Tianqing ZHU

CURRICULUM VITAE

City University of Macau, Macau SAR, China
+853 63540561
tqzhu@cityu.edu.mo

Introduction

I am a Professor, PhD supervisor and Vice Dean at the Faculty of Data Science at City University of Macau, Macao SAR, China. I earned my BEng and MEng degrees from Wuhan University in 2000 and 2004, respectively, and my PhD in Computer Science from Deakin University in Australia in 2014. My research interests lie in the areas of cybersecurity of data analysis, privacy preservation, and security in artificial intelligence.

Research Impact

I have extensive experience teaching and researching in the areas of cybersecurity, data analytics, and security in artificial intelligence. I was entitled as youth talent at Hubei Province. My research work has been recognized through grants from eight Australian National Funding (ARC) and two national funding in China (NSFC). I was selected as Top 2% Scientists Worldwide 2023 by Stanford University. When I was in Australia, I served as a College of Expert of Australian Research Council from 2021-2023. Also, I served as co-director at the Research Centre for Cyber Security and Privacy at the University of Technology Sydney. I have built a core research team comprising two associate professors, two senior lecturers, 26 PhD students, one research fellow, and several top overseas collaborative researchers. This team has achieved significant academic impact, publishing on top conferences such as USENIX and IJCAI, and a series of survey papers on AI privacy and security in top venues such as ACM Computing Surveys and IEEE Transactions on Knowledge and Data Engineering. We also regularly publish in other leading journals, including TDSC and TIFS for cybersecurity and TKDE and TNNLS for data engineering.

Professional Experience

2023-present **Professor**, *School of Data Science*, City University of Macao, China.

2020-2023 **Professor**, *School of Computer Science*, China University of Geosciences (Wuhan) , China.

2020-2023 **Associate Professor (part time)**, *School of Computer Science*, University of Technology Sydney, Australia.

2018 - 2020 **Senior Lecturer**, *School of Computer Science*, University of Technology Sydney, Australia.

2018-2018.6 **Lecturer**, *School of Information Technology*, Deakin University, Australia.

2014 - 2017 **Teaching Scholar**, *School of Information Technology*, Deakin University, Australia.

2004 - 2011 **Lecturer**, *School of Information and Computer Science*, Wuhan Polytechnic University, China.

2000 - 2002 **Research Assistant**, *Central China Electronic Power International Economic & Trade Co. Ltd*, China.

Education

2011 - 2014 **School of Information Technology, PhD**, *Deakin University*, Australia.
- PhD Topic : Differential Privacy and Its Application
- Research area : Social Network, Privacy Preserving, Data Mining

2002 - 2004 **Master of Automatic Engineering**, *Wuhan University*, China.
- Research area : Network Security, Data Mining

1996 - 2000 **Bachelor of Engineering**, *Wuhan University (previously Wuhan University of Hydraulic and Electrical Engineering)*, China.

Associate Editor Experiences

2023 - present **Associate Editor**, *Computer Standard and Interfaces*, Springer.

2020-present **Associate Editor**, *IEEE Transactions on Sustainable Computing*, IEEE.

2020-present **Associate Editor**, *Journal of Ambient Intelligence and Humanized Computing*, Springer.

2018-present **Associate Editor**, *International Journal of Computers, Applications*, (Taylor & Francis).

Teaching Experience

2020-present **City University of Macao**.
- Postgraduate supervision : supervising 6 PhD students, completed 4 master students
- Course coordinator : Big data analysis, Parallel processing

2020-present **China University of Geosciences (Wuhan), China**.
- Course development : the frontier of cyber security
- Course Coordinator : the frontier of cyber security

2018-2020 **University of Technology Sydney**.
- Curriculum development : cybersecurity major for undergraduate students
- Course development : privacy preserving, cybersecurity for data analytics, the insight of cybersecurity for data analytics
- Course coordinator : over ten courses related to the data security and software engineering

2014-2018 **Deakin University**.

- Curriculum development : Online courses for graduate students
- Course development : Database and Information Retrieval, Data Analytic and Cyber Security
- Course coordinator : Enterprise Network Construction, Computer Networks, Classes, Libraries and Algorithms, System Security, Database and Information Retrieval, Data Analytic and Cyber Security, Fundamentals of Information Technology, Enterprise Business Intelligence

2004-2011 **Wuhan Polytechnic University, Lecturer**.

- Course development : Information Security
- Course coordinator : Information Security, Computer Network, Mobile Computing, Software Engineering, C/C++ Language, IT Organization, Software Requirement Analysis

PhD supervision

2020 - 2024 **Yuan Zhao**, working as a data scientist at Accenture, Australia.

2020 - 2024 **Lefeng Zhang**, working as an assistant professor at city university of Macau.

2019 - 2023 **Congcong Zhu**, working as an assistant professor at city university of Macau.

2020 - 2023 **Suleiman Abahussein**, working as a scientist at National Center for Artificial Intelligence, Kingdom of Saudi Arabia.

2019 - 2023 **Minghao Wang**, working as an assistant professor at city university of Macau.

2020 - 2023 **Xiangyu Hu**, working as an assistant professor at University of Electronic Science and Technology of China.

2019 - 2023 **Chi Liu**, working as an assistant professor at city university of Macau.

2019 - 2022 **Zishuo Cheng**, working as a data scientist in Australian Education Management Group, Australia.

2019 - 2022 **Sheng Shen**, working as a post-doc at the University of Sydney, Australia.

2018 - 2022 **Tao Zhang**, working as a senior scientist in seek.com Company, Australia.

2014 - 2018 **Mengmeng Yang**, working as a senior scientist at the Commonwealth Scientific and Industrial Research Organisation (CSIRO), Australia.

Research Grants and Projects

2020 - 2023 **National Natural Science Foundation of China Grant**, *1st CI*, China.

- Project Title : Data privacy for dynamic cross-domain platform
- Funding : 600,000 CNY

2024 - 2027 **ARC Discovery Grant**, *1st Chief Investigator*, University of Technology Sydney, Australia.

- Project Title : Balance and reinforcement : privacy and fairness in high intelligence models
- Funding : 453,000 AUD

2023 - 2026 **ARC Linkage Grant**, *1st Chief Investigator*, University of Technology Sydney, Australia.

- Project Title : Improved Security and Privacy for Online Platform
- Funding : 830,000 AUD

2023 - 2026 **ARC Discovery Grant**, *1st Chief Investigator*, University of Technology Sydney, Australia.

- Project Title : Deep Learning Attacks and Active Defences : A Cybersecurity Perspective
- Funding : 482,610 AUD

2023 - 2026 **ARC Linkage Grant**, *2nd CI*, University of Technology Sydney, Australia.

- Project Title : Secure and Resistant Blockchain for Financial and Business Applications
- Funding : 492,209 AUD

2020 - 2023 **ARC Discovery Grant**, *1st CI*, University of Technology Sydney, Australia.

- Project Title : GDPR modelling in cross-domain social networks
- Funding : 410,000 AUD

2019 - 2022 **ARC Linkage Grant**, *1st CI*, with Belmont Computer Centre Pty.Ltd, Australia.

- Project Title : Privacy preservation for personalised smart device
- Funding : 470,000 AUD

2019 - 2022 **ARC Discovery Grant**, *2nd CI*, University of Technology Sydney, Australia.

- Project Title : Enhancing privacy preserving in dynamic cyberspace
- Funding : 314,000 AUD

2017 - 2020 **ARC Linage Grant**, *2nd CI*, Australia Education Management Group, Australia.

- Project Title : A provable privacy preserving data sharing in cloud environment
- Funding : 540,000 AUD

2017 - 2018 **Industry Grant**, *1st CI*, Deakin University and Australia Education Management Group, Australia.

- Project Title : Student's career analysis and recommendation based on a machine learning model
- Funding : 30,000 AUD

2017 - 2018 **Industry Grant**, *1st CI*, Deakin University and Australia Education Management Group, Australia.

- Project Title : Analysis of big data on education
- Funding : 20,000 AUD

2017 - 2018 **Industry Grant**, *1st CI*, Deakin University and Australia Education Management Group, Australia.

- Project Title : Visualisation of statistics of big data on education
- Funding : 20,000 AUD

2016 - 2017 **Industry Grant**, *1st CI*, Deakin University and Australia Education Management Group, Australia.

- Project Title : Developing a Secure and Privacy-Preserving App for the Cloud Campus System
- Funding : 50,000 AUD

2016 - 2018 **National Natural Science Foundation of China Grant**, *1st CI*, China.

- Project Title : Differentially Private Social Network
- Funding : 190,000 CNY (39,000 AUD)

Publications

My DBLP **https ://dblp.org/pid/19/8310.html**.

Authored books

1. Tianqing Zhu, Gang Li, Wanlei Zhou, Philip S. Yu, Differential privacy and its Applications, ISBN 978-3-319-62002-2, Springer, September 2017.
2. Bo Liu, Wanlei Zhou, Tianqing Zhu, Yong Xiang, Kun Wang, Location Privacy in Mobile Applications, ISBN 978-981-13-1704-0, Springer 2018.

Refereed papers (* is the corresponding author)

2024

3. Xue, Liang; Zhu, Tianqing; , Hybrid resampling and weighted majority voting for multi-class anomaly detection on imbalanced malware and network traffic data, Engineering Applications of Artificial Intelligence, 128, 2024

4. Sun, Hui; Zhu, Tianqing*; Chang, Wenhan; Zhou, Wanlei; , A two-stage model extraction attack on GANs with a small collected dataset, Computers & Security, 137, 2024

5. Liu, Chi; Zhu, Tianqing*; Zhao, Yuan; Zhang, Jun; Zhou, Wanlei; , Disentangling different levels of GAN fingerprints for task-specific forensics, Computer Standards & Interfaces, 89, 2024

6. Zhu, Congcong; Ye, Dayong; Huo, Huan; Zhou, Wanlei; Zhu, Tianqing*; , A location-based advising method in teacher–student frameworks, Knowledge-Based Systems, 285, 2024

7. Chen, Huajie; Liu, Chi; Zhu, Tianqing*; Zhou, Wanlei; , When deep learning meets watermarking: A survey of application, attacks and defenses, Computer Standards & Interfaces, 2024

8. Chen, Huajie; Zhu, Tianqing*; Liu, Chi; Yu, Shui; Zhou, Wanlei; , High-Frequency Matters: Attack and Defense for Image-Processing Model Watermarking, IEEE Transactions on Services Computing, 2024

9. Han, Mengde; Zhu, Tianqing*; Zhou, Wanlei; , Fair Federated Learning with Opposite GAN, Knowledge-Based Systems, 2024

10. Ye, Dayong; Zhu, Tianqing*; Gao, Kun; Zhou, Wanlei; , Defending against Label-only Attacks via Meta-Reinforcement Learning, IEEE Transactions on Information Forensics and Security, 2024

11. Xiang, Yuexin; Li, Tiantian; Ren, Wei; He, Jie; Zhu, Tianqing; Choo, Kim-Kwang Raymond; , AdvEWM: Generating image adversarial examples by embedding digital watermarks, Journal of Information Security and Applications, 80, 2024

12. Zhang, Guangsheng; Liu, Bo; Zhu, Tianqing*; Ding, Ming; Zhou, Wanlei; , PPFed: A Privacy-Preserving and Personalized Federated Learning Framework, IEEE Internet of Things Journal, 2024

13. Wang, Minghao; Zhu, Tianqing*; Zuo, Xuhan; Ye, Dayong; Yu, Shui; Zhou, Wanlei; , Public and Private Blockchain Infusion: A Novel Approach to Federated Learning, IEEE Internet of Things Journal, 2024

2023

14. Tianqing Zhu*, Dayong Ye, Shuai Zhou, Bo Liu, Wanlei Zhou: Label-Only Model Inversion Attacks: Attack With the Least Information. IEEE Transactions on Information Forensics and Security. 18: 991-1005 (2023)
15. Tianqing Zhu*; Dayong Ye; Zishuo Cheng; Wanlei Zhou; Philip S. Yu: Learning Games for Defending Advanced Persistent Threats in Cyber Systems. IEEE Transactions on Systems, Man, and Cybernetics: Systems. Vol. 53. issue 4, pp. 2410 - 2422. 2023

16. Lefeng Zhang, Tianqing Zhu*, Farookh Khadeer Hussain, Dayong Ye & Wanlei Zhou 2023, 'A Game-Theoretic Method for Defending Against Advanced Persistent Threats in Cyber Systems', IEEE Transactions on Information Forensics and Security, vol. 18, pp. 1349–1364, doi:10.1109/tifs.2022.3229595
17. Shuai Zhou, Chi Liu, Dayong Ye, Tianqing Zhu*, Wanlei Zhou, Philip S. Yu. Adversarial Attacks and Defenses in Deep Learning: from a Perspective of Cybersecurity. ACM Computing Survey. 55(8): 161:1-161:35 (2023)
18. Chi Liu, Tianqing Zhu*, Jun Zhang, Wanlei Zhou. Privacy Intelligence: A Survey on Image Privacy in Online Social Networks. 55(8): 161:1-161:35 (2023)
19. Chi Liu, Huajie Chen, Tianqing Zhu*, Jun Zhang & Wanlei Zhou 2023, 'Making DeepFakes More Spurious: Evading Deep Face Forgery Detection via Trace Removal Attack', IEEE Transactions on Dependable and Secure Computing, pp. 1–15, doi:10.1109/tdsc.2023.3241604
20. Tingting Liao, Zhen Lei, Tianqing Zhu, Shan Zeng, Yaqin Li, Cao Yuan: Deep Metric Learning for K Nearest Neighbor Classification. IEEE Trans. Knowl. Data Eng. 35(1): 264-275 (2023)
21. Minghao Wang, Tianqing Zhu*, Xuhan Zuo, Mengmeng Yang, Shui Yu & Wanlei Zhou 2023, 'Differentially private crowdsourcing with the public and private blockchain', IEEE Internet of Things Journal, pp. 1–1, doi:10.1109/jiot.2022.3233360
22. Congcong Zhu, Zishuo Cheng, Dayong Ye, Farookh Khadeer Hussain, Tianqing Zhu*, Wanlei Zhou.Time-driven and Privacy-preserving Navigation Model for Vehicle-to-vehicle Communication Systems.IEEE Transactions on Vehicular Technology. Pp. 1-10. 2023
23. Lefeng Zhang, Tianqing Zhu*, Ping Xiong, Wanlei Zhou, Philip S. Yu: A Robust Game-Theoretical Federated Learning Framework With Joint Differential Privacy. IEEE Trans. Knowl. Data Eng. 35(4): 3333-3346 (2023)
24. Hui Sun, Tianqing Zhu*, Zhiqiu Zhang, Dawei Jin, Ping Xiong, Wanlei Zhou: Adversarial Attacks Against Deep Generative Models on Data: A Survey. IEEE Trans. Knowl. Data Eng. 35(4): 3367-3388 (2023)
25. Xiangyu Hu, Tianqing Zhu*, Xuemeng Zhai, Wanlei Zhou, Wei Zhao: Privacy Data Propagation and Preservation in Social Media: A Real-World Case Study. IEEE Trans. Knowl. Data Eng. 35(4): 4137-4150 (2023)
26. Liu, Baoping; Liu, Bo; Ding, Ming; Zhu, Tianqing*; Yu, Xin; TI2Net: Temporal Identity Inconsistency Network for Deepfake Detection. Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision. 4691-4700. 2023
27. Zhao, Yuan; Liu, Bo; Ding, Ming; Liu, Baoping; Zhu, Tianqing*; Yu, Xin; Proactive Deepfake Defence via Identity Watermarking. Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision. 4602-4611. 2023
28. Tian, Huan; Liu, Bo; Zhu, Tianqing*; Zhou, Wanlei; Philip, S Yu; CIFair: Constructing continuous domains of invariant features for image fair classifications. Knowledge-Based Systems. 110417.2023
29. Huang, Wen; Zhuo, Ming; Zhu, Tianqing*; Zhou, Shijie; Liao, Yongjian; Differential privacy: Review of improving utility through cryptography-based technologies. Concurrency and Computation: Practice and Experience . e7565 2023
30. Yang, Mengmeng; Lam, Kwok-Yan; Zhu, Tianqing; Tang, Chenghua; SPoFC: A framework for stream data aggregation with local differential privacy. Concurrency and Computation: Practice and Experience. e7572 2023
31. Xue, Hanyu; Liu, Bo; Yuan, Xin; Ding, Ming; Zhu, Tianqing; Face image de-identification by feature space adversarial perturbation. Concurrency and Computation: Practice and Experience. e7554 2023
32. Zhiqiu Zhang, Tianqing Zhu*, Wei Ren, Ping Xiong, Kim-Kwang Raymond Choo: Preserving data privacy in federated learning through large gradient pruning. Comput. Secur. 125: 103039 (2023)

33. Tao Zhang, Tianqing Zhu*, Mengde Han, Fengwen Chen, Jing Li, Wanlei Zhou, Philip S. Yu: Fairness in graph-based semi-supervised learning. Knowl. Inf. Syst. 65(2): 543-570 (2023)
34. Yizhi Liu, Xiaohan Hao, Wei Ren, Ruoting Xiong, Tianqing Zhu, Kim-Kwang Raymond Choo, Geyong Min: A Blockchain-Based Decentralized, Fair and Authenticated Information Sharing Scheme in Zero Trust Internet-of-Things. IEEE Trans. Computers 72(2): 501-512 (2023)
35. Yang, Mengmeng; Guo, Taolin; Zhu, Tianqing; Tjuawinata, Ivan; Zhao, Jun; Lam, Kwok-Yan; , Local differential privacy and its applications: A comprehensive survey, Computer Standards & Interfaces, , 2023
36. Zhang, Tao; Zhu, Tianqing; Li, Jing; Zhou, Wanlei; Philip, S Yu; , Revisiting model fairness via adversarial examples, Knowledge-Based Systems, 277, 2023
37. Xiang, Yuexin; Li, Tiantian; Ren, Wei; Zhu, Tianqing; Choo, Kim-Kwang Raymond; , A lightweight privacy-preserving scheme using pixel block mixing for facial image classification in deep learning, Engineering Applications of Artificial Intelligence, 126, 2023
38. Cheng, Zishuo; Zhu, Tianqing; Zhu, Congcong; Ye, Dayong; Zhou, Wanlei; Philip, S Yu; , Privacy and evolutionary cooperation in neural-network-based game theory, Knowledge-Based Systems, 282, 2023
39. Wang, Minghao; Zhu, Tianqing; Zuo, Xuhan; Ye, Dayong; Yu, Shui; Zhou, Wanlei; , Blockchain Empowered Multi-Agent Systems: Advancing IoT Security and Transaction Efficiency, IEEE Internet of Things Journal, 2023
40. Zhu, Congcong; Ye, Dayong; Zhu, Tianqing; Zhou, Wanlei; , Location-Based Real-Time Updated Advising Method for Traffic Signal Control, IEEE Internet of Things Journal, 2023
41. Wang, Minghao; Zhu, Tianqing; Zuo, Xuhan; Ye, Dayong; Yu, Shui; Zhou, Wanlei; , Blockchain-Based Gradient Inversion and Poisoning Defense for Federated Learning, IEEE Internet of Things Journal, 2023

42. 2022

43. Tianqing Zhu, Wei Zhou, Dayong Ye, Zishuo Cheng, Jin Li: Resource Allocation in IoT Edge Computing via Concurrent Federated Reinforcement Learning. IEEE Internet Things J. 9(2): 1414-1426 (2022)
44. Tianqing Zhu, Dayong Ye, Wei Wang, Wanlei Zhou, Philip S. Yu: More Than Privacy: Applying Differential Privacy in Key Areas of Artificial Intelligence. IEEE Trans. Knowl. Data Eng. 34(6): 2824-2843 (2022)
45. Tianqing Zhu, Jin Li, Xiangyu Hu, Ping Xiong, Wanlei Zhou: The Dynamic Privacy-Preserving Mechanisms for Online Dynamic Social Networks. IEEE Trans. Knowl. Data Eng. 34(6): 2962-2974 (2022)
46. Lefeng Zhang, Tianqing Zhu*, Ping Xiong, Wanlei Zhou, Philip S. Yu: More than Privacy: Adopting Differential Privacy in Game-theoretic Mechanism Design. ACM Computing Survey. 54(7): 136:1-136:37 (2022)
47. Dayong Ye, Tianqing Zhu*, Zishuo Cheng, Wanlei Zhou, Philip S. Yu: Differential Advising in Multiagent Reinforcement Learning. IEEE Trans. Cybern. 52(6): 5508-5521 (2022)
48. Dayong Ye, Tianqing Zhu* Sheng Shen, Wanlei Zhou, Philip S. Yu: Differentially Private Multi-Agent Planning for Logistic-Like Problems. IEEE Trans. Dependable Secur. Comput. 19(2): 1212-1226 (2022)
49. Dayong Ye, Sheng Shen, Tianqing Zhu*, Bo Liu, Wanlei Zhou: One Parameter Defense - Defending Against Data Inference Attacks via Differential Privacy. IEEE Transactions on Information Forensics and Security. 17: 1466-1480 (2022)

50. Tao Zhang, Tianqing Zhu*, Jing Li, Mengde Han, Wanlei Zhou, Philip S. Yu: Fairness in Semi-Supervised Learning: Unlabeled Data Help to Reduce Discrimination. IEEE Trans. Knowl. Data Eng. 34(4): 1763-1774 (2022)
51. Wen Huang, Shijie Zhou, Tianqing Zhu, Yongjian Liao: Privately Publishing Internet of Things Data: Bring Personalized Sampling Into Differentially Private Mechanisms. IEEE Internet Things J. 9(1): 80-91 (2022)
52. Yuan Zhao, Bo Liu, Tianqing Zhu, Ming Ding, Wanlei Zhou: Private-encoder: Enforcing privacy in latent space for human face images. Concurr. Comput. Pract. Exp. 34(3) (2022)
53. Ping Xiong, Lin Liang, Yunli Zhu, Tianqing Zhu: PriTxt: A privacy risk assessment method for text data based on semantic correlation learning. Concurr. Comput. Pract. Exp. 34(5) (2022)
54. Sheng Shen, Tianqing Zhu*, Dayong Ye, Minghao Wang, Xuhan Zuo, Andi Zhou: A novel differentially private advising framework in cloud server environment. Concurr. Comput. Pract. Exp. 34(7) (2022)
55. Tao Zhang, Tianqing Zhu*, Renping Liu, Wanlei Zhou: Correlated data in differential privacy: Definition and analysis. Concurr. Comput. Pract. Exp. 34(16) (2022)
56. Sheng Shen, Tianqing Zhu*, Di Wu, Wei Wang, Wanlei Zhou: From distributed machine learning to federated learning: In the view of data privacy and security. Concurr. Comput. Pract. Exp. 34(16) (2022)
57. Ximing Liu, Tianqing Zhu, Cuiqing Jiang, Dayong Ye, Fuqing Zhao: Prioritized Experience Replay based on Multi-armed Bandit. Expert Syst. Appl. 189: 116023 (2022)
58. Zishuo Cheng, Dayong Ye, Tianqing Zhu*, Wanlei Zhou, Philip S. Yu, Congcong Zhu: Multi-agent reinforcement learning via knowledge transfer with differentially private noise. Int. J. Intell. Syst. 37(1): 799-828 (2022)
59. Congcong Zhu, Dayong Ye, Tianqing Zhu*, Wanlei Zhou: Time-optimal and privacy preserving route planning for carpool policy. World Wide Web 25(3): 1151-1168 (2022)
60. Tao Zhang, Tianqing Zhu*, Kun Gao, Wanlei Zhou, Philip S. Yu, "Balancing Learning Model Privacy, Fairness, and Accuracy With Early Stopping Criteria", accepted by IEEE Transactions on Neural Networks and Learning Systems, early access: https://ieeexplore.ieee.org/document/9642428
61. Dayong Ye, Tianqing Zhu*, Congcong Zhu, Wanlei Zhou, Philip S. Yu, "Model-Based Self-Advising for Multi-Agent Learning", Accepted by IEEE Transactions on Neural Networks and Learning Systems, early access: https://ieeexplore.ieee.org/document/9712868
62. Guangsheng Zhang, Bo Liu, Tianqing Zhu, Ming Ding, Wanlei Zhou, "Label-Only Membership Inference Attacks and Defenses In Semantic Segmentation Models", Accepted by IEEE Transactions on Dependable and Secure Computing, early access: https://ieeexplore.ieee.org/document/9723588
63. Xiangyu Hu, Tianqing Zhu*, Xuemeng Zhai, Wanlei Zhou and Wei Zhao, "Privacy Data Diffusion Modeling and Preserving in Online Social Network", accepted by IEEE Transactions on Knowledge and Data Engineering, early access: https://ieeexplore.ieee.org/document/9658172
64. Chenguang Wang, Tianqing Zhu*, Ping Xiong, Wei Ren, Kim-Kwang Raymond Choo: A privacy preservation method for multiple-source unstructured data in online social networks. Comput. Secur. 113: 102574 (2022)
65. Huan Tian, Tianqing Zhu*, Wanlei Zhou: Fairness and privacy preservation for facial images: GAN-based methods. Comput. Secur. 122: 102902 (2022)
66. Xiuting Gu, Tianqing Zhu*, Jie Li, Tao Zhang, Wei Ren, Kim-Kwang Raymond Choo: Privacy, accuracy, and model fairness trade-offs in federated learning. Comput. Secur. 122: 102907 (2022)
67. Xiang Yu, Dongmei Zhang, Tianqing Zhu, Xinwei Jiang: Novel hybrid multi-head self-attention and multifractal algorithm for non-stationary time series prediction. Inf. Sci. 613: 541-555 (2022)
68. Ping Xiong, Guirong Li, Wei Ren, Tianqing Zhu: LOPO: a location privacy preserving path optimization scheme for spatial crowdsourcing. J. Ambient Intell. Humaniz. Comput. 13(12): 5803-5818 (2022)

69. Mingze Ni, Ce Wang, Tianqing Zhu, Shui Yu, Wei Liu: Attacking neural machine translations via hybrid attention learning. Mach. Learn. 111(11): 3977-4002 (2022)
70. Huiying Zou, Xiaofan Liu, Wei Ren, Tianqing Zhu: A Decentralized Electronic Reporting Scheme with Privacy Protection Based on Proxy Signature and Blockchain. Secur. Commun. Networks 2022: 5424395:1-5424395:8 (2022)

71. 2021

72. Ruiyang Xiao, Wei Ren, Tianqing Zhu, Kim-Kwang Raymond Choo: A Mixing Scheme Using a Decentralized Signature Protocol for Privacy Protection in Bitcoin Blockchain. IEEE Trans. Dependable Secur. Comput. 18(4): 1793-1803 (2021)
73. Dayong Ye, Tianqing Zhu*, Sheng Shen, Wanlei Zhou: A Differentially Private Game Theoretic Approach for Deceiving Cyber Adversaries. IEEE Trans. Inf. Forensics Secur. 16: 569-584 (2021)
74. Aneesh Sreevallabh Chivukula, Xinghao Yang, Wei Liu, Tianqing Zhu, Wanlei Zhou: Game Theoretical Adversarial Deep Learning With Variational Adversaries. IEEE Trans. Knowl. Data Eng. 33(11): 3568-3581 (2021)
75. Zhibo Wang, Jing Zhao, Jiahui Hu, Tianqing Zhu, Qian Wang, Ju Ren, Chao Li: Towards Personalized Task-Oriented Worker Recruitment in Mobile Crowdsensing. IEEE Trans. Mob. Comput. 20(5): 2080-2093 (2021)
76. Xin Chen, Tao Zhang, Sheng Shen, Tianqing Zhu*, Ping Xiong: An optimized differential privacy scheme with reinforcement learning in VANET. Comput. Secur. 110: 102446 (2021)
77. Yang Xia, Tianqing Zhu, Xiaofeng Ding, Hai Jin, Deqing Zou: Heterogeneous differential privacy for vertically partitioned databases. Concurr. Comput. Pract. Exp. 33(8) (2021)
78. Yuexin Xiang, Wei Ren, Tiantian Li, Xianghan Zheng, Tianqing Zhu, Kim-Kwang Raymond Choo: A multi-type and decentralized data transaction scheme based on smart contracts and digital watermarks. J. Netw. Comput. Appl. 176: 102953 (2021)
79. Xiaohan Hao, Wei Ren, Ruoting Xiong, Tianqing Zhu, Kim-Kwang Raymond Choo: Asymmetric cryptographic functions based on generative adversarial neural networks for Internet of Things. Future Gener. Comput. Syst. 124: 243-253 (2021)
80. Zhenfei Chen, Tianqing Zhu*, Ping Xiong, Chenguang Wang, Wei Ren: Privacy preservation for image data: A GAN-based method. Int. J. Intell. Syst. 36(4): 1668-1685 (2021)
81. Tiantian Li, Wei Ren, Yuexin Xiang, Xianghan Zheng, Tianqing Zhu, Kim-Kwang Raymond Choo, Gautam Srivastava: FAPS: A fair, autonomous and privacy-preserving scheme for big data exchange based on oblivious transfer, Ether cheque and smart contracts. Inf. Sci. 544: 469-484 (2021)

82. 2020

83. Dayong Ye, Tianqing Zhu*, Wanlei Zhou, Philip S. Yu: Differentially Private Malicious Agent Avoidance in Multiagent Advising Learning. IEEE Trans. Cybern. 50(10): 4214-4227 (2020)
84. Tao Zhang, Tianqing Zhu*, Ping Xiong, Huan Huo, Zahir Tari, Wanlei Zhou: Correlated Differential Privacy: Feature Selection in Machine Learning. IEEE Trans. Ind. Informatics 16(3): 2115-2124 (2020)
85. Jianghua Liu, Jingyu Hou, Xinyi Huang, Yang Xiang, Tianqing Zhu: Secure and efficient sharing of authenticated energy usage data with privacy preservation. Comput. Secur. 92: 101756 (2020)
86. Minghao Wang, Tianqing Zhu*, Tao Zhang, Jun Zhang, Shui Yu, Wanlei Zhou: Security and privacy in 6G networks: New areas and new challenges. Digit. Commun. Networks 6(3): 281-291 (2020)
87. Tianqing Zhu, Ping Xiong, Gang Li, Wanlei Zhou, Philip S. Yu: Differentially private model publishing in cyber physical systems. Future Gener. Comput. Syst. 108: 1297-1306 (2020)
88. Ping Xiong, Lefeng Zhang, Tianqing Zhu, Gang Li, Wanlei Zhou: Private collaborative filtering under untrusted recommender server. Future Gener. Comput. Syst. 109: 511-520 (2020)

89. Dayong Ye, Tianqing Zhu*, Sheng Shen, Wanlei Zhou. A Differentially Private Game Theoretic Approach for Deceiving Cyber Adversaries. IEEE Transactions on Information Forensics and Security. DOI: 10.1109/TIFS.2020.3016842. Page(s): 1 – 1. 2020.
90. Dayong Ye, Tianqing Zhu*, Sheng Shen, Wanlei Zhou, Philip S. Yu. Differentially Private Multi-Agent Planning for Logistic-like Problems. IEEE Transactions on Dependable and Secure Computing. Accepted on 15 Aug 2020.
91. Tao Zhang, Tianqing Zhu*, Jing Li, Mengde Han, Wanlei Zhou, Philip S. Yu. Fairness in Semi-supervised Learning: Unlabeled Data Help to Reduce Discrimination. IEEE Transactions on Knowledge and Data Engineering. Preprints. 2020. 10.1109/TKDE.2020.3002567
92. Jianghua Liu, Jingyu Hou, Xinyi Huang, Yang Xiang, Tianqing Zhu. Secure and efficient sharing of authenticated energy usage data with privacy preservation. Computers & Security, 92, 2020
93. Hanyu Xue, Bo Liu, Ming Ding, Li Song, Tianqing Zhu: Hiding Private Information in Images From AI. ICC 2020: 1-6

94. Before 2019
95. Yaocheng Zhang, Wei Ren, Tianqing Zhu, Yi Ren. SaaS: A situational awareness and analysis system for massive android malware detection. Future Generation Computer Systems 95, 548-559, 2019.
96. Cai Fu, Xiao-Yang Liu, Jia Yang, Laurence T Yang, Shui Yu, and Tianqing Zhu. Wormhole: The hidden virus propagation power of a search engine in social networks. IEEE Transactions on Dependable and Secure Computing, Volume: 16, Issue: 4, 2019, Pages: 693 - 710, (IF= 6.404).
97. Bo Liu, Ming Ding, Tianqing Zhu, Yong Xiang, Wanlei Zhou. Adversaries or allies? Privacy and deep learning in big data era. Concurrency and Computation: Practice and Experience, 2019 .Available online: https://doi.org/10.1002/cpe.5102 (IF=1.167)
98. Mengmeng Yang, Tianqing Zhu, Kaitai Liang, Wanlei Zhou, Robert H Deng. A Blockchain-based Location Privacy-preserving Crowdsensing System. Future Generation Computer Systems. 94, 408-418, 2019. (IF=4.639)
99. Bo Zhang ; Tianqing Zhu ; Chengyu Hu ; Chuan Zhao. Cryptanalysis of a Lightweight Certificateless Signature Scheme for IIOT Environments. IEEE Access, Year: 2018 , Volume: 6 Pages: 73885 – 73894 (IF=4.098)
100. Shixiong Yao; Jing Chen; Kun He; Ruiying Du; Tianqing Zhu; Xin Chen. PBCert: Privacy-Preserving Blockchain-based Certificate Status Validation toward Mass Storage Management. IEEE Access. Year: 2018 , Volume 7, Pages: 6117 - 6128 (IF=4.098)
101. Jinyi Guo, Wei Ren, Yi Ren, Tianqing Zhu. A Watermark-Based In-Situ Access Control Model for Image Big Data. Future Internet. Volume 10. Issue 8. Pages- 69, 2018
102. Ping Xiong, Lefeng Zhang, Tianqing Zhu, Gang Li, Wanlei Zhou. Private collaborative filtering under untrusted recommender server. Future Generation Computer Systems, Accepted on 2018/05, https://doi.org/10.1016/j.future.2018.05.077. (IF= 4.639)
103. Tianqing Zhu, Ping Xiong, Gang Li, Wanlei Zhou, Philip S. Yu. Differentially private model publishing in cyber physical systems. Future Generation Computer Systems. 108, 1297-1306, 2020 (IF=4.639)
104. Mengmeng Yang, Tianqing Zhu, Bo Liu, Yang Xiang, Wanlei Zhou. Differential Private POI Queries via Johnson-Lindenstrauss Transform. IEEE Access 2018, https://doi.org/ 10.1109/ACCESS.2018.2840726 (IF=4.098)
105. Bo Liu, Wanlei Zhou, Tianqing Zhu, Longxiang Gao, Yong Xiang. Location Privacy and its Applications: A Systematic Study. IEEE Access, Volume: 6, pp. 17606 – 17624 https://doi.org/10.1109/ACCESS.2018.2822260 Accepted on 03/04/2018 (IF=4.098)

106. Mengmeng Yang, Tianqing Zhu, Bo Liu, Yang Xiang, Wanlei Zhou. Density-based Location Preservation for Mobile Crowdsensing in Internet-of-Thing. IEEE Access, (Vol 6.) https://doi.org/2018. 10.1109/ACCESS.2018.2816918 pp. 14779-14789 (IF=4.098)
107. Mengmeng Yang, Tianqing Zhu, Bo Liu, Yang Xiang, Wanlei Zhou. Machine Learning based Differential Privacy Multifunctional Aggregation under Fog Computing Architecture. IEEE Access (Vol 6.) 2018. https://doi.org/10.1109/ACCESS.2018.2817523 pp: 17119 - 17129 (IF=4.098)
108. Yangfan Li, Wei Ren, Tianqing Zhu, Yi Ren, Yue Qin, Wei Jie. RIMS: A Real-time and Intelligent Monitoring System for live-broadcasting platforms. Future Generation Computer Systems 87, 259-266, 2018 (IF=4.639).
109. Sheng Zhong; Wei Ren; Tianqing Zhu; Yi Ren; Kim-Kwang Raymond Choo. Performance and Security Evaluations of Identity-and Pairing-based Digital Signature Algorithms on Windows, Android, and Linux Platforms: Revisiting the Algorithms of Cha and Cheon, Hess, Barreto, Libert, McCullagh and Quisquater, and Paterson and Schuldt. IEEE Access. Year: 2018, Volume 6, Pages: 37850 - 37857, (IF=4.098)
110. Lefeng Zhang, Ping Xiong, Wei Ren, Tianqing Zhu. A differentially private method for crowdsourcing data submission. Concurrency and Computation: Practice and Experience. Early access. 2018. https://doi.org/10.1002/cpe.5100 (IF=1.167)
111. Tianqing Zhu, Gang Li, Wanlei Zhou, Philip S. Yu. Differentially Private Data Publishing and Analysis: a Survey. IEEE Transactions on Knowledge and Data Engineering. 29(8) pp:1639-1638, 2017 (IF=3.457)
112. Tianqing Zhu, Gang Li, Ping Xiong, and Wanlei Zhou. Answering differentially private queries for continual datasets release. Future Generation Computer Systems, 87, 2018, pp 816-827. (IF=4.639).
113. Tianqing Zhu, Ping Xiong, Gang Li, Wanlei Zhou. Correlated Differential Privacy: Hiding Information in Non-IID Dataset. IEEE Transactions on Information Forensics & Security, 10(2). 2015. 229-242. (IF= 6.211)
114. Tianqing Zhu, Yongli Ren, Wanlei Zhou, Jia Rong, Ping Xiong. An Effective Privacy Preserving Algorithm for Neighborhood-based Collaborative Filtering. Future Generation Computer Systems, 36, 2014, 142–155 (IF=4.639)
115. Tianqing Zhu, Gang Li, Wanlei Zhou, Ping Xiong, Cao Yuan. Privacy Preserving Topic Model for Tagging Recommender Systems. Knowledge and Information Systems, 46 (1), 2016. pp 33-58, (IF= 2.247)
116. Tianqing Zhu, Gang Li, Lei Pan, Yongli Ren, Wanlei Zhou. (2014). Privacy Preserving Collaborative Filtering for KNN Attack Resisting. Social Network Analysis and Mining. 4 (1), 1-14, 2014.
117. Bo Liu, Wanlei Zhou, Tianqing Zhu, Longxiang Gao, Tom H. Luan, and Haibo Zhou, Silence is Golden: Enhancing Privacy of Location-Based Services by Content Broadcasting and Active Caching in Wireless Vehicular Networks, IEEE Transactions on Vehicular Technology, 2016, 65 (12) pp 9942 - 9953, (IF=5.339)
118. Bo Liu, Wanlei Zhou, Tianqing Zhu, Haibo Zhou, Xiaodong Lin, "Invisible Hand: Economic Model based Trajectory Privacy Preserving Schemes in Mobile Crowd Sensing Applications". IEEE Transactions on Vehicular Technology. 2017, pp 66 (5), 4410-4423. (IF=5.339)
119. Min Li, Cai Fu, Xiao-Yang Liu, Jia Yang, Tianqing Zhu, Lansheng Han, Evolutionary virus immune strategy for temporal networks based on community vitality. Future Generation Computer Systems, Volume 74, September 2017, Pages 276-290 (IF=4.639)
120. Ping Xiong, Lefeng Zhang, Tianqing Zhu. Reward-based spatial crowdsourcing with differential privacy preservation. Enterprise Information Systems, 2017, 11 (10), 1500-1517 (IF=1.908)

121. Ping Xiong, Tianqing Zhu, Wenjia Niu, Gang Li. A Differentially Private Algorithm for Location Data Release. Knowledge and Information Systems, 47 (3), 2016. pp 647–669 (IF= 2.247)
122. Ping Xiong, Lefeng Zhang, Tianqing Zhu. Semantic analysis in location privacy preserving. Concurrency and Computation: Practice and Experience. 28 (6), 2016. pp 1884–1899. (IF=1.167)
123. Daibin Wang, Hai Jin, Deqing Zou, Peng Xu, Tianqing Zhu, Gang Chen. Taming transitive permission attack via bytecode rewriting on Android application. Security and Communication Networks. 9 (13). 2016. pp 2100–2114. (IF=1.067)
124. Mengmeng Yang, Tianqing Zhu, Wanlei Zhou, and Yang Xiang. Attacks and Countermeasures in Social Network Data Publishing. ZTE Communications, Vol.14, June 2016, pp.2-9.
125. Ping Xiong, Xiaofeng Wang, Wenjia Niu, Tianqing Zhu, and Gang Li. Android malware detection with contrasting permission patterns. Communications of China, 11(8), 2014. 1-14.
126. Ping Xiong, Tianqing Zhu, Xiao Gu. Data anonymization-based on restriction of information grain ratio: method and evaluation. Application Research of Computer. Vol 31(3). 2014. pp 819-824.
127. Ping Xiong, Tianqing Zhu, Xiaofeng Wang. A Survey on Differential Privacy and Applications. Chinese Journal of Computers. Vol 37(1), 2014. pp 101-112.
128. Ping Xiong, Tianqing Zhu. A Data Anonymization Approach based on Impurity Gain and Hierarchical Clustering. Journal of Computer Research and Development. 49 (7), 2012. pp 1545-1552.
129. Nicholas Patterson, Michael Hobbs, Tianqing Zhu: A cyber-threat analytic model for autonomous detection of virtual property theft. Information & Computer Security. 2017. pp 25 (4), 358-381.
130. Tianqing Zhu, Ping Xiong, Gang Li, Wanlei Zhou, Philip S. Yu:
Differentially private query learning: From data publishing to model publishing. BigData 2017
131. Bo Liu, Ming Ding, Tianqing Zhu, Yong Xiang, Wanlei Zhou. Using Adversarial Noises to Protect Privacy in Deep Learning Era. 2018 IEEE Global Communications Conference (GLOBECOM), 2019
132. Shaoxiong Ji, Guodong Long, Shirui Pan, Tianqing Zhu, Jing Jiang, Sen Wang, Detecting Suicidal Ideation with Data Protection in Online Communities. International Conference on Database Systems for Advanced Applications, 2019, 225-229
133. Yaocheng Zhang, Wei Ren, Tianqing Zhu, Wei Bi. MoSa: A Modeling and Sentiment Analysis System for Mobile Application Big Data. International Conference on Algorithms and Architectures for Parallel Processing. Pages; 582-595, 2019
134. Lefeng Zhang, Ping Xiong, Tianqing Zhu.A differentially private method for crowdsourcing data submission. Pacific-Asia Conference on Knowledge Discovery and Data Mining. Pages: 142-148, 2018. (Best Student Paper Award)
135. Mengmeng Yang, Tianqing Zhu, Lichuan Ma, Yang Xiang, Wanlei Zhou. Privacy Preserving Collaborative Filtering via the Johnson-Lindenstrauss Transform. TrustCom / BigDataSE / ICESS 2017: proceedings of the TrustCom / BigDataSE / ICESS 2017 International Conference. 2017. 417-424.
136. Mengmeng Yang, Tianqing Zhu, Yang Xiang, and Wanlei Zhou. Personalized privacy preserving collaborative filtering. In International Conference on Green, Pervasive, and Cloud Computing, pages 371–385. Springer, Cham, 2017.
137. Lefeng Zhang, Xiaodan Lu, Ping Xiong, Tianqing Zhu. A Differentially Private Method for Reward-Based Spatial Crowdsourcing. International Conference on Applications and Techniques in Information Security. ATIS2015, page 153-164, 2015. (Best Student Paper Award)
138. Ping Xiong, Tianqing Zhu, Lei Pan, Wenjia Niu, Gang Li. Privacy Preserving in Location Data Release: A Differential Privacy Approach. Advances in Artificial Intelligence, The 13th Pacific Rim International Conference on Artificial Intelligence (PRICAI 2014), Gold Coast, Australia, December 1-5, 2014, Proceedings, Volume 8862 of Lecture Notes in Computer Science, pages 183–195. Springer, 2014.

139. Tianqing Zhu, Gang Li, Wanlei Zhou, Ping Xiong, and Cao Yuan. Deferentially Private Tagging Recommendation Based on Topic Model. Advances in Knowledge Discovery and Data Mining, The 18th Pacific-Asia Conference on Knowledge Discovery and Data Mining (PAKDD 2014), Taiwan, 2014, pages 557–568. Springer, 2014. (Best Student Paper Award)
140. Yongli Ren, Tianqing Zhu, Gang Li, and Wanlei Zhou. Top-n recommendations by learning user preference dynamics. Advances in Knowledge Discovery and Data Mining, The 17th Pacific-Asia Conference on Knowledge Discovery and Data Mining, Gold Coast Australia, April 14-17, 2013, pages 390–401.
141. Tianqing Zhu, Gang Li, Yongli Ren, Wanlei Zhou, and Ping Xiong. Differential privacy for neighborhood-based collaborative filtering. Advanced in Social Networks Analysis and Mining, 2013 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM 2013), Niagara Falls, Canada, August 25-28, 2013, Proceedings, ISBN: 9781450322409, pages 752–759. ACM, 2013
142. Tianqing Zhu, Gang Li, Yongli Ren, Wanlei Zhou, and Ping Xiong. Privacy preserving for tagging recommender systems. Advanced in Web Intelligence and Intelligent Agent Technologies, 2013 IEEE/WIC/ACM International Joint Conferences on Web Intelligence (WI) and Intelligent Agent Technologies (IAT), Atlanta, GA, USA, November 17-20, 2013, Proceedings, Volume 1, pages 81-88. IEEE, 2013.
143. Tianqing Zhu, Ping Xiong, Yang Xiang, Wanlei Zhou. An effective differentially private data releasing algorithm for decision tree. 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, (TrustCom). In Melbourne, Australia, July 16-18, 2013. Pages: 388-395.
144. Ping Xiong and Tianqing Zhu. An anonymization method based on tradeoff between utility and privacy for data publishing. 2012 International Conference on Management of e-Commerce and e-Government (ICMeCG). 20-21 Oct. 2012, Wuhan China, Pages: 72–78.
145. Longxiang Gao, Ming Li, Tianqing Zhu, Alessio Bonti, Wanlei Zhou, and Shui Yu. Amdd: Exploring entropy based anonymous multi-dimensional data detection for network optimization in human associated DTNS. IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Liverpool, United Kingdom 25-27 June 2012. Pages: 1245–1250