Privacy Preserving Data Analysis using Decision Tree learning Algorithm through Additive Homomorphic Encryption

K Durga Prasad, D Vasumathi

***Abstract:** Privacy preserving is an emerging concern in the field of data mining. The Randomization technique protects privacy with loss of accuracy. The secure multi-party computation increases the accuracy and conserves privacy but the computational complexity is more. The encryption of data using cryptography makes the data secure without loss of accuracy and reduces the communication complexity. The proposed technique is privacy preserving decision tree algorithm using cryptographic approach. The data miner collects frequencies and combined frequencies from the users and learns the classification rules from the decision tree. The data miner learns only frequencies of the sensitive data. The experimental result shows that proposed privacy preserving decision tree algorithm is computationally efficient and the accuracy is more than the randomization models. The communication complexity is less compared with the secure multi-party computation models.*

***Keywords:** Cryptographic encryption, Data Analysis, Decision Tree and Privacy Preserving.*

I. INTRODUCTION

Due to tremendous growth in information technologies and storage devices, it is easy to collect a large amount of data from users. Data mining is the process of knowledge discovery from large databases. If no proper measures are taken, the extracted data may violate the privacy of users. The privacy is an important measure in the field of medical, business and financial. For privacy concerns, when the user data is collected for a survey, many are not willing to provide details or may provide false information. When the data analysis is applied for the collected false data, the accuracy becomes low. Many users are willing to provide the data when their data is protected from privacy.

The researchers proposed different techniques to protect the privacy of user's data. Perturbation method protects sensitive data of the user but leads to low accuracy. The secure multi-party computation is another technique which protects the sensitive data of the user, but the communication complexity is more. The other method is homomorphic encryption technique which preserves the privacy of the user with less communication complexity. Most of the research is focused on randomization, anonymization and secure multi-party computation. In these methods, the computational complication is high and useful information is extracted from the centralized database. The proposed technique privacy preserving decision tree algorithm which minimizes the information loss and maximizes accuracy in distributed communication. In this, the data miner receives a row of data from the user and learns the classification rules. The user sensitive data is encrypted using homomorphic encryption; data miner receives encrypted user data and calculates the final frequency of attribute values. The cryptographic encryption is successfully applied to privacy preserving data analysis with the invention of homomorphic encryption by Gentry [9]. The additive and multiplicative homomorphic approaches applied to the encrypted data by the fully homomorphic encryption scheme. The results produced on encrypted are same as the results produced on the original data. The proposed ElGamal additive homomorphic encryption technique encrypts the user sensitive data. The data miner applies a decision tree on the received frequency data. The literature survey presented in section 2, privacy preserving decision tree in section 3, result analysis in section 4 and the conclusion is in section 5.

Manuscript published on 28 February 2019.
***Correspondence Author(s)**

K. Durga Prasad, JNTUK Research scholar, JNT University, Kakinada, AP, India,
D.Vasumathi, Professor, Department of Computer Science Engineering, JNTUHCEH, JNT University, kukatpally, Hyderabad, Telangana, India,

II. LITERATUR REVIEW

The user sensitive data is protected with randomization, secure multi-party computation, and homomorphic encryption. These details of techniques are presented in the following subsections.

A. Randomization Techniques

Random noise is added to the original records in the randomization. Agarwal R et al[11] proposed an approach to estimate the distribution of actual information by reconstruction. Agarwal D et al [18] proved that the actual distribution is estimated using the Expectation-Maximization algorithm. Evfimievski A[1] applied randomization on categorical and numerical data using applied statistics, Du W et al [12] build a decision tree using randomized response techniques for classification. Kargupta H et al [5] proved that the data distortion preserves less privacy and low accuracy. Depending on the level of privacy all the solutions accuracy varies. The accuracy of the model decreases as the privacy of each user increases. In general, the required solution is that provides adequate privacy and accuracy to the user information. To increase the privacy and accuracy secure multi-party computation is proposed and data shuffling by Muralidhar and Sarathy [4]. The original data records are added with noise data in these techniques and these are allowed only on statistical data.

B. Secure Multi-party Computation

In a distributed environment group of parties share the confidential data to the trusted party. The trusted party computes joint operation on the received confidential data.

The trusted party extracts useful patterns from the data through data analysis. The results are shared with the other parties. When the trusted party compromises, the shared information is not secure. In secure multi-party computing, two or more parties share their data with the trusted party. Yao A [6] proposed the secure multi-party computation. The solution for any polynomial functions by secure multi-party computation proved by Goldreich [2]. Lindell Y et al [3] constructed a decision tree successfully using secure multi-party computation without learning anything by the shared parties from shared information. The other approaches like clustering, KNN, and association rule mining have been applied to the shared information. B Pinkas et al[7] implemented Generic constructions to achieve Privacy preserving the two-party.

Lindell Y et al [23] identified the various aspects for the issue of efficiency and difficulties to construct SMC with related to PPDM. The team presented regular concerns that are predominant in the writing when secure multiparty computation methods are connected to PPDM. Orlandi, C [24] prepared some pragmatic arrangements that can be significant for true applications in SMC. Vaidya et al [8] introduced PPDM algorithm of naive Bayes classifier for data partitioned by vertically, Archer, D et al [22] have designed robust security protocols in SMC, illustrated various usecases of SMC and deployment of its products. Kantarcioglu et al [19] proposed an architecture to keep on the privacy of client data and Wright et al [20] introduced privacy preserving technique for distributed heterogeneous data using Bayesian network structure. This approach is not secured when n-2 users and data miners are compromised or corrupted. The discussed techniques provide strong privacy but the performance cost is high. These techniques are applied to a minimum number of parties says two parties. In the above-specified techniques, the communication between the parties is multiple numbers of rounds and communication complexity is high.

C. Homomorphic Encryption Technique

The homomorphic encryption [HE] is a kind of encryption technique that allows parties to do computations on encrypted data, provides an encrypted result is same as the result of operations done on original data. The fully homomorphic encryption allows mathematical operations such as multiplication and addition for encryption and the result of encrypted data by homomorphic encryption same as the results produced on the original data. There are two different distributed PPDM approaches existed, those are for vertically partitioned and horizontally partitioned data.

Many authors proposed cryptographic mechanisms for privacy preserving. Craig Gentry [9] introduced the first Fully homomorphic encryption technique using ideal lattices for data analysis on a ciphertext without revealing sensitive data of the user. Yang Z et al [10] proposed the PPDM classification technique that provides the privacy to the user data without losing any accuracy. To provide privacy for the user sensitive data, all these approaches uses ElGamal public key algorithm. In fully distributed communication, the additive HE scheme of ElGamal algorithm is used for encryption. Zhan [13] presented the homomorphic encryption technique and constructed decision tree to learn classification rules to achieve privacy preserving on vertical data. To preserve the privacy of user data, Chen et al [14] shown how to do backpropagation using the artificial neural network.

Aslett et al [15] proposed a machine learning algorithm on encrypted statistical information to preserve privacy and discussed how to use various software tools in an encrypted statistical machine learning. Kaleli et al [16] proposed a variety of recommendations for the privacy of user data on privacy preserving naive Bayes classifier over the distributed data. Huai et al [17] have proposed privacy preserving naive Bayes classifier for privacy preserving. The homomorphic encryption serves in two categories i.e. additive homomorphic encryption and multiplicative homomorphic encryption. The additive HE encryption property of ElGamal public key algorithm has a finite solution for data sharing among unsecured parties. Durga Prasad K et al [21] has demonstrated how to use ElGamal public key Homomorphic encryption algorithm for data sharing in a distributed environment while preserving privacy.

III. PROPOSED PRIVACY PRESERVING DECISSION TREE

Let assume $\mathrm{U_1, U_2, \ldots, U_n}$ be n users shares their data with the data miner. Each user communicates a row of data to the data miner and a row has m attributes. Each attribute is either continuous or discrete. The discrete data is represented as Boolean value and continuous data is represented using fixed precision. The sensitive discrete attribute values are encrypted using ElGamal additive homomorphic encryption. The sensitive continuous attribute values are transformed using one-way function. The ElGamal additive homomorphic encryption is presented in the next subsection.

A. ElGamal Additive Homomorphic Encryption

The ElGamal is a public key encryption algorithm. The ElGamal algorithm supports additive homomorphism. The security of the algorithm is dependent on the discrete logarithm problem. Let assume p be large prime number and g be the primitive rootless than p. The data miner selects a private key d such that $1 < \mathrm{d} \leq \mathrm{p} - 1$. The public key e corresponding to the data miner's private key d is generated as $\mathrm{e = g^d mod\, p}$. The data miner shares public key e, primitive root g and prime number p to the users. The user $\mathrm{U_i}$sends either Boolean value $\mathrm{b_i}$ or normalized continuous value. The data miner only learns b from the collected data $\mathrm{b = \sum_{i=1}^{n} b_i}$.

The data miner learns b from the following privacy preserving protocol as

$$\mathrm{U_i \rightarrow miner: m = g^r mod\ p} \qquad (1)$$

$$\mathrm{: h_i = b_i * e^r mod\ p\ for\ Boolean\ value} \qquad (2)$$

$$\text{miner:} \; = \sum_{i=1}^{n} h_i \qquad (3)$$

$$b = s * (m^d)^{-1} \bmod p \text{ for Boolean value} \qquad (4)$$

And can prove that privacy preserving protocol computes the sum of the inputs of the user’s correct as

$$b = \textstyle\sum_{i=1}^{n} b_i \qquad (5)$$

$$b = s * (m^d)^{-1}\, mod\; p \qquad (6)$$

$$= \textstyle\sum_{i=1}^{n} h_i * ((g^r)^d)^{-1} mod\; p$$

$$= \textstyle\sum_{i=1}^{n} b_i * e^r * ((g^d)^r)^{-1} mod\; p$$

$$= \textstyle\sum_{i=1}^{n} b_i * e^r * (e^r)^{-1} mod\; p$$

$$= \textstyle\sum_{i=1}^{n} b_i \qquad (7)$$

This protocol is secure even when n-2 users compromise with the data miner.

B. ID3 Decision Tree Algorithm

An ID3 is a decision tree learning algorithm. In which nodes are the attributes and edges are the possible values of the attribute. Each internal node is a test node corresponding to an attribute. The ID3 algorithm works as follows. The Decision tree is constructed using a top-down recursive approach. The root of the tree is selected by evaluating each attribute using statistical measure entropy and information gain. The entropy measures the impurity of the collection of data using the following equation

$$Entropy(S) \equiv \sum_{i=1}^{c} -P_i \log_2 P_i \qquad (8)$$

Where S is the collection of data and c is the number of classes and P_i is the proportion of examples belonging to class i. The information gain measures the expected reduction in entropy caused by partitioning the data according to this attribute. The information gain, Gain(S, A) of attribute A is measure using the following equation

$$Gain(S,A) \equiv Entropy(S) - \textstyle\sum_{v \in Values(A)} \frac{|S_v|}{|S|} Entropy(S_v) \quad (9)$$

Where Values(A) is the set of all possible values for attribute A, and S_v is the subset of S for which attribute A has value v. The highest Gain attribute becomes the root. This procedure is continued at every level of tree construction. If the attribute is a continuous attribute, then have to sort the values in increasing order and divide it into groups using the mean of two consecutive values and then calculate the information gain. The proposed privacy preserving ID3 decision tree algorithm is presented in the sub section 3.3.

C. Privacy Preserving ID3 Algorithm

Assume that each user senders either a Boolean or numeric value to the data miner. A class label V has p classes $(v^1, v^2, \dots, v^p)$ and each discrete attribute $A_i$has r attribute values$(a_{i1}, a_{i2}, \dots, a_{ir})$. The data miner computes the sum $b = \sum_{i=1}^{n} b_i$ without knowing the individual value of the discrete attribute for each user.

The additive homomorphic ElGamal encryption algorithm protects the privacy of the user data. Let P be the large prime and g be the primitive root of P. The user $U_i$maintains two pair of keys x_i, $X_i = g^{x_i} \bmod P$ and y_i, $Y_i = g^{y} \bmod P$ where x_i and y_i are private keys and X_i and Y_i are public keys. Define two common keys X and Y as

$$X = \textstyle\prod_{i=1}^{n} X_i \qquad (10)$$

$$Y = \textstyle\prod_{i=1}^{n} Y_i \qquad (11)$$

Every user uses the common key to send the data to the data miner. Each user $U_i$sends the Boolean value and the data miner learns, $d = \sum_{i=1}^{n} d_i$. Each user $U_i$sends the following pair to the data miner

$$m_i = g^{d_i}.X^{y_i} \qquad (12)$$

$$h_i = Y^{x_i} \qquad (13)$$

The data miner learns d with the received pair of information as

$$r = \textstyle\prod_{i=1}^{n} \frac{m_i}{h_i} \qquad (14)$$

For d = 1 to n
    if $g^d = r$ output d

The pair $(g^{d_i}.X^{y_i}, Y^{x_i})$ = (m_i, h_i) is cipher text of the plain text d_i using Elgamal additive homomorphic encryption algorithm.

The privacy preserving ID3 is presented for discrete and continuous attributes as:

For Discrete Sensitive Attribute

- User U_i Private Keys:

  $$x_{ij}{}^{l}, y_{ij}{}^{l} \; where \; 1 \le i \le n, 1 \le l \le p$$

- User U_i Public Keys:

  $$X_{ij}{}^{l} = g^{x_{ij}{}^{l}}, Y_{ij}{}^{l} = g^{y_i{}^{jl}} 1 \le i \le n, 1 \le l \le p$$

- Common Keys:

  $$X_j{}^{l} = \prod_{i=1}^{n} X_{ij}{}^{l}, Y_j{}^{l} = \prod_{i=1}^{n} Y_{ij}{}^{l}, 1 \le l \le p, j \in S$$

- Representation of Discrete Attribute values
  - Single attribute

    $$a_{i,j}{}^{k,l} = 1 \;\; if\left(a^{k}{}_{i,j}, v^l\right) = \left(a_j{}^{k}, v^l\right)$$

    $$= 0$$

  - The dependency of two attributes

$$a_{i,j}{}^{k,l} \& \, a^{k',l}{}_{i,j'} = 1 \;\; if\left(a^{k}{}_{i,j}, v^l\right) = \left(a_j{}^{k}, v^l\right) \& \left(a^{k'}{}_{i,j'}, v^l\right)$$

$$= \left(a_{j'}{}^{k'}, v^l\right) \quad = 0 \text{ otherwise}$$

  - The dependency of three attributes

$$a_{i,j}{}^{k,l} \& \, a^{k',l}{}_{i,j'} \& \, a^{k'',l}{}_{i,j''} = 1 \quad if\left(a^{k}{}_{i,j}, v^{l}\right)$$

$$= \left(a_j{}^{k}, v^{l}\right) \& \left(a^{k'}{}_{i,j'}, v^{l}\right)$$

$$= \left(a_{j'}{}^{k'}, v^{l}\right) \& \left(a^{k'}{}_{i,j'}, v^{l}\right) = \left(a_{j''}{}^{k''}, v^{l}\right)$$

= 0 otherwise

- The dependency of all sensitive attributes

$$a_{i,j}{}^{k,l} \& \, a^{k',l}{}_{i,j'} \& \; ... \& a^{k^m,l}{}_{i,j^m} = 1 \quad if\left(a^{k}{}_{i,j}, v^{l}\right) =$$

$$\left(a_j{}^{k}, v^{l}\right) \& \left(a^{k'}{}_{i,j'}, v^{l}\right) = \left(a_{j'}{}^{k'}, v^{l}\right) \& \dots \& \left(a^{k^m}{}_{i,j^m}, v^{l}\right) =$$

$$\left(a_{j'}{}^{k'}, v^{l}\right) \qquad = 0 \text{ otherwise}$$

The data miner collects joint probabilities from the users then calculates the entropy and information gain for all attributes.

For continuous sensitive attributes

- The data miner collects transformed data for continuous attribute and sorts the data. Consider a split position as the mean of two consecutive values then calculate entropy and gain for each split point and select the split point which produces the highest gain.

The algorithm is presented below.

Privacy Preserving ID3 (attributes, attribute_ joint_frequencies, class_labels)

```
• Create a Root node for the decision tree
• If all classes are positive, return the single-node tree Root, with the class label is +
• If all classes are negative, return the single-node tree Root, with the class label is –
• If attributes are empty, return the single-node tree Root, with class labels as the most common value of the class_labels
• Otherwise
    o A→ select the best attribute (discrete/continuous) using the highest information gain
    o Root→A
    o If the attribute is discrete then
        ▪ For each possible attribute value $a_i$ of A
            • Add new branch below the Root
            • Consider the subset of joint frequencies corresponding to attribute A
        • If the subset is empty then
            o Add a class label to this branch
        • Else below this new branch add the subtree
        • Privacy Preserving ID3 (attributes-{A}, $attribute\_joint\_frequencies_i$, class_labels)

    o If the attribute is continuous then
        ▪ Add one branch less than the threshold and other greater than the threshold
        • Consider the subset of joint frequencies corresponding to attribute A
        • If the subset is empty then
            o Add a class label to this branch
        • Else below this new branch add the subtree
        • Privacy Preserving ID3 (attributes-{A}, $attribute\_joint\_frequencies_i$, class_labels)
```

The implementation and analysis of the algorithm are presented in the next section.

IV. RESULT ANALYSIS

The privacy preserving ID3 is secure and it protects the user data even when n-2 users compromise with the data miner. The data miner learns only the final frequency. The data miner learns only the final frequency.

The privacy preserving ID3 decision tree is implemented and 20000 users data taken for the survey. The data miner collected the joint frequencies for the discrete attributes and transformed data for continuous attributes. In this, the data miner generates the common key and it took around 2.30 seconds.

Each user shares attribute value frequencies and joint frequencies for the discrete attributes and transformed data for the continuous attributes. Each user prepares a message, which includes the joint frequencies. The data miner decrypts the sum of each attribute and its corresponding values for the discrete attribute. The time to decrypt the sum is presented in Table 1. As the number of users is increasing the time also increasing in seconds and analysis presented in Fig.1.

Table I: Computational Time for discrete sensitive attributes

Number of Users	Sensitive attributes(seconds)
2000	2.8
4000	5.24
6000	10.28
8000	13.06
10000	18.02
12000	21.41
14000	23.36
16000	25.17
18000	30.92
20000	34.09

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

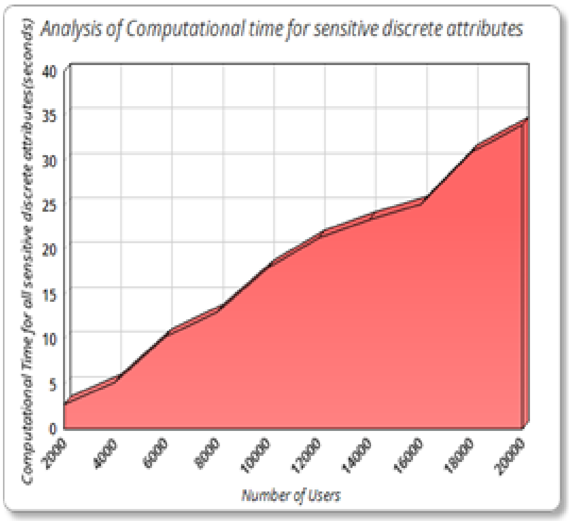

Figure 1: Analysis of Computational time for sensitive discrete attributes

Table II: Computational time for all attributes

Number Attributes	Computational Time (seconds)
2	2.6
3	5.04
5	10.48
6	13.01
8	18.28
10	21.49

The time to decrypt the sum is also increasing as the number of sensitive attributes is increasing and the results are presented in Table 2. and analysis is presented in Fig. 2.

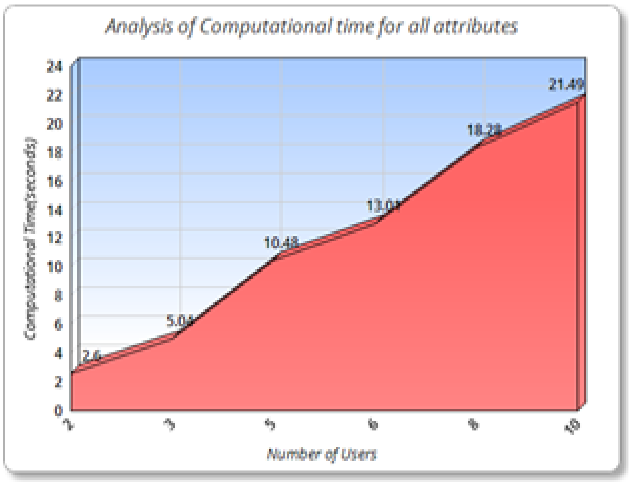

Figure 2: Analysis of Computational time for all attributes

The proposed privacy preserving ID3 decision tree algorithm is producing better accuracy when the number of attributes is limited, but over fits when the number of attributes is increased drastically.

Table III: Comparison of Server's Computational time

Number of Users	PPDANB (s)	PPNBC (s)	Proposed PPDCL(s)
2000	3.6	3.02	2.01
4000	6.34	5.8	4.62
6000	11.62	10.26	9.22
8000	15.54	14.52	13.06
10000	20.02	19.06	18.08
12000	23.09	22.29	21
14000	25.08	24	23.03
16000	27.34	26.98	25.17
18000	31	30.12	30.92
20000	33.62	32.08	31.07

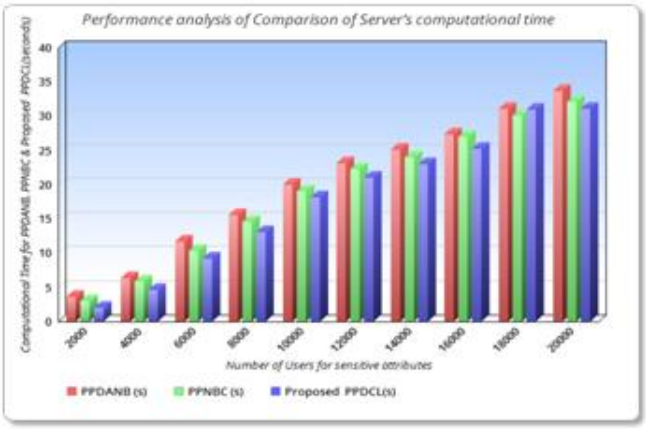

Figure 3: Performance analysis of Comparison of Server's computational time

The accuracy of the proposed algorithm is compared with the existing privacy preserving algorithms and the results are presented in Table 3. and analysis presented in Fig. 3.

V. CONCLUSTION

The proposed privacy preserving ID3 decision tree algorithm protects the user sensitive data in distributed communication. The data miner collects the joint probabilities for the discrete sensitive attributes and transformed value for continuous data. The proposed algorithm is producing maximum accuracy without loss of privacy as the algorithm is implemented using an additive homomorphic ElGamal algorithm. The communication complexity is minimum compared with secure multiparty communication or other randomization methods. The experimental results show that the proposed algorithm is better than existing algorithms.

REFERENCES

1. Evfimievski A, "Randomization in privacy-preserving Data mining". ACM Sigkdd Explorations Newsletter, vol.4, no. 2, pp43-48, 2002.
2. Oded Goldreich, "Secure Multi-Party Computation" 2002 with reference to better exposition provided in Chapter 7 of (Volume 2 of) Foundations of Cryptography. ISBN 0-521-83084-2, Published in the US in May 2004.
3. Lindell Y & Pinkas B, "Secure multiparty computation for privacy-preserving data mining", Journal of Privacy and Confidentiality, vol. 1, no.1, pp.5 – 27,2009

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

4. Krishnamurty Muralidhar & Rathindra Sarathy, “Data Shuffling –A New Masking Approach for Numerical Data Management science”, 2006, Sci.52,658-670. DOI=http://dx.doi.org/10.1287/mnsc.1050.0503.
5. Kargupta H, Datta H, et. al. “On the privacy preserving properties of random data perturbation techniques”, 2003, In The Third IEEE International Conference on Data Mining.
6. A. C. Yao, "Protocols for secure computations" 23rd Annual Symposium on Foundations of Computer Science (sfcs 1982)(FOCS), vol. 00, no. , pp. 160-164, 1982. doi:10.1109/SFCS.1982.88
7. B Pinkas, ”Cryptographic techniques for privacy-preserving data mining” ACM SIGKDD, Volume 4 Issue 2, Pages 12-19, doi - 10.1145/772862.772865,2002.
8. Vaidya J & Clifton C ”Privacy preserving naive Bayes classifier on vertically partitioned data”, SIAM International Conference on Data Mining,2004.
9. Craig Gentry, “Fully homomorphic encryption using ideal lattices” In Proceedings of the forty-first annual ACM symposium on Theory of computing. ACM, New York, NY, USA, 169-178. DOI: https://doi.org/10.1145/1536414.1536440, 2009.
10. Zhiqiang Yang & Sheng Zhong et al “Privacy-Preserving Classification of User Data without Loss of Accuracy”, PG - 92-102, Proceedings of the 2005 SIAM International Conference on Data Mining, 2005,doi - 10.1137/1.9781611972757.9.
11. Agarwal R & Srikant R, “Privacy preserving data mining” In Proc. of ACM SIGMOD Conference on Management of Data, ACM Press, pages 439-450,2000.
12. Du W & Zhan Z, “Using randomized response techniques for privacy-preserving data mining”, In Proc.of the Ninth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining pages 505-510. ACM Press., 2003,doi>10.1145/956750.956810.
13. Zhan J “Using Homomorphic Encryption For Privacy-Preserving Collaborative Decision Tree Classification”, IEEE Symposium on Computational Intelligence and Data Mining, 2007.
14. Chen Tingting & Zhong Sheng, “Privacy-preserving backpropagation neural network learning”, IEEE Transactions, 20(10):1554–1564, DOI: 10.1109/TNN.2009.2026902,2009.
15. Louis J M Aslett & Esperanca M, et al “A review of homomorphic encryption and software tools for encrypted statistical machine learning”, arXiv:1508.06574, 2015b. , 2015.
16. Kaleli C & Polat H “Privacy-Preserving Naïve Bayesian Classifier–Based Recommendations on Distributed Data”, Computational Intelligent,Vol. 31, 2015.
17. Huai Mengdi, Huang Liusheng, et al “Privacy Preserving Naive Bayes Classification” In Proc. of International Conference Knowledge Science, Engineering and Management, Volume 9403, pages 627-638, 2015.
18. Agarwal D, and Agarwal C “On the design and quantification of privacy preserving data mining algorithms” In Proc. of the 20th ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems, ACM Press, pages 247-255, 2001,doi>10.1145/375551.375602.
19. Kantarcioglu M & Vaidya J “Architecture for privacy-preserving mining of client information”, In IEEE ICDM Workshop on Privacy, Security and Data Mining, pages 37-42, 2002.
20. Rebecca Wright and Zhiqiang Yang “Privacy-preserving Bayesian network structure computation on distributed heterogeneous data”, In Proceedings of the tenth ACM SIGKDD international conference on Knowledge discovery and data mining (KDD'04),ACM,NewYork, NY, USA,713-718,2014, DOI=http://dx.doi.org/10.1145/1014052.1014145.
21. Durga Prasad k, et al “Privacy-preserving Data Analysis over Naive Bayesian Classifier for Continuous and Discrete Data”(accepted paper), 2018.
22. Archer, D. W., Bogdanov, D., Lindell, Y., Kamm, L., Nielsen, K., Pagter, J. I., Wright, R. N. “ From Keys to Databases—Real-World Applications of Secure Multi-Party Computation.” The Computer Journal. doi:10.1093/comjnl/bxy090,2018.
23. Lindell, Yehuda & Pinkas, Benny.. “Secure Multiparty Computation for Privacy-Preserving Data Mining.” IACR Cryptology ePrint Archive. 2008. 197. 10.29012/jpc.v1i1.566., 2008.
24. Orlandi, C. “Is multiparty computation any good in practice?” 2011 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). doi:10.1109/icassp.2011.5947691,2011.

AUTHORS PROFILE

K Durga Prasad is working as Assistant professor in department of Information Technology, B V Raju Institute of Technology, Narsapur, Medak district, Telangana, India. He is pursuing Ph.D. in JNT University, Kakinada, A.P, and India. He has obtained PG degree of M. Tech. in Computer Science and Engineering, JNT University, Kakinada, A.P. He has more than 10 years of teaching experience. His research interests include Network security, Web Services, Machine learning techniques and Software Engineering.

Dr. D.Vasumathi presently Professor of CSE, Professor in charge student’s welfare, NSS Coordinator at JNTUH College of Engineering, Jawaharlal Nehru Technological University Hyderabad, Telangana-India. She served and held several academics and administrative positions including hostel warden (JNTUHCEH), Office in charge of examinations (JNTUHCEH), Additional Controller of Examinations (JNTUH), Member of Board of Studies at various JNTUH affiliated colleges and student advisor. She received B.Tech and M.Tech degrees in Computer Science and Engineering from JNT University, Hyderabad and Ph.D in CSE from JNTU, Hyderabad. She is recipient of national award of Savitribai Phule award in 2017. She has guided 12 Ph.D thesis, 60 M.Tech and B.Tech projects and she has published more than 50 research papers in National and International Journals and conferences including IEEE, ACM, Springer and Inderscience publishers. She has 18 years of experience in teaching. She has organized 10 workshops and 3 refreshment courses. She served as confidential team member for EAMCET and Police Recruitment. Her areas of interest are Data Mining, Bigdata Analytics, Cloud Computing and Computer Networks. She is a life member of ISTE and IEEE.