ISSN:0975-9646

Handling Non-Linear Attacks in Multilevel Trust Privacy Preserving Data Mining

Kamaleswari S[1], Balachander T[2]

[1]*M.Tech, Computer Science and Engineering, SRM University, Chennai, India*
[2]*Asst.Professor, Department of Computer Science and Engineering, SRM University, Chennai, India*

***Abstract*— Privacy Preserving Data Mining (PPDM) is the primary task of data mining to develop accurate models about aggregated data, without being able to access precise information in individual data records. Perturbation-based PPDM approach perturbs the correct data with some kind of known random noise and report the noisy data to the data miner. The scope of perturbation-based PPDM is expanded to Multilevel Trust (MLT-PPDM) which allows multiple differently perturbed copies of the same data to be available to data miners at different trusted levels. Under this setting, a malicious data miner may have access to differently perturbed copies of the same data through various means and may combine these diverse copies to jointly infer additional information about the original data that the data owner does not intend to release. The key challenge of providing MLT-PPDM services is to prevent such diversity attacks. Previous solutions of this approach are limited in their assumption that adversaries perform only linear estimation attacks. More powerful adversaries may apply nonlinear techniques to derive original data and recover more information. In this work, this assumption is relaxed and the solution can handle non-linear estimation attacks.**

***Keywords*— Multilevel Trust, Privacy Preserving Data Mining, Random Perturbation, Non-Linear Estimation.**

I. INTRODUCTION

Privacy Preserving Data Mining (PPDM) is aimed at bridging the gap between collaborative data mining and data confidentiality and it involves many areas such as statistics, computer sciences, and social sciences. It is of fundamental importance to homeland security, modern science, and to our society in general. Data perturbation techniques are one of the most popular models for privacy preserving data mining [1, 2]. It is especially convenient for applications where the data owners need to export/publish the privacy sensitive data. The data perturbation procedure can be described as follows. The data owner before publishing the data, randomly introduce uncertainty about individual values in certain way to disguise the sensitive information while preserving the particular data property that is critical for building the data models [3], [5], [6], [7], [8], [9].

Under the single trust level scenario, a data owner generates only one perturbed copy of its data with a fixed amount of uncertainty. In contrast to the single level trust approach, now multiple differently perturbed copies of the same data are available to data miners at different trusted levels known as the Multilevel Trust (MLT). The more trusted a data miner is the less perturbed copy it can access; it may also have access to the perturbed copies available at lower trust levels. A data miner could also access multiple perturbed copies through various other means such as accidental leakage or colluding with others.

The data miner may be able to produce a more accurate reconstruction of the original data, by utilizing diversity across differently perturbed copies. This attack is referred as a diversity attack. Preventing diversity attacks is the key challenge in solving the MLT-PPDM problem, which is addressed in this paper. In particular, the additive perturbation approach is focused where random Gaussian noise is added to the original data with arbitrary distribution, and a systematic solution is provided to handle non-linear estimation attacks.

II. RELATED WORK

Privacy Preserving Data Mining (PPDM) was first proposed in [1] and [9] simultaneously. Researchers have since proposed various solutions to address this problem that fall into two broad categories based on the level of privacy protection they provide. Secure Multiparty Computation (SMC) approach is the first category which provides the strongest level of privacy; it enables mutually distrustful entities to mine their collective data without revealing anything except for what can be inferred from an entity's own input and the output of the mining operation alone. The second category of the partial information hiding approach trades privacy with improved performance in the sense that malicious data miners may infer certain properties of the original data from the disguised data.

The partial information hiding approach can be further divided into three categories: 1) k-anonymity [2], [10], [11], 2) retention replacement (which retains an element with probability p or replaces it with an element selected from a probability distribution function on the domain of the elements) [12], [13], and 3) data perturbation (which introduces uncertainty about individual values before data are published) [1], [3], [4], [5], [6], [7],[14].

The data perturbation approach includes two main classes of methods: additive [1],[3],[5],[6],[14] and matrix multiplicative [4], [7] schemes. These methods apply mainly to continuous data. A multiplicative random projection matrix for privacy preserving distributed data mining was proposed in [7]. Here the problem is directly related to many other data-mining problems such as clustering the similar data, principal component analysis, and classification of data.

Privacy preserving distributed data mining proves that, after perturbation, the distance-related statistical properties of the original data are still well maintained without exposing the dimensionality and the exact data values. The random projection-based technique may be even more powerful when used with some other geometric transformation techniques like scaling, translation, and rotation. Combining this with SMC-based techniques offers another interesting direction.

Multilevel privacy preserving for additive Gaussian noise perturbation was proposed in [14] where a measure was used based on how closely the original values can be reconstructed from the perturbed data. Since it was based on Gaussian noise perturbation, the solution was more suitable for high dimensional data. Reconstruction errors under independence noise were discussed and the security of the scheme was analyzed when collusion occurs, and the computational complexities based on Kroneckor product were studied. It is limited in the sense that it considers only linear attacks. But more powerful adversaries may apply nonlinear techniques to derive original data and recover more information.

III. Proposed Work

In the Multilevel Trust Privacy Preserving Data Mining (MLT-PPDM) problem, a data owner trusts data miners at different levels, M, and generates a series of perturbed copies of its data for different trust levels which is done by adding varying amount of noise to the data. Under the multilevel trust scenario, data miners at higher trust levels can access less perturbed copies. But such less perturbed copies are not accessible by data miners at lower trust levels. At different trust levels, data miners may also collude to share the perturbed copies among themselves. Hence, it is common that data miners can have access to more than one perturbed copy.

Malicious data miners will always attempt to reconstruct a more accurate estimate of the original data given perturbed copies. Hence the terms data miners and adversaries can be used interchangeably. In MLT-PPDM, adversaries may have access to a subset of the perturbed copies of the data. The goal of an adversary is to reconstruct the original data as accurately as possible based on all available perturbed copies.

The reconstruction accuracy depends heavily on the adversaries' knowledge. The same assumption as the one in [5] is made that adversaries have the knowledge of the statistics of the original data and the noise. In addition, it is also assumed that adversaries only perform nonlinear estimation attacks, where estimates can only be nonlinear functions of the perturbed data. Among the family of nonlinear reconstruction methods, nonlinear least squares error estimation is used to check the error between the estimated value and the original value.

The noise added at different levels is properly correlated so that jointly reconstruction of the original data using various copies across M trust levels will be made difficult. Thus the joint estimation based on all existing copies is only as good as the estimation based on the copy with the minimum privacy, and there is no diversity gain in performing the nonlinear estimation jointly.

The following Fig.1 shows the block diagram of the proposed system using non-linear estimation.

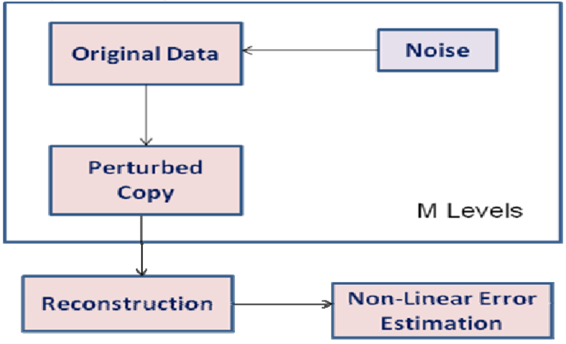

Fig.1 Block Diagram

IV. Implementation details

A network is constructed which consists of a server and the users who may be either the data owner who uploads the data or a consumer, generally the data miner who makes use of the published data. The data owner defines all possible trust levels, say M a priori. The data miners should register themselves with the server so that they will be later authenticated and allowed to access the perturbed copies. The data owner uploads the original dataset on to the server and the sensitive attributes are extracted from it. Perturbed copy for all M levels are generated in one single batch by adding properly correlated noise [14] to the original data. After which the generated perturbed copies are published to the data miners according to their trust level. Reconstruction is made from all the available perturbed copies using nonlinear least square error estimation technique and the estimation error is obtained to be same or greater than the error obtained from the least perturbed copy showing that there is no diversity gain in performing the nonlinear estimation jointly.

Below shown Fig.2 depicts the functional architecture of how the privacy can be preserved by making use of Non-linear techniques in the proposed system.

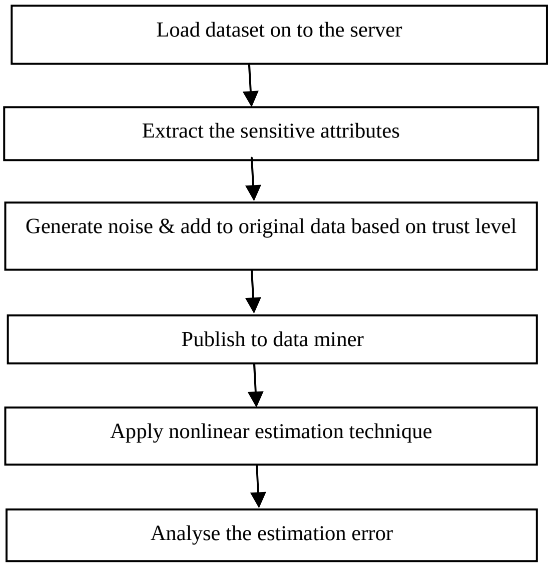
Load dataset on to the server
Extract the sensitive attributes
Generate noise & add to original data based on trust level
Publish to data miner
Apply nonlinear estimation technique
Analyse the estimation error

Fig.2 Functional Architecture

A. *Generation of Perturbed Copies*

Multiple differently perturbed copies of the same data are generated and made available to data miners at different trusted levels. The data owner determines the M trust levels. Additive perturbation [14] is the technique used to obtain the perturbed copies. It is the technique which adds some random noise, Z, to the original data, X, to obtain the perturbed copy, Y as Y = X + Z. This approach tries to preserve data privacy by adding random noise and also it makes sure that the random noise still preserves the original data from so that it can still be accurately estimated. All the M copies are generated in a single batch. In this case all trust levels are predefined.

B. *Reconstruction of Original Data*

Reconstruction of the original data is done by collecting sample perturbed copies from different levels. Nonlinear estimation technique is used to generate the estimate of original data from the perturbed copies. Estimates are obtained for single perturbed copies and also by jointly combining several perturbed copies. An assumption is made that the adversaries will have partial knowledge about the original data and the random noise which was added.

C. *Analysis of Estimation Error*

Data miners can access one or more perturbed copies, either by collusion among themselves or according to the application scenario setting. It is assumed that data miners perform joint nonlinear least square estimation to reconstruct X and also the data miners can access all the M perturbed copies. This scenario represents the most severe attack where data miners jointly estimate X using all the available M perturbed copies. The error in the estimate obtained from single perturbed copy and the error in the estimate obtained from colluding several perturbed copies are compared and analysed. The analysis implies that the joint estimation based on all existing copies is only as good as the estimation based on the copy with the minimum privacy, and there is no diversity gain in performing the nonlinear least square estimation jointly.

V. CONCLUSION

The key challenge in MLT-PPDM lies in preventing the data miners from combining copies at different trust levels to jointly reconstruct the original data more accurate than what is allowed by the data owner. This challenge is addressed by properly correlating noise across copies at different trust levels. Most existing work on perturbation-based PPDM is limited in the sense that it considers only linear attacks. But more powerful adversaries may apply nonlinear techniques to derive original data and recover more information which is considered in this work. Many interesting and important directions can be explored further. For example, it is not clear how to expand the scope of other approaches in the area of partial information hiding, such as retention replacement, random rotation-based data perturbation and k-anonymity to multilevel trust. Extending this approach to handle evolving data streams is also of great interest.

ACKNOWLEDGMENT

The authors are grateful to express sincere thanks and gratitude to our Professor and HOD, Dr.E.Poovammal, Department of Computer Science and Engineering, SRM University for her encouragement and the facilities that were offered to us for carrying out this project. And we take this opportunity to thank our Director, Dr.C.Muthamizchelvan, Ph.D, Faculty of Engineering and Technology, SRM University for providing us with excellent infrastructure that is required for the development of our project.

REFERENCES

[1] R. Agrawal and R. Srikant. Privacy-preserving data mining. Proc. of ACM SIGMOD Conference, 2000.

[2] C.C. Aggarwal and P.S. Yu, “A Condensation Approach to Privacy Preserving Data Mining,” Proc. Int’l Conf. Extending Database Technology (EDBT), 2004.

[3] 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.

[4] K. Chen and L. Liu, “Privacy Preserving Data Classification with Rotation Perturbation,” Proc. IEEE Fifth Int’l Conf. Data Mining, 2005.

[5] Z. Huang, W. Du, and B. Chen, “Deriving Private Information From Randomized Data,” Proc. ACM SIGMOD Int’l Conf. Management of Data (SIGMOD), 2005.

[6] 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.

[7] 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.

[8] S. Papadimitriou, F. Li, G. Kollios, and P.S. Yu, “Time Series Compressibility and Privacy,” Proc. 33rd Int’l Conf. Very Large Data Bases (VLDB ’07), 2007.

[9] Y. Lindell and B. Pinkas, “Privacy Preserving Data Mining,” Proc.Int’l Cryptology Conf. (CRYPTO), 2000.

[10] E. Bertino, B.C. Ooi, Y. Yang, and R.H. Deng, “Privacy and Ownership Preserving of Outsourced Medical Data,” Proc. 21st Int’l Conf. Data Eng. (ICDE), 2005.

[11] D. Kifer and J.E. Gehrke, “Injecting Utility Into Anonymized Datasets,” Proc. ACM SIGMOD Int’l Conf. Management of Data, 2006.

[12] Agrawal, R. Srikant, and D. Thomas, “Privacy Preserving OLAP,” Proc. ACM SIGMOD Int’l Conf. Management of Data, 2005.

[13] W. Du and Z. Zhan, “Using Randomized Response Techniques for Privacy-Preserving Data Mining,” Proc. ACM SIGKDD Int’l Conf.Knowledge Discovery and Data Mining, 2003.

[14] Yaping Li, Minghua Chen, Qiwei Li, and Wei Zhang, “Enabling Multilevel Trust in Privacy Preserving Data Mining”, IEEE Trans. Knowledge and Data Eng., vol. 24, no. 9,pp.1598-1612, Sep. 2012.