International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 04 April 2025
Page No: 1194-1202
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0171

Privacy-Preserving Machine Learning techniques for Horizontal Distributed Data: A Survey

K. Venkata Sravani[1], Dr. A.P. Siva Kumar[2]
[1]Research Scholar, Department of Computer Science and Engineering, JNTUA, Ananthapuramu, Andhra Pradesh, India.
[2]Professor, Department of Computer Science and Engineering, JNTUA, Ananthapuramu, Andhra Pradesh, India.
Emails: *sravaniannareddy77@gmail.com[1], sivakumar.cse@jntua.ac.in[2]*

Abstract

Privacy-preserving machine learning is the development and deployment of Machine learning (ML) models whereby the data should be shielded from personal privacy concerns during model training. This is the main problem in a distributed system when data is spread over several sites, possibly exposing sensitive information while training the data, particularly in the healthcare and finance industries. There are several ways to address these privacy issues, including differential privacy, secure multi-party computation (SMPC), homomorphic encryption (HE), and federated learning. Techniques for deep learning and machine learning (ML) have a lot of promise for raising productivity. To get decent results, however, the data used to train machine learning models must be of very high quality. Only when there is a large amount of flawless data provided for training can any machine learning algorithm function exceptionally well. In this paper, we offer strategies and provide detailed survey and analysis of privacy-preserving ML techniques such as HE, Multi-party Computation, Federated Learning and Differential Privacy. The proposed work includes analysis of existing techniques and information on the design and implementation of various PPML protocols. We also cover the benefit of privacy during computation in real time applications, which, because to its distributed, secure, and private nature, has the ability to address the security issues raised above.

Keywords: *Machine Learning, Deep Learning, Security, Homomorphic Encryption, Privacy Preserving.*

1. Introduction

Because data and computational resources constantly change, machine learning serves as essential for data analysis and decision-making. A key component of Artificial Intelligence (AI) techniques is the collection of vast amounts of data, which are then used to build forecasting techniques by Machine Learning (ML), the core component of AI. But gathering data and using it to identify patterns in its behavior are two distinct things. Furthermore, managing it presents a number of challenges for both people and businesses, including concerns about privacy like data compromises, monetary losses, and damage to one's reputation. Bridging the gap between privacy and gaining the advantages of machine learning is the aim of privacy-preserving machine learning. It is a vital resource for compliance with data privacy regulations and restructuring a data. Despite the advantages of machine learning applications, there is always a risk to data privacy. Take intrusion detection or healthcare apps, for instance. Data leaks and cyber-attacks are growing more frequent and costly to respond to. Because they can steal information that can be used to recognize individuals or additional important details that can be sold, cybercriminals are attracted to massive collections of data stored for use as training. Furthermore, because sensitive data can be extracted from ML models, the models themselves are vulnerable. The privacy-preserving machine learning approach was born out of the current cloud-based situation for deep learning, security of various assets of any organization, and security of data. There won't be a single way to handle all application types using this PPML methodology. Different applications call for different types of privacy care. Additionally, we need to combine the need to create robust, platform-independent procedures with scenario-specific considerations. Despite the recent explosion in research on safeguarding privacy machine learning, there is still a disconnect between theory and practical applications. Massive data privacy concerns surround the benefits of machine learning applications; take intrusion detection or healthcare apps, for example. Data breaches and cyber-attacks are becoming more prevalent and pricier to respond to. Cybercriminals get drawn to large data sets stored for use as training since they seek to steal information that can be used to identify specific people or additional worthwhile data that can be sold. Furthermore, because sensitive information can be extracted from ML models, the models themselves pose a threat. Shokri et al., for example, illustrate how to determine if a record was utilized in the data set used to train for an exact machine acquiring model. They gained 74% and 94% accuracy, respectively, while evaluating the approach they developed on machine learning systems from Google Cloud and Amazon. Significant progress has been achieved in a broad variety of sectors as a consequence of the machine learning algorithm's outstanding ability to discover patterns and predict outcomes using massive amounts of data. However, using machine learning requires sensitive data, such as personal information. Due to the possible negative effects of disclosing such sensitive information, including identity theft, financial fraud, and prejudice, privacy issues emerge. The use of sensitive data in machine learning processes prompted the development of a new field titled PPML, which specializes on constructing techniques and tools for training and employing machine learning models while respecting the privacy of sensitive data. The purpose of PPML [24,25] is to guarantee sensitive data privacy while still enabling the use of machine learning's advantages. PPML is a multidisciplinary field that combines the areas of cryptography, distributed systems, and machine learning, and it presents several technical challenges such as privacy, accuracy, scalability, and robustness [26,27]. The development of PPML algorithms [4,5] and techniques is crucial for the responsible and ethical use of sensitive data in machine learning.

1.1.Motivation

The primary concern in a distributed setting, where the data is dispersed across many sites, maybe that sensitive data might be exposed while the data is being trained, especially in the healthcare and banking industries [7,8]. The rising accessibility of massive volumes of data across multiple organizations or entities has led to the emergence of broadly distributed information systems in which each entity or organization keeps a portion of the data. When attempting to use machine learning algorithms to analyze and derive insights from the aggregate data while maintaining the secrecy of individual data samples, privacy problems might arise. The goal is to make it possible for several entities to collaborate and share knowledge while guaranteeing that sensitive data is kept secure and private.

1.2.Applications

- **Statistical Analysis:** Differential privacy can be used for analyzing data while preserving individual privacy, such as in health data to study trends without exposing patient information.
- **Social Science Research:** Differential privacy can be used for researching sensitive topics, like political inclinations or sexual behavior, without exposing the identity of participants.
- **ML:** Differential privacy is a technique that may be used to train ML models on info while securing the identification of specific data points.
- **Government Surveillance:** Differential privacy may be used to safeguard people's privacy in government surveillance programs and stop phone and inter- net activity from being tracked.
- **Smart Cities**: Differential privacy may be utilized in smart city initiatives to safeguard people's privacy and stop surveillance based on their movements or energy use sensitive data might be exposed

1.3.Privacy Preserving Machine Learning

PPML [11,12] is the creation and implementation of neural network models where the data must be shielded from personal privacy concerns during model training. There can't be a single way to deal with all application kinds using this PPML approach. Numerous applications call for different types of privacy care. Additionally, we need to combine the need to create robust, platform-independent procedures with scenario-specific factors to consider.

1.4.PPML is Required in Several Phases

Compliance: Machine learning models that make use of personally identifiable information must be developed in line with the stringent regulations that many firms are required to abide by regarding the protection of person- ally identifiable information.

Ethics: The use of personal data in machine learning presents ethical questions, especially when the data is used to inform choices that might have a substantial influence on a person's life, such as those relating to healthcare or credit scoring.

Trust: People are becoming more worried about how their personal information is used, therefore in order to earn and keep the confidence of their clients; businesses must be able to show that they are treating it appropriately.

Data security: Since personal information is a valuable resource that may be targeted by cybercriminals, businesses must take precautions to safeguard it in order to avoid data breaches and other types of data misuse.

Data ownership: People have a right to manage their personal information, and businesses should uphold these rights by letting people decide how their information is used and shared. (Figure 1)

2. Approaches to Privacy Preserving Machine Learning

PPML techniques [13,14] are modern cyber security techniques that help to protect the data while sharing, processing, performing computations, or analysis. There are several approaches to PPML. Some of the most commonly used techniques include Differential Privacy, Federated Learning, SMPC, and HE.

Table 1 Different PPML Techniques

Secure multi-party Computation (SMPC)	A method that lets many people to interact and compute on Secret data without disclosing it to each other.	Provides strong privacy guarantees, can handle complex computations	Can be computationally expensive, difficult to implement
Homomorphic Encryption	A technique that makes it possible to do arithmetic on encrypted material without first deciphering it	Provides strong privacy guarantees, can handle complex computations	Can be computationally expensive, notall types of computations can be performed
Differential Privacy	It is a statistical approach that introduces noise into the original data and then utilises this noisy data to train the models.	Provides strong privacy guarantees, widely accepted as a standard for privacy in machine learning	Can be computationally expensive, difficult to implement, and may lead to loss of utility in the data
Federated Learning	It enables model Training on decentralized data silos without sharing raw data.	Allows for collaboration without sharing data, can handle large amounts of data.	Requires a large number of participants, communication overhead can be high

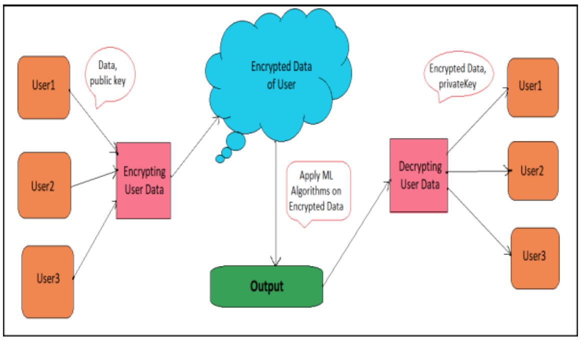

Figure 1 **PPML Model Architecture**

3. Literature Survey

Y. Lindell and Pinkas [1, 23, 24] and Agrawal et al. [1] introduced privacy-preserving data mining.

Various methods are used to build guidelines for reliable multi-party operations, based on the recognized enemy type. The traditional setup for the semi-fair enemy model is a distorted circuits plot. This convention for evaluating Boolean circuits is just two-party, but it is not a "building block" for other conventions, such as n-party ones. A few rounds were conducted in relation to the depth of the plan [38], which addresses this problem for the multi-party scenario and applies to both logic and number-crunching circuits. Limitations on the graded effort, the number of rounds, the computational complexity, and the various nuances of the opponent model are all aspects where many different strategies diverge.

Table 2 **Literature of Existing Techniques and its Drawbacks**

Author/ Reference	**Journal/ Conference**	**Title**	**Drawbacks/ Limitations**
P.N. Annem et.al.,[2]	Journal for Research in Applied Science and Engineering Technology. April 2018	“An Efficient Approach for Privacy Preserving Data Mining using SMC Techniques and Related Algorithms”,	- It is very Simple and constant R is obtained it is easy to retrieve the values
Jiawei Yuan et al., [3]	IEEE Transactions on Cloud Computing Volume: 7, Issue: 2, pp. 568 – 579, 2019	“Practical Privacy-Preserving MapReduce Based K-means Clustering over Large-scale Dataset”	Computational cost is higher.
Yang et al [7]	2005 SIAM international conference on data mining. SIAM; 2005, p. 92–102	Privacy-preserving classification of customer data without loss of accuracy.	The approach is not efficient and useless.
Huai et al [8]	8th International Conference, KSEM 2015, Chongqing, China, October 28-30, 2015	Privacy-preserving naive bayes classification.	Costly and compromises privacy
Li et al., [9]	J.Cluster Computing. 2018 Mar;21:277-86.	Privacy-preserving outsourced classification in cloud computing	High processing cost and poor accuracy
Skarkala ME et.al [10]	J.Computation. 2021 Jan 16;9(1):6	PPDM-TAN: A Multi-party classifier that protects privacy	This is not practical protocol.

4. Practical Privacy Preserving Machine Learning Techniques

In this section, we present very important PPML techniques for real time applications. The use-case, the assets to be safeguarded, and other considerations all influence the choice of a privacy-preserving machine learning technique. Understanding the many elements' aids in choosing the best course of action; there is no magic bullet. Furthermore, we must strike a balance between the requirement to provide portable and reusable methods and scenario-specific requirements. It is important to note that every dataset used in machine learning can theoretically benefit from anonymisation approaches. By doing this, we can prevent or lessen de-anonymization attacks and safeguard people's privacy. These methods can also be used to create a synthetic dataset, which is a new dataset that retains only a few of the original's statistical characteristics but is not produced from it. Furthermore, the model builder can utilize pre-existing, widely-used frameworks rather than particular privacy-preserving ones thanks to anonymisation approaches. However, the accuracy of the target ML model may be impacted if anonymisation approaches are applied independently. Therefore, we address methods that have been specifically studied in relation to machine learning in the sections that follow.

At Initial stages, numerous parties can work together to compute a function on their private data using the confidential multi-party calculating (MPC) technique without compromising their data to one another. While letting them to check out the results of the computation, this method ensures that no one party may access or derive whatever about the private data of the different parties.

4.1.Secure multi-party computation

- **Data Encryption:** Each side employs a safe encryption technique to encrypt its private input data.
- **Data sharing:** The parties exchange encrypted data. Various methods, such as secret sharing, where one party gives the other parties access to a piece of their data, may be used to accomplish this.
- **Computation:** The parties collaborate in order to calculate the encrypted data. This is made possible via homomorphic keys, which allows the parties to perform computations directly on the information that is encrypted by employing encrypted gates. Result Decryption of the computed result occurs after it has been encrypted and distributed to the parties. The parties then decode the output to get the final plaintext output using their decryption keys. (Figure 2)

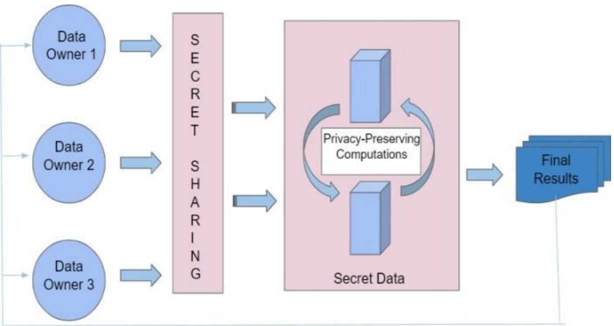

Figure 2 Implementation Diagram of Secure Multi-Party Computation

4.2.Homomorphic Encryption

HE [26,35] is a cryptographic technique that allows encrypted data to be processed without revealing the underlying data. Homomorphic encryption allows machine learning models to be trained on encrypted data while protecting the anonymity of individual data sources.

- **Data Encryption:** The first step is to encrypt the data using a homomorphic encryption algorithm. The encryption algorithm converts the plaintext data into cipher text, which is unreadable without the decryption key.
- **Encryption Key Generation:** To perform computations on the encrypted data, a special key is needed. This key is generated during the encryption process and can be used for encrypting and decrypting the data.
- **Data Transformation:** The encrypted data is translated into a particular for- mat that permits calculations to be conducted on it. This format is intended to allow mathematical operations on encrypted data without disclosing the underly ing plaintext data.

- **Computation:** Once the data has been changed, it may be used to do calculations. Certain mathematical operations, such as addition and multiplication, may be performed on encrypted data using homomorphic encryption. More sophisticated procedures, on the other hand, may need extra phases.
- **Result Decryption:** After the computation is performed, the result is trans- formed back into its original encrypted format. The decryption key is then used to decrypt the result and obtain the final plaintext result. (Figure 3)

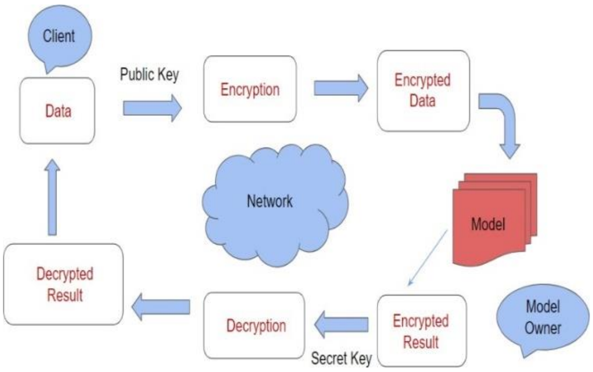

Figure 3 Implementation Diagram of Homomorphic Encryption

Since Gentry's [25,26] first bootstrapping approach was published in 2009, several additions to FHE have been made. A number of surveys compile the work done in FHE and give scholars a good knowledge base.

5. Future Research Directions

Zero-knowledge protocols can be used to stop hostile activity in certain real-life situations [42] where the prover has to establish the verifier. Identifying some more effective techniques made for adversarial computational models in this privacy-preserving distributed rule mining for association's scenario is an additional field of study focus. Developing more computationally efficient mechanisms for adversarial computational models in multi-cloud-based privacy-preserving distributed rule mining of association environments with more precise and accurate rule-sets is our main research priority for the future. Several organizations such as Google, MasterCard, and Facebook are using MPC. Numerous PPNBC [12] (Privacy-Preserving Naive Bayes Classifier) solutions have been put out for a number of applications, including malware detection systems, medical data analytics, and recommendation systems.

Conclusion

A thorough overview and analysis of privacy-preserving machine learning techniques, such as homomorphic cryptography multiparty processing, federation of learning, and differential privacy, is included in this work. The proposed work entails examining current methodologies and data on the development and execution of several Privacy-Preserving Machine Learning (PPML) protocols. We also discussed the advantages of privacy in real-time computation systems, which, due to their dispersed, safe, and confidential characteristics, are capable of addressing the aforementioned security concerns. In conclusion, we will now delineate prospective avenues for further research.

References

[1]. Agrawal, R., and Srikant, R. (2000). Privacy Preserving Data Mining. ACM SIGMOD International Conference on Management of Data, SIGMOD00, Dallas, USA. 439-450.

[2]. P.Annan Naidu, Dr. M. Vamsi Krishna"An Efficient Approach for Privacy Preserving Data Mining using SMC Techniques and Related Algorithms", International Journal for Research in Applied Science & Engineering Technology, April 2018, DOI:10.22214/ijraset.2018.4292

[3]. Jiawei Yuan et al.,Practical Privacy-Preserving MapReduce Based K-means Clustering over Large-scale Dataset" IEEE Transactions on Cloud Computing Volume: 7, Issue: 2, pp. 568 – 579, 2019.

[4]. G. Mathew, Z. Obradovic "A Privacy-Preserving Framework for Distributed Clinical Decision Support", 2011 IEEE 1st International Conference on Computational Advances in Bio and Medical Sciences (ICCABS) 10.1109/ICCABS.2011.5729866

[5]. Zakaria Gheid et.al, "Efficient and Privacy-Preserving k-Means Clustering for Big Data

Mining". 2016 IEEE Trustcom/BigDataSE/ISPA DoI:10.1109/TrustCom.2016.0140, 2016.

[6]. Upmanyu, M.,Namboodiri,A.M., Srinathan,K., Jawahar,C.V. :Efficient Privacy Preserving K-Means Clustering. PAISI 2010. LNCS, vol. 6122, pp. 154166. Springer, Heidelberg (2010).

[7]. Yang Z, Zhong S, Wright RN. Privacy-preserving classification of customer data without loss of accuracy. In: Proceedings of the 2005 SIAM international conference on data mining. SIAM; 2005, p. 92–102. http://dx.doi.org/10.1137/ 1.9781611972757.9

[8]. Huai M, Huang L, Yang W, Li L, Qi M. Privacy-preserving naive bayes classification. InKnowledge Science, Engineering and Management: 8th International Conference, KSEM 2015, Chongqing, China, October 28-30, 2015, Proceedings 8 2015 (pp. 627-638). Springer International Publishing.

[9]. Li P, Li J, Huang Z, Gao CZ, Chen WB, Chen K. Privacy-preserving outsourced classification in cloud computing. Cluster Computing. 2018 Mar;21:277-86.

[10]. Skarkala ME, Maragoudakis M, Gritzalis S, Mitrou L. PPDM-TAN: A privacy-preserving multi-party classifier. Computation. 2021 Jan 16;9(1):6

[11]. Vu DH, Vu TS, Luong TD. An efficient and practical approach for privacy-preserving Naive Bayes classification. Journal of information Security and Applications. 2022 Aug 1;68:103215.

[12]. Duy-Hien Vu, Privacy-preserving Naive Bayes classification in semi-fully distributed data model, Computers & Security, Volume 115, April 2022, 102630.

[13]. Zhang, Q., Yang, L.T., Chen, Z.: Privacy preserving deep computation model on cloud for big data feature learning. IEEE Trans. Comput. 65, 1351–1362 (2016). https://doi.org/10.1109/ TC.2015.2470255.

[14]. Takabi, H., Hesamifard, E., Ghasemi, M.: Privacy preserving multi-party machine learning with homomorphic encryption. In: 29th Annual Conference on Neural Information Process- ing Systems (2016).

[15]. Phong, L.T., Aono, Y., Hayashi, T., Wang, L., Moriai, S.: Privacy-preserving deep learning via additively homomorphic encryption. IEEE Trans. Inf. Forensics Secur. 13, 1333–1345 (2018).

[16]. Wagh, S., Gupta, D., Chandran, N.: SecureNN: 3-party secure computation for neural network training. Proc. Priv. Enhancing Technol. 2019, 26–49 (2019).

[17]. Valeria Nikolaenko, Udi Weinsberg, Stratis Ioannidis, Marc Joye, Dan Boneh, Nina "Privacy-Preserving Ridge Regression on Hundreds of Millions of Records", 2013 IEEE Symposium on Security and Privacy, DOI: 10.1109/SP.2013.30.

[18]. Supriya S. Borhade ,Bipin B. Shinde "Privacy Preserving Data Mining Using Association Rule With Condensation Approach" IJETAE, Volume 4, Issue 3, March 2014.

[19]. Verykios, S., Bertino, E., Fovino, I., Provenza, L., Saygin, Y., Theodoridis, Y.: State of the-art in Privacy Preserving Data Mining. ACM SIGMOD Record 33(1), 5057 (2004).

[20]. X. Juan and Z. Yanqin, ''Application of distributed oblivious transfer protocol in association rule mining,'' in Proc. 2nd IEEE Int. Conf. Comput. Eng. Appl., Washington, DC, USA, Mar. 2010, pp. 204–207.

[21]. H. Chahar, B. N. Keshavamurthy, and C. Modi, ''Privacy-preserving distributed mining of association rules using Elliptic-curve cryptosystem and Shamir's secret sharing scheme,'' Sadhan ¯ a ¯, vol. 42, no. 12, pp. 1997–2007, Dec. 2017.

[22]. Jin Yaoan, Chunhua Su, Na Ruan, and Weijia Jia. "Privacy-Preserving Mining of Association Rules for Horizontally Distributed Databases Based on FP-Tree." International Conference on Information Security Practice and Experience. Springer International Publishing, pp. 300- 314, 2016.

[23]. Lindell, Y, Pinkas, B. (2002). Privacy

Preserving Data Mining. Journal of Cryptology, 15 (3), 177-206. (An extended abstract appeared in Advances in Cryptology, CRYPTO-2000. 36-54.)

[24]. G. Aggarwal, N. Mishra, and B. Pinkas. Secure computation of the kth ranked element. In Proc. Advances in Cryptology EUROCRYPT 2004, volume 3027 of LNCS, pages 4055. Springer, 2004.

[25]. Pinkas, B.: Cryptographic techniques for privacy-preserving data mining. SIGKDD Explor. Newslett. 4(2), 1219 (2002),

[26]. E.Bertino,I.N. Fovino, L.P. Provenza. A Framework for Evaluating Privacy Preserving Data Mining Algorithms. Data Mining and Knowledge Discovery, 11 (2): pp. 121-154, 2005.

[27]. Ouda, Mohamed & Salem, Sameh & Ali, Ihab & Saad, El-Sayed. (2012). Privacy-Preserving Data Mining (PPDM) Method for Horizontally Partitioned Data. IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 5, No 1, September 2012.

[28]. Ankit Chouhan, Sankita Patel, D.C.Jinwala, “Elliptic Curve Cryptography Based Algorithms to Implement Privacy Preserving Clustering through Secure Multiparty Computation”, Journal of Information Security, Scientific Research, 2014, 5, 12-18.

[29]. Harendar Chahar, B N Keshava murthy, and Chirag Modi, Privacy-preserving distributed mining of association rules using Elliptic-curve cryptosystem and Shamir’s secret sharing scheme, Sadhana, Vol. 42, No. 12, December 2017, pp. 1997–2007.

[30]. O. A. Wahab, M. O. Hachami, M. Vivas, G. G. Dagher, and A. Zaffari, ‘‘DARM: A privacy-preserving approach for distributed association rules mining on horizontally-partitioned data,’’ in Proc. 18th Int. Database Eng. Appl. Symp., Porto, Portugal, 2014, pp. 1–8.

[31]. S.U. Fahina “Securing the data in cloud using Algebra Homomorphic Encryption scheme based on updated Elgamal (AHEE)”, International Journal of Emerging Trends & Technology in Computer Science, (2017).

[32]. G. Sathish Kumar, K. Premalatha, G. Uma Maheshwari, P. Rajesh Kanna, No more privacy Concern: A privacy-chain based homomorphic encryption scheme and statistical method for privacy preservation of user’s private and sensitive data, Expert Systems with Applications, Volume 234, 30 December 2023, 121071.

[33]. Clifton C, Kantarcioglu M, Vaidya J, Lin X, Zhu MY. Tools for privacy preserving distributed data mining. ACM SIGKDD Explor Newsl 2002;4(2):28–34.

[34]. Hesamifard, Ehsan, et al. "Privacy-preserving machine learning as a service." Proc. Priv. Enhancing Technol. 2018.3 (2018): 123-142.

[35]. S. Sav, J. P. Bossuat, J. R. Troncoso-Pastoriza, M. Claassen, and J. P. Hubaux, “Privacy-preserving federated neural network learning for disease-associated cell classification,” Patterns, vol. 3, no. 5, p. 100487, 2022, doi: 10.1016/j.patter.2022.100487

[36]. Sen Su, Yiping Teng, Xiang Cheng, Yulong Wang, and Guoliang Li. Privacy-preserving top-k spatial keyword queries over outsourced database. In Proceedings of the 20th International Conference on Database Systems for Advanced Applications, DASFAA’15, pages 589– 608, 2015.

[37]. Payal V Parmar, Shraddha B Padhar, Shafika N Patel, Niyatee I Bhatt and Rutvij H Jhaveri. Article: Survey of Various Homomorphic Encryption algorithms and Schemes. International Journal of Computer Applications 91(8):26-32, April 2014

[38]. Benzekki, Kamal & El Fergougui, Abdeslam & El Belrhiti El Alaoui, Abdelbaki. (2016). A Secure Cloud Computing Architecture Using Homomorphic Encryption. International Journal of Advanced Computer Science and Applications. 7. 10.14569/IJACSA.2016.070241, 2016.

[39]. Pedersen, Thomas & Saygin, Yucel & Savas, Erkay. (2007). Secret Sharing vs. Encryption-based Techniques For Privacy Preserving

Data Mining 1, 2007.

[40]. Nomura, Kenta & Shiraishi, Yoshiaki & Mohri, Masami & Morii, Masakatu. (2020). Secure Association Rule Mining on Vertically Partitioned Data Using Private-Set Intersection. IEEE Access. PP. 1-1. 10.1109/ACCESS.2020.3014330, 2020.

[41]. Behnia, R., Ebrahimi, M., Riasi, A., Chow, S. S. M., Padmanabhan, B., and Hoang, T., “Efficient Secure Aggregation for Privacy-Preserving Federated Machine Learning”, 2023. doi:10.48550/arXiv.2304.03841.

[42]. Z. Liu, J. Guo, K. -Y. Lam and J. Zhao, "Efficient Dropout-Resilient Aggregation for Privacy-Preserving Machine Learning," in IEEE Transactions on Information Forensics and Security, vol. 18, pp. 1839-1854, 2023, doi: 10.1109/TIFS.2022.3163592.

[43]. Chengliang Zhang, Suyi Li, Junzhe Xia, Wei Wang, Feng Yan, and Yang Liu. 2020.Efficient homomorphic encryption for federated learning. In 2020 USENIX annual technical conference (USENIX ATC 20). 493–506.

[44]. Mohassel, P.; Rindal, P. ABY3: A Mixed Protocol Framework for Machine Learning. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, Toronto, ON, Canada, 15–19 October 2018; pp. 35.