Journal of Trends and Challenges in Artificial Intelligence

ASPUR PUBLISHING

Vol. 02, No. 03 (2025) 219-224, DOI: 10.61552/JAI.2025.03.001 - http://jai.aspur.rs

PRIVACY-PRESERVING MACHINE LEARNING ON ENCRYPTED DATA USING HOMOMORPHIC ENCRYPTION

Sandesh Kokad [1]
Pravin Shinde
Karan Rai
Prathamesh Adawale
Harsha Patil

Received 14.07.2024.
Revised 27.08.2024.
Accepted 22.09.2024.

Keywords:

Privacy-preserving machine learning, Homomorphic encryption, Encrypted data, Data privacy, Machine learning [ML] algorithms.

ABSTRACT

The rising adoption of machine learning (ML) across various industries has sparked concerns due to the sensitive nature of the data involved and the opacity surrounding its collection, aggregation, and sharing practices. To address these concerns, researchers are actively developing methods to mitigate privacy risks associated with ML applications. One such approach involves integrating privacy-preserving mechanisms into active learning techniques. By leveraging homomorphic encryption-based federated learning, which enables distributed computation across multiple clients while maintaining strong data privacy, researchers have proposed a scheme that safeguards user data privacy in active learning scenarios. Experimental results indicate that this approach effectively preserves privacy while maintaining model accuracy. Additionally, a comparison with other schemes highlights its superiority in mitigating gradient leakage, with the proposed scheme exhibiting no gradient leakage compared to alternatives that suffer from significant leakage rates exceeding 74%.

The growing adoption of machine learning (ML) is prompting concerns due to the sensitive nature of the data involved and the lack of transparency in data collection, aggregation, and sharing. As a result, various approaches are being devised to mitigate privacy risks and enhance acceptability, particularly in sectors like healthcare where ML's potential remains largely untapped. This study delves into cryptographic and security techniques to develop novel confidentiality assurances for both data and ML models.

1. INTRODUCTION

In an era where data holds immense value, safeguarding it during computations becomes paramount. Privacy-preserving computation encompasses a range of techniques and algorithms designed to process data while upholding its confidentiality and integrity (Tang et al. 2016). These methods ensure that sensitive information remains safeguarded while still enabling the extraction of valuable insights. In today's data-centric landscape, privacy-preserving computation has emerged as a critical priority for businesses and organizations striving to shield sensitive data and adhere to rigorous data protection regulations (Georgiadis & Poels 2021). Conducting a thorough market analysis within the privacy-preserving computation sector is essential for grasping market dynamics, identifying key players, and

[1] Corresponding author: Sandesh Kokad
Email: sandeshkokad@gmail.com

tracking emerging trends (Gupta et al. 2020, Chanal, et al. 2021, Inibhunu et al. 2021).

Privacy-preserving computation encompasses various techniques and algorithms that allow for data processing while maintaining its confidentiality and integrity (Zhang et al. 2021, Kale et al. 2024). These methods ensure the security of sensitive information, enabling valuable insights to be extracted from the data (Thapa & Camtepe 2021). In the current data-driven environment, privacy-preserving computation has gained increasing importance as businesses and organizations aim to safeguard sensitive data and comply with stringent data protection regulations. A comprehensive market analysis of the privacy-preserving computation sector is essential for understanding market dynamics, key players, and emerging trends.

Objective: This report seeks to provide an overview of the technical intricacies surrounding privacy-preserving computation, alongside a comprehensive analysis of the privacy-preserving computation sector. The analysis will delve into aspects such as market size and growth trajectory, prominent industry players, technological innovations, and potential opportunities for start-ups within the field. A comprehensive evaluation of the privacy-preserving computation sector, encompassing an in-depth market analysis, is conducted. This analysis primarily concentrates on the industry's market size and growth, key participants, technological advancements, and potential start-up prospects.

2. LITERATURE REVIEW

The increasing adoption of machine learning (ML) has raised significant concerns about data privacy. Sensitive information, such as medical records, financial data, and personal identifiers, is often used to train ML models. To address these privacy concerns, researchers have explored various techniques, including homomorphic encryption (HE). HE allows for computations on encrypted data without decrypting it, making it a promising tool for privacy-preserving ML.

Practical Privacy-Preserving Machine Learning using Fully Homomorphic Encryption (Brand & Pradel 2023): delves into a practical approach for training machine learning models using FHE, achieving faster training speeds compared to previous works.

Privacy Preserving Machine Learning with Homomorphic Encryption and Federated Learning (Fang & Qian 2021) explores a framework for PPML that combines partially homomorphic encryption (PHE) with federated learning, focusing on mitigating gradient leakage during training.

Challenges and Advancements:

Privacy-Preserving Machine Learning with Fully Homomorphic Encryption for Deep Neural Network (Lee et al. 2022) highlights the limitations of existing PPML models on FHE encrypted data, particularly regarding non-standard activation functions and the lack of bootstrapping for continuous evaluations. It proposes solutions for addressing these challenges.

Homomorphic Encryption for Secure Multi-Party Computation (Das 2018, Kumar et al. 2020, Zhou et al. 2021, Wang & Zhou 2022): Explore research on using HE to enable secure multi-party computation, where multiple parties can collaborate on tasks without revealing their individual data.

Explainable AI with Homomorphic Encryption (Jagatheesaperumal et al. 2022, Saraswat et al. 2022, Dwivedi et al. 2023): Investigate the potential of HE in facilitating explainable AI for models trained on encrypted data. This is relevant to your future scope point on "Explainable AI."

3. OVERVIEW

3.1 Fully Homomorphic Encryption (FHE):

Gentry's breakthrough: Gentry's work in 2009 introduced the concept of FHE, enabling arbitrary computations on encrypted data (Gentry 2009, Gentry et al. 2012).

Recent advancements: Subsequent research has focused on improving the efficiency and practicality of FHE schemes. Gentry (2009) presented fully homomorphic encryption using ideal lattices.

3.2 Linear regression: Several studies have explored the application of HE to linear regression models.

3.3 Neural networks: Deep learning models have also been adapted for privacy preserving training using HE.

3.4 Other algorithms: Other ML algorithms, such as logistic regression and support vector machines, have been investigated in the context of HE.

3.5 Privacy-Preserving in Machine Learning:

Privacy-preserving machine learning (PPML) is a subfield of machine learning that focuses on protecting the privacy of sensitive data while still enabling effective model training and inference. This is particularly important in domains where data contains personal or confidential information, such as healthcare, finance, and government.

3.6 Homomorphic Encryption:

Homomorphic Encryption (HE) is a cryptographic strategy that permits computations to be performed on scrambled information without decoding it.

Encryption: Data is encrypted using a public key, resulting in a cipher text. Computation: Operations (e.g., addition, multiplication) are performed directly on the cipher text.

Decryption: The result of the computation is unscrambled utilizing a private key, uncovering the plain text result.

3.7 Working with Homomorphic Encryption:

Homomorphic Encryption (HE) is a cryptographic procedure that permits computations to be performed straightforwardly on scrambled information without unscrambling it (Figure 1). This is particularly useful for scenarios where data privacy is paramount and computations need to be outsourced to untrusted parties.

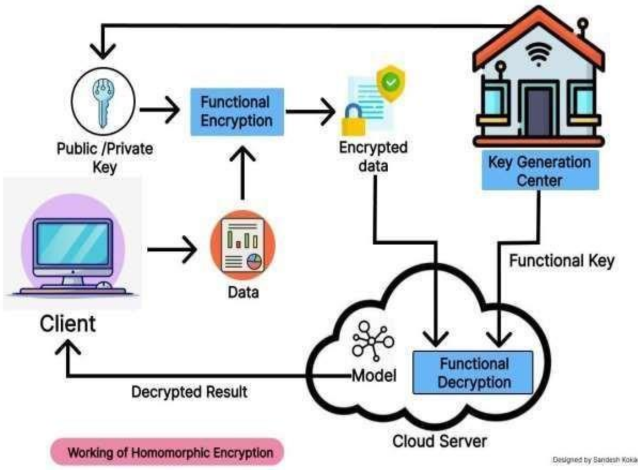

Figure 1-Working of Homomorphic Encryption

Key Generation:

A combination of public and private keys is generated. The open key is used for encryption, whereas the private key is used for unscrambling.

Encryption:

Plain text data is encrypted using the public key to produce cipher text.

The cipher text is indistinguishable from random noise, ensuring data confidentiality.

Operations (e.g., addition, multiplication) are performed directly on the ciphertext. Homomorphic encryption schemes allow these operations to be carried out without revealing the underlying plain text.

Decryption:

The computation result (still in cipher text form) is decrypted using the private key. This reveals the plain text result of the operation.

3.8 Homomorphic Encryption Protects Data Privacy in Search Operations:

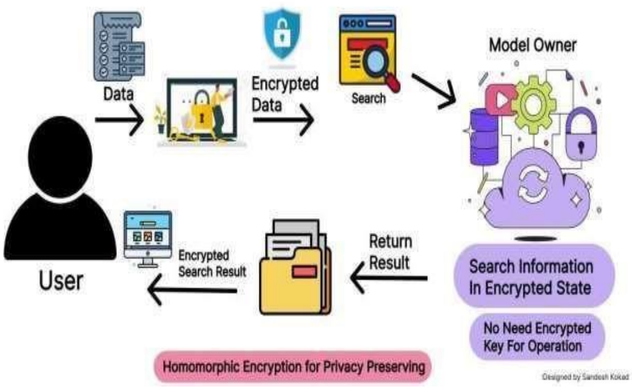
Data
Encrypted Data
Search
Model Owner
User
Encrypted Search Result
Return Result
Search Information In Encrypted State
No Need Encrypted Key For Operation
Homomorphic Encryption for Privacy Preserving
Designed by Sandesh Kokad

Figure 2 - Homomorphic Encryption for privacy Preserving

Presents how homomorphic encryption enables privacy-preserving operations by allowing computations on encrypted data without compromising its confidentiality (Figure 2). This is particularly useful in scenarios where data privacy is a critical concern, such as in cloud computing, machine learning, and data analytics.

Data: The user's data is represented by the document icon.

Encryption: The data is encrypted using a public key, ensuring its confidentiality. This is represented by the lock icon and the label "Encrypted Data." Search: The encrypted data is sent to the model owner for search.

Search Information in Encrypted State: The model owner performs the search operation directly on the encrypted data without decrypting it. This is possible due to homomorphic encryption, which allows computations on encrypted data. Return Result: The search result is returned to the user in an encrypted state.

No Need for Encrypted Key for Operation: A key point is that the model owner does not need the encrypted key to perform the search operation. This further enhances privacy as the model owner does not have access to the plain text data.

4. METHODOLOGY

Data Encryption: Data is encrypted using homomorphic encryption methods, like partially homomorphic encryption (PHE) or Fully Homomorphic Encryption (FHE). This ensures that the data remains secure even during computations.

Model Training: The machine learning model is trained using the encrypted data, ensuring that sensitive information is never exposed during the training process.

Evaluation: The performance of the trained model is evaluated on encrypted test data to ensure it can perform well without compromising data privacy.

Decryption: After the computations, the final model or prediction outputs can optionally be decrypted to obtain plaintext results if necessary.

Privacy Assurance: The privacy guarantees of the homomorphic encryption scheme are validated by analyzing its security properties, ensuring that sensitive information remains protected throughout the entire process.

Performance Optimization: Techniques like batching operations and model simplification are implemented to improve computation efficiency and speed on encrypted data.

Deployment: The system is deployed in real-world applications, adhering to relevant privacy regulations and standards.

5. CHALLENGES

Computational Overhead:

Homomorphic encryption is computationally expensive, leading to increased processing time and resource consumption compared to traditional ML methods. **Scalability:** Scaling homomorphic encryption for large datasets or complex ML models can be difficult, as the computational load grows exponentially challs. **Model Accuracy:** Balancing privacy and accuracy is challenging. Some encryption schemes may introduce noise or reduce precision, potentially impacting the model's performance.

Data Management: Managing encrypted data across distributed systems adds complexity, particularly in ensuring data consistency and integrity.

Regulatory Compliance: Ensuring compliance with various data protection regulations while using encryption methods can be a complex legal challenge.

6. BENIFITS

Enhanced Privacy: Homomorphic encryption ensures that sensitive data remains encrypted throughout the ML process, significantly reducing the risk of data breaches.

Collaboration and Data Sharing: Enables secure collaboration across different organizations or departments by allowing them to share encrypted data without exposing sensitive information.

Regulatory Compliance: Helps organizations comply with stringent data protection laws by providing strong privacy guarantees.

Data Utility: Despite the encryption, useful insights and predictions can still be derived from the data, ensuring that the data remains valuable.

Cross-Domain Applications: The approach is particularly beneficial in domains like healthcare and finance, where data privacy is crucial but data sharing is also essential for innovation.

7. DIFFICULTY

Data Privacy in Machine Learning: With the increasing adoption of ML across industries, the privacy of sensitive data has become a significant concern. Traditional ML methods often require access to raw data, leading to potential privacy breaches.

Gradient Leakage: In some ML methods, gradients can leak sensitive information, which poses a risk, especially in federated learning environments where multiple clients are involved.

8. SOLUTION

Homomorphic Encryption-Based ML: This approach integrates homomorphic encryption with ML, allowing computations to be performed on encrypted data without ever needing to decrypt it. This method addresses privacy concerns by ensuring that sensitive data remains encrypted throughout the entire process.

Federated Learning: The use of homomorphic encryption in federated learning environments allows multiple clients to collaboratively train a model without sharing their raw data, thus preventing gradient leakage and enhancing privacy.

Advanced Encryption Techniques: Implementing fully homomorphic encryption (FHE) and optimizing computations to make them more efficient can further enhance privacy while maintaining model accuracy and performance.

9. RESULTS

Improved privacy: Data remains encrypted throughout processing, reducing the risk of data breaches. Secure **multi-party computation:** Enables collaborative machine learning while maintaining data confidentiality. **Private data analysis:** Train models on encrypted data, ensuring sensitive information remains protected. **Secure outsourcing:** Send encrypted data to third-party services for computation, without exposing the data. **Collaborative learning:** Multiple parties can jointly train models on their combined encrypted data, without revealing individual data.

10. DISCUSSION

Homomorphic encryption is computationally intensive, slowing down machine learning processes. Balancing privacy, computational efficiency, and model accuracy. Developing more efficient homomorphic encryption schemes and optimizing machine learning algorithms for encrypted data.

11. FUTURE SCOPE

The future scope of privacy-preserving machine learning on encrypted data using homomorphic encryption in bullet points Enable multiple parties to jointly train machine learning models on their combined encrypted data, without revealing individual data. Advancements in HE algorithms and hardware acceleration will reduce computational overhead, making PPML more practical.

Multi-Party Computation: He will enable secure multi-party computation, allowing multiple parties to collaborate on machine learning tasks without revealing their data. Homomorphic encryption will enable secure multi-party computation, allowing multiple parties to jointly perform computations on their combined encrypted data. Homomorphic encryption will facilitate explainable AI, enabling secure interpretation of machine learning models trained on encrypted data. Optimized homomorphic encryption for deep learning. Facilitate secure data sharing between organizations, enabling collaboration while maintaining data confidentiality.

12. CONCLUSION

In conclusion, leveraging homomorphic encryption for privacy-preserving machine learning on encrypted data offers a ground breaking solution to protect sensitive information while still enabling valuable insights to be extracted. This approach not only addresses privacy concerns but also opens up new opportunities for collaboration and data sharing across domains. Moving forward, continued advancements in this field will be crucial to realizing the full potential of secure and collaborative machine learning in various industries.

Acknowledgement:
We would like to express our sincere gratitude to Prof. Harsha Patil for her invaluable guidance and support throughout the course of our research. Her expertise and insightful feedback greatly contributed to the development of this work. We also extend our heartfelt thanks to our peers and the faculty at MIT ACSC Alandi, Pune, for their encouragement and assistance. This research was conducted as part of our final year MSC CA program, and we are deeply appreciative of the resources and opportunities provided by the institution.

References:

Brand, M., & Pradel, G. (2023). Practical Privacy-Preserving Machine Learning using Fully Homomorphic Encryption. *Cryptology ePrint Archive*. Accessed 10.08.2024: https://eprint.iacr.org/2023/1320.pdf

Chanal, P. M., Kakkasageri, M. S., & Manvi, S. K. S. (2021). Security and privacy in the internet of things: computational intelligent techniques-based approaches. In *Recent trends in computational intelligence enabled research* (pp. 111-127). Academic Press.

Das, D. (2018, January). Secure cloud computing algorithm using homomorphic encryption and multi-party computation. In *2018 International Conference on Information Networking (ICOIN)* (pp. 391-396). IEEE.

Dwivedi, R., Dave, D., Naik, H., Singhal, S., Omer, R., Patel, P., ... & Ranjan, R. (2023). Explainable AI (XAI): Core ideas, techniques, and solutions. *ACM Computing Surveys*, *55*(9), 1-33.

Fang, H., & Qian, Q. (2021). Privacy preserving machine learning with homomorphic encryption and federated learning. *Future Internet*, *13*(4), 94.

Gentry, C. (2009, May). Fully homomorphic encryption using ideal lattices. In *Proceedings of the forty-first annual ACM symposium on Theory of computing* (pp. 169-178).

Gentry, C., Halevi, S., & Smart, N. P. (2012, August). Homomorphic evaluation of the AES circuit. In *Annual Cryptology Conference* (pp. 850-867). Berlin, Heidelberg: Springer Berlin Heidelberg.

Georgiadis, G., & Poels, G. (2021). Enterprise architecture management as a solution for addressing general data protection regulation requirements in a big data context: a systematic mapping study. *Information Systems and e-Business Management*, *19*, 313-362.

Gupta, R., Tanwar, S., Al-Turjman, F., Italiya, P., Nauman, A., & Kim, S. W. (2020). Smart contract privacy protection using AI in cyber-physical systems: tools, techniques and challenges. *IEEE access*, *8*, 24746-24772.

Inibhunu, C., & McGregor, C. (2021, March). Privacy Preserving Framework for Big Data Management in Smart Buildings. In *2021 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops)* (pp. 667-673). IEEE.

Jagatheesaperumal, S. K., Pham, Q. V., Ruby, R., Yang, Z., Xu, C., & Zhang, Z. (2022). Explainable AI over the Internet of Things (IoT): Overview, state-of-the-art and future directions. *IEEE Open Journal of the Communications Society*, *3*, 2106-2136.

Kale, R. S., Hase, J., Deshmukh, S., Ajani, S. N., Agrawal, P. K., & Khandelwal, C. S. (2024). Ensuring data confidentiality and integrity in edge computing environments: A security and privacy perspective. *Journal of Discrete Mathematical Sciences and Cryptography*, *27*, 421-430.

Kumar, A. V., Sujith, M. S., Sai, K. T., Rajesh, G., & Yashwanth, D. J. S. (2020, December). Secure Multiparty computation enabled E-Healthcare system with Homomorphic encryption. In *IOP Conference Series: Materials Science and Engineering* (Vol. 981, No. 2, p. 022079). IOP Publishing.

Lee, J. W., Kang, H., Lee, Y., Choi, W., Eom, J., Deryabin, M., ... & No, J. S. (2022). Privacy-preserving machine learning with fully homomorphic encryption for deep neural network. *iEEE Access*, *10*, 30039-30054.

Saraswat, D., Bhattacharya, P., Verma, A., Prasad, V. K., Tanwar, S., Sharma, G., ... & Sharma, R. (2022). Explainable AI for healthcare 5.0: opportunities and challenges. *IEEE Access*, *10*, 84486-84517.

Tang, J., Cui, Y., Li, Q., Ren, K., Liu, J., & Buyya, R. (2016). Ensuring security and privacy preservation for cloud data services. *ACM Computing Surveys (CSUR)*, *49*(1), 1-39.

Thapa, C., & Camtepe, S. (2021). Precision health data: Requirements, challenges and existing techniques for data security and privacy. *Computers in biology and medicine*, *129*, 104130.

Wang, C., & Zhou, R. G. (2022). Secure multi-party convex hull protocol based on quantum homomorphic encryption. *Quantum Information Processing*, *22*(1), 24.

Zhang, Q., Xin, C., & Wu, H. (2021). Privacy-preserving deep learning based on multiparty secure computation: A survey. *IEEE Internet of Things Journal*, *8*(13), 10412-10429.

Zhou, J., Feng, Y., Wang, Z., & Guo, D. (2021). Using secure multi-party computation to protect privacy on a permissioned blockchain. *Sensors*, *21*(4), 1540.

Sandesh Kokad
MIT ACSC, Alandi Pune - 412105
India.
sandeshkokad@gmail.com

Pravin Shinde
MIT ACSC, Alandi Pune - 412105
India.
pravin1920shinde@gmail.com

Karan Rai
MIT ACSC, Alandi Pune - 412105
India.
karankaushalendrarai@gmail.com

Prathamesh Adawale
MIT ACSC, Alandi Pune - 412105
India.
prathameshadawale@gmail.com

Harsha Patil
MIT ACSC, Alandi Pune - 412105
India.
hrpatel888@gmail.com
ORCID: 0000-0001-6519-9987