ISSN 2394-739X
IJRSET
International Journal for Research in Science Engineering and Technology

A REVIEW ON PRIVACY PRESERVING IN DATA MINING

[1] SUDHA. S, [2] Dr. P. LOGESWARI
[1] Research Scholar, [2] Assistant Professor
[2] Department of Computer Science,
[1, 2] Sri Krishna Arts & Science College,
[1, 2] Coimbatore, Tamilnadu, India.

ABSTRACT - The amount of information that is caught, gathered, and put away by a wide assortment of associations is developing at a dramatic rate. The potential for such information to help logical revelation and enhancement of existing frameworks is huge, yet just in the event that it very well may be incorporated and examined in a significant manner by a wide scope of agents. In this paper we survived 15 Literature survey forPrivacy Preserving in Data Mining. To protect security while mining a lot of information dispersed among various gatherings, cryptography based privacy preserving distributed data mining (PPDDM) has arisen as a significant other option. While many accept that information sharing is attractive, there are additionally protection and security concerns, established in morals and the law that regularly forestalls many authentic and critical applications. The cryptographic apparatuses can be utilized to make provably secure conventions which ensure the protection of the information of all gatherings in data mining.

Keywords: [Privacy-preserving, Data mining, Cryptography, Anonymity, Taxonomy.]

1. INTRODUCTION

Data mining is the way toward finding inconsistencies, patterns and connections within enormous data sets to anticipate results. Data mining is defined as a cycle used to remove usable data from a bigger arrangement of any crude data. It infers analyzing data patterns in huge bunches of data using at least one programming. Data mining has applications in various fields, similar to science and exploration. As a use of data mining, businesses can study their clients and foster more compelling methodologies identified with different business capacities and in turn influence assets in a more ideal and insightful way. This assists businesses with being nearer to their target and settle on better choices. Data mining involves successful data assortment and warehousing just as PC processing. For segmenting the data and evaluating the likelihood of future occasions, data mining utilizes complex numerical calculations. Data mining is otherwise called Knowledge Discovery in Data (KDD). Data Mining is tied in with discovering covered up, unsuspected, and already obscure yet legitimate connections among the data.

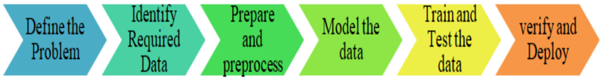

Figure 1. Data Mining Phases

Types of Data

Data mining can be performed on following types of data

- Relational databases
- Data warehouses
- Advanced DB and information repositories
- Object-oriented and object-relational databases
- Transactional and Spatial databases
- Heterogeneous and legacy databases
- Multimedia and streaming database
- Text databases
- Text mining and Web mining

Privacy Preserving Important in data mining

In data mining, the protection and legitimate issues that might result are the main keys to the growing contentions. Consistently the public authority and corporate elements accumulate colossal measures of information about clients, storing it in data distribution centers. Some portion of the worry is that whenever data is gathered and put away in a data warehouse, who will approach this information? In many cases a person may not know that the information gathered about him/her isn't simply imparted to who gathered the information. With the innovations that are accessible today, data mining can be utilized to remove data from the data distribution centers, finding distinctive information and connections about clients and making associations dependent on this extraction, which may put client's information and protection in danger. Data mining requires data courses of action that can cover purchaser's information, which might think twice about and security. One way for this to happen is through data aggregation where data is collected from various sources and set together with the goal that they can be broke down.

Steps ForData Mining For Preserving

Currently, several privacy preservation methods for data mining are available. These include

- K-anonymity
- Classification
- Clustering
- association rule
- distributed privacy preservation
- L-diverse, randomization, taxonomy tree

2. LITERATURE SURVEY

1. P. G. Shynu, H. Md. Shayan. And C. L. Chowdhary, (2020) et.al proposed "A Fuzzy based Data Perturbation Technique for Privacy Preserved Data mining," In current days there is a momentous expansion in information collection because of the advancement in the field of information technology. The outcomes, driven by an information mining algorithm can be utilized in numerous areas like Image Analysis, Marketing, climate forecasting and so on This paper depicts an arrangement of the fluffy choice help structure for recognizing confirmation of impending customer in 5 circumstances of information variety and imprecision, which can be used by explicit financial experts for further developing their exhibiting exertion.

Merits

Fuzzy logic is applied to preserve the individual information while revealing the subtleties out in the open.

SRBA has been set to a degree for any gathering that is in the reach (0-10) or some other reach as the system requires.

Demerits

MFs are huge for a specific issue since they sway on a fuzzy deduction framework.

2. W. Ouyang and Q. Huang, (2019) et.al proposed "A Privacy Preserving Algorithm for Mining Rare Association Rules by

Homomorphic Encryption," another efficient algorithm to find privacy-safeguarding uncommon affiliation rule mining strategies. The primary guideline thought is that with the safe two-party computation hypothesis we utilize homomorphic encryption to conceal private information. Through the application protocol, each gathering doesn't really move its data to an unbiased outsider. The homomorphic cryptographic computation of this safe two-party case can effectively deal with the computation issue, accordingly each gathering's data privacy can be ensured.

Merits

While the association rules can be mined from regular item sets, uncommon association rules can be found from uncommon item sets.

No member can derive the private data information of different members dependent on their own data and the public calculation yields.

Demerits

The standard for secure multiparty calculation can mirror the degree of secrecy that could be getting by performing free calculations with a confided in outsider.

3. M. M. Hasan, S. Hossain, M. K. Paul and A. H. M. S. Sattar (2019) et.al proposed "A New Hybrid Approach for Privacy Preserving Data Mining Using Matrix Decomposition Technique," Lately; many models and strategies have been intended for preserving protection, for example, utilizing network decomposition methods. In this paper, Scarified Singular Value Decomposition (SSVD) and Non-negative Matrix Factorization (NMF) are utilized and a half and half methodology dependent on those techniques has been proposed. The primary downside of our technique is, it takes more running time than the first SVD-based and NMF-based strategies however it's anything but a major issue since we simply apply this cycle just a single time prior to distributing the dataset. Every one of the classifiers utilized for this trial have shown over 90% exactness and the security protection metrics have shown better results.

Merits

The fundamental benefit of NMF is it requires some investment contrasted and other matrix decomposition methods.

SVM method gives fewer mistakes than the SVD-based methods however more blunder than the NMF while NMF gives less privacy and high information utility.

Demerits

Then, at that point in the event that we delete the district of the patient, it will be more difficult to identify, etc. On the other hand in the event that we delete the blood gathering and age of the patient, it will be more difficult to identify.

4. S. G. Teo, J. Cao and V. C. S. Lee (2020)et.al proposed "DAG: A General Model for Privacy-Preserving Data Mining" Secure multi-party computation (SMC) permits gatherings to mutually compute a capacity over their information sources while keeping each information secret. SMC has been broadly applied in assignments with privacy prerequisites, for example, privacy-preserving information mining (PPDM), to learn task yield and simultaneously ensure input information privacy. Nonetheless, existing SMC-based solutions are impromptu – they are proposed for explicit applications, and consequently can't be applied to different applications straightforwardly. DAG is a model for privacy-preserving computation. We have hypothetically examined the blunder of the model and demonstrated its security. Our model is general; it very well may be applied in a wide scope of applications.

Merits

The yields of the upper stream nodes are the contributions of the downstream nodes.

Security prerequisites are authorized on the operators. In particular, we formulate every operator as a SMC protocol

Demerits

The source node has a sensitive data that was use careful it will lose the process was difficult.

5. A. Afrin, M. K. Paul and A. H. M. S. Sattar (2019) et.al proposed "Privacy Preserving Data Mining Using Non-Negative Matrix Factorization and Singular Value Decomposition," The fast developing further developed technologies and further developed data mining algorithms make it simple for enemies to uncover touchy information. So there is consistently a hesitation while people share their own information. That is the reason privacy protection is a significant thought at each phase of the data mining measure. Privacy-Preserving Data Mining (PPDM) keeps up with data utility and secures privacy simultaneously. NMF and SVD strategy is utilized for privacy preservation. The current consolidated NMF and SVD technique performs better compared to the first SVD and NMF-based strategies as for privacy protection measurements

Merits

Further developed data mining calculations make it simple for foes to uncover touchy information.

Individuals' privacy should be protected with the goal that enemies can't uncover delicate information.

Demerits

NMF and SVD methods or more successful methods are required for further developing query accuracy

6. L. Zhang, W. Wang and Y. Zhang (2019) "Privacy Preserving Association Rule Mining: Taxonomy, Techniques, and Metrics," Data mining (DM) innovation has gotten progressively famous. In any case, the unreasonable collection and analysis of data might disregard the protection of people and associations, which raises security concerns. Accordingly, another exploration region known as security protecting data mining (PPDM) has arisen and drawn in the consideration of numerous researchers who are keen on forestalling security divulgence during data mining. In this paper, we give an extensive audit of studies on a particular PPDM, known as protection saving association rule mining (PPARM). The undeniable advantages and striking disadvantages of the current algorithms are examined and stressed. Finally, we present different measurements to gauge PPARM algorithms. The introduced overview shows the steadily expanding interest of researchers in the space of shielding touchy data and mined patterns from malignant users.

Merits

Randomization-based Useful and straightforward for hiding information

Remaking based Have lesser incidental effects than heuristic-based methodology

Heuristic hindering based Maintain information quality since it simply impedes the first value as opposed to embeddings a false value

Demerits

Concealing just each standard in turn and generating undesired ghost rules, which decreases the utility of the delivered database.

The expert does most of the calculation.

However invented data are added in datasets, the expert can learn huge information about different data owner's raw data from the got datasets.

7. S. Qiu, B. Wang, M. Li, J. Liu and Y. Shi (2020) "Toward Practical Privacy-Preserving Frequent Item set Mining on Encrypted Cloud Data," With the dramatic expansion in the size of datasets gathered and put away with cloud administrations as of late, it is promising to convey this computation-concentrated mining measure in the cloud. Measure of work likewise moved the approximate mining computation into the specific computation, where such strategies not just further develop the exactness additionally plan to upgrade the proficiency. Be that as it may, while mining information put away on open mists, definitely presents privacy worries on touchy datasets. To ensure information privacy and computation effectiveness, we embrace two distinct homomorphic encryption plans and plan a protected and powerful comparison conspire. Our first protocol accomplishes more proficient mining execution while our subsequent protocol gives a more grounded privacy ensure. Accomplishes an amazingly higher mining execution while our Protocol. Gives a more grounded privacy ensures. Toward more commonsense effectiveness, we improve the exhibition of our second protocol by utilizing a minor spillage of privacy to accomplish our Protocol

Merits

The ones with low supports and certainty unmistakably don't show valuable relations. Least help and least certainty can be utilized as two thresholds to recognize significant relations.

enormous scope data from multiple and variable data sources (e.g., a great many clients and gadgets) are gathered by cloud services

Demerits

The CSP keeps a transaction database, which incorporates countless transactions contributed from various clients.

8. I. Anikin and R. Gazimov, (2019) et.al proposed "Approach to Privacy Preserved Data Mining in Distributed Systems," All the more regularly industrial systems are carried out in a dispersed manner, which prompts the need of utilizing data digging techniques for appropriated data. It could impact the infringement of data security. Source data can be revealed during its transmission through the public organizations or on account of catching data storage. This paper is given to taking care of the data security issue for conveyed data mining systems. We present a privacy-preserving DBSCAN bunching calculation over in an upward direction parceled data, dissect the security of this calculation with regards to various foes and show its performance. DBSCAN bunching calculation that permits giving the assurance of data situated in conveyed storage. We research the security level of this calculation according to the perspective of various foe types. In the last area, we assessed the performance of the proposed calculation in regards to the quantity of members and data volume. The recommended approach could be generally utilized for data privacy preservation in industrial systems

Merits

Untrustworthy members acquire their yield information if and just if fair members get their yield information.

An internal adversary might be in agreement with the external adversary and passes him it's in private information.

Demerits

Perform mathematical operations on private data and obtain result corresponds operations on original data.

9. S. Yaji and B. Neelima (2019) et.al proposed "Optimizing Privacy-Preserving Data Mining Model in Multivariate Datasets," The investigation introduced in this paper shows that the FM radio spectrum is underutilized in the space of the mainland United States that have a populace of 100 000 or less. These locations have an empty FM radio spectrum of somewhere around 13 MHz with adequate spectrum spacing between adjoining FM radio channels. The spectrum spacing gives the necessary transfer speed to information transmission and gives sufficient data transfer capacity to limit obstruction presented by adjoining anticipated and unpredicted FM radio broadcasts and other low-power short-range Internet of Thing (IoT) gadgets. To accomplish the maximum capacity of the empty spectrum, CIoT gadgets should work in a low-power short-range mode to work with frequency reuse amongst CIoT gadgets. Low-power short-range CIoT gadgets utilizing frequency-reuse can acquire potential bitrates of around 30 Mbps.

Merits

executing the calculations on a state-by-state basis, in lieu of the entire United States at once, significantly reduced the computation processing time

Demerits

TVWS is pivotal in light of the fact that it will set priority and cultivate further exploration of underutilized spaces of the radio spectrum, for example, the empty FM radio spectrum.

10. Y. Zhou, Y. Tian, F. Liu, J. Liu and Y. Zhu (2019) et.al proposed "Privacy Preserving Distributed Data Mining Based on Secure Multi-party Computation," Lately, secure multiparty computation (MPC) shows its expected ability for taking care of this issue. In the interim, there are various issues to be addressed prior to using them in a business climate. In this paper, we call attention to two unsupported undertakings of MPC that are common in reality. Towards this end, we plan algorithms dependent on streamlined lattice computation with one hot encoding and LU disintegration to help these in MPC setting prerequisites. The arrangements have been carried out dependent on the SPDZ convention. To assess the legitimacy and execution of our implementation, we set up two tests on cotton exchanging records. The assessment results show that the mining aftereffects of our implementation are satisfactory in precision and efficiency contrasted with traditional standalone implementation.

Merits

Studying the relationship between factors by linear regression is another significant data mining task.

Secret sharing alludes to a technique for dispersing a secret among a gathering of members, where secrets are parted into a few offers.

Demerits

The performance of our execution could be improved by using graphic processing unit (GPU) acceleration. It would be hard for mining an extra-enormous scope dataset.

11. S. G. Teo, J. Cao and V. C. S. Lee (2020) et.al proposed "DAG: A General Model for Privacy-Preserving Data Mining," Secure multi-party calculation (SMC) permits gatherings to mutually figure a capacity over their information sources while keeping each information classified. It has been broadly applied in assignments with privacy prerequisites, for example, privacy-preserving information mining (PPDM), to learn task yield and simultaneously ensure input information privacy. Nonetheless, existing SMC-based arrangements are specially appointed – they are proposed for explicit applications, and consequently can't be applied to different applications straightforwardly. DAG is a model for privacy-preserving calculation. We have hypothetically analyzed the mistake of the model and demonstrated its security. Our model is general; it very well may be applied in a wide scope of applications. Our contextual investigation in both bit regression and Naive Bayes shows that our model can deliver accurate outcomes.

Merits

Interface different administrators to perform more confounded functions. The outputs of all administrators with the exception of the last ones are viewed as moderate results

Source nodes are private contributions of the gatherings associated with the errands. Sink nodes are the outputs of the model

Demerits

The operators expected to anticipate the class mark for testing information are additionally up to predictor and reaction variables.

12. M. Rathi and A. Rajavat (2020) et.al proposed High Dimensional Data Processing in Privacy Preserving Data Mining. In business insight data is a fundamental element in dynamic. A deficient or absence of data can harm the whole task thoughts. In this manner sometimes unique business dimensions are teaming up their touchy and individual data for improving decisional capacity. During this, the dataset is altogether filling in dimensions. Thusly it is much extraordinary to discover a strategy by which the higher dimensional data can be taken care of. This paper contributes two key bearings of the PPDM (privacy-preserving data mining), initial, a review was led on the different PPDM models to comprehend the working and necessities of the PPDM frameworks. Privacy-preserving data mining prompts various issues and exploration challenges; among them precise data processing is a key examination issue. During such sort of data displaying and distributing the accompanying circumstances can influence the demonstrating of data.

Merits

Memory utilizations of an algorithm show the space intricacy of the cycle. That is the piece of the fundamental memory which is used during the execution of the cycle.

datasets are utilized in different AI and data mining applications as a benchmark dataset

Demerits

The data measurement is a difficult issue for data mining algorithms

The feature selection methods require an additional measure of time for processing data.

13. S. Sharma and D. Shukla (2016) et.al, proposed Efficient Multi-Party Privacy Preserving Data Mining for Vertically Partitioned Data. Data mining and their techniques are utilized in different applications for deciding, pattern recognition, learning and others. The mining method applied on data is relies upon the nature and sort of data utilized for mining. The data can be accessible in both the sorts' organized and unstructured arrangement. The data in computational space put away in computerized design. This arrangement of data burns-through less exertion and capacity. Accordingly various association and foundations are preserving their data in this arrangement. In this introduced work the data and their privacy is the fundamental space of study. In the proposed work an association is viewed as where the decisions are made with the diverse office based data and their attributes. Also to settle on decisions the attributes of the multitude of divisions are required. In any case, the offices can't uncover the privacy of data proprietor. Thusly to consolidate the data attributes and mining of the joined data need a privacy preserving method for forestalling the privacy issues in a unify database. The proposed work is expected to discover the answer for privacy preserving data mining strategy in effective and precise way. Along these lines various exploration articles are contemplated and a multiparty privacy preserving data mining strategy is proposed. The proposed strategy can consolidate multiparty in an upward direction divided data safely. Along these lines the server end creates the arbitrary cryptographic key. This key is utilized to scramble or encode the data before the mining of data. The scrambled data is utilized as the images for an obscure dataset and utilizing the pre-arranged new encoded data the mining is performed for decision making. The mining of encoded data is performed with the assistance of C4.5 decision tree algorithm.

Merits

The proposed work is planned to discover the answer for privacy preserving data mining method in effective and accurate manner.

Demerits

The method is extendable for the hieratical data mining based privacy issues.

14.S. Khan, T. Gorhe, R. Vig and B. A. Patil (2015) et.al proposed Enabling Multi-Level Trust in Privacy Preserving Data Mining. There are numerous applications related with data mining which manage privacy concern. Bank transactions, hospital records, and web traffic are a few models. Data mining in such privacy-sensitive phase is confronting developing issues. We need to foster techniques that are sensitive to the privacy issue. Privacy preserving data mining can possibly build the span and advantages of data mining technology. Notwithstanding, we should have the option to legitimize that privacy is saved for this; we should have the option to communicate what we mean by privacy preserving. The current combination of definition, with each paper having its own meaning of what privacy is kept up with, will prompt disarray among possible adopters off the technology. The paper presents some idea for characterizing and checking privacy safeguarding .We show how this identify with both privacy strategy and practice in the more extensive community and to techniques in privacy preserving data mining. This is in no way, shape or form the authoritative word regarding the matter. While a few measures, for example, the differential entropy metric of, have clear mathematical establishment and Application, others have solid potential for additional turn of events .Adopting a typical framework for conversation of privacy conservation will empower cutting edge data mining technology to make considerable advances in alleviating privacy concerns. In this paper the Expanded PPDM to multilevel trust (MLT) is presented and we builds the extent of PPDM, where in existing framework single level trust is accessible .Multilevel Trust Privacy Preserving Data Mining permits to create multilevel trust fragmented copies of data for created by data proprietor. The primary test is to forestall data miners or assailant from consolidating the fragmented copies of numerous trust levels to shape unique data set created by data proprietor. We discover answer for this test by adding the commotion in the numerous fragmented copies at various trust level. Our most awesome aspect of this exploration is we permit data proprietor to produce fragmented copies of its data set at self-assertive trust level on base of interest. This arrangement gives greatest flexibility to the data proprietor.

Merits

Adopting a typical framework for conversation of privacy protection will empower cutting edge data mining technology to make generous advances in alleviating privacy concerns.

Demerits

To prevent data miners or aggressor from joining the fragmented copies of various trust level to shape unique data set created by data proprietor.

15. A. Kaur and S. Sofat (2016) et.al proposed A Proposed Hybrid Approach for Privacy Preserving Data Mining. Every single organization needs to gather the data of its clients or users for either reason. This data can be put away on a unified server or on the cloud. In the event that the data is being put away on the brought together storehouse then the control of the data is with the archive controllers of the organization. With the developing technology and measure of data, the utilization of cloud and brought together servers is expanding. At the point when the data of the people is put away by the outsider it prompts the frailty of abuse of their information in the people. Data Mining is carried on this data put away over cloud to get valuable information, examination and decision making purposes. In any case, alongside the way toward mining, privacy preservation is the key concern. Because of expansion in the data stockpiling over the cloud, the need of utilizing the data mining techniques for Privacy Preservation is expanding quickly. A great deal of exploration has been done in the field of anonymization and cryptographic techniques. Anonymization and perturbation techniques can be viewed as better when contrasted with cryptographic techniques as far as complexity and proficiency for huge number of users. At the point when looked at based on information misfortune and privacy accomplished anonymization experiences an essentially high information misfortune. The proposed hybrid strategy can successfully accomplish the objective of privacy preservation with no information misfortune as the utilizing the algorithm the distorted values can be returned to its unique values successfully.

Merits

The proposed hybrid method can successfully accomplish the objective of privacy preservation with no information misfortune as the utilizing the algorithm the distorted values can be returned to its unique values successfully.

Demerits

Cryptographic techniques as far as complexity and not effectiveness for huge number of users.

CONCLUSION

Privacy preserving in data mining is a very important task to do. As the data is collected from various individuals, it's the duty of the organization to preserve the data of the individuals. For preserving the data, many techniques have to get implemented to keep the data safe and secure. Privacy preservation is a significant problem while real world datasets are dealt with. The process of data modification and limiting information loss is known as Privacy Preservation Data Mining. While handling real-world datasets, privacy preservation is a major problem in online environment where immense measures of individual information are shared and moved far and wide immediately. This survey paper gives the clear idea of the concepts, methods and techniques. This research gives the information about the efficient techniques and the advantages of the techniques. It helps to get know about the power packed concepts with fewer efforts.

REFERENCES

[1]. S. Sharma and D. Shukla, "Efficient multi-party privacy preserving data mining for vertically partitioned data," 2016 International Conference on Inventive Computation Technologies (ICICT), 2016, pp. 1-7, doi: 10.1109/INVENTIVE.2016.7824852.

[2]. M. G. Vinay and V. G. Ravi Kumar, "A New Model for Privacy Preserving Multiparty Collaborative Data Mining," 2017 International Conference on Current Trends in Computer, Electrical, Electronics and Communication (CTCEEC), 2017, pp. 394-397, doi: 10.1109/CTCEEC.2017.8455035.

[3]. A. Kaur and S. Sofat, "A proposed hybrid approach for privacy preserving data mining," 2016 International Conference on Inventive Computation Technologies (ICICT), 2016, pp. 1-6, doi: 10.1109/INVENTIVE.2016.7823283.

[4]. V. Baby and N. S. Chandra, "Distributed threshold k-means clustering for privacy preserving data mining," 2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2016, pp. 2286-2289, doi: 10.1109/ICACCI.2016.7732393.

[5]. R. S. Mohammed, E. M. Hussien and J. R. Mutter, "A novel technique of privacy preserving association rule mining," 2016 Al-Sadeq International Conference on Multidisciplinary in IT and Communication Science and Applications (AIC-MITCSA), 2016, pp. 1-6, doi: 10.1109/AIC-MITCSA.2016.7759930.

[6]. K. Kalaiselvi and V. J. B. Sara, "Privacy preserving in data mining classification and visualization: Empirical study," 2017 2nd International Conference on Communication and Electronics Systems (ICCES), 2017, pp. 51-55, doi: 10.1109/CESYS.2017.8321147.

[7]. S. Wang, R. Sinnott and S. Nepal, "Privacy-protected place of activity mining on big location data," 2017 IEEE International Conference on Big Data (Big Data), 2017, pp. 1101-1108, doi: 10.1109/BigData.2017.8258035.

[8]. B. K. Samanthula, "Privacy-preserving outsourced collaborative frequent itemset mining in the cloud," 2017 IEEE International Conference on Big Data (Big Data), 2017, pp. 4827-4829, doi: 10.1109/BigData.2017.8258556.

[9]. S. Sharma And D. Shukla, "Efficient Multi-Party Privacy Preserving Data Mining For Vertically Partitioned Data," 2016 International Conference On Inventive Computation Technologies (Icict), 2016, Pp. 1-7, Doi: 10.1109/Inventive.2016.7824852.

[10]. S. Khan, T. Gorhe, R. Vig And B. A. Patil, "Enabling Multi-Level Trust In Privacy Preserving Data Mining," 2015 International Conference On Green Computing And Internet Of Things (Icgciot), 2015, Pp. 1369-1372, Doi: 10.1109/Icgciot.2015.7380680.

[11]. A. Kaur And S. Sofat, "A Proposed Hybrid Approach For Privacy Preserving Data Mining," 2016 International Conference On Inventive Computation Technologies (Icict), 2016, Pp. 1-6, Doi: 10.1109/Inventive.2016.7823283.

[12]. A. W. Putri and L. Hira, "Hybrid Transformation In Privacy-Preserving Data Mining," 2016 International Conference On Data And Software Engineering (Icodse), 2016, Pp. 1-6, Doi: 10.1109/Icodse.2016.7936114.

[13]. S. Liu, Q. Qu, L. Chen and L. M. Ni, "SMC: A Practical Schema for Privacy-Preserved Data Sharing over Distributed Data Streams," in *IEEE Transactions on Big Data*, vol. 1, no. 2, pp. 68-81, 1 June 2015, doi: 10.1109/TBDATA.2015.2498156.

[14]. V. Baby And N. S. Chandra, "Distributed Threshold K-Means Clustering For Privacy Preserving Data Mining," 2016 International Conference On Advances In Computing, Communications And Informatics (Icacci), 2016, Pp. 2286-2289, Doi: 10.1109/Icacci.2016.7732393.

[15]. R. S. Mohammed, E. M. Hussien And J. R. Mutter, "A Novel Technique Of Privacy Preserving Association Rule Mining," 2016 Al-Sadeq International Conference On Multidisciplinary In It And Communication Science And Applications (Aic-Mitcsa), 2016, Pp. 1-6, Doi: 10.1109/Aic-Mitcsa.2016.7759930.