朱天清簡歷

朱天清 博士

教授 博導/碩導

數據科學學院副院長（科研）

電子信箱 E-mail：tqzhu@cityu.edu.mo

聯繫電話 Contact：+853-85902275

學歷

2014 計算機科學 博士，迪肯大學，澳大利亞

2004 檢測技術與自動化裝置 碩士，武漢大學，中國

2000 應用化學 學士，武漢大學，中國

現任

澳門城市大學數據科學學院副院長

澳門城市大學數據科學學院教授，博導

個人簡介

朱天清曾任澳大利亞迪肯大學講師、悉尼科技大學副教授以及中國地質大學（武漢）教授。並曾任澳大利亞自然科學基金領域專家（Australian Research Council College of Expert）。曾主持和參與澳大利亞國家自然科學基金八項，共計研究經費四百餘萬澳元。曾主持中國國家自然科學基金青年項目一項，面上

項目一項，均為人工智能及數據安全類主題。以通信/一作發表 NDSS，S&P，USENIX，IEEE Transactions 等 CCF A 類論文 40 餘篇。SCI 論文近 300 篇。擔任安全國際會議 CCS 2025 的 PC Member、人工智能國際會議 AAAI，IJCAI PC member、以及 3 個 SCI 期刊 Associate Editor；2023 年入選斯坦福全球前 2%科學家。目前培養博士生二十餘人。致力於人工智能安全領域的研究，專注於智能模型安全攻防、數據隱私以及安全和公平性關系等關鍵科學問題，提升智能模型的安全保障、隱私保護和輸出公平性。

研究方向

人工智能安全、隱私保護、網絡空間安全

近三年部分研究成果

1.Ye, Dayong; Zhu, Tianqing*; Li, Jiayang; Gao, Kun; Liu, Bo; Zhang, Leo Yu; Zhou, Wanlei; Zhang, Yang. Data Duplication: A Novel Multi-Purpose Attack Paradigm in Machine Unlearning. 34rd USENIX Security Symposium (USENIX Security 2025, Accepted on Feb 2025). (CCF A)

2.Ye, Dayong; Zhu, Tianqing*; Wang, Shang; Liu, Bo; Zhang, Leo Yu; Zhou, Wanlei; Zhang, Yang. Data-Free Model-Related Attacks: Unleashing the Potential of Generative AI. 34rd USENIX Security Symposium (USENIX Security 2025 Accepted on Feb 2025). (CCF A)

3.Ye, Dayong; Zhu, Tianqing*; Zhu, Congcong; Wang, Derui; Gao, Kun; Shi, Zewei; Shen, Sheng; Zhou, Wanlei; Xue, Minhui. Reinforcement Unlearning. Reinforcement Unlearning. The Network and Distributed System Security (NDSS) Symposium 2025. (CCF A)

4.Han, Changzhou; Deng, Zehang; Ma, Wanlun; Zhu, Xiaogang; Xue, Jason (Minhui); Zhu, Tianqing; Wen, Sheng; Xiang, Yang. Codebreaker: Dynamic Extraction Attacks on Code Language Models. IEEE Symposium on Security and Privacy 2025 (IEEE S&P 2025 Accepted on March 2025) (CCF A)

5.Ye, Dayong; Chen, Huiqiang; Zhou, Shuai; Zhu, Tianqing*; Zhou, Wanlei; Ji, Shouling. "Model Inversion Attack Against Transfer Learning: Inverting a Model Without

Querying It," in IEEE Transactions on Dependable and Secure Computing, 05 March 2025, doi: 10.1109/TDSC.2025.3548119. (CCF A)

6.Sun, Hui; Zhu, Tianqing*; Li, Jie; Zhou, Wanlei. "Average and Strict GAN-based Reconstruction for Adversarial Example Detection," in IEEE Transactions on Dependable and Secure Computing, 27 February 2025. doi: 10.1109/TDSC.2025.3545879. (CCF A)

7.Ye, Dayong; Zhu, Tianqing*; Gao, Kun; Zhu, Congcong; Zhou, Wanlei. "Cooperating or Kicking Out: Defending against Poisoning Attacks in Federated Learning via the Evolution of Cooperation," in IEEE Transactions on Dependable and Secure Computing, 21 January 2025. doi: 10.1109/TDSC.2025.3532351. (CCF A)

8.Chen, Huiqiang; Zhu, Tianqing*; Zhou, Wanlei; Zhao, Wei. "AFed: Algorithmic Fair Federated Learning," in IEEE Transactions on Neural Networks and Learning Systems, 22 January 2025, doi: 10.1109/TNNLS.2025.3528012.

9.Chen, Huajie; Zhu, Tianqing*; Zhang, Lefeng; Liu, Bo; Wang, Derui; Zhou, Wanlei; Xue, Minhui. "QUEEN: Query Unlearning Against Model Extraction," in IEEE Transactions on Information Forensics and Security, vol. 20, pp. 2143-2156, 2025, doi: 10.1109/TIFS.2025.3538266. (CCF A)

10.Han, Mengde; Zhu, Tianqing*; Zhang, Lefeng; Huo, Huan; Zhou, Wanlei. "Vertical Federated Unlearning via Backdoor Certification," in IEEE Transactions on Services Computing, 29 January 2025. doi: 10.1109/TSC.2025.3536312. (CCF A)

11.Tian, Huan; Liu, Bo; Zhu, Tianqing*; Zhou, Wanlei; Philip, S Yu. "MultiFair: Model Fairness With Multiple Sensitive Attributes," in IEEE Transactions on Neural Networks and Learning Systems, vol. 36, no. 3, pp. 5654-5667, March 2025, doi: 10.1109/TNNLS.2024.3384181.

12.Chen, Huiqiang; Zhu, Tianqing*; Yu, Xin; Zhou, Wanlei. 2024. Machine unlearning via null space calibration. In Proceedings of the Thirty-Third International Joint Conference on Artificial Intelligence (IJCAI 2024). Article 40, 358–366. https://doi.org/10.24963/ijcai.2024/40. (CCF A)

13.Tian, Huan; Zhang, Guangsheng; Liu, Bo; Zhu, Tianqing *; Ding, Ming; Zhou, Wanlei. 2024. When fairness meets privacy: exploring privacy threats in fair binary

classifiers via membership inference attacks. In Proceedings of the Thirty-Third International Joint Conference on Artificial Intelligence (IJCAI 2024). Article 57, 512–520. https://doi.org/10.24963/ijcai.2024/57. (CCF A)

14.Chen, Huiqiang; Zhu, Tianqing*; Liu, Bo; Zhou, Wanlei; Philip, S Yu. "Fine-tuning a Biased Model for Improving Fairness," in IEEE Transactions on Big Data, 13 September 2024. doi: 10.1109/TBDATA.2024.3460537.

15.Tian, Huan; Liu, Bo; Zhu, Tianqing*; Zhou, Wanlei; Philip, S Yu. "Distilling Fair Representations From Fair Teachers," in IEEE Transactions on Big Data, 13 September 2024. doi: 10.1109/TBDATA.2024.3460532.

16.Du, Xiaobiao; Sun, Haiyang; Lu, Ming; Zhu, Tianqing; Yu, Xin. “DreamCar: Leveraging Car-Specific Prior for In-the-Wild 3D Car Reconstruction.” IEEE Robotics and Automation Letters 10 (2024): 1840-1847.

17.Guan, Faqian; Zhu, Tianqing*; Sun, Hui; Zhou, Wanlei; Philip, S Yu. "Large Language Models for Link Stealing Attacks Against Graph Neural Networks," in IEEE Transactions on Big Data, 07 November 2024. doi: 10.1109/TBDATA.2024.3489427.

18.Zhang, Lefeng; Zhu, Tianqing*; Xiong, Ping; Zhou, Wanlei. 2024. The Price of Unlearning: Identifying Unlearning Risk in Edge Computing. ACM Trans. Multimedia Comput. Commun. Appl. May 2024). https://doi.org/10.1145/3662184.

19.Xu, Heng; Zhu, Tianqing*; Zhang, Lefeng; Zhou, Wanlei; Zhao, Wei. "Toward Efficient Target-Level Machine Unlearning Based on Essential Graph," in IEEE Transactions on Neural Networks and Learning Systems, 26 December 2024, doi: 10.1109/TNNLS.2024.3514607.

20.Xu, Heng; Zhu, Tianqing*; Zhou, Wanlei; Zhao, Wei. "Don't Forget Too Much: Towards Machine Unlearning on Feature Level," in IEEE Transactions on Dependable and Secure Computing, 23 July 2024. doi: 10.1109/TDSC.2024.3432169. (CCF A)

21.Xu, Heng; Zhu, Tianqing*; Zhang, Lefeng; Zhou, Wanlei; Philip, S Yu. "Update Selective Parameters: Federated Machine Unlearning Based on Model Explanation," in IEEE Transactions on Big Data, 05 June 2024. doi: 10.1109/TBDATA.2024.3409947.

22.Zhou, Shuai; Zhu, Tianqing*; Ye, Dayong; Zhou, Wanlei; Zhao, Wei. "Inversion-

Guided Defense: Detecting Model Stealing Attacks by Output Inverting," in IEEE Transactions on Information Forensics and Security, vol. 19, pp. 4130-4145, 2024, doi: 10.1109/TIFS.2024.3376190. (CCF A)

23.Zhang, Guangsheng; Liu, Bo; Tian, Huan; Zhu, Tianqing; Ding, Ming; Zhou, Wanlei. 2024. How does a deep learning model architecture impact its privacy? a comprehensive study of privacy attacks on CNNs and transformers. In Proceedings of the 33rd USENIX Conference on Security Symposium (USENIX 2024). USENIX Association, USA, Article 380, 6795–6812. (CCF A)

24.Ye, Dayong; Zhu, Tianqing*; Gao, Kun; Zhou, Wanlei. "Defending Against Label-Only Attacks via Meta-Reinforcement Learning," in IEEE Transactions on Information Forensics and Security, vol. 19, pp. 3295-3308, 2024, doi: 10.1109/TIFS.2024.3357292. (CCF A)

25.Chen, Huajie; Zhu, Tianqing*; Liu, Chi; Yu, Shui; Zhou, Wanlei. "High-Frequency Matters: Attack and Defense for Image-Processing Model Watermarking," in IEEE Transactions on Services Computing, vol. 17, no. 4, pp. 1565-1579, July-Aug. 2024, doi: 10.1109/TSC.2024.3349784. (CCF A)

26.Xu, Heng; Zhu, Tianqing*; Zhang, Lefeng; Zhou, Wanlei; Yu, Philip S. 2023. Machine Unlearning: A Survey. ACM Computing Surveys. 56, 1, Article 9 (January 2024), 36 pages. https://doi.org/10.1145/3603620. (Highly Cited Paper)

27.Sun, Hui; Zhu, Tianqing*; Li, Jie; Ji, Shoulin; Zhou, Wanlei. "Attribute-Based Membership Inference Attacks and Defenses on GANs," in IEEE Transactions on Dependable and Secure Computing, vol. 21, no. 4, pp. 2376-2393, July-Aug. 2024, doi: 10.1109/TDSC.2023.3305591. (CCF A)

28.Chen, Huiqiang; Zhu, Tianqing*; Zhang, Tao; Zhou, Wanlei; Yu, Philip S. 2023. Privacy and Fairness in Federated Learning: On the Perspective of Tradeoff. ACM Computing Surveys. 56, 2, Article 39 (February 2024), 37 pages. https://doi.org/10.1145/3606017. (Highly Cited Paper)

29.Zhou, Shuai; Zhu, Tianqing*; Ye, Dayong; Yu, Xin; Zhou, Wanlei. "Boosting Model Inversion Attacks With Adversarial Examples," in IEEE Transactions on Dependable and Secure Computing, vol. 21, no. 3, pp. 1451-1468, May-June 2024, doi: 10.1109/TDSC.2023.3285015. (CCF A)

30.Zhang, Lefeng; Zhu, Tianqing*; Zhang, Haibin; Xiong, Ping; Zhou, Wanlei. "FedRecovery: Differentially Private Machine Unlearning for Federated Learning Frameworks," in IEEE Transactions on Information Forensics and Security, vol. 18, pp. 4732-4746, 2023, doi: 10.1109/TIFS.2023.3297905. (CCF A)

31.Liu, Chi; Zhu, Tianqing*; Shen, Sheng; Zhou, Wanlei. 2023. Towards robust gan-generated image detection: a multi-view completion representation. In Proceedings of the Thirty-Second International Joint Conference on Artificial Intelligence (IJCAI '23). Article 52, 464–472. https://doi.org/10.24963/ijcai.2023/52. (CCF A)

32.Zhu, Congcong; Cheng, Zishuo; Ye, Dayong; Hussain, Farookh Khadeer; Zhu, Tianqing*; Zhou, Wanlei. "Time-Driven and Privacy-Preserving Navigation Model for Vehicle-to-Vehicle Communication Systems," in IEEE Transactions on Vehicular Technology, vol. 72, no. 7, pp. 8459-8470, July 2023, doi: 10.1109/TVT.2023.3248613.

33.Liu, Chi; Chen, Huajie; Zhu, Tianqing*; Zhang, Jun; Zhou, Wanlei. "Making DeepFakes More Spurious: Evading Deep Face Forgery Detection via Trace Removal Attack," in IEEE Transactions on Dependable and Secure Computing, vol. 20, no. 6, pp. 5182-5196, Nov.-Dec. 2023, doi: 10.1109/TDSC.2023.3241604. (CCF A)

34.Zhu, Tianqing*; Ye, Dayong; Zhou, Shuai; Liu, Bo; Zhou, Wanlei. "Label-Only Model Inversion Attacks: Attack With the Least Information," in IEEE Transactions on Information Forensics and Security, vol. 18, pp. 991-1005, 2023, doi: 10.1109/TIFS.2022.3233190. (CCF A)

35.Zhu, Tianqing*; Ye, Dayong; Cheng, Zishuo; Zhou, Wanlei; Philip, S Yu. "Learning Games for Defending Advanced Persistent Threats in Cyber Systems," in IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 53, no. 4, pp. 2410-2422, April 2023, doi: 10.1109/TSMC.2022.3211866.

36.Hao, Xiaohan; Ren, Wei; Fei, Yangyang; Zhu, Tianqing; Choo, Kim-Kwang Raymond. "A Blockchain-Based Cross-Domain and Autonomous Access Control Scheme for Internet of Things," in IEEE Transactions on Services Computing, vol. 16, no. 2, pp. 773-786, 1 March-April 2023, doi: 10.1109/TSC.2022.3179727.(CCF A)

37.Zhang, Lefeng; Zhu, Tianqing*; Hussain, Farookh Khadeer; Ye, Dayong; Zhou, Wanlei. "A Game-Theoretic Method for Defending Against Advanced Persistent

Threats in Cyber Systems," in IEEE Transactions on Information Forensics and Security, vol. 18, pp. 1349-1364, 2023, doi: 10.1109/TIFS.2022.3229595. (CCF A)

38.Liu, Yizhi; Hao, Xiaohan; Ren, Wei; Xiong, Ruoting; Zhu, Tianqing; Choo, Kim-Kwang Raymond; Min, Geyong. "A Blockchain-Based Decentralized, Fair and Authenticated Information Sharing Scheme in Zero Trust Internet-of-Things," in IEEE Transactions on Computers, vol. 72, no. 2, pp. 501-512, 1 Feb. 2023, doi: 10.1109/TC.2022.3157996. (CCF A)

39.Zhang, Lefeng; Zhu, Tianqing*; Xiong, Ping; Zhou, Wanlei; Philip, S Yu. "A Game-Theoretic Federated Learning Framework for Data Quality Improvement," in IEEE Transactions on Knowledge and Data Engineering, vol. 35, no. 11, pp. 10952-10966, 1 Nov. 2023, doi: 10.1109/TKDE.2022.3230959. (CCF A)

40.Yang, Mengmeng; Tjuawinata, Ivan; Lam, Kwok-Yan; Zhu, Tianqing; Zhao, Jun. "Differentially Private Distributed Frequency Estimation," in IEEE Transactions on Dependable and Secure Computing, vol. 20, no. 5, pp. 3910-3926, 1 Sept.-Oct. 2023, doi: 10.1109/TDSC.2022.3227654. (CCF A)

41.Zhou, Shuai; Liu, Chi; Ye, Dayong; Zhu, Tianqing*; Zhou, Wanlei; Yu, Philip S. 2022. Adversarial Attacks and Defenses in Deep Learning: From a Perspective of Cybersecurity. ACM Computing Surveys. 55, 8, Article 163 (August 2023), 39 pages. https://doi.org/10.1145/3547330.

42.Hu, Xiangyu; Zhu, Tianqing*; Zhai, Xuemeng; Wang, Hengming; Zhou, Wanlei; Zhao, Wei. "Privacy Data Diffusion Modeling and Preserving in Online Social Network," in IEEE Transactions on Knowledge and Data Engineering, vol. 35, no. 6, pp. 6224-6237, 1 June 2023, doi: 10.1109/TKDE.2022.3176948. (CCF A)

43.Zhang, Guangsheng; Liu, Bo; Zhu, Tianqing; Ding, Ming; Zhou, Wanlei. "Label-Only Membership Inference Attacks and Defenses in Semantic Segmentation Models," in IEEE Transactions on Dependable and Secure Computing, vol. 20, no. 2, pp. 1435-1449, 1 March-April 2023, doi: 10.1109/TDSC.2022.3154029. (CCF A)

44.Ye, Dayong; Zhu, Tianqing*; Zhu, Congcong; Zhou, Wanlei; Philip, S Yu. "Model-Based Self-Advising for Multi-Agent Learning," in IEEE Transactions on Neural Networks and Learning Systems, vol. 34, no. 10, pp. 7934-7945, Oct. 2023, doi: 10.1109/TNNLS.2022.3147221.

45.Liu, Chi; Zhu, Tianqing*; Zhang, Jun; Zhou, Wanlei. 2022. Privacy Intelligence: A Survey on Image Privacy in Online Social Networks. ACM Computing Survey. 55, 8, Article 161 (August 2023), . https://doi.org/10.1145/3547299.

46.Zhang, Lefeng; Zhu, Tianqing*; Xiong, Ping; Zhou, Wanlei; Philip, S Yu."A Robust Game-Theoretical Federated Learning Framework With Joint Differential Privacy," in IEEE Transactions on Knowledge and Data Engineering, vol. 35, no. 4, pp. 3333-3346, 1 April 2023, doi: 10.1109/TKDE.2021.3140131. (CCF A)

47.Sun, Hui; Zhu, Tianqing*; Zhang, Zhiqiu; Jin, Dawei; Xiong, Ping; Zhou, Wanlei. "Adversarial Attacks Against Deep Generative Models on Data: A Survey," in IEEE Transactions on Knowledge and Data Engineering, vol. 35, no. 4, pp. 3367-3388, 1 April 2023, doi: 10.1109/TKDE.2021.3130903. (CCF A)

48.Hu, Xiangyu; Zhu, Tianqing*; Zhai, Xuemeng; Zhou, Wanlei; Zhao, Wei. "Privacy Data Propagation and Preservation in Social Media: A Real-World Case Study," in IEEE Transactions on Knowledge and Data Engineering, vol. 35, no. 4, pp. 4137-4150, 1 April 2023, doi: 10.1109/TKDE.2021.3137326. (CCF A)

49.Zhang, Tao; Zhu, Tianqing*; Gao, Kun; Zhou, Wanlei; Philip, S Yu. "Balancing Learning Model Privacy, Fairness, and Accuracy With Early Stopping Criteria," in IEEE Transactions on Neural Networks and Learning Systems, vol. 34, no. 9, pp. 5557-5569, Sept. 2023, doi: 10.1109/TNNLS.2021.3129592.

50.Liao, Tingting; Lei, Zhen; Zhu, Tianqing; Zeng, Shan; Li, Yaqin; Yuan, Cao. "Deep Metric Learning for K Nearest Neighbor Classification," in IEEE Transactions on Knowledge and Data Engineering, vol. 35, no. 1, pp. 264-275, 1 Jan. 2023, doi: 10.1109/TKDE.2021.3090275. (CCF A)

51.Ye, Dayong; Shen, Sheng; Zhu, Tianqing*; Liu, Bo; Zhou, Wanlei. "One Parameter Defense—Defending Against Data Inference Attacks via Differential Privacy," in IEEE Transactions on Information Forensics and Security, vol. 17, pp. 1466-1480, 2022, doi: 10.1109/TIFS.2022.3163591. (CCF A)

52.Zhang, Lefeng; Zhu, Tianqing*; Xiong, Ping; Zhou, Wanlei; Yu, Philip S. 2021. More than Privacy: Adopting Differential Privacy in Game-theoretic Mechanism Design. ACM Computing Surveys. 54, 7, Article 136 (September 2022), 37 pages.

https://doi.org/10.1145/3460771.

53.Zhu, Tianqing*; Zhou, Wei; Ye, Dayong; Cheng, Zishuo; Li, Jin. "Resource Allocation in IoT Edge Computing via Concurrent Federated Reinforcement Learning," in IEEE Internet of Things Journal, vol. 9, no. 2, pp. 1414-1426, 15 Jan.15, 2022, doi: 10.1109/JIOT.2021.3086910.

54.Zhu, Tianqing; Li, Jin; Hu, Xiangyu; Xiong, Ping; Zhou, Wanlei. "The Dynamic Privacy-Preserving Mechanisms for Online Dynamic Social Networks," in IEEE Transactions on Knowledge and Data Engineering, vol. 34, no. 6, pp. 2962-2974, 1 June 2022, doi: 10.1109/TKDE.2020.3015835. (CCF A)

55.Ye, Dayong; Zhu, Tianqing*; Cheng, Zishuo; Zhou, Wanlei; Philip, S Yu. "Differential Advising in Multiagent Reinforcement Learning," in IEEE Transactions on Cybernetics, vol. 52, no. 6, pp. 5508-5521, June 2022, doi: 10.1109/TCYB.2020.3034424.

56.Zhu, Tianqing*; Ye, Dayong; Wang, Wei; Zhou, Wanlei; Philip, S Yu. "More Than Privacy: Applying Differential Privacy in Key Areas of Artificial Intelligence," in IEEE Transactions on Knowledge and Data Engineering, vol. 34, no. 6, pp. 2824-2843, 1 June 2022, doi: 10.1109/TKDE.2020.3014246. (CCF A)

57.Ye, Dayong; Zhu, Tianqing*; Shen, Sheng; Zhou, Wanlei; Philip, S Yu. "Differentially Private Multi-Agent Planning for Logistic-Like Problems," in IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 2, pp. 1212-1226, 1 March-April 2022, doi: 10.1109/TDSC.2020.3017497. (CCF A)

58.Zhang, Tao; Zhu, Tianqing*; Li, Jing; Han, Mengde; Zhou, Wanlei; Yu, Philip. "Fairness in Semi-Supervised Learning: Unlabeled Data Help to Reduce Discrimination," in IEEE Transactions on Knowledge and Data Engineering, vol. 34, no. 4, pp. 1763-1774, 1 April 2022, doi: 10.1109/TKDE.2020.3002567. (CCF A)