List of Publications on IEEE TIFS

1. Xiaoyuan Liu, Hongwei Li, Guowen Xu, Xilin Zhang, **Tianwei Zhang**, Jianying Zhou, Secure and Lightweight Feature Selection for Horizontal Federated Learning, Accepted by IEEE Transactions on Information Forensics and Security
2. Hangcheng Liu, Yuan Zhou, Ying Yang, Qingchuan Zhao, **Tianwei Zhang**, Tao Xiang, Stealthiness Assessment of Adversarial Perturbation: From A Visual Perspective, IEEE Transactions on Information Forensics and Security, Volume: 20, December 2024
3. Hanxiao Chen, Hongwei Li, Meng Hao, Jia Hu, Guowen Xu, Xilin Zhang, **Tianwei Zhang**, SecBNN: Efficient Secure Inference on Binary Neural Network, IEEE Transactions on Information Forensics and Security, Volume: 19, November 2024
4. Zhirui Zeng, Tao Xiang, Shangwei Guo, Jialing He, Qiao Zhang, Guowen Xu, **Tianwei Zhang**, Contrast-then-Approximate: Analyzing Keyword Leakage of Generative Language Models, IEEE Transactions on Information Forensics and Security, Volume: 19, April 2024
5. Renyang Liu, Wei Zhou, **Tianwei Zhang**, Kangjie Chen, Jun Zhao, Kwok-Yan Lam, Boosting Black-box Attack to Deep Neural Networks with Conditional Diffusion Models, IEEE Transactions on Information Forensics and Security, Volume: 19, April 2024
6. Rui Xue, Kaiping Xue, Bin Zhu, Xinyi Luo, **Tianwei Zhang**, Qibin Sun, Jun Lu, Differentially Private Federated Learning with an Adaptive Noise Mechanism, IEEE Transactions on Information Forensics and Security, Volume: 19, September 2023
7. Hangcheng Liu, Tao Xiang, Shangwei Guo, Han Li, **Tianwei Zhang**, Xiaofeng Liao, Erase and Repair: An Efficient Box-Free Removal Attack on High-Capacity Deep Hiding, IEEE Transactions on Information Forensics and Security, Volume: 18, August 2023
8. Jianfei Sun, Guowen Xu, **Tianwei Zhang**, Xuehuan Yang, Mamoun Alazab, Robert Deng, Privacy-aware and Security-enhanced Efficient Matchmaking Encryption, IEEE Transactions on Information Forensics and Security, Volume: 18, July 2023
9. Meng Hao, Hongwei Li, Hanxiao Chen, Pengzhi Xing, **Tianwei Zhang**, FastSecNet: An Efficient Cryptographic Framework for Private Neural Network Inference, IEEE Transactions on Information Forensics and Security, Volume: 18, March 2023
10. Hanxiao Chen, Hongwei Li, Yingzhe Wang, Meng Hao, Guowen Xu, **Tianwei Zhang**, PriVDT: An Efficient Two-Party Cryptographic Framework for Vertical Decision Trees, IEEE Transactions on Information Forensics and Security, Volume: 18, December 2022
11. Jianfei Sun, Guowen Xu, **Tianwei Zhang**, Xuehuan Yang, Mamoun Alazab, Robert Deng, Verifiable, Fair and Privacy-preserving Broadcast Authorization for Flexible Data Sharing in Clouds, IEEE Transactions on Information Forensics and Security, Volume: 18, December 2022
12. Jianfei Sun, Guowen Xu, **Tianwei Zhang**, Mamoun Alazab, Robert H. Deng, A Practical Fog-based Privacy-preserving Online Car-hailing Service System, IEEE Transactions on Information Forensics and Security, Volume: 17, August 2022