International Journal of Soft Computing and Engineering (IJSCE)
ISSN: 2231-2307 (Online), Volume-14 Issue-1, March 2024

Effectiveness in Collaborative Framework for Non-Invasive in AI Algorithms

Sandeep Kulkarni, B.Vijayendra Reddy

***Abstract:** The topic of study and practice known as "privacy-preserving machine learning (PPML)" is devoted to creating methods and strategies that enable the training and application of machine learning models while protecting the privacy of sensitive data for convolution neural network and Machine learning algorithms. Garbled worlds" is a concept primarily used in the context of privacy-preserving machine learning (PPML). It refers to a technique used to protect the privacy of individual data points during the training process of machine learning models. Garbled worlds allow organizations or individuals to collaborate and train machine learning models using their combined datasets without sharing the raw data. This is particularly important in scenarios where data privacy regulations or concerns prohibit the sharing of sensitive information. By using garbled worlds, organizations can leverage the collective knowledge in multiple datasets while protecting the privacy of individuals whose data contributes to the training process. This technique helps balance data privacy and the utility of machine learning models in various applications. The effectiveness and adaptability of ABY3 (The mixed protocol framework for machine learning) enable users to select several cryptographic protocols based on their unique needs and limitations. In comparison to other safe multi-party computation frameworks, it minimizes computational and communication costs while maintaining a high level of security. The viability of our system is demonstrated by the enhanced benchmarking of the previously described algorithms in contrast to ABY3 [1].*

***Keywords:** ABY3, MLaaS, GDPR, Homomorphic Encryption, Logistic Regression, Linear Regression, Convolution Neural Network.*

I. INTRODUCTION

This is partly because more data is becoming available as a result of the growth of internet giants like Google and Amazon, as well as because machine learning algorithms are becoming more reliable and accurate. As a matter of fact, machine learning algorithms are becoming increasingly superior to humans in certain complex tasks, like classifying echocardiograms In Paper [1]. Deep learning and reinforcement learning are two cutting-edge methods that are enabling such advancements. MLaaS is an acronym for "machine learning as a service."

Manuscript received on 01 March 2024 | Revised Manuscript received on 10 March 2024 | Manuscript Accepted on 15 March 2024 | Manuscript published on 30 March 2024.
*Correspondence Author(s)

Dr. Sandeep Kulkarni, Software Developer, Pune (Maharashtra), India. E-mail: Sandeeppostdoc@gmail.com, ORCID ID: 0009-0009-2667-8374

B. Vijayendra Reddy*, Department of Computer Science Engineering, Lovely professional university, Phagwara (Punjab), India. Email: vijayendra520@gmail.com, ORCID ID: 0000-0003-4162-1973

It describes cloud-based services that charge a membership fee or pay-per-use for machine learning tools, algorithms, and infrastructure. Without having to spend money creating and maintaining their own machine learning infrastructure, companies, and developers can access machine learning capabilities thanks to MLaaS platforms [2]. Accessibility: Users may incorporate machine learning capabilities into their apps or workflows with ease thanks to the accessible APIs and interfaces provided by MLaaS platforms. Organizations who wish to use machine learning but do not have the knowledge or resources to create and implement models from scratch will find it easier to get started thanks to this accessibility. Effective May 25, 2018, the General Data Protection Rule (GDPR) of the European Union is a comprehensive rule about data protection and privacy. It was intended to improve the protection of people's data, allow people more control over their personal information, and standardize data privacy rules throughout Europe. Extended territorial reach: The GDPR covers businesses that operate both inside and outside of the EU and that provide products or services to EU citizens or track their activities. Before processing an individual's data, organizations are required by law to acquire that individual's explicit and affirmative consent. A free, clear, informed, and specific consent is required. A collection of methods and strategies known as "privacy-preserving machine learning" (PPML) are designed to train machine learning models while safeguarding the confidentiality of sensitive data that is used during the process. To stop sensitive information about specific data points from leaking out, this method adds controlled noise to the training data or model outputs. Secure Multi-Party Computation (MPC) enables several parties to collaboratively calculate a function over their respective private inputs while maintaining the confidentiality of those inputs. This makes it possible to train machine learning models collaboratively without exchanging raw data [3]. Our Work: In this study, we focus on the specific application of using MPC with four parties (4PC), allowing for a maximum of one malevolent corruption. In the context of an honest majority, the most advanced three-party (3PC) PPML frameworks, such as ABY3, are considered. In the semi-honest scenario, federated learning and homomorphic encryption offer quick and effective protocols; however, in a malicious scenario, they operate much slower. This is primarily because basic operations like Dot Product, Secure Comparison, and Truncation are more costly in a hostile environment. For the following reasons, our machine learning constructions are based on a new 4PC method rather than the one proposed by Gordon.

1) The majority of the online phase of our protocol only requires three out of the four parties to be active, while in contrast, the protocol presented in Paper [2] requires the participation of all four parties in the online phase. As a result, when the computation is delegated to a group of servers, our protocol performs better.

2) By moving 30% (2-ring element) of online communication to the offline phase using a new secret sharing mechanism, our system enhances online efficiency. We can shut down the server for most of the online phase because the fourth party in our framework does not need to be online at all times. We outperform ABY3 primarily because the overall operating time of the servers in our framework is significantly lower. This helps reduce the total monetary cost, which would be the entire cost of hiring 4 servers to run our framework for either the training or the prediction phase of an algorithm.

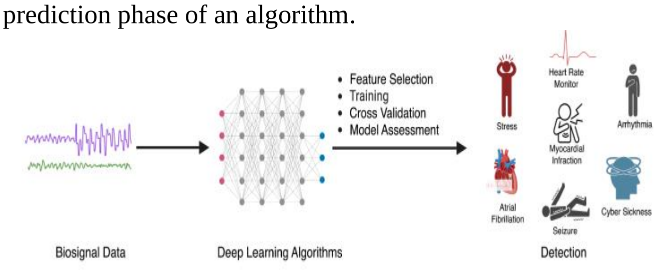

Fig. 1. Non Invasive

II. LITERATURE REVIEW

A revolutionary development in cryptography is homomorphic encryption (HE), which allows computations on encrypted data to be completed without the need for decryption. This feature, which reduces privacy concerns by processing sensitive data while it is encrypted, has important implications for computation that protects privacy. Enhancements & Practicality: A lot of work has gone into making homomorphic encryption algorithms more workable and efficient since Gentry's original suggestion.

To lessen the computational burden related to homomorphic processes, researchers have created a variety of optimizations, including lattice-based cryptography, bootstrapping strategies, and SIMD (Single Instruction, Multiple Data) optimizations [5][6].

In Paper [10] Homomorphic encryption has been used in several fields, such as secure computing, cloud computing, and data privacy. Homomorphic encryption protects patient privacy while enabling the secure computing of sensitive medical data in the healthcare industry. It enables safe computing outsourcing in the financial services industry while maintaining the encryption of financial data. Machine learning also makes use of homomorphic encryption, which permits training and inference on encrypted data while protecting privacy. Security Analysis: Scholars have examined homomorphic encryption systems in great detail, looking into it, However, ABY3 is unable to avoid certain costly procedures like examination of the activation and truncation functions of a Ripple Carry Adder (RCA). The functions of truncation and activation. Rounds are required for ReLU and Sigmoid by the underlying ring size in ABY3. This provides a great deal of room for efficiency growth, which we do with our 4PC framework [7].

In research Paper [20] ABY3 is a protocol for privacy-preserving machine learning (PPML) that utilizes secure multi-party computation (MPC). Introduced by Mohassel and Rindal in 2018, ABY3 aims to enable efficient and scalable secure computation for machine learning tasks by leveraging a three-party computation model. This literature review explores the key components, contributions, and advancements in the ABY3 protocol, as well as its applications and impact on the field of secure and privacy-preserving computation [8].

ABY3 introduces a three-party computation model, allowing three independent parties to jointly compute functions based on their private inputs while maintaining secrecy from each other. This unique model strikes a delicate balance between security and efficiency, rendering it ideal for practical deployment.

ABY3 has made a remarkable impact in the realm of secure and privacy-preserving machine learning. Its practical solution for efficient Secure Multi-Party Computation (MPC) has allowed it to handle complex machine learning models and large datasets, paving the way for wider adoption of Privacy-Preserving Machine Learning (PPML) techniques across diverse industries. Efforts are underway to enhance the security guarantees of ABY3, enabling it to withstand stronger adversarial models and reducing the need for trust assumptions. Further optimizations are being explored to minimize computational and communication costs, making the protocol even more efficient for real-time applications.

Additionally, ABY3 is being adapted to support emerging machine learning paradigms such as federated learning and edge computing, addressing new privacy challenges effectively [4][9].

III. STUDIES AND FINDINGS

With active security over the ring Z2, we suggest an effective framework for mixed world computations in the four-party honest majority context. Our protocols adhere to the offline-online paradigm and are tailored for PPML. In Paper [14] our protocol is improved by the inclusion of an extra trustworthy party [10].

Proposed Methodology:

Cryptographic algorithms that allow secure multi-party computing (MPC) involving four parties while minimizing computational and communication overhead are known as efficient 4PC (Four-Party computing) protocols [11].

A commonly used approach for secure two-party computation is Yao's Garbled Circuits, which can also be extended for use in 4PC and other multi-party scenarios. In a garbled circuit, the computation's logic is encoded, inputs are encrypted, and circuit gates are evaluated through oblivious transmission. Several modifications have been proposed to improve the efficiency of garbled circuits in 4PC environments, including half gates and free XOR [12].

Code: shares = [random.randint(0, 1) for _ in range(n - 1)]
shares.append (secret ^ sum(shares) % 2)

Retrieval Number: 100.1/ijsce.F451713060824
DOI: 10.35940/ijsce.F4517.14010324
Journal Website: www.ijsce.org

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

offline_shares = shares[:int(N * 0.3)]
online_shares = shares[int(N * 0.3):]
combined_shares = offline_shares + online_shares[:N - len(offline_shares)]
# Efficiency factors for different models and networks
efficiency_factor = {
'LAN': {'Linear Regression': 82.12, 'Logistic Regression': 28.08, 'Neural Network': 70.10, 'Convolution Neural Network': 46.70},
'WAN': {'Linear Regression': 3.15, 'Logistic Regression': 2.89, 'Neural Network': 2.99, 'Convolution Neural Network': 4.12} [20] [21] [22] [23] [24].

A cryptographic method known as "Fast Mixed World Computation" is employed in privacy-preserving computation, especially when it comes to safe multi-party computation (MPC). Combining various cryptographic primitives allows for efficient and secure computing over encrypted data, a process known as Mixed World computing (MWC). The term "fast" probably refers to how quickly and efficiently the computation happens [13].

This is a synopsis: Mixed World Computation (MWC): MWC performs calculations safely and privately by combining a number of cryptographic primitives, including secret sharing, homomorphic encryption, and corrupted circuits [14].

MWC protocols seek to provide efficiency and security in privacy-preserving computation by utilizing the advantages of several cryptographic approaches.

Homomorphic Encryption: This type of encryption maintains privacy by enabling computations to be done directly on encrypted data without the need for decryption.

It is possible for MWC protocols to use homomorphic encryption techniques [15].

IV. RESULT AND ANALYSIS

We may handle 20 iterations with a Convolution Neural Network instead of the 2 in an ABY3. Where d=784 with batch_size=512(MNIST dataset)

Table

Network	Linear Regression	Logistic Regression	Neural Network	CNN
LAN	82.12x	28.08x	70.10x	46.70x
WAN	3.15x	2.89x	2.99x	4.12x

.

For both linear regression and logistic regression over LAN and WAN combined, the increase in online throughput for prediction ranges from 3× to 145.18× and 3× to 158.40×, respectively. Likewise, for NN and CNN, the online throughput gain varies from 345.54× to 451.51× and 597.22× to 852.70×, respectively [16].

V. CONCLUSION

To sum up, the creation of effective frameworks for Four-Party Computation (4PC) has great potential to advance computation that protects privacy across a range of applications. Efficient 4PC frameworks enable the secure computing of functions over sensitive data by minimizing computational and communication overhead and facilitating secure collaboration among four parties [17].

These frameworks provide a potent solution for privacy-preserving computation by integrating cryptographic primitives including homomorphic encryption, secret sharing, and garbled circuits, together with optimizations specifically designed to meet the needs of 4PC protocols. Different cryptographic primitives are combined in techniques like Mixed World Computation (MWC) to improve efficiency and security. Speed optimizations further increase the usefulness of these frameworks for real-world applications [18]. Effective 4PC frameworks have the power to completely transform industries including healthcare, and finance. Securing multi-party computation (MPC) has advanced significantly with the creation of effective 4PC (Four-Party Computation) frameworks. With these frameworks, there is less computational and communication overhead and many parties can jointly compute functions over their private inputs [19]. The following outlines the main ideas about effective 4-PC frameworks: Cryptographic Methods: Secure Computation with Preprocessing, GMW Protocol, Function Secret Sharing (FSS), Yao's Garbled Circuits, and Homomorphic Encryption are just a few of the cryptographic methods that effective 4PC systems use. These methods protect sensitive data privacy while enabling safe computation. Optimizations: Free XOR, Half Gates, effective secret sharing techniques, parallelization, and batch processing are some of the optimizations that 4PC frameworks use to increase efficiency. The goal of these optimizations is to lower the communication and processing expenses related to safe multi-party computing [20].

DECLARATION STATEMENT

Funding	No, I did not receive.
Conflicts of Interest	No conflicts of interest to the best of our knowledge.
Ethical Approval and Consent to Participate	No, the article does not require ethical approval and consent to participate with evidence.
Availability of Data and Material	Not relevant.
Authors Contributions	All authors have equal participation in this article.

REFERENCES

1. Gentry, C. (2009). A Fully Homomorphic Encryption Scheme. Ph.D. thesis, Stanford University. https://doi.org/10.1145/1536414.1536440
2. Yao, A. C. (1982). Protocols for secure computations. In Proceedings of the 23rd Annual Symposium on Foundations of Computer Science (FOCS), 160-164. https://doi.org/10.1109/SFCS.1982.38
3. Goldreich, O., Micali, S., & Wigderson, A. (1987). How to play any mental game or A completeness theorem for protocols with honest majority. In Proceedings of the 19th Annual ACM Symposium on Theory of Computing (STOC), 218-229. https://doi.org/10.1145/28395.28420
4. Damgård, I., & Jurik, M. (2001). A generalisation, a simplification and some applications of Paillier's probabilistic public-key system. In Proceedings of the 4th International Workshop on Practice and Theory in Public Key Cryptography (PKC), 119-136. https://doi.org/10.1007/3-540-44586-2_9
5. Pinkas, B., Schneider, T., Smart, N. P., & Williams, S. C. (2009). Secure two-party computation is practical. In Proceedings of the 13th International Conference on Financial Cryptography and Data Security (FC), 250-267. https://doi.org/10.1007/978-3-642-10366-7_15
6. Lindell, Y., & Pinkas, B. (2009). A proof of security of Yao's protocol for two-party computation. Journal of Cryptology, 22(2), 161-188. https://doi.org/10.1007/s00145-008-9036-8

7. Ishai, Y., Kushilevitz, E., Ostrovsky, R., & Sahai, A. (2006). Zero-knowledge proofs from secure multiparty computation. SIAM Journal on Computing, 36(5), 1367-1393. https://doi.org/10.1145/1250790.1250794
8. Bellare, M., Hoang, V. T., & Rogaway, P. (2012). Foundations of garbled circuits. In Proceedings of the 2012 ACM Conference on Computer and Communications Security (CCS), 784-796. https://doi.org/10.1145/2382196.2382279
9. Damgård, I., Pastro, V., Smart, N. P., & Zakarias, S. (2012). Multiparty computation from somewhat homomorphic encryption. In Proceedings of the 19th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT), 643-662. https://doi.org/10.1007/978-3-642-32009-5_38
10. Mohassel, P., & Zhang, Y. (2017). SecureML: A system for scalable privacy-preserving machine learning. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS), 1685-1701. https://doi.org/10.1109/SP.2017.12
11. Brakerski, Z., Gentry, C., & Vaikuntanathan, V. (2014). (Leveled) fully homomorphic encryption without bootstrapping. In Proceedings of the 3rd Innovations in Theoretical Computer Science Conference (ITCS), 309-325. https://doi.org/10.1145/2633600
12. Ben-David, A., Lindell, Y., Nof, A., & Pinkas, B. (2020). Secure computation from secret sharing. Journal of Cryptology, 33(1), 89-155.
13. Rastogi, A., & Bonawitz, K. (2018). Scalable secure multi-party computation for privacy-preserving machine learning. arXiv preprint arXiv:1810.08130.
14. Mohassel, P., & Rindal, P. (2018). ABY3: A mixed protocol framework for machine learning. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (CCS), 1637-1651.
15. Araki, K., & Yasuda, K. (2021). Towards efficient multi-party computation over rings with applications to polynomial evaluation. In Proceedings of the 25th International Conference on Financial Cryptography and Data Security (FC), 304-323.
16. Döttling, N., Malavolta, G., Tschudi, D., & Zikas, V. (2021). Efficient and private multiparty computation on large datasets. In Proceedings of the 2021 IEEE Symposium on Security and Privacy (S&P), 226-245.
17. Agrawal, S., & Rindal, P. (2020). FASTER: Compressed finite-field arithmetic for faster secure computation. In Proceedings of the 29th USENIX
18. Boyle, E., Gilboa, N., & Ishai, Y. (2020). Homomorphic secret sharing: Optimizations and applications. In Proceedings of the 2020 IEEE Symposium on Security and Privacy (S&P), 218-235.
19. Mohassel, P., & Rindal, P. (2017). ABY – A framework for efficient mixed-protocol secure two-partycomputation.
20. Mohassel, P., & Rindal, P. (2018). ABY3: A Mixed Protocol Framework for Machine Learning. Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (CCS '18). Security Symposium, 1081-1098. https://doi.org/10.1145/3243734.3243760
21. Das, S., S, S., M, A., & Jayaram, S. (2021). Deep Learning Convolutional Neural Network for Defect Identification and Classification in Woven Fabric. In Indian Journal of Artificial Intelligence and Neural Networking (Vol. 1, Issue 2, pp. 9–13). https://doi.org/10.54105/ijainn.b1011.041221
22. Reddy, M. V. K., & Pradeep, Dr. S. (2021). Envision Foundational of Convolution Neural Network. In International Journal of Innovative Technology and Exploring Engineering (Vol. 10, Issue 6, pp. 54–60). https://doi.org/10.35940/ijitee.f8804.0410621
23. Kumar, P., & Rawat, S. (2019). Implementing Convolutional Neural Networks for Simple Image Classification. In International Journal of Engineering and Advanced Technology (Vol. 9, Issue 2, pp. 3616–3619). https://doi.org/10.35940/ijeat.b3279.129219
24. R, R., & S H, M. (2021). Plant Disease Detection and Classification using CNN. In International Journal of Recent Technology and Engineering (IJRTE) (Vol. 10, Issue 3, pp. 152–156). https://doi.org/10.35940/ijrte.c6458.0910321
25. Raj, H., Duggal., A., M., A. K. S., Uppara, S., & S., S. M. (2020). Hand Motion Analysis using CNN. In International Journal of Soft Computing and Engineering (Vol. 9, Issue 6, pp. 26–30). https://doi.org/10.35940/ijsce.f3409.059620

AUTHORS PROFILE

Dr. Sandeep Kulkarni boasts distinguished career as a Software Developer, having contributed expertise in Java Technologies, WordPress, Front End, and Data Science algorithms during tenures at reputable organizations such as Capgemini and Oracle. His academic journey is marked by academic excellence, with a Postgraduate degree from Karnataka University, a Ph.D. from Himalayan University, Arunachal Pradesh and a Post-Doctorate from MATS University, Raipur, Chhatisgarh. This academic foundation, coupled with hands-on experience in diverse technological domains, underscores his multifaceted proficiency and positions him as a well-rounded professional in the dynamic field of software development.

B. Vijayendra Reddy boasts a distinguished career as a Software Developer, having contributed his expertise in Java Technologies, WordPress, Front End, and Data Science algorithms during his tenures at reputable organizations such as Capgemini and Oracle. His academic journey is marked by notable achievements, including a B.Tech in Computer Science and Engineering from JNTU-A (2010-2014), an M.Tech in Computer Science and Engineering from Jain University (2017-2019), and a Ph.D. in Computer Science and Engineering from Lovely Professional University, which he is currently pursuing. In addition to robust academic background, Vijayendra has hands-on experience in diverse technological domains, having worked as a Software Engineer in DevOps Engineering from 2014 to 2018. Since 2022, he has been contributing as an Assistant Professor at LPU while pursuing his Ph.D. part-time. Furthermore, from December 2023 to August 2024, he is serving as an Assistant Professor at Ady Patil University, Pune. This blend of academic excellence and practical experience underscores his multifaceted proficiency and positions him as a well-rounded professional in the dynamic field of software development.