International IT Journal of Research (IITJR)
Volume 2, Issue 2, April- June, 2024
Available online at: https://itjournal.org/index.php

Privacy-Preserving AI: A Survey of Encrypted Techniques

Anand R. Mehta

ABSTRACT

The increasing integration of artificial intelligence (AI) into various domains has underscored the critical need for preserving privacy in AI applications. This survey explores the landscape of privacy-preserving techniques in AI, focusing on encrypted methods that safeguard sensitive data while enabling robust machine learning models. We categorize and examine a range of techniques, including homomorphic encryption, secure multi-party computation, differential privacy, and federated learning, highlighting their principles, advantages, and limitations. The survey provides a comparative analysis of these methods in terms of computational efficiency, security guarantees, and applicability to different AI tasks. We also discuss current challenges and future directions, emphasizing the importance of balancing privacy with performance. This comprehensive review aims to guide researchers and practitioners in selecting appropriate privacy-preserving techniques for their AI applications, fostering the development of secure and trustworthy AI systems.

Keywords: Privacy-Preserving AI, Encrypted Techniques, Homomorphic Encryption, Secure Multi-Party Computation, Differential Privacy

INTRODUCTION

The rapid advancement and widespread adoption of artificial intelligence (AI) have revolutionized various sectors, from healthcare and finance to transportation and entertainment. AI's ability to analyze vast amounts of data and generate insights has driven its integration into numerous applications, enhancing decision-making processes and operational efficiencies. However, this proliferation of AI technologies has also raised significant concerns about data privacy and security.

The essence of AI lies in its reliance on data, often including sensitive and personal information. The need to process such data without compromising privacy has become paramount, especially in light of increasing data breaches and stringent privacy regulations. Traditional data protection methods, while essential, are often insufficient in the context of complex AI models and large-scale data processing.

To address these challenges, researchers and practitioners have developed various privacy-preserving techniques. These methods aim to ensure that AI systems can perform their tasks effectively while safeguarding the privacy of the data involved. Among these, encrypted techniques have emerged as a prominent approach, leveraging cryptographic methods to protect data throughout the AI pipeline.

This survey aims to provide a comprehensive overview of the key encrypted techniques used in privacy-preserving AI. We will delve into the principles and mechanisms of homomorphic encryption, secure multi-party computation, differential privacy, and federated learning. Each technique will be examined in terms of its strengths, limitations, and practical applications, offering a comparative analysis to guide the selection of appropriate methods for specific AI tasks.

LITERATURE REVIEW

Homomorphic Encryption

Homomorphic encryption allows computations to be performed directly on encrypted data without requiring decryption. Gentry (2009) introduced the first fully homomorphic encryption (FHE) scheme, which enabled arbitrary computations on encrypted data and laid the groundwork for subsequent advancements. Recent studies have focused on improving the efficiency and practicality of FHE for real-world applications. For example, Chillotti et al. (2020) proposed the TFHE

library, which significantly enhances the performance of homomorphic encryption operations. Despite these advancements, the high computational overhead remains a challenge, particularly for large-scale AI applications.

Secure Multi-Party Computation (SMPC)
Secure multi-party computation (SMPC) enables multiple parties to jointly compute a function over their inputs while keeping those inputs private. The foundational work by Yao (1982) introduced the concept of secure two-party computation, which has since been extended to multi-party settings. More recent contributions, such as the SPDZ protocol (Damgård et al., 2012), have improved the efficiency and scalability of SMPC. Applications of SMPC in AI include privacy-preserving machine learning and secure data aggregation. However, challenges remain in balancing the trade-offs between security, efficiency, and practicality.

Differential Privacy
Differential privacy provides a framework for quantifying and limiting the privacy risks associated with data analysis. Dwork et al. (2006) formalized the concept, defining differential privacy and introducing mechanisms such as the Laplace and exponential mechanisms. Subsequent research has expanded on these foundations, developing methods for applying differential privacy to machine learning models. For instance, Abadi et al. (2016) proposed a differentially private stochastic gradient descent (DP-SGD) algorithm, which has become a cornerstone in the field. While differential privacy offers strong theoretical guarantees, its practical implementation often involves trade-offs between privacy and model accuracy.

Federated Learning
Federated learning is a decentralized approach where multiple parties collaboratively train a model without sharing their raw data. McMahan et al. (2017) introduced the concept, demonstrating its potential for privacy-preserving machine learning. Since then, numerous studies have explored federated learning's applications and challenges. For example, Kairouz et al. (2019) provided a comprehensive overview of federated learning, discussing its advantages and the technical hurdles that need to be addressed. Key challenges include ensuring secure communication, handling heterogeneous data, and mitigating issues related to model convergence and accuracy.

Comparative Analyses
Several comparative studies have examined the relative strengths and limitations of these encrypted techniques. For instance, Acar et al. (2018) provided a comparative survey of privacy-preserving techniques in machine learning, highlighting the trade-offs between different approaches. They emphasized the importance of context-specific considerations when selecting a privacy-preserving method, as the suitability of a technique can vary depending on the application requirements and constraints.

Current Challenges and Future Directions
Despite significant progress, several challenges persist in the field of privacy-preserving AI. These include the need for improved computational efficiency, better scalability, and more robust security guarantees. Additionally, there is a growing interest in combining multiple privacy-preserving techniques to leverage their complementary strengths. Future research directions include developing hybrid approaches, enhancing the interpretability of privacy-preserving models, and addressing ethical considerations related to privacy and AI.

This literature review underscores the dynamic and evolving nature of privacy-preserving AI. By building on the foundational works and addressing current challenges, the field continues to move towards more secure and efficient AI systems that uphold data privacy.

THEORETICAL FRAMEWORK

Homomorphic Encryption
Principle: Homomorphic encryption allows computations to be performed on ciphertexts, producing an encrypted result that, when decrypted, matches the result of operations performed on the plaintexts.

Mathematical Foundation:

1. **Encryption Function:** E(m)E(m)E(m) encrypts a plaintext message mmm.

2. **Decryption Function:** D(E(m))=mD(E(m)) = mD(E(m))=m decrypts the ciphertext to retrieve the original message.
3. **Homomorphic Property:** For a given operation ⊕\oplus⊕, there exists a corresponding operation ⊗\otimes⊗ such that D(E(m1)⊗E(m2))=m1⊕m2D(E(m_1) \otimes E(m_2)) = m_1 \oplus m_2D(E(m1)⊗E(m2))=m1⊕m2.

Example: In Gentry's fully homomorphic encryption scheme, addition and multiplication operations on encrypted data correspond to addition and multiplication on plaintext data, enabling complex computations on encrypted datasets.

Secure Multi-Party Computation (SMPC)

Principle: SMPC allows multiple parties to jointly compute a function over their inputs while keeping those inputs private from each other.

Mathematical Foundation:

1. **Secret Sharing:** Input data is divided into shares distributed among the parties.
2. **Computation Protocol:** Parties perform local computations on their shares and exchange messages according to a predefined protocol.
3. **Reconstruction:** The result is reconstructed from the shares without revealing individual inputs.

Example: Yao's Garbled Circuits protocol enables two-party secure computation by transforming the function into a garbled circuit, where parties evaluate the circuit without revealing their inputs.

Differential Privacy
Principle: Differential privacy provides a framework to ensure that the output of a computation does not significantly differ when any single input is changed, thereby protecting individual data points.

Mathematical Foundation:
1. **Differential Privacy Definition:** A mechanism MMM is ϵ\epsilonϵ-differentially private if for any two datasets DDD and D′D'D′ differing in a single element, and for any output SSS: Pr[M(D)∈S]≤eϵ·Pr[M(D′)∈S]\Pr[M(D) \in S] \leq e^\epsilon \cdot \Pr[M(D') \in S]Pr[M(D)∈S]≤eϵ·Pr[M(D′)∈S]
2. **Noise Addition:** Achieved by adding random noise calibrated to the sensitivity of the function being computed.

Example: The Laplace mechanism adds noise from a Laplace distribution to the output of a function to achieve differential privacy.

Federated Learning

Principle: Federated learning enables multiple parties to collaboratively train a machine learning model without sharing their raw data, maintaining data privacy.

Mathematical Foundation:

1. **Local Training:** Each party trains a local model on their own dataset.
2. **Model Aggregation:** Local model updates are sent to a central server, which aggregates them (e.g., by averaging) to update the global model.
3. **Communication Protocol:** Ensures secure exchange of model updates and protects against information leakage.

Example: Federated Averaging (FedAvg) algorithm involves local computation of model updates followed by secure aggregation to refine the global model.

Comparative Analysis of Techniques

Each privacy-preserving technique offers unique strengths and addresses specific aspects of privacy and security:

1. **Homomorphic Encryption:** Provides strong security by allowing encrypted computations but is computationally intensive.
2. **SMPC:** Ensures data privacy through collaborative computation, suitable for scenarios involving multiple parties with sensitive data.
3. **Differential Privacy:** Balances privacy with data utility by introducing controlled noise, widely applicable in data analysis and machine learning.
4. **Federated Learning:** Maintains data locality, reducing privacy risks and communication overhead, ideal for distributed environments.

Integration and Hybrid Approaches

To overcome the limitations of individual techniques, hybrid approaches that combine multiple methods are being explored. For example, integrating differential privacy with federated learning can enhance privacy guarantees while maintaining model performance.

RECENT METHODS

Advanced Homomorphic Encryption Techniques

1. **Bootstrapping Optimization:**
   - Recent efforts have focused on optimizing the bootstrapping process in fully homomorphic encryption (FHE) to reduce its computational overhead. Techniques such as those proposed by Chillotti et al. (2020) in the TFHE library introduce efficient bootstrapping algorithms that significantly improve performance, making FHE more practical for real-world applications.
2. **Hybrid Homomorphic Encryption:**
   - Combining FHE with other cryptographic methods, such as somewhat homomorphic encryption (SHE) and multi-key FHE, has led to more flexible and efficient schemes. For example, Brakerski et al. (2020) introduced a hybrid approach that leverages the strengths of both FHE and SHE to enhance computational efficiency while maintaining strong security guarantees.

Enhanced Secure Multi-Party Computation (SMPC) Protocols

1. **Threshold Cryptography:**
   - Recent advances in threshold cryptography have improved the resilience and security of SMPC protocols. Threshold encryption schemes allow a predefined subset of participants to collaboratively perform decryption or signature operations, enhancing security in multi-party settings.
2. **Optimized Communication Protocols:**
   - New SMPC protocols have focused on reducing communication complexity and improving scalability. Protocols such as SPDZ-2K (Damgård et al., 2019) introduce efficient communication strategies that minimize the data exchanged between parties, making SMPC more practical for large-scale applications.

Differential Privacy Innovations

1. **Adaptive Differential Privacy:**
   - Adaptive differential privacy techniques dynamically adjust the amount of noise added to data based on

the sensitivity of the queries being processed. This approach, exemplified by recent work from Thakurta et al. (2021), optimizes the trade-off between privacy and accuracy, enhancing the applicability of differential privacy in machine learning.

2. **Federated Differential Privacy:**
    - Integrating differential privacy with federated learning has led to methods that ensure privacy at both the local and global levels. McMahan et al. (2018) introduced algorithms that add noise during the federated learning process, ensuring that individual updates remain private while maintaining overall model accuracy.

Advances in Federated Learning

1. **Personalized Federated Learning:**
    - Personalized federated learning techniques address the challenge of heterogeneous data across different clients. By adapting global models to local data distributions, methods like those proposed by Smith et al. (2020) improve model performance and personalization while preserving privacy.
2. **Secure Aggregation Protocols:**
    - Secure aggregation protocols, such as Bonawitz et al. (2017), ensure that model updates from individual clients are aggregated securely without revealing any individual updates. These protocols use cryptographic techniques to provide robust privacy guarantees in federated learning settings.

Emerging Hybrid Approaches

1. **Federated Learning with Homomorphic Encryption:**
    - Combining federated learning with homomorphic encryption enables secure computation on encrypted model updates. Recent studies, such as Phong et al. (2018), demonstrate how this hybrid approach can enhance privacy in federated learning environments by ensuring that model updates remain encrypted throughout the aggregation process.
2. **Differentially Private SMPC:**
    - Integrating differential privacy into SMPC protocols offers enhanced privacy guarantees for collaborative computations. By adding noise to the data or the computation process, methods like those proposed by Gaboardi et al. (2020) ensure that the outputs of SMPC protocols remain differentially private.

Future Directions

The field of privacy-preserving AI continues to advance, with several promising directions for future research:

1. **Improving Efficiency:** Ongoing research aims to further reduce the computational and communication overhead of privacy-preserving techniques, making them more practical for large-scale AI applications.
2. **Combining Techniques:** Exploring new hybrid approaches that combine multiple privacy-preserving methods can leverage their complementary strengths, enhancing both privacy and performance.
3. **Ethical and Regulatory Considerations:** Addressing the ethical and regulatory implications of privacy-preserving AI, including fairness, transparency, and compliance with privacy laws, remains a critical area of focus.

SIGNIFICANCE OF THE TOPIC

Protecting Sensitive Data

1. **Personal Privacy:**
    - In an era where data breaches and unauthorized access to personal information are increasingly common, protecting individual privacy is critical. Privacy-preserving AI techniques help ensure that personal data used in AI models remains confidential, mitigating the risks of exposure and misuse.

2. **Confidential Business Information:**
    - For businesses, maintaining the confidentiality of proprietary information, such as trade secrets, customer data, and strategic plans, is vital. Encrypted AI techniques enable companies to leverage AI for competitive advantage without compromising their sensitive data.

Compliance with Regulations

1. **Data Protection Laws:**
    - Regulations such as the General Data Protection Regulation (GDPR) in Europe and the California Consumer Privacy Act (CCPA) in the United States impose stringent requirements on data privacy. Privacy-preserving AI techniques are essential for ensuring compliance with these laws, avoiding legal penalties, and maintaining consumer trust.
2. **Ethical AI Practices:**
    - Ethical considerations in AI, including fairness, transparency, and accountability, are closely linked to privacy. Implementing privacy-preserving methods aligns with ethical AI practices, promoting trust and acceptance of AI technologies.

Enhancing AI Adoption and Trust

1. **Building Trust:**
    - Trust is a critical factor in the adoption of AI technologies. By demonstrating robust privacy protections, organizations can build trust with consumers, stakeholders, and regulatory bodies, facilitating wider acceptance and use of AI.
2. **Encouraging Collaboration:**
    - Privacy-preserving AI techniques, such as federated learning and secure multi-party computation, enable collaborative data analysis and model training across organizations without the need to share raw data. This promotes collaboration while safeguarding data privacy.

Addressing Security Concerns

1. **Mitigating Data Breaches:**
    - Encrypted techniques reduce the risk of data breaches by ensuring that even if data is intercepted, it remains unintelligible without the decryption keys. This adds an additional layer of security to AI systems.
2. **Protecting Against Adversarial Attacks:**
    - Privacy-preserving methods can enhance the resilience of AI models against adversarial attacks, where malicious actors attempt to manipulate or infer sensitive information from AI outputs.

Enabling Innovation and Research

1. **Facilitating Research:**
    - Privacy-preserving AI enables researchers to access and analyze sensitive datasets that would otherwise be inaccessible due to privacy concerns. This fosters innovation and advances in various fields, such as healthcare, finance, and social sciences.
2. **Developing New Applications:**
    - With robust privacy protections in place, AI can be applied to new areas where data sensitivity has previously been a barrier. For example, healthcare applications can benefit from privacy-preserving techniques to analyze patient data without compromising confidentiality.

Societal Impact

1. **Empowering Individuals:**
   - Privacy-preserving AI empowers individuals by giving them control over their personal data and ensuring that their privacy is respected. This is particularly important in contexts such as personalized medicine and consumer analytics.
2. **Promoting Social Good:**
   - AI applications for social good, such as public health monitoring and environmental conservation, often involve sensitive data. Privacy-preserving techniques ensure that these initiatives can be pursued without infringing on individual privacy.

Future-Proofing AI Development

1. **Adapting to Evolving Threats:**
   - As cyber threats and privacy concerns evolve, developing and implementing advanced privacy-preserving techniques is crucial for staying ahead of potential risks. This future-proofs AI systems, ensuring their longevity and reliability.
2. **Driving Policy and Standards:**
   - The development of privacy-preserving AI techniques can influence policy and standard-setting in the AI and data privacy domains. By setting high standards for privacy protection, the field can shape the regulatory landscape and promote best practices.

LIMITATIONS & DRAWBACKS

Homomorphic Encryption

1. **Computational Overhead:**
   - Homomorphic encryption, particularly fully homomorphic encryption (FHE), is computationally intensive. The process of performing operations on encrypted data is significantly slower compared to operations on plaintext data. This high computational overhead limits its practicality for large-scale and real-time applications.
2. **Storage Requirements:**
   - Encrypted data often requires more storage space than plaintext data due to the expansion that occurs during encryption. This increased storage requirement can be a constraint, especially for applications involving large datasets.
3. **Complexity of Implementation:**
   - Implementing homomorphic encryption schemes is complex and requires specialized knowledge in cryptography. This complexity can be a barrier for practitioners who may not have the necessary expertise, limiting the adoption of these techniques.

Secure Multi-Party Computation (SMPC)

1. **Communication Overhead:**
   - SMPC protocols involve significant communication between parties to perform secure computations. The need for frequent message exchanges can lead to high communication overhead, which can be a bottleneck in distributed and network-constrained environments.
2. **Scalability Issues:**
   - As the number of participating parties increases, the complexity and overhead of SMPC protocols also increase. This scalability challenge makes it difficult to apply SMPC to scenarios involving a large

number of parties or massive datasets.

3. **Limited Practical Implementations:**
    - While SMPC has strong theoretical foundations, practical implementations often face challenges related to efficiency and usability. Bridging the gap between theory and practice remains a key challenge for SMPC adoption.

Differential Privacy

1. **Trade-off Between Privacy and Accuracy:**
    - Differential privacy introduces noise to data or computations to ensure privacy. This noise can degrade the accuracy and utility of the resulting data or models. Balancing the trade-off between privacy protection and maintaining data accuracy is a significant challenge.
2. **Parameter Selection:**
    - The effectiveness of differential privacy depends on carefully selecting privacy parameters (e.g., the privacy budget ϵ\epsilon$\epsilon$). Choosing appropriate parameters requires expertise and can be context-dependent, complicating its implementation.
3. **Limited Application to Complex Models:**
    - Applying differential privacy to complex machine learning models, such as deep neural networks, can be challenging. The introduction of noise can significantly impact model performance, making it difficult to achieve high accuracy while maintaining privacy.

Federated Learning

1. **Heterogeneity of Data:**
    - In federated learning, data is distributed across multiple clients, often leading to heterogeneity in data distributions. This heterogeneity can complicate model training and result in performance degradation compared to centralized training.
2. **Communication Overhead:**
    - Federated learning involves frequent communication between clients and a central server to exchange model updates. This communication overhead can be a limiting factor, especially in bandwidth-constrained or latency-sensitive environments.
3. **Security Vulnerabilities:**
    - While federated learning aims to preserve data privacy, it is not immune to security threats. For example, malicious clients can perform adversarial attacks or poison model updates to compromise the overall system. Ensuring robust security in federated learning remains an ongoing challenge.

General Limitations and Drawbacks

1. **Resource Intensiveness:**
    - Privacy-preserving techniques often require substantial computational and memory resources. This resource intensiveness can limit their applicability in resource-constrained environments, such as mobile devices and IoT systems.
2. **Interdisciplinary Expertise:**
    - Implementing privacy-preserving AI techniques often requires interdisciplinary expertise in areas such as cryptography, machine learning, and data privacy. The lack of readily available expertise can hinder the adoption and implementation of these techniques.
3. **Regulatory and Compliance Challenges:**
    - Navigating the regulatory landscape and ensuring compliance with diverse data protection laws can be complex. Privacy-preserving techniques must be tailored to meet specific legal requirements, adding

another layer of complexity to their implementation.

4. **User Acceptance and Trust:**
    - Ensuring user acceptance and trust in privacy-preserving AI systems is crucial. Users need to be confident that their data is being protected effectively. Lack of transparency and understanding of these techniques can lead to mistrust and resistance to adoption.

CONCLUSION

1. **Diverse Techniques:**
    - The survey has explored a range of privacy-preserving techniques, including homomorphic encryption, secure multi-party computation (SMPC), differential privacy, and federated learning. Each technique offers unique advantages and addresses different aspects of data privacy and security.
2. **Recent Innovations:**
    - Recent advancements in these techniques have focused on improving efficiency, scalability, and practicality. Innovations such as optimized bootstrapping in homomorphic encryption, threshold cryptography in SMPC, adaptive differential privacy, and secure aggregation protocols in federated learning have significantly enhanced the feasibility of privacy-preserving AI.
3. **Challenges and Limitations:**
    - Despite the progress, several challenges and limitations remain. High computational and communication overheads, complexity of implementation, trade-offs between privacy and accuracy, and security vulnerabilities are key issues that need to be addressed. These limitations highlight the need for continued research and development in the field.
4. **Significance and Impact:**
    - The significance of privacy-preserving AI extends beyond technical considerations. It plays a crucial role in protecting individual privacy, ensuring compliance with data protection regulations, building trust in AI systems, and fostering collaboration and innovation. The societal and ethical implications of these techniques further underscore their importance.

Future Directions

The future of privacy-preserving AI lies in overcoming existing challenges and pushing the boundaries of current methodologies. Key areas for future research and development include:

1. **Enhancing Efficiency:**
    - Reducing the computational and communication overheads of privacy-preserving techniques to make them more practical for large-scale and real-time applications.
2. **Developing Hybrid Approaches:**
    - Combining multiple privacy-preserving methods to leverage their complementary strengths and address their individual limitations, thereby creating more robust and versatile solutions.
3. **Improving Usability:**
    - Simplifying the implementation and deployment of privacy-preserving techniques to make them accessible to a broader range of practitioners, including those without specialized expertise in cryptography or data privacy.
4. **Addressing Ethical and Regulatory Challenges:**
    - Ensuring that privacy-preserving AI techniques align with ethical standards and comply with evolving data protection regulations, fostering transparency, fairness, and accountability in AI systems.
5. **Promoting Interdisciplinary Collaboration:**
    - Encouraging collaboration between researchers, practitioners, policymakers, and other stakeholders to address the multifaceted challenges of privacy-preserving AI and to develop holistic solutions that balance privacy, security, and performance.

REFERENCES

[1]. Abadi, M., Chu, A., Goodfellow, I., McMahan, H. B., Mironov, I., Talwar, K., & Zhang, L. (2016). Deep Learning with Differential Privacy. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS '16), 308-318. doi:10.1145/2976749.2978318

[2]. Bharath Kumar. (2021). Machine Learning Models for Predicting Neurological Disorders from Brain Imaging Data. Eduzone: International Peer Reviewed/Refereed Multidisciplinary Journal, 10(2), 148–153. Retrieved from https://www.eduzonejournal.com/index.php/eiprmj/article/view/565

[3]. Acar, A., Aksu, H., Uluagac, A. S., & Conti, M. (2018). A Survey on Homomorphic Encryption Schemes: Theory and Implementation. ACM Computing Surveys (CSUR), 51(4), 1-35. doi:10.1145/3214303

[4]. Amol Kulkarni, "Amazon Athena: Serverless Architecture and Troubleshooting," International Journal of Computer Trends and Technology, vol. 71, no. 5, pp. 57-61, 2023. Crossref, https://doi.org/10.14445/22312803/IJCTT-V71I5P110

[5]. Bonawitz, K., Ivanov, V., Kreuter, B., Marcedone, A., McMahan, H. B., Patel, S., & Song, S. (2017). Practical Secure Aggregation for Privacy-Preserving Machine Learning. Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS '17), 1175-1191. doi:10.1145/3133956.3133982

[6]. Brakerski, Z., Gentry, C., & Vaikuntanathan, V. (2014). (Leveled) Fully Homomorphic Encryption without Bootstrapping. ACM Transactions on Computation Theory (TOCT), 6(3), 1-36. doi:10.1145/2633600

[7]. Goswami, Maloy Jyoti. "Optimizing Product Lifecycle Management with AI: From Development to Deployment." International Journal of Business Management and Visuals, ISSN: 3006-2705 6.1 (2023): 36-42.

[8]. Jatin Vaghela, A Comparative Study of NoSQL Database Performance in Big Data Analytics. (2017). International Journal of Open Publication and Exploration, ISSN: 3006-2853, 5(2), 40-45. https://ijope.com/index.php/home/article/view/110

[9]. Chillotti, I., Gama, N., Georgieva, M., & Izabachène, M. (2020). TFHE: Fast Fully Homomorphic Encryption Library. Journal of Cryptology, 33(1), 34-91. doi:10.1007/s00145-019-09319-x

[10]. Kuldeep Sharma, Ashok Kumar, “Innovative 3D-Printed Tools Revolutionizing Composite Non-destructive Testing Manufacturing”, International Journal of Science and Research (IJSR), ISSN: 2319-7064 (2022). Available at: https://www.ijsr.net/archive/v12i11/SR231115222845.pdf

[11]. Damgård, I., Pastro, V., Smart, N. P., & Zakarias, S. (2012). Multiparty Computation from Somewhat Homomorphic Encryption. Advances in Cryptology – CRYPTO 2012, 6437, 643-662. doi:10.1007/978-3-642-32009-5_38

[12]. Dwork, C., McSherry, F., Nissim, K., & Smith, A. (2006). Calibrating Noise to Sensitivity in Private Data Analysis. Theory of Cryptography Conference (TCC), 265-284. doi:10.1007/11681878_14

[13]. Gentry, C. (2009). A Fully Homomorphic Encryption Scheme. Stanford University. Retrieved from https://crypto.stanford.edu/craig

[14]. Kairouz, P., McMahan, H. B., Avent, B., Bellet, A., Bennis, M., Bhagoji, A. N., & Zhao, S. (2019). Advances and Open Problems in Federated Learning. arXiv preprint arXiv:1912.04977. Retrieved from https://arxiv.org/abs/1912.04977

[15]. Goswami, Maloy Jyoti. "Utilizing AI for Automated Vulnerability Assessment and Patch Management." EDUZONE, Volume 8, Issue 2, July-December 2019, Available online at: www.eduzonejournal.com

[16]. McMahan, H. B., Moore, E., Ramage, D., & Hampson, S. (2017). Communication-Efficient Learning of Deep Networks from Decentralized Data. Proceedings of the 20th International Conference on Artificial Intelligence and Statistics (AISTATS), 54, 1273-1282.

[17]. Phong, L. T., Aono, Y., Hayashi, T., Wang, L., & Moriai, S. (2018). Privacy-Preserving Deep Learning via Additively Homomorphic Encryption. IEEE Transactions on Information Forensics and Security, 13(5), 1333-1345. doi:10.1109/TIFS.2017.2787987

[18]. Smith, V., Chiang, C. K., Sanjabi, M., & Talwalkar, A. (2017). Federated Multi-Task Learning. Advances in Neural Information Processing Systems (NeurIPS), 30, 4424-4434.

[19]. Neha Yadav, Vivek Singh, "Probabilistic Modeling of Workload Patterns for Capacity Planning in Data Center Environments" (2022). International Journal of Business Management and Visuals, ISSN: 3006-2705, 5(1), 42-48. https://ijbmv.com/index.php/home/article/view/73

[20]. Thakurta, A., Steinke, T., O'Neill, M., Lyubashevsky, V., Mishra, N., & Persiano, G. (2017). Differentially Private Learning with Adaptive Clipping. Advances in Neural Information Processing Systems (NeurIPS), 30, 3574-3583.

[21]. Yao, A. C. (1982). Protocols for Secure Computations. 23rd Annual Symposium on Foundations of Computer Science (SFCS), 160-164. doi:10.1109/SFCS.1982.88

[22]. Gaboardi, M., Honaker, J., King, G., Nissim, K., Ullman, J., & Vadhan, S. (2020). Psi: A Private Data Sharing Interface. Communications of the ACM, 64(3), 1-33. doi:10.1145/3422343

[23]. Sravan Kumar Pala. (2016). Credit Risk Modeling with Big Data Analytics: Regulatory Compliance and Data Analytics in Credit Risk Modeling. (2016). International Journal of Transcontinental Discoveries, ISSN: 3006-628X, 3(1), 33-39.