Date: 01-07-2021
Course: CSE3000
Professor: Kaitai Liang
Supervisor: Rui Wang

Contact: e.filip@student.tudelft.nl

AN OVERVIEW ON HYBRID APPROACHES IN HORIZONTAL FEDERATED LEARNING

EDUARD FILIP

TU Delft

1. BACKGROUND

Horizontal Federated Learning (HFL): datasets share similar features, but the sample space is different.

Currently HFL faces challenges towards privacy and security.
Two main privacy enhancements for HFL:

- Homomorphic encryption (HE)
- Differential Privacy (DP)

Both have good features, however at the cost of affecting model training, accuracy and performance.

Recently, researchers looked for hybrid implementations that may exploit the potential of the two main privacy enhancement, as well as add new security guarantees and even improve performance, accuracy and model training.

2. RESEARCH QUESTION

How do different hybrid approaches for HFL perform compared to the classic ones?

Compare the hybrid models based on the following criteria:

1. Performance
   - Model training
   - Communication cost
   - Complexity time
2. Privacy level
3. Security guarantees

4. KEY ANALYSIS RESULTS

- Fastest training: BlockFLA
- Lowest communication cost: HybridAlpha
- Highest security: BlockFLA
- All models do not offer security solutions for data poisoning and inference evasion (1 exception).
- All models improve scalability and training time.
- Unique features:
  - dropout & join tolerant: HybridAlpha
  - attacker detection: BlockFLA

3. ANALYSIS

Framework	Privacy-preserving enhancement	Security threat model	Time complexity	Communication cost
FL with DP and SMC [1]	DP and SMC	honest but curious	$O(Nk)$	$O(2N-t+1)$
HybridAlpha [2]	DP and SMC	honest but curious	$O(mN+m+N)$	$O(mN+m+N)$
Turbo-Aggregate [3]	Secure Aggregate	honest but curious	$O(N\,logN)$	$O(N\,logN)$
BlockFLA [4]	public + private blockchain	honest but curious	$O(N+\frac{1}{\sqrt{NT}}+\frac{N}{T})$	$O(2N)$
PermiDAG [5]	hybrid blockchain	honest	$O(etN)$	$O(etN)$

Figure 1: Comparison between the presented frameworks

5. CONCLUSION

- Hybrid models are capable of signifficantly improving the performance of the FL while still preserving privacy
- They make HFL more practical for real-life scenarios
- Intersting to go even further: HFL with blockchain and DP
- Investigation over data posioning and inference evasion should be made

References:
1. Truex, S., Baracaldo, N., Anwar, A., Steinke, T., Ludwig, H., Zhang, R., & Zhou, Y. (2019, November). A hybrid approach to privacy-preserving federated learning. In Proceedings of the 12th ACM Workshop on Artificial Intelligence and Security (pp. 1-11).
2. Xu, R., Baracaldo, N., Zhou, Y., Anwar, A., & Ludwig, H. (2019, November). Hybridalpha: An efficient approach for privacy-preserving federated learning. In Proceedings of the 12th ACM Workshop on Artificial Intelligence and Security (pp. 13-23).
3. So, J., Güler, B., & Avestimehr, A. S. (2021). Turbo-aggregate: Breaking the quadratic aggregation barrier in secure federated learning. IEEE Journal on Selected Areas in Information Theory, 2(1), 479-489.
4. Desai, H. B., Ozdayi, M. S., & Kantarcioglu, M. (2021, April). BlockFLA: Accountable federated learning via hybrid blockchain architecture. In Proceedings of the Eleventh ACM Conference on Data and Application Security and Privacy (pp. 101-112).
5. Lu, Y., Huang, X., Zhang, K., Maharjan, S., & Zhang, Y. (2020). Blockchain empowered asynchronous federated learning for secure data sharing in internet of vehicles. IEEE Transactions on Vehicular Technology, 69(4), 4298-4311.