A SURVEY ON PRIVACY-PRESERVING DATA MINING TECHNIQUES

D.Kavitha
Research scholar
Assistant Professor**,** CSE Department, Institute of Aeronautical Engineering. Hyderabad, Telangana, India.

Dr. T.Adilakshmi
Supervisor
Professor and HOD, CSE Department, Vasavi College of Engineering Hyderabad, Telangana, India.

Dr. M.ChandraMohan
Co-Supervisor
Additional Controller of Exams, JNTU, Kukatpally, Hyderabad, Telangana, India.

ABSTRACT

Privacy-preserving Data Mining (PPDM) is the process of hiding and protecting sensitive data of individuals. The enormous amount of detailed private data is recurrently collected and analyzed by applications using data mining, sharing of these data is useful to the application users. While sharing private data, PPDM is becoming an increasingly significant issue. Since the last two decades, many Privacy-Preserving Data Mining techniques are used today. This paper presents various methods which are used to perform PPDM procedures and also tabulates their advantages and disadvantages.

Keywords: Data Mining, Privacy-Preserving, Privacy-Preserving Data Mining Techniques**.**

I. INTRODUCTION

Data mining is the process of extracting useful information from the massive amount of data stored in databases, data warehouses, and other information repositories. The mined data can be a frequent pattern, association rules, clusters and classification models. During the whole process of data mining this data typically holds sensitive individual information such as medical and Financial data. The massive amount of data available means that it is possible to acquire knowledge of a lot of information about individuals from public data. Privacy-preserving has started as an essential concern concerning the favorable outcome of data mining. Privacy-preserving data mining (PPDM) deals with protecting

the privacy of individual data or sensitive data without sacrificing the usefulness of the data. In recent years, the area of privacy has become aware of fast advances because of the increases in the power to store data.

In particular, recent advances in the data mining field have led to privacy-preserving techniques.The goal of privacy-preserving data mining(PPDM) algorithms is to mine useful information from vast amounts of data while protecting sensitive information at the same time.

Many privacy-preserving methods have been proposed for data mining and machine learning such as decision tree classification, clustering, association rule mining, Neural Networks, and Bayesian Belief Networks. The most important concern of these algorithms is to preserve the privacy of different parties' sensitive data. One of the most difficulties in data mining is the process of discovering frequent itemsets and, consequently, association rules. Association rule mining is usually used in various fields. Most of the privacy-preserving data mining techniques put in an application for a transformation which reduces the use of the underlying data when it is applied to data mining techniques or algorithms.

Privacy concerns can keep away from the building of a centralized warehouse – scattered among several places; no one is allowed to transfer their data to a different location. In preserving the privacy of data, the problem is how securely results are gained but not with data mining results but. As an example, suppose some hospitals want to get useful aggregated knowledge about a specific diagnosis from their patients‟ records while each hospital is not allowed, due to the privacy acts, to make known individuals‟ private data.

Therefore, they call to run a common and secure protocol on their distributed database to reach the required information. In many cases data is assigned and fetching the data collected in one position for analysis is not possible due these privacy acts or regulation. Mining association rules require iterative scanning of the database, which is quite expensive, in processing. These techniques can be demonstrated in centralize as well as a distributed environment where data can be varying among the different sites. Distributed database scenarios can be classified in horizontally partitioned data and vertically partitioned data.

1. Horizontally partitioned data: It divides the database into some separate horizontal partitions. In this type of data, different places have a mixed record of the same entities which are used for mining purposes. Many of these methods use specialized versions of the common approaches discussed for various problems.

The below figure gives a snapshot of Horizontally partitioned data.

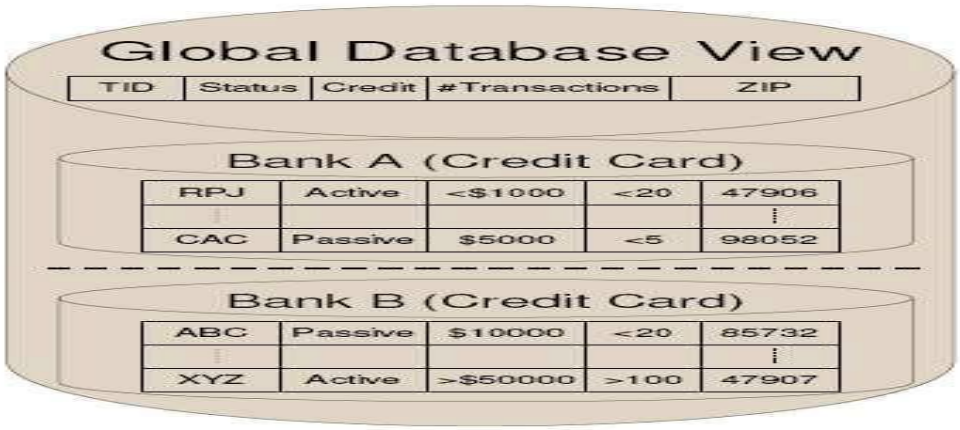

Fig 1.Horizontal Partitioning

2. Vertically partitioned data: In Vertically partitioned data sets; each site has a different number of attributes with the same amount of the transaction. The technique, of vertically partitioned mining, has been expanding to a variety of data mining applications such as decision trees, SVM Classification, Naïve Bayes Classifier, and k-means clustering.

The below figure gives a snapshot of vertically partitioned data.

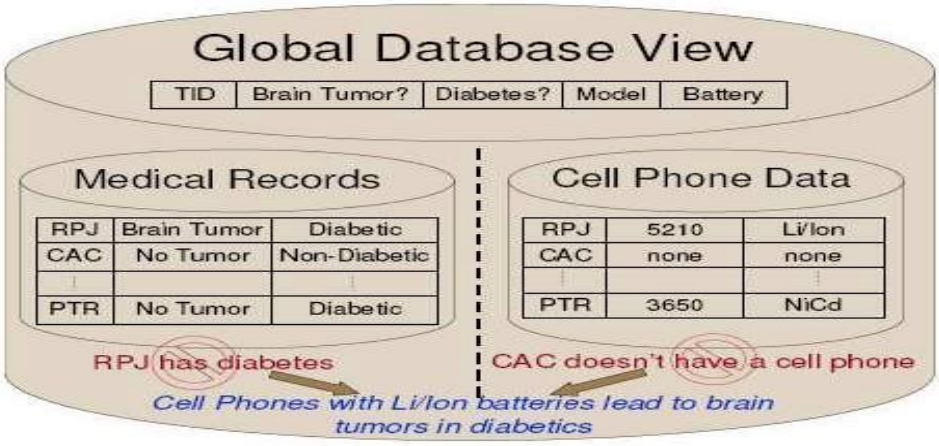

Fig 2.Vertical Partitioning

1.1. PPDM Framework

Data mining is the process of mining knowledge from large amounts of data in data warehouses[1]. The extracted knowledge can be used for decision making, process, information management, query processing and so on. Nowadays, data mining is used widely in many applications, and the massive volume of data is collected. As data mining extracts information from large databases, which may make the data vulnerable and lead to misuse. Some examples of sensitive data are credit card/debit card details, criminal records, medical history, identity information, etc. Thus, it is necessary to have some privacy policy to secure the sensitive personal data of individuals.

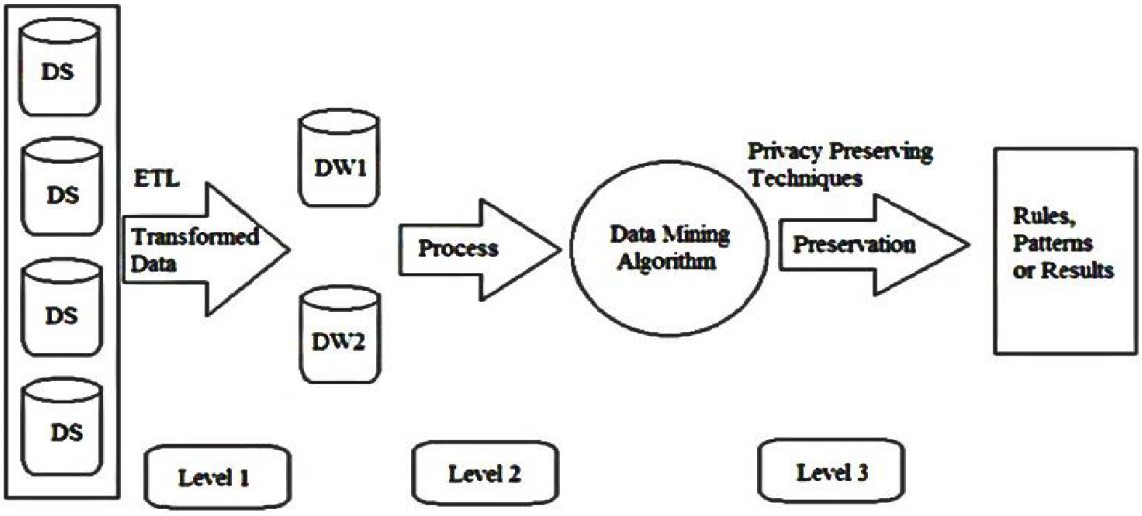

Figure 3. Framework for Privacy Preserving Data Mining

In the recent era, Privacy-Preserving Data Mining has emerged as a critical research area. Privacy Preserving Data Mining deals with protecting individual's sensitive data.

This paper presents a detailed and comparative survey on recent algorithms developed for achieving Privacy Preserving Data mining. The following Privacy Preserving Data Mining techniques have been studied and analyzed in this paper: - Data Perturbation approach, Anonymization approach, and Cryptographic approach. (M. B. Malik, M. A. Ghazi, and R. Ali) introduced a framework for Privacy Preserving Data Mining shown in Figure 4. Data from different data sources are aggregated and pre-processed by using ETL tools.

The transformed data from Level 1 are stored in data warehouses. In Level 2, data mining algorithms are applied to the data in the warehouse to find the patterns and discover the knowledge. In Level 3, mining privacy preservation techniques are used to protect data from unauthorized access.

2. Techniques

Developing data mining practices that do not increase the risk of misuse [2] of data of an individual and not degrade the use of information is the primary goal of PPDM. A majority of these techniques modify the raw data in some form for attaining privacy preservation. Then, the modified data which is ready to mine should comply with privacy needs and at the same time not lose the [2] benefit of the process of mining. The particular information regarding a person gets stored in the form of a table (that is, a relation) of rows (or records) and columns (or attributes), as stated by [3]. Many privacy-preserving techniques about data publishing like cell suppression, randomization, data swapping, sampling, and perturbation are constructed for publication of microdata [4]. Privacy preservation has evolved through different stages of development. As the existing technique involves a level of complexity, the intention of privacy preservation is treated as a new research area. Personal

identifications are removed before the publication of information to mine data. Protection of privacy which has been considered as a crucial matter is attained by using various techniques.

Privacy-preserving data mining techniques can be classified into three major categories such as Perturbation, Anonymization and Cryptography are shown in Figure 4.

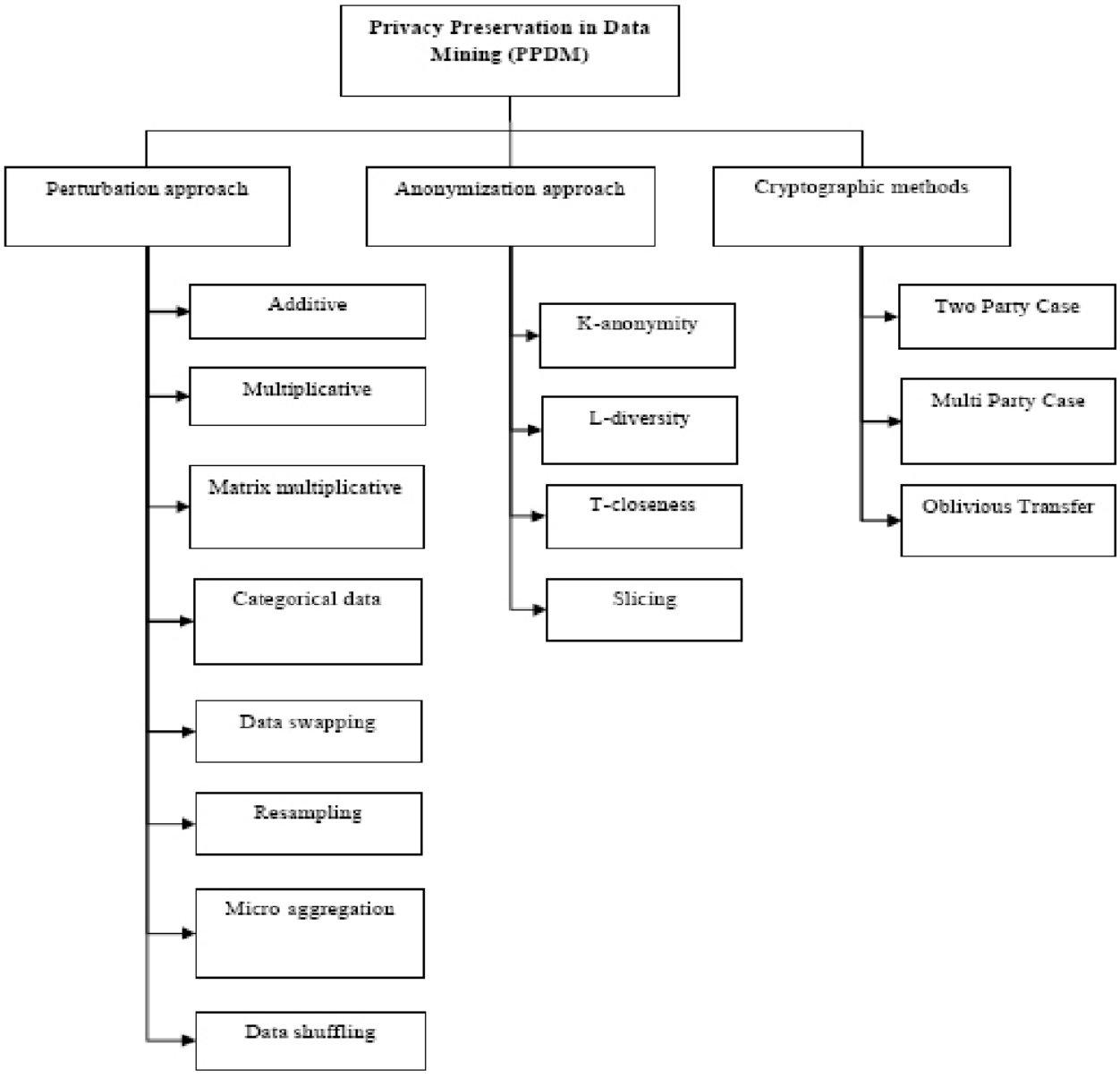

Figure 4. Classification of Privacy Preserving Data Mining Techniques.

2.1 Data Collection Privacy

To ensure privacy at data collection time, the sensory device transforms the raw data by randomizing the captured values, before sending them to the collector. The assumption is that the entity collecting the data is not to be trusted. Therefore, and to prevent privacy disclosure, the original values are never stored, and used only in the transformation process. Consequently, **randomization** must be performed individually for each captured value.

2.1.1 Perturbation

Data Perturbation [5, 6] is a method used to modify data with the use of the random process. Apparently, this method disfigures delicate data values through altering them by subtracting, adding, or by some other mathematical procedure. This method may be able to cope with various data types: Boolean type, character type, integer, and classification type. It is essential to preprocess the raw data set before entering the perturbation method. Perturbation of data is known by other names such as data noise and data distortion. Securing sensitive data is vital and critical, and the data perturbation process performs a crucial role in the preservation of delicate data. Distortion can be applied using various techniques like data rearrangement matrix, adding noise, by adding unfamiliar values, and so on. Randomization is considered as one of the frequently used approaches in PPDM research.

2.1.1(a) Randomization

This method involves adding noise to the actual data for creating values of each record. Perturbations mixed with authentic data are sufficiently enormous for maintaining privacy, and hence one cannot recover the actual data. Randomized Response scheme and random-noise-based perturbation help Randomization techniques to achieve both knowledge discovery and privacy preservation. Although involving a huge loss of information, this technique is comparatively a better and efficient process. Randomization proves to have the ability to preserve some semantics and anonymize the entire dataset. Among the currently used privacy preserving data mining methods. Randomization is treated as the crucial method. Harmony between utility and privacy [7] as well as knowledge discovery are provided by this. After being balanced, the randomized data gets transmitted to the concerned recipient. Using a distribution reconstruction algorithm, the recipient will receive the data. This method offers an effective and simple way of ensuring the person's privacy and also preserving the use of data to some extent.

Table 1.Summary of the Privacy preserving techniques at data collection

Scenario: At data collection, an untrustworthy collector adversary may gather and improperly use private, sensitive data from individuals. Randomization is employed to transform the original data to prevent privacy disclosure. The original data is not further used, not stored.			
Randomization Method	**Description**	**Advantages and Disadvantages**	**Applications**
Additive Noise [8]	Data is randomized by adding noise with a known statistical distribution.	[+] Performs independently for each captured value (suitable for data collection) [+] Preserves statistical properties after reconstruction of the original distribution. [-] limits data utility to the use of aggregate distributions. [-] masking extreme values (such as outliers) requires a great quantity of noise, severely degrading data utility. [-] Noise reduction techniques can be used to accurately estimate the original individual values.	[9,10]
Multiplicative Noise[11]	Data is randomized by multiplying noise with a known statistical distribution.	[+] More effective than additive noise at preserving privacy, since the reconstruction of the original individual values is more difficult. [+] Performs independently for each captured value (suitable for data collection) [+] Preserves statistical properties after reconstruction of the original distribution. [-] limits data utility to the use of aggregate distributions. [-] Making extreme values (such as outliers) requires great quantities of noise, severely degrading data utility.	[12,13]

2.2 DATA Publishing Privacy

Entities may wish to release data collections either publicly or to third parties for data analysis without disclosing the ownership of the sensitive data. In this situation, preservation of privacy can be achieved by anonymizing the records before publishing. PPDM at data publishing is also known as Privacy Preserving Data Publishing (PPDP). Anonymization is considered as one of the frequently used approaches in PPDM research.

2.2.1 Anonymization

Information is frequently published through the removal of important identity indicators like social security number and name from individual records. Even so, the combination of different attributes from different datasets (quasi-identifiers) may be used for identifying individual records accurately. For instance, certain attributes like birth, race, zip, and sex appear in voter list. If such indicators appear in a sensitive database such as medical data, quasi-identifiers are employed for gathering identification of the concerned person by linking the two datasets together.

2.2.1(a) k-anonymity

In many applications, the data records are made available by simply removing key identifiers such as the name and social security numbers from personal records. However, other kinds of attributes (known as pseudo-identifiers) can be used to accurately identify the records. For example, attributes such as age, zip-code, and sex are available in public records such as census rolls. When these attributes are also available in a given dataset, they can be used to infer the identity of the corresponding individual. A combination of these attributes can be very powerful since they can be used to narrow down the possibilities to a small number of individuals. In *k*-anonymity techniques, we reduce the granularity of representation of these pseudo-identifiers with the use of techniques such as *generalization* and *suppression*. In the method of *generalization*, the attribute values are generalized to a range to reduce the granularity of representation. For example, the date of birth could be generalized to a range such as year of birth, to reduce the risk of identification. In the method of *suppression*, the value of the attribute is removed completely. It is obvious that while such strategies reduce identification risk in the public records usage, they reduce the precision of operations on the modified data. Including this two more attacks called homogeneity attack and background knowledge attack [14] is also possible in this method.

2.2.1(b) L-diversity

The two major attacks called Homogeneity attack and background knowledge attack lead to the creation of a new technique called l-diversity which is an advancement of the k-anonymity model where it protects privacy even though the data owner is not aware of any information that the intruder holds [14]. This method is derived from the k-anonymity model where k records in the dataset will match with k-1 other data in the records with reduction of the scale or level of detail from the dataset to form an l-diverse dataset.

Definition: *Let a q*-block be a set of tuples such that its non-sensitive values generalize to q*. A q*-block is l-diverse if it contains l"well represented" values for the sensitive attribute S. A table is l-diverse if every q* - block in it is l-diverse.*

2.2.1(c) T-closeness

To achieve l-diversity, every set of records in the dataset which approves k-anonymity needs to have l well-represented values for each sensitive attribute. In addition to this, the previous technique cannot safeguard the dataset from disclosure of the attributes. For these cases, the t-closeness method was discovered, and it overcomes the problem of k-anonymity and l-diversity.

The t-closeness concept which we have introduced in this section is defined by [15].Every dataset assumes to satisfy t-closeness if every equivalence classes have t-closeness. The model of t-closeness is an enhancement of the l-diversity model. An important feature of the l-diversity model is that it takes all given value attributes in the same way irrespective of its dispensation in the data.

Table 2.Summary of the Privacy preserving techniques at data publishing regarding the employed sanitization methods.

Scenario: Entities may seek to publish their data publicly for further research, and analysis. However, malicious individuals/adversaries may attempt to de-anatomize or target record owners for malevolent purposes. Privacy models are implemented to the datasets before the release, as to effectively anonymize records.				
Privacy Model	**Sanitization Method**	**Description**	**Advantages and Disadvantages**	**Applications and Domains**
K-anonymity [16], [17]	Generalization, Suppression	Anonymity is guaranteed by the existence of at least other K-1undistinguishable (w.r.t the QID) records for each record in a database. This group of K distinguishable records is referred to as an equivalence class.	[+] Simplicity of definition. [+] great amount of existing algorithms. [-] Assumes that each record represents a unique individual. If this is not the case, an equivalence class with K records does not necessarily like to K different individuals. [-] Sensitive attributes are not taken into consideration for the anonymization, which can	1. Wireless sensor networks [18]. 2. Location-based services [19, 20]. 3. Cloud [21]. 4. E-health [22].

			disclose information, Especially if all records in a class have the same value for the sensitive attribute.	
l-diversity[23]	Generalization, Suppression	Expands the K-anonymity model by requiring every equivalence class to have at least *l* "well represented" value for the sensitive attributes.	[+] The diversity of sensitive attribute values is taken into consideration for the anonymization. [-] Does not take into consideration the distribution of the sensitive values, which can lead to privacy branches when the sensitive values are distributed in a skewed way.	1. E-health [22]. 2. Location-based services [20], [25], [26].
t-closeness[27]	Generalization, Suppression	Solve the *l*-diversity problem of skewed sensitive values distribution by requiring that the distribution of the sensitive values in each equivalence class to be "close" to the corresponding distribution in the original table, where close means upper bounded by a threshold *t*.	[+] Takes into consideration the distribution of the sensitive values when forming the equivalence classes. [-]The information about the correlation between quasi-identifier attributes and sensitive attributes is lost as *t* decreases (as privacy increases).	1. Location-based services [28].

2.3 Cryptography

Cryptography is one method used to preserve sensitive data. The cryptographic technique is very much favored as it offers safety and security of sensitive attributes, and was suggested by authors in [29]. The privacy of a person's record may be broken for final data mining. Consider for example a situation in which several medical institutions look for conducting a joint study on the datasets for certain mutual benefits, while not disclosing unwanted information. It is possible that sometimes when a data mining algorithm is passed to a dataset formed by combining two data sets, there is some possibility that the results may disclose private information about the individual. But, this kind of leakage is inevitable.

2.3.1 The Two Party Case

A protocol called constant-round was proposed by [30] for calculating any probabilistic polynomial time function (the opponent is malicious or partly honest). Consider two parties with inputs a and b as an example. These two parties are very much interested in performing functionality jointly to their inputs for some mutual benefits. Let the functionality be g(x,y)= (g1(x,y),g2(x,y)). Finally, g1(x,y) is given to the first

party, and g2(x,y) is given to the second party. The security here is that only the output is shared with the parties. Other than the output, parties can't learn anything about the protocol.

2.3.2 The Multiparty Case

The protocols of the multiparty case allow the participants to calculate their inputs with a combined method as well as not leaking related data regarding the inputs. Which means the parties are able to evaluate the function by protecting the privacy of the input as in the previous model. This was achieved and demonstrated by many researchers in [31-33], for various scenarios. The protocol of multi-party case needs every pair of parties to interchange messages so that each gate of the circuit can compute functions effectively. But this is impossible in some situations like web applications. Because the application running between the server and the client does not support effective communication between every pair of parties. Another overhead in this scenario is communication and computations are linear to each other concerning the size of the circuit.

2.3.3 Oblivious Transfer

This protocol is considered to be an important building block for protected computation. The idea of 1-out-2 oblivious protocol was proposed by [34]. In the protocol of oblivious transfer, two parties are required, a sender and a recipient. Sender's input is a pair (X0, X1) and receiver's input is Q € {0, 1}. After the protocol ends sender cannot learn anything and receiver can only learn X_Q. Although the accuracy and security of altered data are ensured in Cryptographic methods, when several participants are involved, this approach falls short of delivering. Furthermore, confidentiality of individual records may be breached by the data mining results. Although there are a lot of solutions while using semi-honest models, a very low number of studies has been conducted when it comes to malicious models.

The advantages and limitations of all PPDM techniques are tabulated in Table 3.

Table 3. Advantages and Limitations of PPDM Techniques

Technique	Advantages	Limitations
Perturbation technique of PPDM	Preserves various attributes independently.	Information loss and Cannot regenerate original data values.
Randomized Response technique of PPDM	It provides good efficiency. Simple and useful for keeping the individual information secretly	The loss of an individual's information. Not much good for database containing several attributes

Anonymization technique of PPDM	Data owner's sensitive or private data are to be secreted.	More information loss, Linking attack.
Cryptography technique of PPDM	Data transformation is accurate and protected. Provides better privacy and data utility.	It is particularly hard to scale if multiple parties are involved.

3. Conclusion

The primary objective of PPDM is promoting algorithms to conceal sensitive data or offer privacy. These sensitive data do not get revealed to unapproved parties or invaders. In data mining, there exists a trade-off between utility and privacy of data. When we accomplish one, it inevitably leads to a detrimental impact on the other. Many PPDM techniques in existence are reviewed in the paper. Ultimately, it is concluded with the fact that there is no single PPDM technique in existence that outshines every other technique with relation to each possible criterion such as the use of data, performance, difficulty, compatibility with procedures for data mining, and so on. A particular algorithm may function better when compared to another, on a specific criterion. Researchers are doing extensive research in ensuring that the sensitive data of the individual is not revealed as well as not compromising the utility of data so that the data can be useful for many purposes.

IV. REFERENCES

[1] J. Han and M. Kamber, "Data Mining: Concepts and Techniques," 3rd edition.

[2] Wang PS. Survey on Privacy Preserving Data Mining. International Journal of Digital Content Technology and its Applications. 2010; 4(9):1–7. https://doi.org/10.4156/jdcta.vol4.issue9.1

[3]. Latanya S. k-anonymity: a model for protecting privacy. International Journal of Uncertainty, Fuzziness, and Knowledge-based Systems. 2002 Oct; 10(5):557–70. https://doi.org/10.1142/S0218488502001648

[4]. Yan Z, Ming D, Jiajin L, Yongcheng L. A Survey on Privacy Preserving Approaches in Data Publishing. IEEE Computer Society. 2009; 128–31.
[5]. Jinfei L, Jun L, Joshua ZH. Rating: Privacy Preservation for Multiple Attributes with Different Sensitivity requirements. Proceedings of 11th IEEE International Conference on Data Mining Workshops, China, IEEE. 2011. p. 666–73.
[6]. Kargupta H, Datta S, Wang Q, Krishnamoorthy S. On the Privacy Preserving Properties of Random Data Perturbation Techniques. Proceedings of the Third IEEE International Conference on Data Mining USA. 2003. p. 99. https://doi.org/10.1109/ICDM.2003.1250908
[7]. Clifton C, Murat K, Jaideep V, Xiadong L, Michale YZ. Tools for privacy-preserving distributed data mining. ACM SIGKDD Explorations. 2002 Dec; 4(2):28–34. https://doi.org/10.1145/772862.772867
[8] R. Agrawal and R. Srikant, ``Privacy-preserving data mining," *ACM SIGMOD Rec.*, vol. 29, no. 2, pp. 439_450, 2000.
[9] C. Dwork, ``Differential privacy," in *Automata, Languages and Programming*, vol. 4052. Venice, Italy: Springer-Verlag, Jul. 2006, pp. 1_12.
[10] S. R. M. Oliveira and O. R. Za_ane, ``Privacy preserving clustering by data transformation," *J. Inf. Data Manage.*, vol. 1, no. 1, p. 37, 2010.
[11] J. J. Kim and W. E. Winkler, ``Multiplicative noise for masking continuous data," Statist. Res. Division, U.S. Bureau Census, Washington, DC, USA, Tech. Rep. 2003-01, 2003.
[12] J. J. Kim and W. E. Winkler, ``Multiplicative noise for masking continuous data," Statist. Res. Division, U.S. Bureau Census, Washington, DC, USA, Tech. Rep. 2003-01, 2003.
[13] K. Liu, H. Kargupta, and J. Ryan, ``Random projection-based multiplicative data perturbation for privacy-preserving distributed data mining," *IEEE Trans. Knowl. Data Eng.*, vol. 18, no. 1, pp.
[14]. Ashwin M, Johannes G, Daniel K, Muthuramakrishnan V. ℓ-Diversity: Privacy beyond k-Anonymity. ACM Transactions on Knowledge Discovery from Data. 2007 Mar; 1(1).
[15]. Ninghui L, Tiancheng L, Suresh V. t-Closeness: Privacy beyond K-Anonymity and l-Diversity. Proceedings of the IEEE 23rd International Conference on Data Engineering, Istanbul. 2007 Apr. p. 106–15.
[16] P. Samarati and L. Sweeney, ``Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression," in *Proc. IEEE Symp. Res. Secure. Privacy*, 1998, pp. 384_393.
[17] P. Samarati and L. Sweeney, ``Generalizing data to provide anonymity when disclosing information," in *Proc. PODS*, 1998, p. 188.
[18] M. M. Groat, W. Hey, and S. Forrest, ``KIPDA: k-indistinguishable privacy-preserving data aggregation in wireless sensor networks," in *Proc. IEEE INFOCOM*, Apr. 2011, pp. 2024_2032.
[19] A. R. Beresford and F. Stajano, ``Location privacy in pervasive computing," *IEEE Pervasive Comput.*, vol. 2, no. 1, pp. 46_55, Jan./Mar. 2003.
[20] B. Bamba, L. Liu, P. Pesti, and T.Wang, ``Supporting anonymous location queries in mobile environments with privacy grid," in *Proc. ACM 17th Int. Conf. World Wide Web*, 2008, pp. 237_246.

[21] X.-M. He, X. S. Wang, D. Li, and Y.-N. Hao, ``Semi-homogenous generalization: Improving homogenous generalization for privacy preservation in cloud computing," *J. Comput. Sci. Technol.*, vol. 31, no. 6, pp. 1124_1135, 2016.
[22] T. S. Gal, Z. Chen, and A. Gangopadhyay, ``A privacy protection model for patient data with multiple sensitive attributes," *Int. J. Inf. Secure. Privacy*, vol. 2, no. 3, p. 28, 2008.
[23] A. Machanavajjhala, D. Kifer, J. Gehrke, and M. Venkitasubramaniam, ```-diversity: Privacy beyond k-anonymity," *ACM Trans. Knowl. Discov- ery Data*, vol. 1, no. 1, p. 3, 2007.
[24] S. Kim, M. K. Sung, and Y. D. Chung, ``A framework to preserve the privacy of electronic health data streams," *J. Biomed. Inform.*, vol. 50, pp. 95_106, Aug. 2014.
[25] M. Xue, P. Kalnis, and H. K. Pung, ``Location diversity: Enhanced privacy protection in location based services," in *Location and Context Awareness*. Berlin, Germany: Springer-Verlag, 2009, pp. 70_87.
[26] F. Liu, K. A. Hua, and Y. Cai, ``Query l-diversity in location-based services," in *Proc. IEEE 10th Int. Conf. Mobile Data Manage. Syst., Services Middleware (MDM)*, May 2009, pp. 436_442.
[27] N. Li, T. Li, and S. Venkatasubramanian, ``t-closeness: Privacy beyond k-anonymity and l-diversity," in *Proc. IEEE 23rd Int. Conf. Data Eng. (ICDE)*, Apr. 2007, pp. 106_115.
[28] D. Riboni, L. Pareschi, C. Bettini, and S. Jajodia, ``Preserving anonymity of recurrent location-based queries," in *Proc. IEEE 16th Int. Symp. Temporal Represent. Reason. (TIME)*, Jul. 2009, pp. 62_69.
[29]. Data Perturbation and Features Selection in Preserving Privacy. Available from: http://ieeexplore.ieee.org/document/6335531/. Date Accessed: 20/09/2012.
[30]. Andrew CCY. How to generate and exchange secrets. Proceedings of the 27th Annual Symposium on Foundations of Computer Science (FOCS). 1987. p. 218–29. PMid: 3572436 PMCid: PMC1031495
[31]. Goldreich O, Micali S, Wigderson A. How to Play any Mental Game - A Completeness Theorem for Protocols with Honest Majority. Proceedings of the 19th Annual Symposium on the Theory of Computing, ACM, USA. 1987; 218–29.
[32]. Michale BO, Shafi G Wigderson A. Completeness theorems for non-cryptographic fault tolerant distributed computation, Proceedings of the 20th Annual Symposium on the Theory of Computing (STOC), ACM, and Israel. 1988; 1–10.
[33]. Bhanumathi S, Sakthivel P. Preservation of Private Information using Secure Multi-Party Computation. Indian Journal of Science and Technology. 2016 Apr; 9(14):1–6. https://doi.org/10.17485/ijst/2016/v9i14/74588
[34]. Shimon E, Oded G, Abraham L. A Randomized Protocol for Signing Contracts. Communications of the ACM. 1985 Jun; 28(6):637–47. https://doi.org/10.1145/3812.3818
92_106, Jan. 2006. [Online]. Available: http://dx.doi.org/10.1109/TKDE.2006.14