* امنیت در یادگیری فدراسیونی [a0]
  1. توضیحات FL [a12]
     1. FL چیست؟
     2. کاربردهای FL [a13]
     3. FL چگونه کار می کند؟ [a20]
  2. امنیت در FL [a30]
     1. آسیب پذیری [b22]
        1. چالش ارتباط با بیرون
        2. چالش تعداد شرکت کنندگان [a44]
        3. نقاط شکست [a45]
     2. انواع حمله به FL
        1. آلوده سازی (مدل و دیتا) [b25, b56, b60]
        2. مبتی بر GAN [b61, b62, b63]
        3. حمله های در پشتی [b80, d70]
     3. راهکارهای دفاع در برابر حملات [d0]
        1. دفاع حملات آلوده سازی (مدل و دیتا) [d50, d51]
        2. دفاع حمله مبتی بر GAN [b61, b62]
        3. دفاع حمله های در پشتی [d71, d70]
        4. دفاع در بلاک چین [d90, d91]
  3. حریم خصوصی در FL
     1. حملات به حریم خصوصی [f11]
        1. نشت ناخواسته و بازسازی مدل[f12]
        2. تخریب سرور[f13]
        3. حملات استنتاجی مبتنی بر GAN [f14]
        4. حملات استنتاجی عضویت[f15]
     2. دفاع حملات به حریم خصوصی
        1. افزودن نویز گرادیان[f16]
        2. بزرگنمایی دسته ها، بالا بردن وضوح داده[f17]
        3. دفاع سرور مخرب[f13]
        4. محاسبات امن چندطرفه[f18]
        5. حریم خصوصی دیفرانسیل[f19]
        6. پنهان کردن تکرارها[f20]
        7. چارچوب تایید[f21]
        8. حفظ حریم خصوصی از طریق فناوری بلاک چین[f22]

References:

1. [a0] Gosselin, R., Vieu, L., Loukil, F., & Benoit, A. (2022). Privacy and security in federated learning: A survey. *Applied Sciences*, *12*(19), 9901.
2. [a12] Banabilah, S., Aloqaily, M., Alsayed, E., Malik, N., & Jararweh, Y. (2022). Federated learning review: Fundamentals, enabling technologies, and future applications. *Information processing & management*, *59*(6), 103061.
3. [a13] Bharati, S., Mondal, M., Podder, P., & Prasath, V. B. (2022). Federated learning: Applications, challenges and future directions. *International Journal of Hybrid Intelligent Systems*, *18*(1-2), 19-35.
4. [a20] Yu, B., Mao, W., Lv, Y., Zhang, C., & Xie, Y. (2022). A survey on federated learning in data mining. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *12*(1), e1443.
5. [a30] Li, H., Li, C., Wang, J., Yang, A., Ma, Z., Zhang, Z., & Hua, D. (2023). Review on security of federated learning and its application in healthcare. *Future Generation Computer Systems*, *144*, 271-290.
6. [b22] Bouacida, N., & Mohapatra, P. (2021). Vulnerabilities in federated learning. *IEEE Access*, *9*, 63229-63249.
7. [a44] Bhagoji, A. N., Chakraborty, S., Mittal, P., & Calo, S. (2019, May). Analyzing federated learning through an adversarial lens. In *International Conference on Machine Learning* (pp. 634-643). PMLR.
8. [a45] Bagdasaryan, E., Veit, A., Hua, Y., Estrin, D., & Shmatikov, V. (2020, June). How to backdoor federated learning. In *International conference on artificial intelligence and statistics* (pp. 2938-2948). PMLR.
9. [b25] Rodríguez-Barroso, N., Jiménez-López, D., Luzón, M. V., Herrera, F., & Martínez-Cámara, E. (2023). Survey on federated learning threats: Concepts, taxonomy on attacks and defences, experimental study and challenges. *Information Fusion*, *90*, 148-173.
10. [b56] Gupta, P., Yadav, K., Gupta, B. B., Alazab, M., & Gadekallu, T. R. (2023). A Novel Data Poisoning Attack in Federated Learning based on Inverted Loss Function. *Computers & Security*, *130*, 103270.
11. [b60] Nuding, F., & Mayer, R. (2022, April). Data poisoning in sequential and parallel federated learning. In *Proceedings of the 2022 ACM on International Workshop on Security and Privacy Analytics* (pp. 24-34).
12. [b61] Tabassum, A., Erbad, A., Lebda, W., Mohamed, A., & Guizani, M. (2022). Fedgan-ids: Privacy-preserving ids using gan and federated learning. *Computer Communications*, *192*, 299-310.
13. [b62] Lai, J., Huang, X., Gao, X., Xia, C., & Hua, J. (2022). GAN-based information leakage attack detection in federated learning. *Security and Communication Networks*, *2022*.
14. [b63] Zhang, J., Chen, B., Cheng, X., Binh, H. T. T., & Yu, S. (2020). PoisonGAN: Generative Poisoning Attacks against Federated Learning in Edge Computing Systems. *IEEE Internet of Things Journal, 1–1*. doi:10.1109/JIOT.2020.3023126
15. [b80] Zhang, Z., Panda, A., Song, L., Yang, Y., Mahoney, M., Mittal, P., ... & Gonzalez, J. (2022, June). Neurotoxin: Durable backdoors in federated learning. In *International Conference on Machine Learning* (pp. 26429-26446). PMLR.
16. [d70] Lu, S., Li, R., Liu, W., & Chen, X. (2022). Defense against backdoor attack in federated learning. *Computers & Security*, *121*, 102819.
17. [d71] Lu, S., Li, R., Liu, W., & Chen, X. (2022). Defense against backdoor attack in federated learning. *Computers & Security*, *121*, 102819.
18. [d50] Xia, G., Chen, J., Yu, C., & Ma, J. (2023). Poisoning Attacks in Federated Learning: A Survey. *IEEE Access*, *11*, 10708-10722.
19. [d51] Zhang, Z., Zhang, Y., Guo, D., Yao, L., & Li, Z. (2022). SecFedNIDS: Robust defense for poisoning attack against federated learning-based network intrusion detection system. *Future Generation Computer Systems*, *134*, 154-169.
20. [d90] Mahmood, Z., & Jusas, V. (2022). Blockchain-enabled: Multi-layered security federated learning platform for preserving data privacy. *Electronics*, *11*(10), 1624.
21. [d0] Liu, P., Xu, X., & Wang, W. (2022). Threats, attacks and defenses to federated learning: issues, taxonomy and perspectives. *Cybersecurity*, *5*(1), 1-19.
22. [d91] Li, D., Luo, Z., & Cao, B. (2022). Blockchain-based federated learning methodologies in smart environments. *Cluster Computing*, *25*(4), 2585-2599.
23. [f11] Khalil, M., Esseghir, M., & Boulahia, L. M. (2023). Privacy-Preserving federated learning: An application for big data load forecast in buildings. *Computers & Security*, *131*, 103211.
24. [f12] Boenisch, F., Dziedzic, A., Schuster, R., Shamsabadi, A. S., Shumailov, I., & Papernot, N. (2023, July). When the curious abandon honesty: Federated learning is not private. In *2023 IEEE 8th European Symposium on Security and Privacy (EuroS&P)* (pp. 175-199). IEEE.
25. [f13] Zhang, Z., Cao, X., Jia, J., & Gong, N. Z. (2022, August). FLDetector: Defending federated learning against model poisoning attacks via detecting malicious clients. In *Proceedings of the 28th ACM SIGKDD Conference on Knowledge Discovery and Data Mining* (pp. 2545-2555).
26. [f14] Vo, H., Tang, M., Zheng, X., & Yu, S. (2022, October). BI-GAN: batch inversion membership inference attack on federated learning. In *Proceedings of the 17th ACM Workshop on Mobility in the Evolving Internet Architecture* (pp. 31-36).
27. [f15] Gu, Y., Bai, Y., & Xu, S. (2022). CS-MIA: Membership inference attack based on prediction confidence series in federated learning. *Journal of Information Security and Applications*, *67*, 103201.
28. [f16] Li, Z., Zhang, J., Liu, L., & Liu, J. (2022). Auditing privacy defenses in federated learning via generative gradient leakage. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition* (pp. 10132-10142).
29. [f17] Shin, S., Boyapati, M., Suo, K., Kang, K., & Son, J. (2023). An empirical analysis of image augmentation against model inversion attack in federated learning. *Cluster Computing*, *26*(1), 349-366.
30. [f18] Kanagavelu, R., Wei, Q., Li, Z., Zhang, H., Samsudin, J., Yang, Y., ... & Wang, S. (2022). CE-Fed: Communication efficient multi-party computation enabled federated learning. *Array*, *15*, 100207.
31. [f19] El Ouadrhiri, A., & Abdelhadi, A. (2022). Differential privacy for deep and federated learning: A survey. *IEEE access*, *10*, 22359-22380.
32. [f20] Kanchan, S., Jang, J. W., Yoon, J. Y., & Choi, B. J. (2023). Efficient and privacy-preserving group signature for federated learning. *Future Generation Computer Systems*, *147*, 93-106.
33. [f21] Yang, J., Zheng, J., Baker, T., Tang, S., Tan, Y. A., & Zhang, Q. (2023). Clean‐label poisoning attacks on federated learning for IoT. *Expert Systems*, *40*(5), e13161.
34. [f22] Javed, A. R., Hassan, M. A., Shahzad, F., Ahmed, W., Singh, S., Baker, T., & Gadekallu, T. R. (2022). Integration of blockchain technology and federated learning in vehicular (iot) networks: A comprehensive survey. *Sensors*, *22*(12), 4394.