have to check the database for updated records.

B. Outlines of the system:

The proposed system works in the following three modules:

1. Data Miner Module:

- Data miner authentication: Data miner sends the request to the system for required data. The system server performs the necessary registration details of the data miner and after registration it performs the login activity.
- Loading of dataset: We have used student datasets, other type of datasets can also be used such as banking or medical datasets. The data miner selects the required dataset and the dataset is loaded into the database.
- Request for data: Data miner gives the required attribute names and the system search in the specified directory where the generated perturbed copies are stored. If the perturbed copies are available, the system application shows the contents of perturb copy to the data miner. Suppose there are five perturbed copies of the required data from the selected dataset for that trust level are available in the directory, then one of the random perturb copy among the five perturbed copies will be given to the data miner. If the perturbed copies



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

are not available then the new perturb copies are generated by the data owner. But, prior to this data owner has to login to the system.

2. Data Owner Module:

- Data owner authentication: The data owner login is done, when the perturbed copies for the required data are not present in the directory of perturbed copies. The necessary authentication of the data owner is done by the server.
- Selection of Dataset: The required dataset is selected from the data warehouse and loaded to the database.
- Role Determination: In this phase trust level of the data miner and the required attribute names and their types are selected by the data miner. Also the number perturbed copies to be generated for the selected attribute data are given by the data miner.
- Generation of perturbed copies: In this phase, given number of perturb copies are generated by using the group generation algorithm.

3. Data Streaming Module:

- Listening Request from Data Miner: When the data miner sends the request for showing the perturbed copy of updated records, if the records are updated. Data owner listen the request of data miner.
- Check Data set for modification: In this phase, we have used a simple website in which data owner has to login as admin, select the required dataset and he can insert new records for into the required dataset.
- Send the modified perturb copy to data miner: When the records in the database are updated, at the same time perturb copy generated for data miner is also updated. The data miner sends the updated perturb copy to data miner. This is the advantage for the data miner.

VI. RESULTS

Our project application has three modules:

- Data miner module
- Data owner module
- Streaming module.

A. Data Miner Module

In this module, the data miner authentication is performed by the system. Data miner can give the request for required data from the specific dataset to the data owner. Data miner can select the needed dataset and attribute data through this module. If the data miner gives the request for the data from the particular dataset and if for the required data, perturbed copies are already generated previously by the data owner, the system randomly picks one of the perturbed copy from the set of randomly generated copies and gives to the data miner. Data miner can see the contents of the perturbed copy given by the data owner in this module. This module is important for both the entities data miner and data owner. Data owner comes to know which attribute data is required by data miner.

The fig .2 shows login screen for Data miner and data owner.

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015



Fig. 2 Data miner and Data Owner Login

1. Registration and Login:

The following fig. 3 shows the user or data miner has done the necessary registration and login and can give the request for required data. It shows the authentication of data miner is successful.



Fig. 3 Data miner Authentication

2. Select dataset:

The fig. 4 shows two options, first is to select required dataset, and next is explore perturb copies which shows the available perturb copies from the specified directory. If the data miner wants to give the data request, then he/she has to click on select data table option.

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

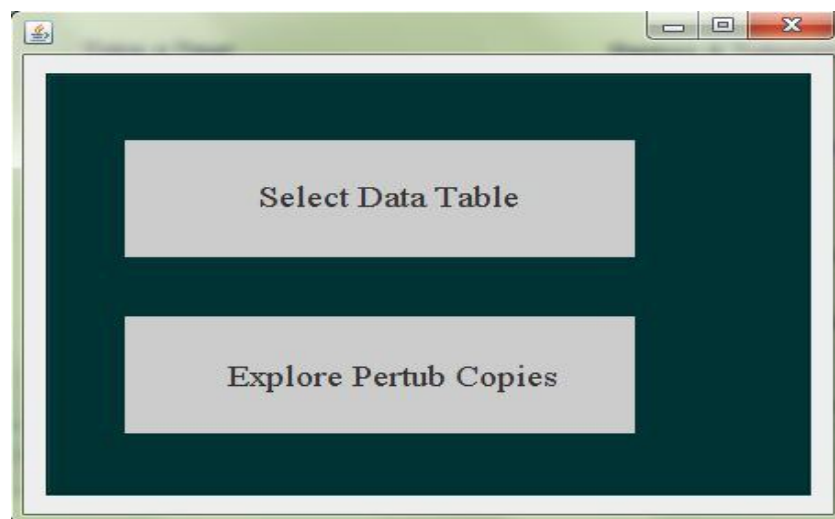


Fig. 4 Selection of Dataset

The following fig. 5 shows that the data miner has selected the required dataset. The data set consists of the .xls file and is stored in the My SQL database. We have used student datasets, this system also can work on other types of dataset such as banking or medical.

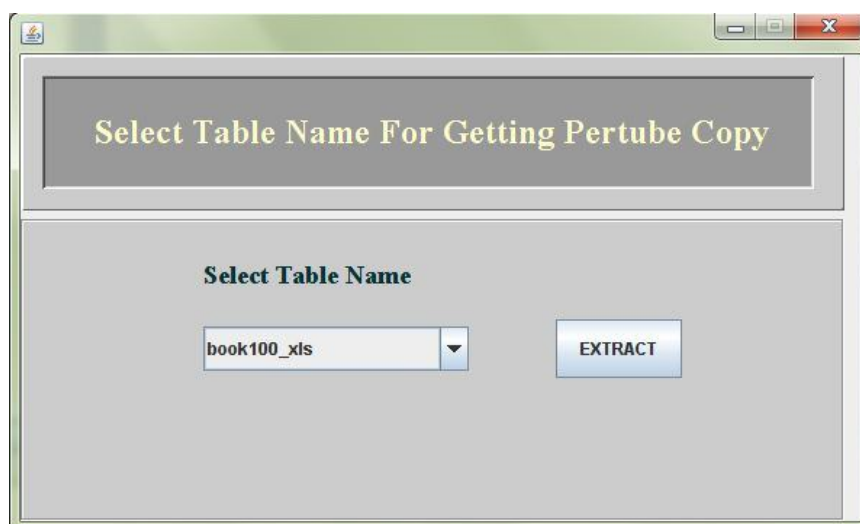


Fig. 5 Input Dataset

3. Data request:

After selection of necessary required dataset, data miner can give the required attribute column names which it wants access. The attribute type by default is id attribute type. The following screen shows the request given by the data miner by selecting the necessary column names.

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

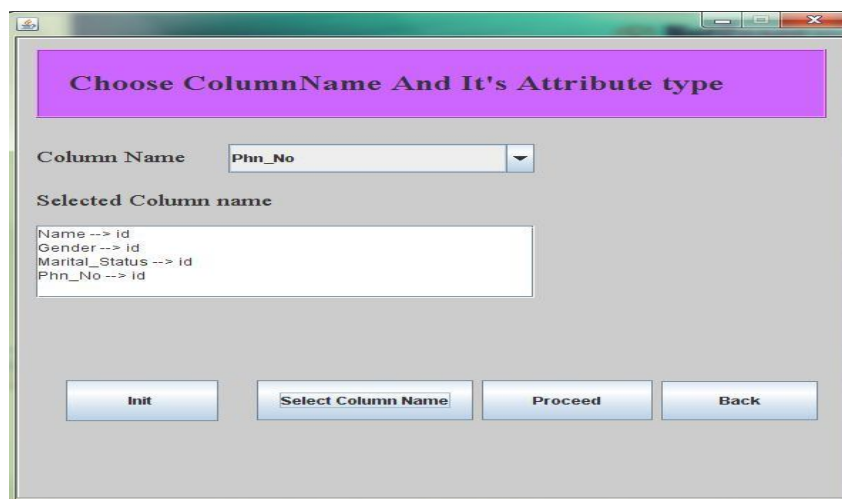


Fig .6 Request for data

The fig. 7 shows that for the given request, perturb copies are already available and one of the random perturb copy will be displayed to the data miner from previously generated set of perturbed copies. This makes the task of data miner easier.

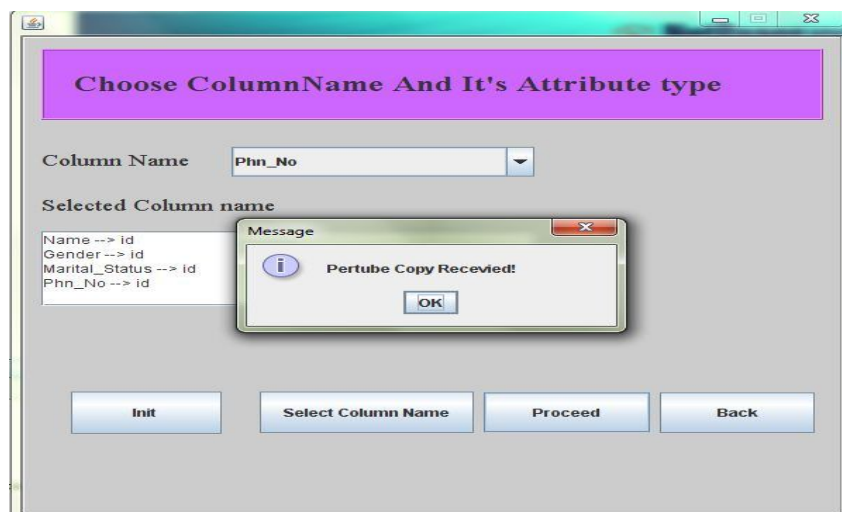


Fig .7 Available perturb copy for requested data

The following fig. 8 shows contents the available perturb copy for requested data to the data miner. All contents in the perturbed copy are perturbed according to the trust level of data miner.

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

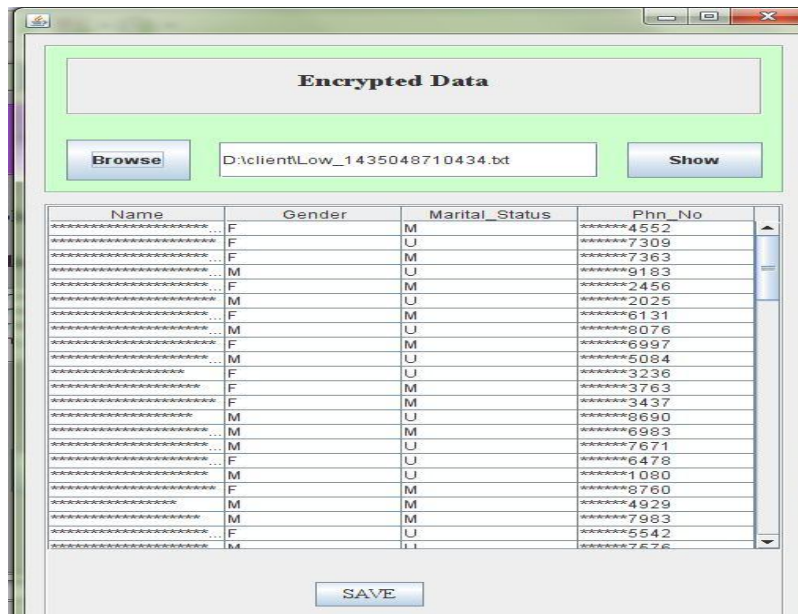


Fig. 8 Contents of available perturbed copy

The following fig. 9 shows that the perturb copy is not generated for the requested data. The perturbed copies are not present in the specified directory. So, the perturbed copies have to be generated by the data owner. Now the actual task of the data owner starts.

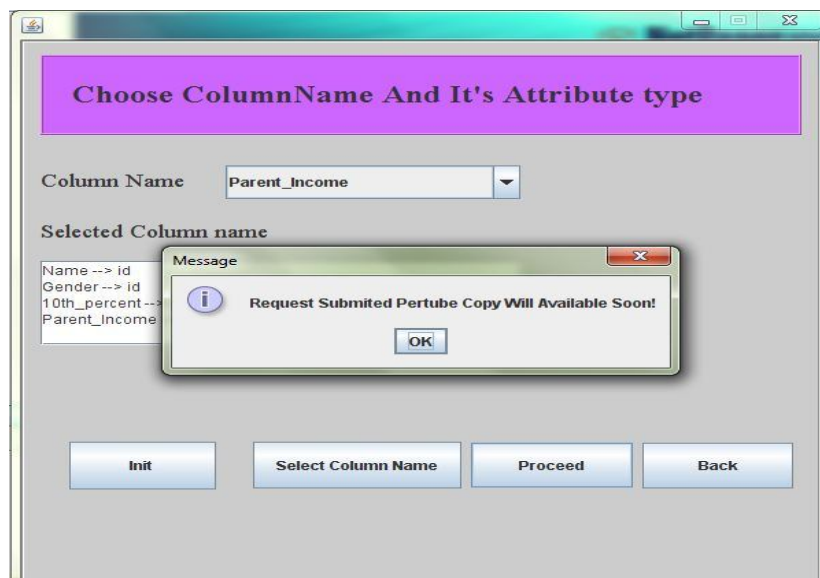


Fig. 9 Perturb copy not available

B. Data Owner Module:

In this module data owner has to generate the new perturbed copies for the requested data by the data miner, because the perturbed copies for the required data set are not available. Data owner performs various different and important tasks which are mentioned below in this section.

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

1. Data owner login:

The following figure shows the data owner login. Authentication of data owner is also performed by the system. The fig. 10 shows that the data owner authentication is successful.



Fig. 10 Data owner authentication

2. Select Data Set and Determine Trust Level:

The following screen shows that the data owner selects the dataset from which the data miner needs the data. There are four student datasets maintained by the system. Data owner has to select that dataset, for which the request for data is given by the data miner.

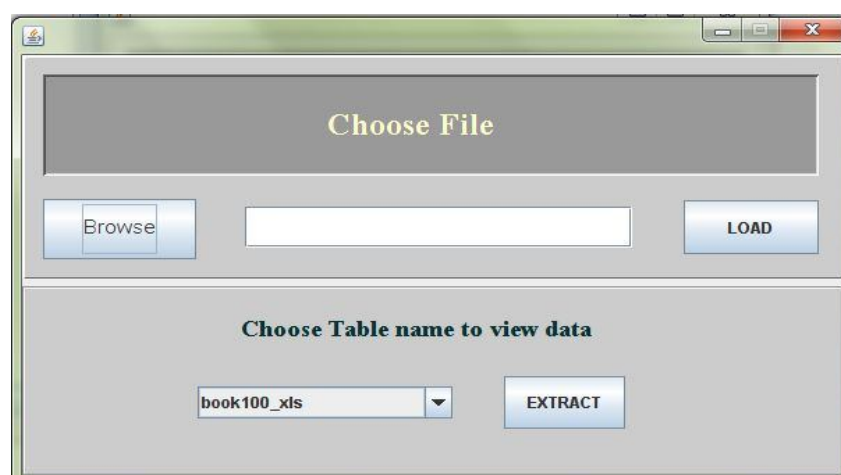


Fig. 11 Select dataset

In the following fig. 12 data owner selects trust level of data miner. Below screen shows that the trust level very high is selected. Here if the trust level is high or very high, then less perturbation is done by the data owner. If the trust level is low then more amount of perturbation is performed by the data owner. Percentage of noise to be added to the original data is based on trust level of the data miner.

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015



Fig .12 Trust level selection

3. Select Attributes to Generate Perturb Copies:

The following fig .13 shows the attribute data required by the authorized data miner are selected for generating the perturbed copies. These data are mapped by selecting the their appropriate types. Five types are specified by the system for determining the type of attribute data, they are Id attribute, numeric attribute, boolean attribute, multivalued attribute, phone attribute. The attribute type of name is always id attribute type. Before generation of perturbed copies data owner has to determine the quantity of perturbed copies to be generated. The amount of pertubed copies to be generated is determined only by the data owner.

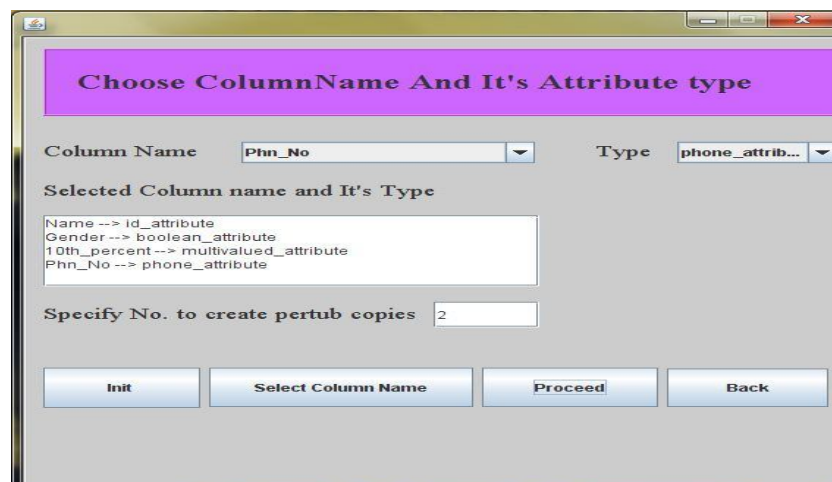


Fig. 13 Selection of attribute data and type mapping

The fig. 14 shows the perturb copies are successfully generated and are stored in the specified directory. The data miner can see the available perturbed copy for the required attribute data.

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

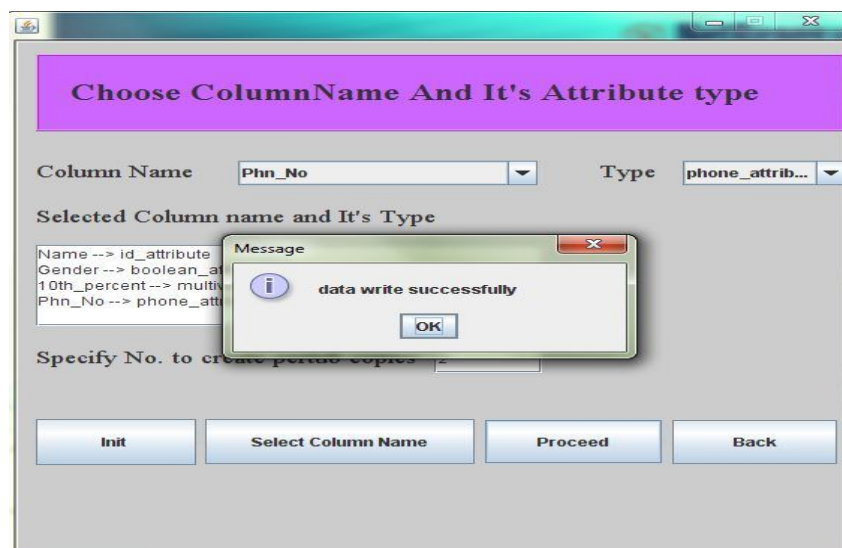


Fig. 14 Generation of perturb copies

C. Streaming Module:

In the Streaming module when the change takes place into a dataset at the same time data miner receives the modified perturbed copy for newly added records. The following fig. 15 shows the home screen of the streaming module. This screen provides information about the services provided by the system. It also shows the available datasets.

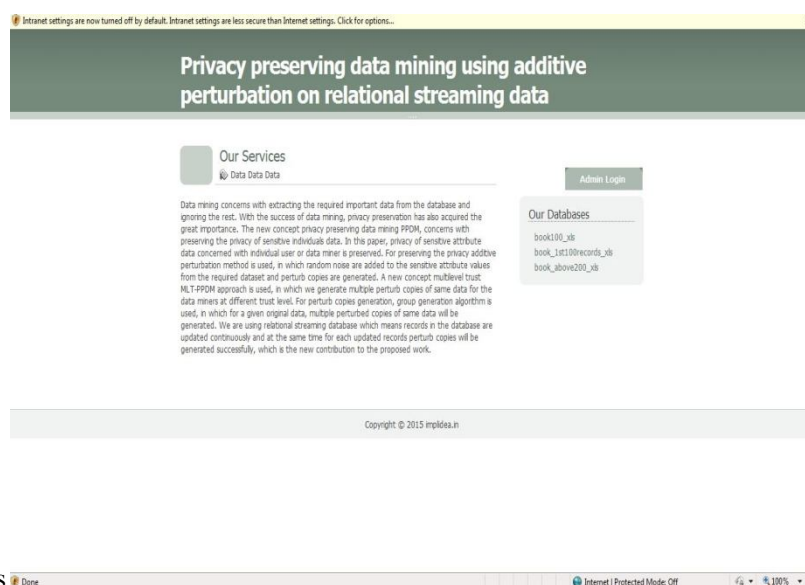


Fig. 15 Home Screen for streaming module

1. Insertion of new record:

The data owner updates the dataset by inserting the new records into the selected data set. The following screen shows the insertion of records by filling the required data fields. After filling each details record gets added to the database.

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

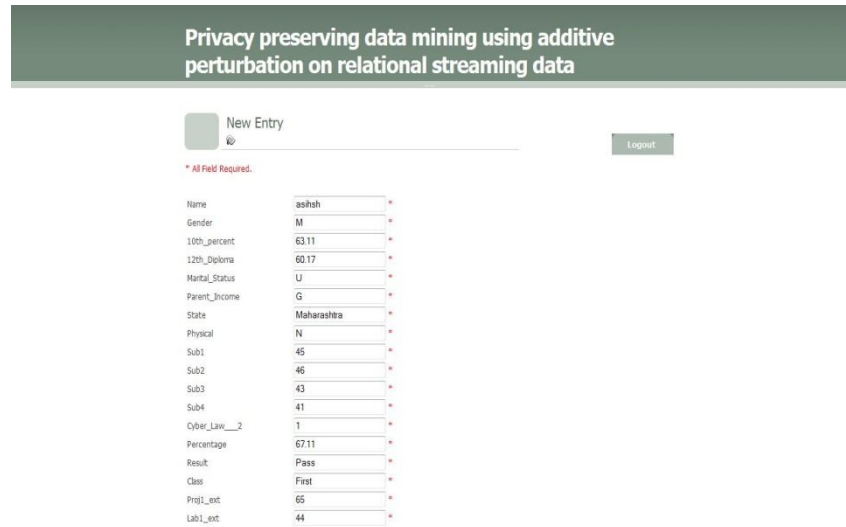
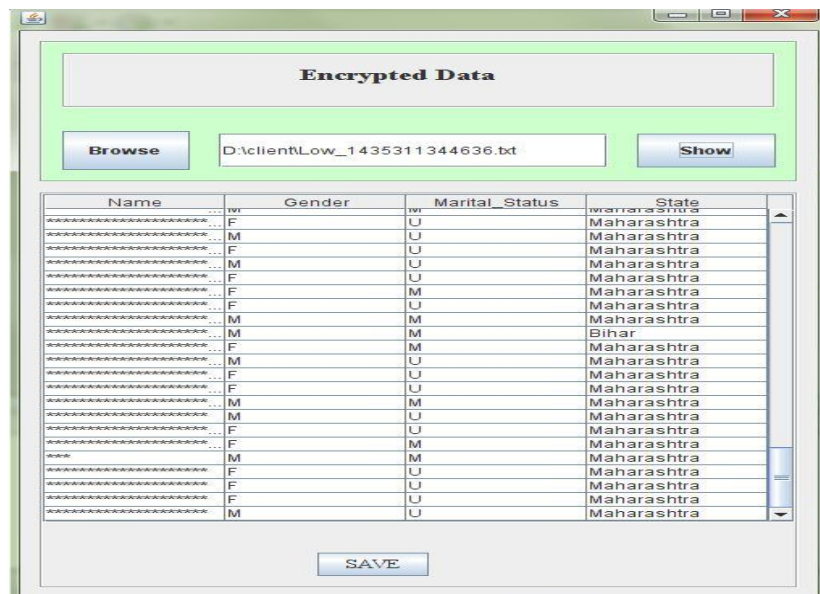


Fig. 16 Insertion of new record

2. Perturbed copy before update of dataset:

The following fig.17 shows the contents of perturb copy before update of dataset. The data owner checks the contents.



Name	Gender	Marital_Status	State
.....	F	U	Maharashtra
.....	M	U	Maharashtra
.....	F	U	Maharashtra
.....	M	U	Maharashtra
.....	F	U	Maharashtra
.....	F	M	Maharashtra
.....	F	U	Maharashtra
.....	M	M	Maharashtra
.....	M	M	Bihar
.....	F	M	Maharashtra
.....	M	U	Maharashtra
.....	F	U	Maharashtra
.....	F	U	Maharashtra
.....	M	M	Maharashtra
.....	M	U	Maharashtra
.....	F	U	Maharashtra
.....	F	U	Maharashtra
.....	F	M	Maharashtra
.....	M	M	Maharashtra
.....	F	U	Maharashtra
.....	F	U	Maharashtra
.....	F	U	Maharashtra
.....	M	U	Maharashtra

Fig. 17 Contents of perturb copy before dataset update

3. Perturbed copy after update of dataset:

The following fig .18 shows the contents of perturbed copy after the update of dataset. The new added record is perturbed by the data owner.

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

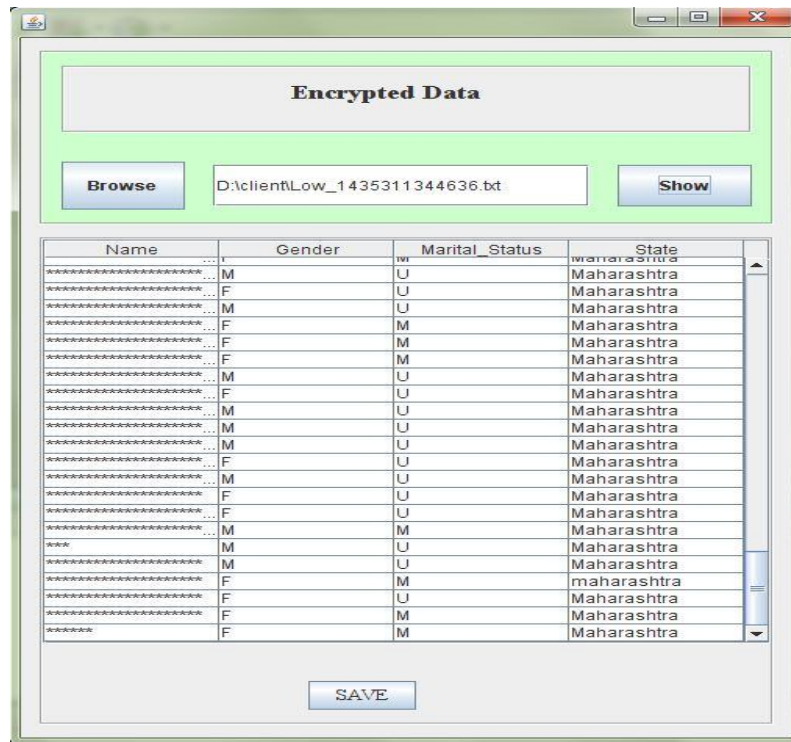


Fig .19 Contents of perturb copy after dataset update

In this way the perturbed copy for updated relational database is generated successfully and is given to data miner. We have calculated the time required for generation of different numbers of perturbed copies for the database consisting of 300 records. The perturbed copies for even more number of records can be generated by our application. We have maintained the data set consisting of around 1200 records. As the records get increased, the time for generation of perturbed copies are also increased.

The following table shows the time required for generation of different number of perturbed copies for the student dataset of 300 records.

Table I Time required for generation of perturbed copies

NO OF PERTURBED COPIES	TIME REQUIRED FOR GENERATION OF PERTURBED COPIES(sec)
10	59
15	95
20	126
25	160
30	195
35	245
40	292
45	340
50	374

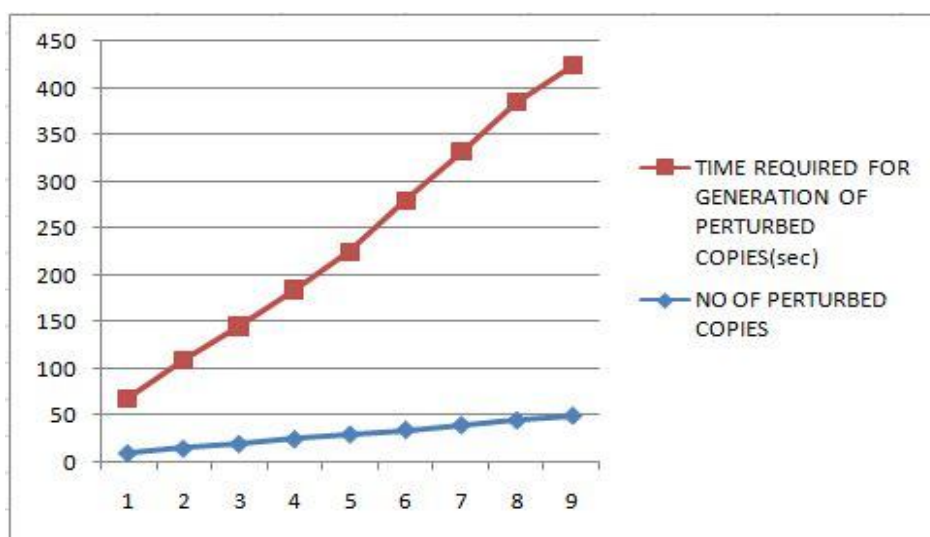
International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

The following line chart shows the result of time required for generation of perturbed copies for the dataset consisting of 300 records. As the number of perturbed copies to be generated are increased, the time required for generation of perturbed copies is also increased.

Line Chart I



VII. CONCLUSION AND FUTURE WORK

In this system, privacy of sensitive data records of relational streaming database is preserved by generating the perturbed copies. In this work we generate the multiple numbers of perturbed copies for a selected trust level of data miner. We discussed the additive perturbation technique and group generation algorithm for generation of perturbed copies.

We have successfully shown our new contribution for the generation of perturbed copies for the updated relational streaming database. To reduce the time for generation of multiple perturbed copies for the large dataset and to extend this system to Hadoop and Big Data will be the subject of future work.

REFERENCES

1. Yaping Li, Minghua Chen, Qiwei Li, and Wei Zhang, "Enabling Multilevel trust in Privacy preserving data mining", IEEE TRANSACTIONS ON KNOWLEDGE AND ENGINEERING, VOL. 24, NO. 9, SEPTEMBER 2012.
2. Shweta Taneja, Shashank Khanna, Sugghanda Tilwalia, Ankita, "A Review on Privacy Preserving Data Mining: Techniques and Research Challenges", INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND INFORMATION TECHNOLOGY (IJCSIT), VOL 5(2), 2014, 2310-2315.
 - a. C. Yao, "How to generate and exchange secrets," in *Proceedings 27th IEEE Symposium on Foundations of Computer Science*, 1986, pp. 162-167.
3. O. Goldreich, S. Micali, and A. Wigderson, "How to play any mental game," in *Proceedings of the 19th annual ACM symposium on Theory of Computing*, 1987, PP. 218-229.
4. O. Goldreich, "Secure Multiparty Computation", Final incomplete draft, version 1.4, 2002.
5. Y. Lindell and B. Pinkas, "Privacy Preserving Data Mining", Proc. Proc. Int'l Cryptology Conf. (CRYPTO), 2000.
6. D. Agrawal and C.C. Aggarwal, "On the Design and Quantification of Privacy Preserving Data Mining Algorithms," Proc. 20th ACM SIGMOD-SIGACT-SIGART Symp. Principles of Database Systems (PODS '01), pp. 247-255, May 2001.
7. R. Agrawal and R. Srikant, "Privacy Preserving Data Mining," Proc. ACM SIGMOD Int'l Conf. Management of Data (SIGMOD '00), 2000.
8. K. Chen and L. Liu, "Privacy Preserving Data Classification with Rotation Perturbation," Proc. IEEE Fifth Int'l Conf. Data Mining, 2005.
9. Z. Huang, W. Du, and B. Chen, "Deriving Private Information From Randomized Data," Proc. ACM SIGMOD Int'l Conf. Management of Data (SIGMOD), 2005.



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

10. F. Li, J. Sun, S. Papadimitriou, G. Mihaila, and I. Stanoi, "Hiding in the Crowd: Privacy Preservation on Evolving Streams Through Correlation Tracking," Proc. IEEE 23rd Int'l Conf. Data Eng. (ICDE), 2007.
11. K. Liu, H. Kargupta, and J. Ryan, "Random Projection-Based Multiplicative Data Perturbation for Privacy Preserving Distributed Data Mining," IEEE Trans. Knowledge and Data Eng., vol. 18, no. 1, pp. 92-106, Jan. 2006.
12. L. Sweeney, "K-Anonymity: A Model for Protecting Privacy," Int'l, J. Uncertainty, Fuzziness and Knowledge-Based Systems (IJUFKS), vol. 10, pp. 557-570, 2002.
13. Walid .G. Aref, Arif Ghaffor and nagabhushana Prabhu, Accuracy constrained privacy preserving Access control Mechanism Relational data iee transactions on knowledge and data engineering, vol 26, NO. 4, April 2014.

BIOGRAPHY

Ashish E. Mane: I am a post graduate student in Department Of Computer Engineering at Dr. D. Y. Patil, School Of Engineering, Charoli, Lohegaon, Pune. I am pursuing Master of Engineering (M.E) post graduation degree course in Computer Engineering. I have completed my B.E in Computer Science and Engineering from T.K.I.E.T, Warananagar, Kolhapur.

Prof. Pankaj Agarkar: He works as Assistant Professor in Department Of Computer Engineering at Dr. D. Y. Patil School of Engineering, Charoli, Lohegaon, Pune.