ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 9, September 2014

Privacy of Confidential Numerical Data

Vibhor Sharma [1], Shashi Bhushan[2], Ankur Choudhary[3], Sohan Lal[4]

Research Scholar, CSE, Tula's (The Engineering & Management College), Dehradun, India[1,3,4]

Assistant Professor, CSE, Tula's (The Engineering & Management College), Dehradun, India [2]

Abstract: In this paper, we have proposed a Dilation Based Transformation (DBT) algorithm for securing numerical attributes before they are shared for joint analysis. If we talk about the application of DBT, we have to consider horizontally partitioned data. So if this proposed work gets implemented we are able to preserve the privacy of confidential numerical data. If we are looking data for easily accessible locally by using distribution. We can use it for business growth. So for calculating meaningful, useful, previously unknown data from large databases, we used data mining technique and that for with preserving privacy use for shared data. So clustering on partitioned data and that for with preserving privacy of confidential data has been a vast area of research.

Keywords: DBT, Clustering, Classification, Data mining, Data Matrix.

I. INTRODUCTION

In knowledge discovery database process, we use data mining to extract useful information from large set of databases which is distributed locally among organizations for effective decision making and fruitful business growth. Data mining can be defined as the process of fetching of patterns in large datasets. Pattern means to extract useful and unknown knowledge from large data bases which can be used by organizations' personnel for effective decision making. The assumption of knowledge discovery database process is that the data is accessible at a centralized point through some access mechanism from different locations. Data aggregation can be used for this in which data from different sources are collected at a centralized point and then it can be analyzed. This process is not considered as data mining but the result of data preparation before analysis process. Security attack may take place in a situation when anyone gets access to the newly tested data and He/she is able to identify the individuals. In data mining process, there may be some problem when sensitive data is uncovered. Research community and government statistical agencies have a long term goal to provide security to sensitive data against unauthorized access. Hence, providing security to revealed data in the process of data mining techniques is an important area of research. When sharing of data takes place among organizations for effective business growth, there is a need to invent some techniques to preserve sensitivity of data among the communicating teams.

Classification and Prediction: Both classification and prediction are two important forms of data analysis which are used to fetch different models to describe classes and predict data trends in future. Both provide the best way to understand the large data from different data sets. For example, a classification model can be built to categorize the loan applications of a bank to verify that it is safe or risky and a prediction model can be built to predict all the expenditures. Some issues are there to prepare the data for classification and prediction. First is data cleaning, in which data is cleaned in the form of removing noise and clearing missing values. Second is relevance analysis in which attributes are identified that they are interrelated or not. Third one is Data transformation or consolidation using generalization or normalization.

Clustering: In clustering, data is partitioned in to a set of meaningful sub-classes which are called clusters. It is also called unsupervised classification. In this process, objects having similar properties are positioned in a class of objects. Objects having same characteristics are ordered in a common class. Partitioning is done by making a number of clusters. Each object belongs to one cluster. Different methods such as partitioning methods, Hierarchical agglomerative methods, SLINK (Single Link Method), CLINK (Complete Link Method), Group average methods are used for performing the clustering.

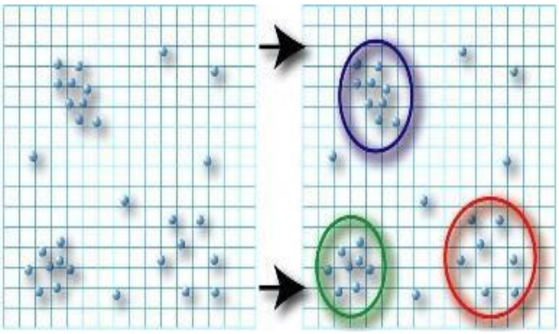
Association Rules: In data mining, these rules are used to analyze and predict customer behavior. These association rules are if/then statements to uncover the relationships between unrelated data in data base. For example, if a customer buys bread then there is 80% chance that he will purchase butter too. Two criteria support and confidence are used to identify the relationships among data. Support indicates how frequently a product appears in data base and confidence indicates the correctness of the statement.

Regression: Regression function is used to identify the relationship between dependent and independent variables. Dependent variables are those variables whose values are predicted and this prediction is based on independent variables. There are three types of regression models used in data mining: linear, logistic and polynomial regression. Linear model and polynomial model are used for dependent variables having numeric values. On the other hand, logistic regression is used for dependent variables having categorization.

Outlier Detection: In this process, Events, items, observations or objects are identified which do not generate an expected pattern. It is an unsupervised data mining function to identify the unusual cases. It is used to detect network intrusion, fraud and other doubtful events which are difficult to find. It is single-class classification because only one class of training data is presented to detect the anomalies. The classification process should be based on training data which holds the previous examples based on those, anomalies could be detected. Outlier detection can be categorized in three parts: First is Unsupervised anomaly detection, In this technique, unlabeled data is tested for finding anomalies which is based on the assumption that most of the instances are in normalized form in the data set. Second is supervised anomaly detection, in this technique, a training classifier is indulged and labelled data set either normal or abnormal is required. Third is Semi-supervised anomaly detection, in this technique, a model is developed which represents the normal behaviour of data based on the training data set.

II. CLUSTERING AND ITS CATEGORIZATION

Cluster analysis or clustering is the task of grouping a set of objects in such a way that objects in the same group (called cluster) are more similar (in some sense or another) to each other than to those in other groups (clusters). It is a main task of exploratory data mining, and a common technique for statistical data analysis used in many fields, including machine learning, pattern recognition, image analysis, information retrieval, and bioinformatics.



The goal of clustering analysis is to find high-quality clusters such that the inter-cluster similarity is low and the intra-cluster similarity is high. Clustering, like classification, is used to segment the data. Unlike classification, clustering models segment data into groups that were not previously defined which is known as unsupervised learning. Classification models segment data by assigning it to previously-defined classes, which are specified in a target and is known as supervised learning. Clustering models do not use a target. Clustering is useful for exploring data. If there are many cases and no obvious groupings, clustering algorithms can be used to find natural groupings. Clustering can also serve as a useful data-preprocessing step to identify homogeneous groups on which to build supervised models.

In image recognition, clustering can be used to discover clusters in handwritten character recognition systems. Suppose we have a dataset of handwritten digits, where each digit is labeled as either 1,2,3 and so on. Note that there can be a large variance in the way in which people write the same digit. Take the number 2, for example. Some people may write it with a small circle at left bottom part, while some may not. Clustering can be used to determine subclasses for '2', each of which represents a variation on the way in which 2 can be written. Using multiple models based on the subclasses can improve overall recognition accuracy.

Clustering has also found many applications in Web search. For example, a keyword search may often return a very large number of hits due to extremely large number of web pages. Clustering can be used to organize the search results into groups and present the results in a concise and easily accessible way. Clustering techniques have been developed to cluster documents into topics, which are commonly used in information retrieval practice.

As a data mining function, cluster analysis can be used as a standalone tool to gain insight into distribution of data, to observe the characteristics of each cluster, and to focus on a particular step for other algorithm. As a cluster is a collection of data objects that are similar to one another within the cluster and dissimilar to objects in other clusters, a cluster of data objects can be treated as an implicit class. So, with respect to this clustering is sometimes also called automatic classification.

Clustering is known as **unsupervised learning** because the class label information is not present. Hence, clustering is a form of learning by observation, rather than learning by examples.

Categorization of Clustering Algorithms:

Major clustering methods as mentioned in [33] can be classified into following categories:

1) Partitioning methods: A partitioning method constructs *k* partitions of dataset, where each partition represents a cluster and $k \le n$, where n is number of objects. It classifies the data into k groups such that a) Each group must contain at least one object and b) each object must belong to exactly one group. Given k, the number of partitions to construct, a partitioning method creates an initial partitioning. It then uses an iterative relocation technique which attempts to improve the partitioning by moving objects from one cluster to another.

Most partitioning methods are distance-based. Given.
Achieving global optimality in partitioning-based clustering is often computationally prohibitive, potentially requiring an exhaustive enumeration of all the possible partitions. Instead, most applications adopt popular heuristic methods, such as greedy approaches like k-means and k-medoids, which progressively improves the cluster quality and approach a local optimum.
e.g 1) k-means
2) k-medoids

2) Hierarchical methods: A hierarchical method creates a hierarchical decomposition of the given data objects. It can further be classified as *agglomerative* or *divisive*, based on how the hierarchical decomposition is formed. The *agglomerative(bottom-up)* approach starts with each object forming a separate group. It successively merges the objects or groups close to one another, until all of the groups are merged into one or until a termination condition holds. The *divisive (top-down)* approach starts with all objects in the same cluster. In each successive iteration, a cluster is split up into smaller clusters, until eventually each object is in one cluster, or until a termination condition holds.

3)Density-based methods: Most partitioning methods cluster objects based on the distance between objects. Such methods can find only spherical-shaped clusters and encounter difficulty at discovering clusters of arbitrary shapes. Clustering methods have been developed based on the notion of *density*. The key idea is to keep expanding the cluster until density in the neighborhood exceeds some threshold. It means for each point within cluster, the neighborhood of a given radius has to contain at least a minimum number of points. Such methods can be used to filter outliers and discover clusters of different shapes.
Density based methods can divide a set of objects into multiple exclusive clusters, or a hierarchy of clusters. Typically, density based methods consider exclusive clusters only, and do not consider fuzzy clusters. Moreover, density based methods can be extended from full space to subspace clustering.

4) Grid Based methods: A grid-based method quantizes the object space into a finite number of cells which form a grid structure. It then performs all of the clustering operations on the grid structure. The main advantage of this approach is it s fast processing time which is typically independent of the number of data objects, and dependent only on the number of cells in each dimension in the quantized space. STING is the most typical example of grid based method.

Fig1: Method	General Characteristics
Fig2: Partitioning methods	Fig1: Find mutually exclusive clusters of spherical shape Fig2: - Distance based Fig3: - May use mean or medoid to represent cluster center Fig4: - Effective for small to medium size data sets
Fig5: Hierarchical methods	Figure 1. - Clustering is hierarchical decomposition Figure 2. - Cannot correct erroneous merges or splits
Fig7: Density-based methods	Fig7: - Can find arbitrarily shaped clusters Fig8: - Clusters are dense regions of objects in space that are separated by low density regions Fig9: - May filter outliers
Fig10: Grid-based methods	Fig10: - Use multi resolution grid data structure Fig11: - Fast processing time (typically independent of number of data objects)

TABLE 3.1 Classification of Clustering Algorithms

Here for the scope of this dissertation work only k-Means clustering method is used for obtaining results. So only this particular method is described in detail here.

III. A LOOK AT PRIVACY PRESERVING DATA MINING

Increasing network complexity, affording greater access, sharing information and a growing emphasis on the internet have made information security and privacy a major concern for individuals and organizations. Data mining is a well known technology for automatically and intelligently extracting knowledge from large amount of data. Such a process, however can also disclose sensitive information about individuals compromising the individual's right to privacy. Privacy preserving data mining(PPDM) is a new era of research in data mining. Its ultimate goal is to develop efficient algorithms that allow one to extract relevant knowledge from large amount of data, while prevent sensitive information from disclosure or inference. The problem of privacy-preserving data mining has become more important in recent years because of the increasing ability to store personal data about users, and the increasing sophistication of data mining algorithms to leverage this information.

Privacy and data mining can coexist. The problem with the above scenario is not the data mining results, but how they are obtained. If the results could be obtained without sharing information between the data sources, and the results were truly summary and could not be used to deduce private information, there would be no loss of privacy through data mining. While obtaining globally meaningful results without sharing information may seem impossible, it can be done.

The key directions in the field of privacy-preserving data mining as described in [4] are as follows:

Privacy-Preserving Data Publishing: These techniques tend to study different transformation methods associated with privacy. These techniques include methods such as *randomization*, *k-anonymity*, and *l-diversity*. Another related issue is how the perturbed data can be used in conjunction with classical data mining methods such as association rule mining. Other related problems include that of determining privacy-preserving methods to keep the underlying data useful (utility-based methods), or the problem of studying the different definitions of privacy, and how they compare in terms of effectiveness in different scenarios.

Changing the results of Data Mining Applications to preserve privacy:
In many cases, the results of data mining applications such as association rule or classification rule mining can compromise the privacy of the data. This has spawned a field of privacy in which the results of data mining algorithms such as association rule mining are modified in order to preserve the privacy of the data.

***Cryptographic Methods for Distributed Privacy*:** In many cases, the data may be distributed across multiple sites, and the owners of the data across these different sites may wish to compute a common function. In such cases, a variety of cryptographic protocols may be used in order to communicate among the different sites, so that secure function computation is possible without revealing sensitive information.

***Theoretical Challenges in High Dimensionality*:** Real data sets are usually extremely high dimensional and this makes the process of privacy preservation extremely difficult both from a computational and effectiveness point of view. It has been shown that opti k-anonymization is NP-hard.

Classification of PPDM
According to [16] work done in PPDM can be classified according to different categories. These are:

Data Distribution- The PPDM algorithms can be first divided into two major categories, centralized and distributed data, based on the distribution of data. In a centralized database environment, data are all stored in a single database; while, in a distributed database environment, data are stored in different databases. Distributed data scenarios can be further classified into horizontal and vertical data distributions. Horizontal distributions refer to the cases where different records of the same data attributes are resided in different places. While in a vertical data distribution, different attributes of the same record of data are resided in different places.

***Hiding Purposes* -** The PPDM algorithms can be further classified into two types, data hiding and rule hiding, according to the purposes of hiding. Data hiding refers to the cases where the sensitive data from original database like identity, name, and address that can be linked, directly or indirectly, to an individual person are hided. Majority of the PPDM algorithms used data hiding techniques. Most PPDM algorithms hide sensitive patterns by modifying data.

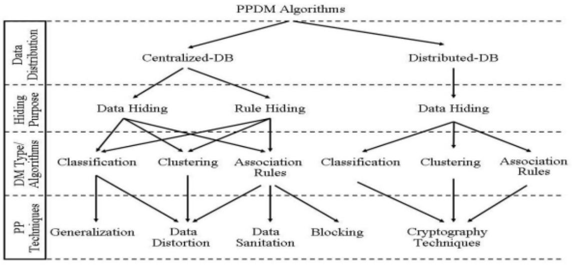


Fig. 4.2.1 Classification of PPDM Methods

Data Mining Tasks / Algorithms: Currently, the PPDM algorithms are mainly used on the tasks of classification, association rule and clustering. Association analysis involves the discovery of associated rules, showing attribute value and conditions that occur frequently in a given set of data. Classification is the process of finding a set of models (or functions) that describe and distinguish data classes or concepts, for the purpose of being able to use the model to predict the class of objects whose class label is unknown. Clustering Analysis concerns the problem of decomposing or partitioning a data set (usually multivariate) into groups so that the points in one group are similar to each other and are as different as possible from the points in other groups.

***Privacy Preservation Techniques* -** PPDM algorithms can further be divided according to privacy preservation techniques used. Four techniques – sanitation, blocking, distort, and generalization **--** have been used to hide data items for a centralized data distribution. The idea behind data sanitation is to remove or modify items in a database to reduce the support of some frequently used item sets such that sensitive patterns cannot be mined. The blocking approach replaces certain attributes of the data with a question mark. In this regard, the minimum support and confidence level will be altered into a minimum interval. As long as the support and/or the confidence of a sensitive rule lie below the middle in these two ranges, the confidentiality of data is expected to be protected.

Techniques of PPDM
Most methods for privacy computations use some form of transformation on the data in order to perform the privacy preservation. Typically, such methods reduce the granularity of representation in order to reduce the privacy. This reduction in granularity results in some loss of effectiveness of data management or mining algorithms. This is the natural trade-off between information loss and privacy. Some examples of such technique as described in [4] are:

***Randomization method* -** The randomization technique uses data distortion methods in order to create private representations of the records .In this which noise is added to the data in order to mask the attribute values of records In most cases, the individual records cannot be recovered, but only aggregate distributions can be recovered. These aggregate distributions can be used for data mining purposes. Data mining techniques can be developed in order to work with these aggregate distributions. Two kinds of perturbation are possible with the randomization method:

Additive Perturbation **-** In this case, randomized noise is added to the data records. The overall data distributions can be recovered from the randomized records. Data mining and management algorithms re designed to work with these data distributions.

Multiplicative Perturbation- In this case, the random projection or random rotation techniques are used in order to perturb the records.

The k-anonymity model and l-diversity: The *k*-anonymity model was developed because of the possibility of indirect identification of records from public databases. This is because combinations of record attributes can be used to exactly identify individual records. In the *k*-anonymity method, the granularity of data representation is reduced with the use of techniques such as generalization and suppression. This granularity is reduced sufficiently that any given record maps onto at least *k* other records in the data. The *l*-diversity model was designed to handle some weaknesses in the *k*-anonymity model since protecting identities to the level of *k*-individuals is not the same as protecting the corresponding sensitive values, especially when there is homogeneity of sensitive values within a group.

Downgrading Application Effectiveness - In many cases, even though the data may not be available, the output of applications such as association rule mining, classification or query processing may result in violations of privacy. This has lead to research in downgrading the effectiveness of applications by either data or application modifications.

Distributed privacy preservation- In many cases, individual entities may wish to derive aggregate results from data sets which are partitioned across these entities. Such partitioning may be horizontal (when the records are distributed across multiple entities) or vertical (when the attributes are distributed across multiple entities). While the individual entities may not desire to share their entire data sets, they may consent to limited information sharing with the use of a variety of protocols. The overall effect of such methods is to maintain privacy for each individual entity, while deriving aggregate results over the entire data.

The term "Data Distribution" means the manner in which the data has been stored at the sites or database servers. Primarily there are two kinds of data distribution 1) Centralized and 2) Partitioned Data. In centralized dataset all data is stored at single server or machine. It can be possible that for maintaining the consistency and presence of data during some type of problem in main database server, mirrored server is implemented. But this case cannot be considered as partitioned data server.

While in partitioned data server the complete set of records of database is partitioned in some particular manner and each partition resides on different database server. Partitioned data can further be classified as 1) Horizontally Partitioned and 2) Vertically Partitioned.

State of Art in Secure Multiparty Computation

Consider a set of parties who do not trust each other, nor the channels by which they communicate. Still, the parties wish to correctly compute some common function of their local inputs, while keeping their local data as private as possible. This, in a nutshell, is the problem of Secure Multiparty Computation (SMC). It is clear that the problem we wish to solve, privacy-preserving data mining, is a special case of the secure multi-party computation problem. Before proposing algorithms that preserve privacy, it is important to define the notion of privacy. The framework of secure multiparty computation provides a solid theoretical underpinning for privacy. The key notion is to show that a protocol reveals nothing except the results. This is done by showing how everything seen during the protocol can be simulated from knowing the input and the output of the protocol.

Trusted Third Party Model

In cryptography, a trusted third party (TTP) is an entity which facilitates interactions between two parties who both trust the third party; The Third Party reviews all critical transaction communications between the parties, based on the ease of creating fraudulent digital content. In TTP models, the relying parties use this trust to secure their own interactions. TTPs are common in any number of commercial transactions and in cryptographic digital transactions as well as cryptographic protocols, for example, a certificate authority (CA) would issue a digital identity certificate to one of the two parties in the next example. The CA then becomes the Trusted-Third-Party to that certificates issuance.

IV. PROPOSED WORK

Privacy Preserving Clustering of Horizontally Partitioned Data through Dilation- A solution:

General terms used:

Data Matrix

Objects (e.g. individuals, patterns, events) are usually represented as points (vectors) in a multidimensional space. Each dimension represents a distinct attribute describing the object. Thus, an object is represented as an m x n matrix D, where there are m rows, one for each object, and n columns, one for each attribute. This matrix is referred to as a data matrix, represented as follows:

$$\begin{bmatrix} \boldsymbol{a_{11}} & \cdots & \boldsymbol{a_{1k}} & \cdots & \boldsymbol{a_{1n}} \\ \boldsymbol{a_{21}} & \cdots & \boldsymbol{a_{2k}} & \cdots & \boldsymbol{a_{2n}} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \boldsymbol{a_{m1}} & \cdots & \boldsymbol{a_{mk}} & \cdots & \boldsymbol{a_{mn}} \end{bmatrix}$$

Data Normalization

The measurement unit used can affect the data analysis. For example, changing units from kilograms to pounds for weight may lead to different results. So to avoid dependence on the choice of measurement units, the data should be *normalized* or *standardized.* This transforms the data to fall within a smaller or common range such as [-1,1] or [0.0,1.0]. Normalizing the data attempts to give equal weights to all attributes. It helps prevent attributes with initially large ranges (e.g., income) from outweighing attributes with initially smaller ranges (e.g., binary attributes). It is also useful when given no prior knowledge of the data.

The attributes in a data matrix are normalized before being used. There are many methods for data normalization. We review two of them in this section: min-max normalization and z-score normalization.

Min-Max normalization performs a linear transformation on the original data. Suppose that $\min_A$ and $\max_A$ are the minimum and maximum values of an attribute A. Min-Max normalization maps a value v_i , of A to v_i' in range [new_min_A, new_max_A] by following equation:

In **z-score** normalization, the values for an attribute A, are normalized based on the mean and standard deviation of A. v_i is normalized to v_i' by following equation:

$$v_i' = \frac{v_i - A}{\sigma_A}$$

where A and σ_A are the mean and standard deviation, respectively of attribute A.

Although any normalization technique can be used for the proposed work , here z-score normalization is used for normalizing the numerical attributes before applying the proposed DBT algorithm.

Non Isometric Transformation: Isometric transformations preserve the angles and also the distances of the points before and after the transformation. The transformation used in this work is non-isometric. Dilation is used for transforming the points. Dilation is a transformation that produces an image that is the same shape as original, but is a different size. Dilation stretches or shrinks the original figure. This is the geometric definition of dilation. While if we consider it in terms of matrices similar transformation can be obtained by scaling matrix transformation. Hence the procedure proposed in this dissertation is mainly concentrated on **Dilation Based Transformation (DBT)**. The dilation is non isometric transformation which does not preserve distances between points but it preserves angle measure, parallelism, co linearity, midpoint, orientation. So the distance is not considered as the main factor for allocating the data points to the clusters. Key part for considering cluster is orientation and co linearity in this work.

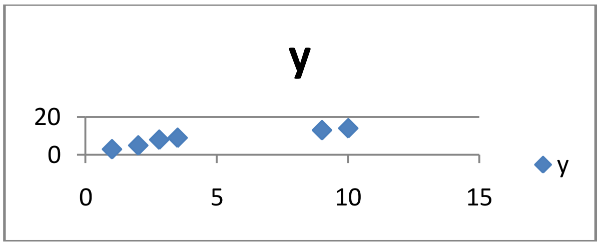


Fig. 5.3.1 Sample data points

Now let us assume that a scaling factor of 2.5 is taken, then the modified data points are as shown in following graph:

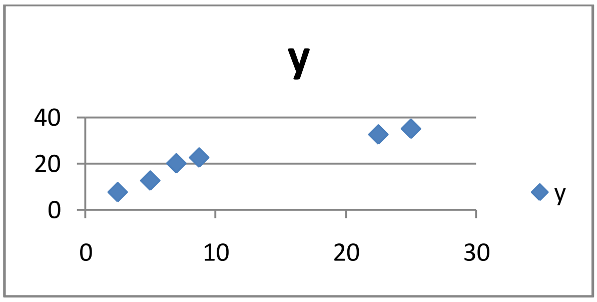


Fig. 5.3.1 Sample data points (after scaling)

Hence, observing the given two graphs, it is clear that the distribution of data points remains the same even after scaling them to the new scale.

Dilation Based Transformation (DBT)

In this section, proposed Dilation Based Transformation is introduced. This method is designed to protect the ~~und~~erlying attribute values by scaling them to a different scale, two attributes at a time.

General Assumptions

The proposed work to distort data points in n-dimensional space draws following assumptions:

Only numerical attributes are considered for applying proposed DBT, which are presented in data matrix D
The primary key of data (e.g. ID) can be revealed, but it has to be suppressed, as it is of no use in mining operation.
The attributes like name, address, class, etc. are hidden or removed before applying DBT because DBT works only on numerical data.

First of all, the numerical attributes are normalized and then, the normalized data is distorted by using our Dilation Based Transformation method.

DBT Application Scenario

The dilation based transformation transforms the numerical attributes of data objects and hence hides the underlying original data values to preserve privacy. This transformation preserves the cluster distribution. The situation that is taken under consideration is of horizontally partitioned data. The same attribute set is distributed to several participating sites with different set of records local to each of them. So in this case the proposed DBT algorithm has to be applied on the participating sites before contributing its local data for common clustering purpose.

The following diagram represents the scenario for application of DBT.

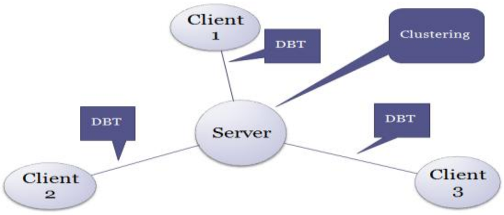


Fig 5.4.1 Application Scenario for DBT

In this diagram Client1, Client2, Client3 represents the participating sites while server represents the machine where data mining operation is performed. Here clustering is performed at server and its results are sent back to the participating sites. Server can be considered as secure third party if we consider third party model.

Hence this represented the possible solution called Dilation Based Transformation for preserving privacy of the data objects contributing for clustering purpose for mutual benefit.

IV. CONCLUSION

So by this proposal work, an attempt was made to secure the individual's confidential data like salary, SSN, bank account numbers, etc. Moreover, a particular situation was considered, where multiple organizations want to analyze their data in order to get some interesting information that may prove to be beneficial for all the participating organizations. But here came an issue of privacy of individual's confidential data. All participating sites needed to contribute their local data to single server (analysing machine) for join analysis. So, there was a risk of leakage of privacy of local data. Hence, the primary goal of this dissertation was to suggest some method or algorithm through which privacy of local data is maintained without affecting the outputs and results of mutual analysis.

So, a Dilation Based Transformation (DBT) algorithm was designed in order to hide the original data values and transform it into some other values which cannot be identified. Along with providing the privacy of data, DBT algorithm also preserves the cluster distribution of data, which was the goal of problem statement of this work.

REFERENCES

[1] “Metal Detector Basics”, Fortress Technology Inc. V 2-1, 1999.
[2] J. Baker-Javis, R. Kaiser, and M. D. Janezic, “Phantom materials used to model detection of concealed weapons and effects on implant devices in metal detectors”, IEEE Transactions on Magnetics, vol. 27, pp. 537-541, 2001.
[3] Metal Detector basics and theory URL:http://www.minelab.com/__files/f/11043/METAL%20DETECTOR%20BASICS%20AND%20THEORY.pdf
[4] Metal detection Guide URL:http://www.adsdetection.com/Metal-Detection-Guide.pdf
[5] Does exposure to metal detectors cause any medical problems? URL:http://www.helium.com/items/1616565-do-metal-detectors-cause-medical-problems
[6] Pregnancy & Prolonged Exposure to Metal Detectors URL:http://www.ehow.com/about_5415456_pregnancy-prolonged-exposure-metal-detectors.html
[7] Medical Devices URL:http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/PublicHealthNotifications/ucm062288.htm
[8] Metal Detectors and School Safety URL:http://www.schoolsecurity.org/trends/school_metal_detectors.html
[9] Shoplifter & Metal Detectors Effect Pacemakers, ICDs, Spinal Cord Stimulators URL:http://www.medicinenet.com/script/main/art.asp?articlekey=7330
[10] Metal detector URL:http://en.wikipedia.org/wiki/Metal_detector Security Screening URL:http://hps.org/publicinformation/ate/faqs/securityscreening.html
[11] History of the Metal Detector URL:http://arizonagoldprospectors.com/history.html
[12] History of the Metal Detector URL:http ://inventors.about.com/od/pstartinventions/a/Metal_Detector.htm