Haibo Hu

Tel: +852-3400 3557
Fax:+852-2362 8439
E-mail: haibo.hu@polyu.edu.hk
Web: https://www.haibohu.org
ORCID: 0000-0002-9008-2112
Scopus ID: 8986988800
Web of Science ID: AAS-5704-2020

Address:
Dept. of Electrical and Electronic Engineering
The Hong Kong Polytechnic University
Hung Hom, Kowloon
Hong Kong SAR, China

Research Interests

Data privacy and security, adversarial machine learning, mobile and spatiotemporal databases.

Education

09/2001 – 08/2005
Doctor of Philosophy in Computer Science, Hong Kong University of Science and Technology (HKUST)
Direct admission scheme offered by Ministry of Education for talented students
Dissertation: “Spatial and Continuous Spatial Queries on Smart Mobile Clients”

09/1997 – 06/2001
Bachelor of Engineering, Shanghai Jiao Tong University, China
Major in Computer Science and Engineering, Minor in Finance

Working Experience

07/2023 present
Professor and Associate Head, Department of Electrical and Electronic Engineering, The Hong Kong Polytechnic University

- Associate Head (Learning and Teaching), from 07/2024.
- Programme Leader, BSc (Hons) Degree in Information Security, until 06/2024.
- Teach full-time courses: “Network Technologies and Security”, “Intrusion Detection and Penetration Test”, and “Integrated Project”
- Director, “Applied Security, Trust and Privacy Lab for Enterprise” (ASTAPLE)
- Manager, PolyU Catch-The-Flag (CTF) Team

07/2019 – 06/2023
Associate Professor, Department of Electronic and Information Engineering, The Hong Kong Polytechnic University

- Programme Leader, BSc (Hons) Degree in Information Security
- Teach full-time courses: “Intrusion Detection and Penetration Test”, “Security in Data Communication” and “Integrated Project”
- Director, “Applied Security, Trust and Privacy Lab for Enterprise” (ASTAPLE)
- Manager, PolyU Catch-The-Flag (CTF) Team

09/2015 – 06/2019
Assistant Professor, Department of Electronic and Information Engineering, The Hong Kong Polytechnic University

- Deputy Programme Leader, BSc (Hons) Degree in Information Security
- Teach full-time undergraduate courses: "Network Technologies and Security”, “Intrusion Detection and Prevention”, and “Integrated Project”
- Director, “Applied Security, Trust and Privacy Lab for Excellence” (ASTAPLE)

09/2008 – 08/2015 **Assistant Professor / Research Assistant Professor**, Department of Computer Science, Hong Kong Baptist University

- Teach full-time undergraduate courses: "Object-oriented Programming”, “Mobile Computing”, “Information Systems Security and Auditing” and “Advanced Algorithm Design, Analysis and Implementation”
- Conduct research in privacy-aware data management and data security

09/2006 – 08/2008 **Postdoctoral (Teaching) Fellow**, Department of Computer Science, Hong Kong Baptist University

- Teach full-time undergraduate courses: "Computer Organization", “Data Communications and Networking”, and “Object-oriented Programming”
- Conduct research in privacy-aware data management and mobile database

09/2005 – 08/2006 **Postdoctoral Fellow,** Department of Computer Science, Hong Kong University of Science and Technology

- Conduct research in spatiotemporal database and mobile data management

09/2001 – 08/2005 **Research Assistant**, Department of Computer Science, Hong Kong University of Science and Technology

- Conduct research in data management for broadcasting and wireless systems
- Conduct research in mobile and location-based services

Publications

Peer-Reviewed Journal Papers

1. R. Li, **H. Hu**, and Q. Ye. “RFTrack: Stealthy Location Inference and Tracking Attack on Wi-Fi Devices.” *IEEE Transactions on Information Forensics and Security* (TIFS), accepted to appear, 2024.

2. J. Duan, Q. Ye, **H. Hu**, and X. Sun. “LDPTube: Theoretical Utility Benchmark and Enhancement for LDP Mechanisms in High-dimensional Space.” *IEEE Transactions on Knowledge and Data Engineering (TKDE)*, accepted to appear, 2024.

3. K. Huang, G. Ouyang, Q. Ye, **H. Hu**, B. Zheng, X. Zhao, R. Zhang, X. Zhou. “LDPGuard: Defenses against Data Poisoning Attacks to Local Differential Privacy Protocols.” *IEEE Transactions on Knowledge and Data Engineering (TKDE)*, accepted to appear, 2024.

4. H. Yan, **H. Hu**, Q. Ye, and J. Xu. “Multi-hop Sanitizable Signature for Collaborative Edge Computing.” *Journal of Computer Security*, accepted to appear, 2024.

5. L. Yang, F. Ye, **H. Hu**, H. Lu, Y. Wang, and W. Chang. “A data-driven rule-base approach for carbon emission trend forecast with environmental regulation and efficiency improvement.” *Sustainable Production and Consumption*, Volume:45, March 2024, 316-332.

6. F. Ye, L. Yang, H. Lu, **H. Hu**, and Y. Wang. “Enterprise performance online evaluation based on extended belief rule-base model.” *Expert Systems with Applications*, Volume 247, 1 August 2024, 123255.

7. J. Huang, T. Huang, H. Wei, J. Zhang, H. Yan, D. Wong, and **H. Hu**. “zkChain: A Privacy-Preserving Model Based on zk-SNARKs and Hash Chain for Efficient Transfer of Assets.” *Transactions on Emerging Telecommunications Technologies* (*ETT*), Volume 35, Number 4, pp. 4709, 2024.

8. X. Sun, Q. Ye, **H. Hu**, J. Duan, Q. Xue, T. Wo, and J. Xu. “PUTS: Privacy-Preserving and Utility-Enhancing Framework for Trajectory Synthesization.” *IEEE Transactions on Knowledge and Data*

Engineering (TKDE), Volume: 36, Issue: 1, January 2024, 296 - 310.

9. L. Wang, Q. Ye, **H. Hu**, X Meng. "EPS: Privacy Preserving Set-Valued Data Analysis in the Shuffle Model." *IEEE Transactions on Knowledge and Data Engineering (TKDE)*, accepted to appear, 2023.

10. Y. Mao, Q. Ye, Q. Wang, **H. Hu**. "Utility-Aware Time Series Data Release with Anomalies under TLDP". *IEEE Transactions on Mobile Computing (TMC)*, accepted to appear, 2023.

11. K. Huang, Y. Cui, Q. Ye, Y. Zhao, X. Zhao, Y. Tian, K. Zheng, **H. Hu**, and X. Zhou. "TED+: Towards Discovering Top-k Edge-Diversified Patterns in a Graph Database." *IEEE Transactions on Knowledge and Data Engineering (TKDE)*, Volume 36, Issue 5, May 2024, 2224-2238.

12. L. Tang, Q. Ye, **H. Hu**, Q. Xue, and Y. Xiao. "DeepMark: A Scalable and Robust Framework for DeepFake Video Detection." *ACM Transactions on Privacy and Security* (*TOPS*), Volume 27, Issue 1, February 2024, 1-26.

13. H. Yan, **H. Hu**, and Q. Ye. "Partial Message Verification in Fog-based Industrial Internet of Things." *Computers & Security*, Volume 135, December 2023, 103530.

14. Y. Fu, Q. Ye, R. Du, and **H. Hu**. "Collecting Multi-type and Correlation-Constrained Streaming Sensor Data with Local Differential Privacy." *ACM Transactions on Sensor Networks* (*TOSN*), accepted to appear, 2023.

15. I. Ghafoor, P. Tse, T. Chan, and **H. Hu**. "The design of a non-contact inspection system integrated with the Time of Flight-Based Flaw Detection TOFFD criterion to investigate the structural integrity of the rail track." *IEEE Transactions on Instrumentation and Measurement* (*TIM*), Volume 73, Article Sequence Number: 7001913, 05 January 2024.

16. L. Tang, Q. Ye, **H. Hu**, and M. H. Au. "Secure Traffic Monitoring with Spatio-temporal Metadata Protection Using Oblivious RAM." *IEEE Transactions on Intelligent Transportation Systems*, Volume: 24, Issue: 12, December 2023, pp. 14903 – 14913.

17. T. Li, C. Fung, H. Wong, T. Chan, **H. Hu**. "Functional Subspace Variational Autoencoder for Domain-Adaptive Fault Diagnosis." *Mathematics* 2023, 11(13), 2910.

18. M Marus, Y Mukha, HT Wong, TL Chan, A Smirnov, A Hubarevich, **H. Hu**. "Tsuchime-like Aluminum Film to Enhance Absorption in Ultra-Thin Photovoltaic Cells." *Nanomaterials* 13 (19), 2650, 2023.

19. L. Yang, T. Ren, F. Ye, **H. Hu**, H. Wang, and H. Zheng. "Extended belief rule base with ensemble imbalanced learning for lymph node metastasis diagnosis in endometrial carcinoma." *Engineering Applications of Artificial Intelligence* 126: 106950, 2023.

20. X. Sun, Q. Ye, **H. Hu**, Y. Wang, K. Huang, T. Wo, and J. Xu. "Synthesizing Realistic Trajectory Data With Differential Privacy." *IEEE Transactions on Intelligent Transportation Systems*, Volume: 24, Issue: 5, May 2023, pp. 5502 – 5515.

21. M. Marus, Y. Mukha, H.T. Wong, T. Chan, A. Smirnov, A. Hubarevich, and **H. Hu**. "Tsuchime-like cost-efficient aluminum film to enhance absorption in thin and ultra-thin photovoltaic cells." *Nanomaterials 2023, 13(19), 2650.*

22. L. Yang, T. Ren, **H. Hu**, F. Ye, and Y. Wang. "Extended belief rule base inference model based on clustering ensemble and activation factor." *Control and Decision*, 2023, 38(3): 815-824.

23. L. Yao, X. Wang, **H. Hu**, and G. Wu. “A Utility-aware Anonymization Model for Multiple Sensitive Attributes Based on Association Concealment.” *IEEE Transactions on Dependable and Secure Computing (TDSC)*, accepted to appear, 2023.

24. H. Yan, S. Li, Y. Wang, Y. Zhang, K. Sharif, **H. Hu**, and Y. Li. “Membership Inference Attacks against Deep Learning Models via Logits Distribution”. *IEEE Transactions on Dependable and Secure Computing* (*TDSC*), Volume: 20, Issue: 5, 01 Sept.-Oct. 2023.

25. Q. Qian, Q. Ye, **H. Hu**, K. Huang, T. Chan, and J. Li. “Collaborative Sampling for Partial Multi-dimensional Value Collection under Local Differential Privacy.” *IEEE Transactions on Information Forensics & Security (TIFS)*, Volume 18, 3948 - 3961, June 2023.

26. H. Yan, A. Yan, L. Hu, J. Liang, and **H. Hu**. “MTL-Leak: Privacy Risk Assessment in Multi-task Learning”. *IEEE Transactions on Dependable and Secure Computing* (*TDSC*), Volume: 21, Issue: 1, Jan.-Feb. 2024, pp. 204-215.

27. G. Zhang, J. Zhang, Y. Liu, **H. Hu**, J. Lee, and V. Aggarwal. “Adaptive Video Streaming with Automatic Quality-of-Experience Optimization.” *IEEE Transactions on Mobile Computing (TMC),* Volume: 22, Issue: 8, 01 August 2023.

28. Q. Xue, Q. Ye, **H. Hu**, Y. Zhu, and J. Wang. “DDRM: A Continual Frequency Estimation Mechanism with Local Differential Privacy.” *IEEE Transactions on Knowledge and Data Engineering (TKDE)*, Volume: 35, Issue: 7, July 2023, pp. 6784-6797.

29. Z. Han, **H. Hu**, and Q. Ye. “ReFlat: A Robust Access Pattern Hiding Solution for General Cloud Query Processing Based on K-Isomorphism and Hardware Enclave.” *IEEE Transactions on Cloud Computing (TCC),* Volume: 11, Issue: 2, 01 April 2023, pp. 1474-1486.

30. N. Fu, W. Ni, **H. Hu**, and S. Zhang. “Multidimensional Grid-based Clustering with Local Differential Privacy.” *Information Sciences*, Volume 623, April 2023, pp. 402-420.

31. B. C. Singh, Q. Ye, **H. Hu**, and B. Xiao. “Efficient and lightweight indexing approach for multi-dimensional historical data in blockchain.” *Future Generation Computer Systems,* Volume 139, February 2023, Pages 210-223.

32. Q. Ye, **H. Hu**, X. Meng, H. Zheng, K. Huang, C. Fang, and J. Shi. “PrivKVM*: Revisiting Key-Value Statistics Estimation with Local Differential Privacy.” *IEEE Transactions on Dependable and Secure Computing* (*TDSC*), Volume: 20, Issue: 1, Jan., pp 17-35, 2023.

33. G. Zhang, K. Liu, **H. Hu**, V. Aggarwal, and Y. B. Lee. “Post-Streaming Wastage Analysis – A Data Wastage Aware Framework in Mobile Video Streaming.” *IEEE Transactions on Mobile Computing (TMC),* 22(1) January 2023, 389 - 401.

34. Q. Ye, **H. Hu**, M. H. Au, X. Meng, X. Xiao. “LF-GDPR: A Framework for Estimating Graph Metrics with Local Differential Privacy.” *IEEE Transactions on Knowledge and Data Engineering (TKDE),* Vol 34, Issue 10, pages 4905 - 4920, 2022.

35. Z. Han, Q. Ye, and **H. Hu**. “OTKI-F: An Efficient Memory-secure Multi-keyword Fuzzy Search Protocol.” *Journal of Computer Security*, vol. 31, no. 2, pp. 129-152, 2023.

36. Z. Peng, J. Xu, **H. Hu**, and L. Chen. “BlockShare: A Blockchain Empowered System for Privacy-Preserving Verifiable Data Sharing.” *Bulletin of the IEEE Computer Society Technical Committee on*

Data Engineering, June 2022, pp.14-24.

37. L. Tang, Q. Ye, H. Zheng, **H. Hu**, Z. Han, and N-F. Law. "Stateful-CCSH: An Efficient Authentication Scheme for High-Resolution Video Surveillance System." *IEEE Internet of Things Journal,* Volume: 9, Issue: 19, 19373 – 19386, October 2022.

38. H. Yan, **H. Hu**, Q. Ye, and L. Tang. "SPMAC: Scalable Prefix Verifiable Message Authentication Code for Internet of Things." *IEEE Transactions on Network and Service Management (TNSM)*, Volume: 19, Issue: 3, Page(s): 3453 – 3464, September 2022.

39. G. Zhang, J. Zhang, K. Liu, J. Guo, J. Lee, **H. Hu**, and V. Aggarwal. "DUASVS: A Mobile Data Saving Strategy in Short-form Video Streaming." *IEEE Transactions on Services Computing (TSC)*, Volume: 16, Issue: 2, 01 March 2023, pp. 1066 - 1078.

40. H. Zheng, Q. Ye, **H. Hu**, F. Cheng, and J. Shi. "Protecting Decision Boundary of Machine Learning Model with Differentially Private Perturbation." *IEEE Transactions on Dependable and Secure Computing (TDSC*), 19(3), pp. 2007-2022, May 2022.

41. X. Pan, S. Nie, **H. Hu**, P. Yu, J. Guo, and L. Wu. "Reverse Nearest Neighbor Search in Semantic Trajectories for Location based Services." *IEEE Transactions on Services Computing (TSC),* 15(2), pp 986-999, 2022.

42. K. Huang, **H. Hu**, S. Zhou, J. Guan, Q. Ye, and X. Zhou. "Privacy and Efficiency Guaranteed Social Subgraph Matching." *The VLDB Journal (VLDBJ)*, Volume 31, pages 581–602, 2022.

43. L. Yao, Z. Chen, **H. Hu**, G. Wu, and B. Wu. "Privacy Preservation for Trajectory Publication Based on Differential Privacy." *ACM Transactions on Intelligent Systems and Technology (TIST)*, Vol. 13, No. 3, Article 42, April 2022.

44. G. Zhang, J. Lee, K. Liu, **H. Hu**, and V. Aggarwal, "A Unified Framework for Flexible Playback Latency Control in Live Video Streaming." *IEEE Transactions on Parallel and Distributed Systems (TPDS)*, Volume: 32, Issue: 12, Dec 2021, 3024-3037.

45. D. K. Mondal, B. C. Singh, **H. Hu**, S.Biswas, Z. Alom, M. A. Azim. "SeizeMaliciousURL: A Novel Learning Approach to Detect Malicious URLs." *Journal of Information Security and Applications*, Volume 62:102967, September 2021.

46. B. C. Singh, Z. Alom, **H. Hu**, M. M. Rahman, M. K. Baowal, Z. Aung, M. A. Azim, and M. Ali. "Moni *COVID-19 Pandemic Outbreak in the Subcontinent: A data-driven analysis." *Journal of Personalized Medicine*, 2021, 11(9), 889.

47. L. Yang, F. Ye, J. Liu, Y. Wang, and **H. Hu**. "An improved fuzzy rule-based system using evidential reasoning and subtractive clustering for environmental investment prediction." *Fuzzy Sets and Systems*, 421, 44-61, 2021.

48. L. Yang, S. Wang, F. Ye, J. Liu, Y. Wang, and **H. Hu**. "Environmental investment prediction using extended belief rule-based system and evidential reasoning rule." *Journal of Cleaner Production*, Volume 289, 20 March 2021, 125661.

49. Z. Han and **H. Hu**. "ProDB: A memory-secure database using hardware enclave and practical oblivious RAM." *Information Systems*, Volume 96, February 2021, 101681.

50. L. Yao, Z. Chen, **H. Hu**, G. Wu, and B. Wu. "Sensitive attribute privacy preservation of trajectory

data publishing based on l-diversity.” *Distributed and Parallel Databases*, Volume 39, pages 785–811, 2021.

51. H. Zheng, **H. Hu**, and Z. Han, “Preserving User Privacy for Machine Learning: Local Differential Privacy or Federated Machine Learning?” *IEEE Intelligent Systems*. 35(4): pp 5-14, 2020.

52. H. Zheng and **H. Hu**. “MISSILE: A System of Mobile Inertial Sensor-Based Sensitive Indoor Location Eavesdropping.” *IEEE Transactions on Information Forensics and Security (TIFS)*, Volume 15, September 2019, 3137 - 3151.

53. C. Liu, S. Zhou, **H. Hu**, Y. Tang, J. Guan, and Y. Ma. “CPP: Towards Comprehensive Privacy Preserving for Query Processing in Information Networks.” *Information Sciences*, Volume 467, October 2018, pages 296-311.

54. C. Xu, Q. Chen, **H. Hu**, J. Xu, and X. Hei. “Authenticating Aggregate Queries over Set-Valued Data with Confidentiality.” *IEEE Transactions on Knowledge and Data Engineering (TKDE),* 30(4):630-644, Apr 2018.

55. Q. Zhu, **H. Hu**, C. Xu, J. Xu, and W. Lee. “Geo-Social Group Queries with Minimum Acquaintance Constraints”, *The VLDB Journal*, 26(5), 709-727, October 2017.

56. X. Lin, J. Xu, **H. Hu** and Z. Fan, “Reducing Uncertainty of Probabilistic Top-k Ranking via Pairwise Crowdsourcing”, *IEEE Transactions on Knowledge and Data Engineering (TKDE)*, 29(10): 2290 - 2303, Oct. 2017.

57. **H. Hu**, Q. Chen, J. Xu, and B. Choi, “Assuring Spatio-Temporal Integrity on Mobile Devices with Minimum Location Disclosure”, *IEEE Transactions on Mobile Computing (TMC)*, 16(11): 3000-3013, November 2017.

58. Z. Zhao, Y. Cheung, **H. Hu**, and X. Wu, “Corrupted and Occluded Face Recognition via Cooperative Sparse Representation”, *Pattern Recognition*, Vol. 56, pp. 77-87, August 2016.

59. S. Gao, J. Xu, T. Haerder, B. He, B. Choi, and **H. Hu**. "PCMLogging: Optimizing Transaction Logging and Recovery Performance with PCM." *IEEE Transactions on Knowledge and Data Engineering (TKDE)*, 27(12):3332-3346, December 2015.

60. X. Lin, J. Xu, and **H. Hu**. "Reverse Keyword Search for Spatio-Textual Top-k Queries in Location-Based Services." *IEEE Transactions on Knowledge and Data Engineering (TKDE)*, 27(11): 3056-3069, Nov. 2015.

61. Y. Li, R. Chen, J. Xu, Q. Huang, **H. Hu**, and B. Choi. "Geo-Social K-Cover Group Queries for Collaborative Spatial Computing." *IEEE Transactions on Knowledge and Data Engineering (TKDE)*, 27(10):2729 – 2742, October, 2015 (spotlight paper).

62. Z. Fan, B. Choi, Q. Chen, J. Xu, **H. Hu** and S. S. Bhowmick. "Structure-Preserving Subgraph Query Services." *IEEE Transactions on Knowledge and Data Engineering (TKDE),* 27(08): 2275-2290, August, 2015.

63. Z. Zhao, Y. Cheung, **H. Hu**, X Wu. "Expanding Dictionary for Robust Face Recognition: Pixel Is Not Necessary While Sparsity Is." *IET Computer Vision*, 9 (5), 648-654, 2015.

64. R. Chen, Y. Peng, B. Choi, J. Xu, and **H. Hu**. "A private DNA Motif Finding Algorithm." *Journal of Biomedical Informatics (JBI),* 50: 122-132, 2014.

65. Y. Peng, B. Choi, J. Xu, **H. Hu**, and S. S. Bhowmick. "Side-Effect Estimation: A Filtering Approach to the View Update Problem." *IEEE Transactions on Knowledge and Data Engineering (TKDE)*, 26(9): 2307 - 2322, August, 2014.

66. X. Lin, J. Xu, **H. Hu**, and W.-C. Lee. "Authenticating Location-Based Skyline Queries in Arbitrary Subspaces." *IEEE Transactions on Knowledge and Data Engineering (TKDE)*, 26(6): 1479-1493, June 2014.

67. J. Deng, B. Choi, J. Xu, **H. Hu**, and S. S. Bhowmick. "Incremental Maintenance of the Minimum Bisimulation of Cyclic Graphs." *IEEE Transactions on Knowledge and Data Engineering* (TKDE), 25(11): 2536 - 2550, Nov 2013.

68. X. Lin, J. Xu, and **H. Hu**. "Range-based Skyline Queries in Mobile Environments." *IEEE Transactions on Knowledge and Data Engineering (TKDE)*, 25(4): 835-849, April 2013.

69. Y. Li, S. T. On, J. Xu, B. Choi, and **H. Hu**. "Optimizing Non-Indexed Join Processing in Flash Storage-Based Systems." *IEEE Transactions on Computers (TC)*, 62(7): 1417-1431, July 2013.

70. H. Li, **H. Hu**, J. Xu. "Nearby Friend Alert: Location Anonymity in Mobile Geo-Social Networks". *IEEE Pervasive Computing*, 12(4): 62-70, 2013.

71. S. T. On, J. Xu, B. Choi, **H. Hu,** and B. He. "Flag Commit: Supporting Efficient Transaction Recovery in Flash-based DBMSs." *IEEE Transactions on Knowledge and Data Engineering (TKDE)*, 24(9): 1624-1639, Sept 2012.

72. **H. Hu**, J. Xu, S. T. On, J. Du, and K. Y. Ng. "Privacy-Aware Location Data Publishing". *ACM Transactions on Database Systems (TODS)*, 35(3), July 2010.

73. **H. Hu** and J. Xu. "2PASS: Bandwidth-Optimized Location Cloaking for Anonymous Location-Based Services." *IEEE Transactions on Parallel and Distributed Systems (TPDS)*, 21(10): 1458-1472, October 2010 (spotlight paper).

74. **H. Hu**, J. Xu and D. L. Lee. "PAM: An Efficient and Privacy-Aware Monitoring Framework for Continuously Moving Objects." *IEEE Transactions on Data and Knowledge Engineering (TKDE)*, 22(3): 404-419, March 2010.

75. J. Xu, X. Tang, **H. Hu** and J. Du. "Privacy-Conscious Location-Based Queries in Mobile Environments." *IEEE Transactions on Parallel and Distributed Systems (TPDS)*, 21(3): 313-326, March 2010.

76. S. T. On, **H. Hu**, Y. Li, and J. Xu. "Flash-Optimized B+-Tree." *Journal of Computer Science and Technology (JCST)*, 25(3): 509-522, 2010.

77. **H. Hu** and D. L. Lee. "Range Nearest Neighbor Query." *IEEE Transactions on Data and Knowledge Engineering (TKDE)*, 18(1): 78-91, 2006.

78. **H. Hu** and D. L. Lee. "Energy-Efficient Monitoring of Spatial Predicates over Moving Objects." *IEEE Data Engineering Bulletin*, 28(3): 19-26 (2005)

79. D. L. Lee, M. Zhu and **H. Hu**. "When location-based services meet databases." *Mobile Information Systems*, Volume 1, Number 2, 2005.

80. C.-W. Lin, **H. Hu** and D. L. Lee. "Adaptive realtime bandwidth allocation for wireless data delivery." *ACM/Kluwer Journal of Wireless Networks (WINET)*, 10(2), 103-120, March 2004.

Peer-Reviewed Conference Papers

81. L. Wang, Q. Ye, **H. Hu**, X. Meng. "PriPL-Tree: Accurate Range Query for Arbitrary Distribution under Local Differential Privacy." *Proceedings of the VLDB Volume 17 (PVLDB '24)*, Guangzhou, China, August 2024.

82. J. Fu, Q. Ye, **H. Hu**, Z. Chen, L. Wang, K. Wang, X. Ran. "DPSUR: Accelerating Differentially Private Stochastic Gradient Descent Using Selective Update and Release." *Proceedings of the VLDB Volume 17 (PVLDB '24)*, Guangzhou, China, August 2024.

83. C. Zhang, C. Xu, **H. Hu**, and J. Xu. "COLE: A Column-based Learned Storage for Blockchain Systems." *Proc. of the 22nd USENIX Conference on File and Storage Technologies* (*FAST '24*), Santa Clara, CA, USA, 2024.

84. X. Ran, Q. Ye, **H. Hu**, X. Huang, J. Xu, and J. Fu. "Differentially Private Graph Neural Networks for Link Prediction." *Proc. of the 40th IEEE International Conference on Data Engineering (ICDE '24)*, Utrecht, Netherlands, May 2024.

85. Y. Mao, Q. Ye, **H. Hu**, Q. Wang, and K. Huang. "PrivShape: Extracting Shapes in Time Series under User-Level Local Differential Privacy." *Proc. of the 40th IEEE International Conference on Data Engineering (ICDE '24)*, Utrecht, Netherlands, May 2024.

86. Y. Fu, Q. Ye, R. Du, and **H. Hu**. "Interactive Trimming against Evasive Online Data Manipulation Attacks: A Game-Theoretic Approach." *Proc. of the 40th IEEE International Conference on Data Engineering (ICDE '24)*, Utrecht, Netherlands, May 2024.

87. H. Wang, C. Xu, X. Chen, C. Zhang, **H. Hu**, S. Tian, Y. Yan, and J. Xu. "Authenticating Multi-Chain Queries: Verifiable Virtual Filesystem Is All You Need." *Proc. of the 40th IEEE International Conference on Data Engineering (ICDE '24)*, Utrecht, Netherlands, May 2024.

88. X. Sun, Q. Ye, **H. Hu,** J. Duan, T. Wo, J. Xu, and R. Yang. "LDPRecover: Recovering Frequencies from Poisoning Attacks against Local Differential Privacy." *Proc. of the 40th IEEE International Conference on Data Engineering (ICDE '24)*, Utrecht, Netherlands, May 2024.

89. K. Huang, Y. Li, Q. Ye, Y. Tian, X. Zhao, Y. Cui, **H. Hu**, X. Zhou. "FRESH: Towards Efficient Graph Queries in an Outsourced Graph." *Proc. of the 40th IEEE International Conference on Data Engineering (ICDE '24)*, Utrecht, Netherlands, May 2024.

90. H. Yan, **H. Hu**, and Q. Ye. "Time-Specific Integrity Service in MQTT protocol." 23rd *ACM/IEEE International Conference on Information Processing in Sensor Networks* (*IPSN*), Hong Kong, China, May 2024.

91. L. Wang, Q. Ye, **H. Hu**, X. Meng, and K. Huang. "LDP-Purifier: Defending Against Poisoning Attacks in Local Differential Privacy." *29th International Conference on Database Systems for Advanced Applications* (*DASFAA*), Gifu, Japan, July 2024.

92. Y. Zhang, Q. Ye, R. Chen, **H. Hu**, and Q. Han. "Trajectory Data Collection with Local Differential Privacy." *Proceedings of the VLDB Volume 16 (PVLDB '23),* Vancouver, Canada, August 2023.

93. H. Tian, **H. Hu**, and Q. Ye. "CGP: Centroid-guided Graph Poisoning for Link Inference Attacks in Graph Neural Networks." *IEEE International Conference on Big Data* (*IEEE BigData*), Sorrento, Italy, December 2023.

94. H. Li, Q. Ye, **H. Hu**, J. Li, L. Wang, C. Fang, J. Shi. "3DFed: Adaptive and Extensible Framework for Covert Backdoor Attack in Federated Learning." *IEEE Symposium on Security and Privacy* (*S&P*), San Francisco, CA, USA, May 2023, pp. 1893-1907.

95. K. Huang, **H. Hu**, Q. Ye, K. Tian, B. Zheng, and X. Zhou. "TED: Towards Discovering Top-*k* Edge-Diversified Patterns in a Graph Database." *2023 ACM SIGMOD International Conference on Management of Data*, Seattle, Washington, USA, June 2023.

96. Q. Ye, **H. Hu**, K. Huang, M. H. Au, and Q. Xue. "Stateful Switch: Optimized Time Series Release with Local Differential Privacy". *IEEE International Conference on Computer Communications (INFOCOM)*, New York, USA, May 2023.

97. R. Du, Q. Ye, Y. Fu, **H. Hu**, J. Li, C. Fang, and J. Shi. "Differential Aggregation against General Colluding Attackers". *Proc. of the 39th IEEE International Conference on Data Engineering (ICDE '23)*, Anaheim, CA, USA, April 2023.

98. Y. Yan, Q. Ye, **H. Hu**, R. Chen, Q. Han, and L. Wang. "Towards Defending Against Byzantine LDP Amplified Gain Attacks." *28th International Conference on Database Systems for Advanced Applications (DASFAA)*, Tianjin, China, Apr 2023.

99. Y. Xiao, Q. Ye, **H. Hu**, H. Zheng, C. Fang, and J. Shi. "MExMI: Pool-based Active Model Extraction Crossover Membership Inference." *36th Conference on Neural Information Processing Systems (NeurIPS 2022)*, New Orleans, USA.

100. J. Duan, Q. Ye, and **H. Hu**. "Utility Analysis and Enhancement of LDP Mechanisms in High-Dimensional Space." *Proc. of the 38th IEEE International Conference on Data Engineering (ICDE '22)*, Kuala Lumpur, Malaysia, May 2022.

101. K. Huang, Q. Ye, J. Zhao, X. Zhao, **H. Hu**, X. Zhou. "VINCENT: towards efficient exploratory subgraph search in graph databases." *Proceedings of the VLDB Endowment 15 (12), 3634-3637*, 2022.

102. Y. Fu, Q. Ye, R. Du, and **H. Hu**. "Unified Proof of Work: Delegating and Solving Customized Computationally Bounded Problems in A Privacy-preserving Way." *The 6th APWeb-WAIM International Joint Conference on Web and Big Data (APWeb-WAIM)*, 2022.

103. Q. Ye, **H. Hu**, N. Li, X. Meng, H. Zheng, H. Yan. "Beyond Value Perturbation: Differential Privacy in the Temporal Setting." *Proc. of IEEE International Conference on Computer Communications (INFOCOM'21)*, Virtual, May 2021.

104. R. Du, Q. Ye, Y. Fu, and **H. Hu**. "Collecting High-Dimensional and Correlation-Constrained Data with Local Differential Privacy." *Proc. of 18th IEEE International Conference on Sensing, Communication and Networking (SECON)*, Virtual, 2021.

105. G. Zhang, K. Liu, **H. Hu**, and Jing Guo. "Short Video Streaming with Data Wastage Awareness." (Poster) *Proc. of IEEE International Conference on Multimedia and Expo (ICME) 2021*, Virtual, July 5-9.

106. T. Wen, **H. Hu**, and H. Zheng. "An extraction attack on image recognition model using VAE-kdtree model." *Proc. SPIE 11766, International Workshop on Advanced Imaging Technology (IWAIT) 2021*. **(Best Paper Award)**

107. L. Tang and **H. Hu**. "OHEA: Secure Data Aggregation in Wireless Sensor Networks against Untrusted Sensors." *29th ACM International Conference on Information and Knowledge Management (CIKM '20)*, Oct 19-23, 2020, Online, pp 1425–1434.

108. Y. Fu, M. H. Au, R. Du, **H. Hu** and D. Li. Cloud Password Shield: A Secure Cloud-based Firewall against DDoS on Authentication Servers (poster) *Proc. of 40th IEEE International Conference on Distributed Computing Systems* (*ICDCS* '20) July 8 - 10, 2020, Singapore.

109. Q. Ye, **H. Hu**, M. H. Au, X. Meng, X. Xiao. Towards Locally Differentially Private Generic Graph Metric Estimation. *Proc. of the 36th IEEE International Conference on Data Engineering (ICDE '20)*, Dallas, USA, Apr. 2020, pp 1922-1925.

110. H. Zheng, Q. Ye, **H. Hu**, F. Cheng, and J. Shi. "A Boundary Differential Private Layer against Machine Learning Model Extraction Attacks." *Proc. of the 24th European Symposium on Research in Computer Security (ESORICS '19)*, Luxembourg, Sept 2019, pp 66-83.

111. H. Zheng, **H. Hu**, and Han Ziyang. "Preserving User Privacy For Machine Learning: Local Differential Privacy or Federated Machine Learning?" *Proc. of 1st International Workshop on Federated Machine Learning for User Privacy and Data Confidentiality (FML'19), in conjunction with IJCAI'19*. **(Best Theory Paper Award)**

112. L. Yao, X. Wang, X. Wang, **H. Hu**, and G. Wu. "Publishing Sensitive Trajectory Data Under Enhanced l-Diversity Model." Proc. of *20th IEEE International Conference on Mobile Data Management (MDM'19)*, Hong Kong SAR, China. (**Best Paper Award**)

113. Q. Ye, **H. Hu**, X. Meng, and H. Zheng. "PrivKV: Key-Value Data Collection with Local Differential Privacy." *Proc. of 40th IEEE Symposium on Security and Privacy (SP'19)*, San Francisco, USA, May 2019, pp 311-325.

114. M. Zhu, Q. Ye, X. Yang, X. Meng, and **H. Hu**. "AppPrivacy: Analyzing Data Collection and Privacy Leakage from Mobile App." (poster) *Proc. of 40th IEEE Symposium on Security and Privacy (SP'19)*, San Francisco, USA, May 2019.

115. Y. Ji, C. Xu, J. Xu, **H. Hu**. "vABS: Towards Verifiable Attribute-Based Search over Shared Cloud Data." (demo) *Proc. of 35th IEEE International Conference on Data Engineering (ICDE '19)*, Macau SAR, China, Apr. 2019, pp 2028-2031.

116. C. Xu, J. Xu, **H. Hu**, and M. H. Au. "When Query Authentication Meets Fine-Grained Access Control: A Zero-Knowledge Approach." *Proc. of the 2018 ACM SIGMOD International Conference on Management of Data,* Houston, USA, Jun 2018, pp 147-162.

117. C. Xu, Q. Chen, **H. Hu**, J. Xu, and X. Hei. "Authenticating Aggregate Queries over Set-Valued Data with Confidentiality." (poster) *34th IEEE International Conference on Data Engineering (ICDE '18)*, Paris, France, Apr 2018.

118. L. Chen, J. Xu, X. Lin, C. S. Jensen, and **H. Hu**. "Answering Why-Not Spatial Keyword Top-k Queries via Keyword Adaption." *Proc. of the 32nd IEEE International Conference on Data Engineering (ICDE '16)*, Helsinki, Finland, May 2016, pp 697-708.

119. Z. Chen, **H. Hu**, and J. Yu. "Privacy-Preserving Large-Scale Location Monitoring Using Bluetooth Low Energy." *Proc. of 11th IEEE International Conference on Mobile Ad-hoc and Sensor Networks (MSN 2015)*, Shenzhen, China, December 2015, pp 69-78.

120. Q. Chen, **H. Hu**, and J. Xu. "Authenticated Online Data Integration Services." *Proc. of the 2015 ACM SIGMOD International Conference on Management of Data*, pp 167-181.

121. L. Chen, X. Lin, **H. Hu**, C. S. Jensen, and J. Xu. "Answering Why-not Questions on Spatial Keyword Top-k Queries." *Proc. the 31th IEEE International Conference on Data Engineering (ICDE '15)*, Seoul, Korea, April 2015.

122. Lu Wang, X. Meng, **H. Hu**, and J. Xu. "Bichromatic Reverse Nearest Neighbor Query without Information Leakage." *Proc. the 20th International Conference on Database Systems and Applications (DASFAA'15)*, Hanoi, Vietnam, April 2015.

123. **H. Hu,** J. Xu, X. Xu, K. Pei, B. Choi, and S. Zhou. "Private Search on Key-Value Stores with Hierarchical Indexes", *Proc. of the 30th IEEE International Conference on Data Engineering (ICDE '14)*, Chicago, IL, USA, April 2014, pp 628-639**.**

124. Q. Chen, **H. Hu**, and J. Xu. "Authenticating Top-k Queries in Location-based Services with Confidentiality." *Proc. of the VLDB Endowment (PVLDB '14)*, 49-60.

125. **H. Hu**, Q. Chen, and J. Xu. "VERDICT: Privacy-Preserving Authentication of Range Queries in Location-based Services" *Proc. of the 29th IEEE International Conference on Data Engineering (ICDE '13),* demo paper, 1312 – 1315.

126. X. Lin, **H. Hu**, H. P. Li, J. Xu, and B. Choi. "Private Proximity Detection and Monitoring with Vicinity Regions." *Proceedings of 12th International ACM SIGMOD Workshop on Data Engineering for Wireless and Mobile Access (MobiDE '13)*, pp. 5-12, New York, June 2013.

127. Jing Wang, Zhong-Qiu Zhao, Xuegang Hu, Yiu-ming Cheung, and **Haibo Hu**. "Online Learning Towards Big Data Analysis in Health Informatics". *The 2013 International Conference on Brain and Health Informatics*, *Special Session on Intelligent Healthcare Data Analytics*.

128. **H. Hu,** J. Xu, Q. Chen, and Z. Yang. "Authenticating Location-based Services without Compromising Privacy." *Proc. of the 2012 ACM SIGMOD International Conference on Management of Data*, pp. 301 – 312.

129. Z. Huo, X. Meng, **H. Hu**, and Y. Huang. "You Can Walk Alone: Trajectory Privacy-preserving through Significant Stays Protection." *Proc. of the 17th International Conference on Database Systems for Advanced Applications (DASFAA '12),* pp. 351 – 366.

130. **H. Hu**, J. Xu, C. Ren, and B. Choi. “Processing Private Queries over Untrusted Data Cloud through Privacy Homomorphism.” *Proc. of the 27th IEEE International Conference on Data Engineering (ICDE '11),* pp. 601 – 612.

131. X. Lin, J. Xu, and **H. Hu**. “Authentication of Location-based Skyline Queries.” *Proc. of the 20th ACM Conference on Information and Knowledge Management (CIKM '11),* pp. 1583 – 1588.

132. S. Gao, J. Xu, B. He, B. Choi, and **H. Hu**. “PCMLogging: Reducing Transaction Logging Overhead with PCM.” *Proc. of the 20th ACM Conference on Information and Knowledge Management (CIKM '11), poster.*

133. Y. Li, J. Xu, B. Choi, and **H. Hu**. "StableBuffer: Optimizing Write Performance for DBMS Applications on Flash Devices." *Proc. the 19th ACM International Conference on Information and Knowledge Management (CIKM '10)*, Toronto, Canada, October 2010.

134. S. Gao, Y. Li, J. Xu, B. Choi, and **H. Hu**: "DigestJoin: Expediting Joins on Solid-State Drives." *DASFAA 2010*: 428-431.

135. **H. Hu** and J. Xu. "Non-Exposure Location Anonymity." *Proc. the 25th IEEE Int. Conf. on Data Engineering (ICDE '09)*, Shanghai, China, pp. 1120-1131.

136. Y. Li, S. T. On, J. Xu, B. Choi, and **H. Hu**. "DigestJoin: Exploiting Fast Random Reads for Flash-based Joins." *Proc. the 10th International Conference on Mobile Data Management (MDM '09)*, Taipei, Taiwan, May 2009.

137. S. T. On, **H. Hu**, Y. Li, and J. Xu. "Lazy-Update B+-Tree for Flash Devices." *Proc. the 10th International Conference on Mobile Data Management (MDM '09), Taipei, Taiwan, May 2009.*

138. J. Du, J. Xu, X. Tang, and **H. Hu**. "iPDA: Supporting Privacy-Preserving Location-Based Mobile Services." *Proc. the 8th Int. Conf. on Mobile Data Management (MDM '07)*, Mannheim, Germany, May 2007. (Demo)

139. Chen, C. Lai, X. Meng, J. Xu, and **H. Hu**. "Clustering Moving Objects in Spatial Networks." *Proc. the 12th Int. Conf. on Database Systems for Advanced Applications (DASFAA '07)*, Bangkok, Thailand, April 2007.

140. **H. Hu** and D. L. Lee. “Distance Indexing on Road Networks” *Proc. of the 32th International Conference on Very Large Data Bases,* Seoul, Korea, 2006, pp. 894-905.

141. **H. Hu**, D. L. Lee and J. Xu. “Fast Nearest Neighbor Search on Road Networks” *Proc. of the 10th Int. Conf. on Extending Database Technology (EDBT’06)*, 186-203, Munich, Germany, 2006.

142. **H. Hu**, J. Xu and D. L. Lee. “A Generic Framework for Monitoring Continuous Spatial Queries over Moving Objects” *Proc. of the 24th ACM SIGMOD International Conference on Management of Data*, Baltimore, Maryland, 2005, pp. 479-490.

143. **H. Hu**, J. Xu, W. S. Wong, B. Zheng and D. L. Lee. "Proactive Caching for Spatial Queries in Mobile Environments." *Proc. of the 21th IEEE International Conference on Data Engineering (ICDE '05)*, Tokyo, Japan, pp. 403-414.

144. **H. Hu** and D. L. Lee. "GAMMA: A Framework for Moving Object Simulation." *Proc. of 9th Int. Symp. on Spatial and Temporal Databases (SSTD’05)*, Angra dos Reis, Brazil, pp. 37-54.

145. **H. Hu** and D. L. Lee. "Semantic Location Modeling for Location Navigation in Mobile Environment." *Proc. of the 5th Int. Conf. on Mobile Data Management (MDM '04)*, Berkeley, California, USA, 2004, pp. 52-61.

146. **H. Hu**, M. Zhu and D. L. Lee. "Towards Real-time Parallel Processing of Spatial Queries." *Proc. of the Int. Conf. on Parallel Processing (ICPP '03)*, Kaohsiung, Taiwan, 2003, pp. 565-572.

147. **H. Hu**, J. Xu and D. L. Lee. "Adaptive Power-Aware Prefetching Schemes for Mobile Environments." *Proc. of the 4th Int. Conf. on Mobile Data Management (MDM '03)*, Melbourne, Australia, Jan. 2003, Springer-Verlag LNCS, vol. 2574, pp. 374-380.

Invited Papers and Tutorials

148. Q. Ye and **H. Hu.** "Local Differential Privacy: Tools, Challenges, and Opportunities." *20th International Conference on Web Information Systems Engineering (WISE 2019)*, pp. 13-23.

Books, Chapters and Editorials

149. 杨隆浩，叶菲菲，王应明，**胡海波**,《置信规则库的建模新方法与应用》。科学出版社，2023.
150. **H. Hu**, R. Sarkar, and Z. Chen (Eds.) Introduction to the Special Issue on Retrieving and Learning from Internet of Things Data, ACM Transactions on Data Science, Volume 1, Issue 4, November 2020.
151. S. Zhou, W. Qian, **H. Hu** (Eds.) Proceedings of the Second International Workshop on Data Management for Emerging Network Infrastructures (DaMEN 2013), Springer, April 2013.
152. C. S. Jensen, **H. Hu** and D. Wu (Eds.). Proceedings of the First International Workshop on Next-Generation Location-Based Services (LBS n.0), IEEE, June 2013.
153. **H. Hu**, H. Wang, B. Zheng: Challenges in Managing and Mining Large, Heterogeneous Data. DASFAA (2) 2011: 462.
154. A. Zhou, Y. Ishikawa, **H. Hu** and W. Qian (Eds.) Proceedings of the First International Workshop on Data Management for Emerging Network Infrastructures (DaMEN 2011), Springer, 2011.
155. X. Meng, Z. Ding and **H. Hu** (Eds.) Proceedings of the Third International Workshop on Cloud Data Management (CloudDB 2011), ACM, 2011.
156. **H. Hu**, J. Zhou, J. Xu and K. Y. Ng. “Positioning and Privacy in Location-based Services.” Handheld Computing for Mobile Commerce: Applications, Concepts and Technologies. Wen-Chen Hu and Yanjun Zuo, Eds., IGI Global, 2010.
157. **H. Hu**, J. Xu, and X. Tang. “Energy Efficient Sensor Data Management.” Sensor Network and Configuration: Fundamentals, Standards, Platforms, and Experiments. N. P. Mahalik et al, the Springer-Verlag Publishing, Germany, 2007.
158. J. Xu, **H. Hu**, X. Tang, and B. Zheng. "Mobile Cache Management." Wireless Information Highways, D. Katsaros, A. Nanopoulos, and Y. Manolopoulos, Eds., Idea Group Publishing, 2005.

Citations (as of Jun 23, 2024)

Google Scholar

- ➢ Total citations: 4675
- ➢ H-index: 41

Patents

- **H. Hu**, H. Zheng, Q. Ye, C. Fang, J. Shi. Data theft prevention method and related product, US Patent Application 17/698,619, Jun 30 2022.

- Q. Ye and **H. Hu**. Method and apparatus for collecting key-value pair data. US Patent No. 11,615,099 B2, Mar 2023.
- 郑桦迪，叶青青，**胡海波**.“数据防窃取方法和相关产品”，中国专利发明(China Patent)，申请号 201910897929.1, Sep 2019.
- 叶青青，**胡海波**.“键值对数据的收集方法和装置”，中国专利发明(China Patent)，申请号 201811161746.5, Sept 2018**.**
- **H. Hu**, Q. Chen, and J. Xu. "Method and Apparatus for Assuring Location Data Integrity with Minimum Location Disclosure." US Patent No. 9,973,514 B2, May 2018.
- **H. Hu**, Z. Chen, and J. Yu. "Privacy-Preserving Large-Scale Location Monitoring." US Patent No. 9,756,461 B1, Sept 2017.
- J. Xu and **H. Hu**. "A System and Method for Providing Proximity Information." US Patent No. 9,351,116 B2, May 2016.
- **H. Hu**, J. Xu, and Q. Chen. "Method and Apparatus for Authenticating Location-based Services without Compromising Location Privacy." US Patent No. 9,043,927 B2, May 2015.

Professional Qualifications and Services

- **Professional Qualifications**
  - Certified Instructor, Cisco CCNA Security (since 2016)

- **Memberships**
  - ACM (Member-2005, **Senior Member**-2022)
  - IEEE (Member-2013, **Senior Member**-2020)
  - China Computer Federation, 中国计算机学会 (Member-2015, **Senior Member**-2020)
  - Technical Committee on Databases, CCF 中国计算机学会数据库专委会执行委员 (since 2016), by election
  - Technical Committee on Privacy Protection, China Confidentiality Association, CCA 中国保密协会隐私保护专委会 (since 2016), founding member
  - EC Member, ACM China Council SIGSPATIAL Chapter (since 2021).

- **Conference Organization**
  - Program Co-Chair: 6th EAI International Conference on Security and Privacy in New Computing Environments (EAI SPNCE 2023)
  - Program Co-Chair: ChinaPrivacy 2023 (第六届中国数据安全与隐私保护大会)
  - Local Chair: International Workshop on Advanced Image Technology 2022 (IWAIT 2022)
  - Tutorial Co-Chair: 28th ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems (SIGSPATIAL 2020)
  - Workshop Co-Chair: IEEE International Conference on Data Science in Cyberspace (ICDSC 2020)
  - Program Co-Chair: The 2019 International Workshop on Mobile Ubiquitous Systems and Technologies (MUST 2019)
  - Advanced Seminar Co-Chair: 20th IEEE International Conference on Mobile Data Management (MDM 2019)
  - Track Co-Chair: IEEE BigData Congress 2018 “Security and Privacy” Track
  - Program Co-Chair: 1st International Workshop on Next-Generation Location-Based Services (LBS n.0), in conjunction with IEEE MDM 2013
  - Program Co-Chair: 2nd International Workshop on Data Management for Emerging Network Infrastructures (DaMEN), in conjunction with APWeb 2013
  - Program Co-Chair: Third International Workshop on Cloud Data Management (CloudDB 2011),

in conjunction with ACM CIKM 2011

- Program Co-Chair: 1st International Workshop on Data Management for Emerging Network Infrastructures (DaMEN), in conjunction with DASFAA 2011
- Panel Co-Chair: 16th Database Systems for Advanced Applications (DASFAA'11)

- **Journal Editorship and Conference Program Committee Member**
  - Associate editor, IEEE Transactions on Knowledge and Data Engineering(TKDE), 2023-present.
  - Associate editor, IEEE Transactions on Information Forensics and Security (TIFS), 2023-present.
  - Associate editor, ACM Transactions on Privacy and Security (TOPS), 2022 - present.
  - Guest editor, ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM), 2023-2024.
  - Leading guest editor, ACM Transactions on Data Science (TDS), 2019-2020.
  - Review board member, International Conference on Very Large Data Bases (VLDB '24, '23, '18)
  - PC member, IEEE International Conference on Data Engineering (ICDE '23, '22, '21, '20, '18)
  - PC member, SIAM International Conference on Data Mining (SDM '22)
  - PC member, IEEE International Conference on Data Mining (ICDM '23, '22, '21)
  - PC member, 29th ACM International Conference on Information and Knowledge Management (CIKM '20).
  - PC member, Pacific-Asia Conference on Knowledge Discovery and Data Mining (PAKDD '22, '21,'20)
  - International Conference on Web Information Systems Engineering (WISE'20, '19)
  - PC member, 20th IEEE International Conference on Mobile Data Management (MDM '19).
  - Asia Pacific Web (APWeb) and Web-Age Information Management (WAIM) Joint Conference on Web and Big Data (APWeb-WAIM '22, '21, '20, '19, '18, '17, '16, '15, '06)
  - International Conference on Database Systems for Advanced Applications (DASFAA '22, '21, '16, '15, '14,'13, '12, '11, '10, '08, '07)
  - International Conference on Big Data Computing and Communication (BIGCom '17)
  - Mobile Geographic Information Systems (ACM MobiGIS '16, '14, '13, '12)
  - International Conference on Parallel and Distributed Systems (ICPADS'13, '12)
  - 8th International Conference on Broadband and Wireless Computing, Communication, and Applications (BWCCA '13)
  - Third International Conference on Social Informatics (SocInfo'11)
  - Ninth IEEE International Symposium on Parallel and Distributed Processing with Applications (ISPA'11)
  - 44th International Conference on Parallel Processing (ICPP '11)
  - 2008 International Conference on Communications in Computing (CIC'08)
  - International Conference on Wavelet Analysis and Pattern Recognition (ICWAPR'08)
  - 2nd International Conference on Scalable Information Systems (INFOSCALE'07)

- **Journal External Reviewer**
  - ACM Transactions on Database Systems (TODS)
  - IEEE Transactions on Knowledge and Data Engineering (TKDE)
  - IEEE Transactions on Information Forensics and Security (TIFS)
  - IEEE Transactions on Dependable and Secure Computing (TDSC)
  - IEEE Transactions on Parallel and Distributed Systems (TPDS)
  - IEEE Transactions on Mobile Computing (TMC)
  - IEEE Transactions on Service Computing (TSC)
  - The VLDB Journal
  - World Wide Web

- **Invited Keynotes/Talks**
  - “Extracting Large Machine Learning Models: Theory and Practice,” Invited talk in Future Generative AI Security & Application Summit, Singapore, Mar 2024.

- “Model Privacy and Security in Machine Learning at Scale,” Invited talk in ChinaPrivacy 2023.
- “Model Privacy and Security in Machine Learning at Scale,” Invited talk in EAI SPNCE 2023 - 6th EAI International Conference on Security and Privacy in New Computing Environments.
- Demystifying Extraction Attacks on Big Models. Invited talk and Panelist in “Socio-Technical Principles for Big Models: Privacy, Fairness, Interpretability and Beyond” track, Huawei Strategy and Technology Workshop, Sep 2022.
- How Safe is AI? Privacy and Security Challenges and Responses in Artificial Intelligence, Invited talk in Noah’s Ark Lab, Huawei, Feb 2022.
- Reliability of machine learning models: How safe is AI? Invited talk in Hong Kong Science Park, May 2021.
- “浅谈对抗机器学习与隐私保护的对立与统一”, Invited talk in 内地-香港前沿学科发展论坛, Oct 2020.
- "Local Differential Privacy: Tools, Challenges, and Opportunities." Tutorial at 20th International Conference on Web Information Systems Engineering (WISE 2019), Jan 2020.
- “Harnessing Knowledge but Not Privacy in Internet of Things and Artificial Intelligence”, **Keynote talk** in the 11th International Symposium on Cyberspace Safety and Security (CSS), December 2019, Guangzhou, China.
- “物联网和人工智能中的隐私保护”, Invited talk in the 4th China Conference on Data Security and Privacy (ChinaPrivacy), October 2019, Guilin, China.
- “Privacy and Security Challenges in Urban Mobility”, Invited talk in ACM SIGSPATIAL 2020 Pre-Workshop, June 2019.
- “Ensuring Privacy and Integrity against Untrusted Cloud for Internet of Things Applications”, Invited Talk in the 35th National Database Conference (NDBC), Oct 2018.
- “Integrity Assurance for Outsourced Databases in Cloud Computing Era,” Invited Talk in IEEE International Conference on Data Science in Cyberspace, June 2018.
- “Beware of Your Location Privacy and Integrity in Social Networks,” Hong Kong **RGC Public Lectures on Cyber Security**, May 7, 2017.
- “Who Moved My Cheese: Integrity Assurance Know-How in Web 3.0”, **Distinguished Young Lecturer Talk**, 17th International Conference on Web-Age Information Management, JiangXi, China, June 2016.
- “Eyebb: A Hassle-free Indoor Localization Infrastructure and Care System with Bluetooth Low Energy,” Hong Kong Science & Technology Parks Soft-landing Series “Invent a Better Tomorrow: Advanced Technology Networking Seminar”, Nov 4, 2014.
- “Enabling User Privacy and Integrity in Location-based Services,” SIGMA XI Presentation, General Motors R&D Center Auditorium, Apr. 4, 2014.

Industrial and Social Services

- Admission Panel Member for Incubation Programmes of the Hong Kong Science Technology Parks Corporation (HKSTP), 2022 – 2024.
- Principal Security Consultant, Working Dwell on DT (浙江华坤道威数据科技公司, top-100 Internet company in China), 2022 – 2023.

Administrative Services

- Scheme Leader, BEng(Hons)/BSc(Hons) Scheme in Information and Artificial Intelligence Engineering, 2023 - present
- Programme Leader, BSc (Hons) Degree in Information Security, 2020 - present.
- Panel Member, Project of Strategic Importance, Hong Kong Polytechnic University, 2021.
- Member, Faculty Board, 2019 - 2021.
- Member, Departmental Management Committee, 2018 - 2023.
- Member, Departmental Research Committee, 2019 - 2023.
- Member, Departmental Working Team on Publicity and Alumni, 2015 - 2023.
- Member, Departmental Project Management Team, 2016 - present.
- Manager, PolyU Capture-The-Flag Team, 2019 – present.

Externally-Funded Competitive Grants

- Right To Be Forgotten Made Easy: Machine Unlearning, Differential Privacy and Beyond (**PI**: RGC/GRF, 15224124, 2025-2027, HK$ 1,038,967)
- Local Tweaks for Privacy-Preserving Training in Machine Learning at Scale (**PI**: RGC/GRF, 15210023, 2024-2026, HK$ 1,228,619)
- Federated Graph Management and Querying: Subgraphs, Keywords, and Privacy (Co-PI: RGC/**YCRF**, C2003-23Y, 2024-2026, HK$ 4,854,870, PI: Dr. Huang Xin)
- 基础模型窃取测评及防御关键技术(**PI**: Huawei Collaborative Research, 2023-2025, HK$ 2,440,000)
- Evasive Federated Learning Attacks through Differential Privacy: Mechanisms and Mitigations (**PI**: RGC/GRF, 15209922, 2023-2025, HK$941,434)
- Mutual Security Analysis of Machine Learning Models on Untrusted Data Sources 数据源和机器学习模型双向安全策略研究 (**PI**: National Natural Science Foundation of China 国家自然科学基金**重大研究计划**培育项目负责人, 92270123, 2023-2025, CNY 800,000)
- User-Controlled Secure Data Sharing and Analytics with Blockchain and Trusted Computing Technologies (Co-PI: RGC/**CRF**, C2004-21GF, 2022-2025, HK$ 6,734,880, PI: Prof. Xu Jianliang)
- Sword of Two Edges: Adversarial Machine Learning from Privacy-Aware Users (**PI**: RGC/GRF, 15226221, 2022-2024, HK$838,393)
- Securing Models and Data for Machine Learning at the Edge (**PI**: RGC/GRF, 15203120, 2021-2023, HK$845,055)
- Integrity Assurance and Fraud Detection for Machine Learning as a Service 机器学习即服务中的防欺诈和完整性验证研究 (**PI**: National Natural Science Foundation of China 国家自然科学基金面上项目负责人, 62072390, 2021-2024, CNY 570,000)
- Mechanism on Model Privacy Protection (**PI**: Huawei Collaborative Research, 2020-2022, HK$ 2,304,600)
- Centre for Advances in Reliability and Safety (Co-PI/Project Leader, ITF-InnoHK, 2020-2025)

- vMPOS: Virtual Mobile POS using Smartphone and Near Field Communication (**PI**: ITF-PRP, PRP/051/19FX, 2020-2023, HK$ 3,927,250)
- Auditing Machine Learning as a Service (**PI**: RGC/GRF, 15218919, 2020-2022, HK$ 731,089)
- Integrity Assurance for Vehicular Telematics Data (**PI**: RGC/GRF, 15222118, 2019-2021, HK$ 693,000)
- AI Model Protection from Inversion Attacks (**PI**: Huawei Contract Research, 2019-2020, HK$ 764,520)
- Privacy-Preserving Mobile User Behavior Statistics Collection (**PI**: Huawei Innovation Research Program, 2017-2018, HK$ 232,656)
- Security and Privacy-enhancing Technologies for Cloud Storage of Big Data (Co-PI: RGC/**CRF**, C1008-16G, 2017-2020, HK$ 5,983,404, PI: Prof. Jia Xiaohua)
- Privacy Preservation Techniques for Query Processing in Big Data 大数据查询处理的隐私保护技术 (Co-PI: Joint Funds of National Natural Science Foundation of China (**Key Program**) 国家自然科学基金联合基金**重点支持项目**合作单位负责人, U1636205, 2017-2020 **CNY 2,520,000**, PI: Prof. Zhou Shuigeng)
- Protecting Metadata Privacy for Mobile Crowdsensing Using Oblivious RAM (**PI**: RGC/GRF, 15238116, 2017-2020, HK$ 482,605)
- Mutual Privacy Protection on Private Queries over Large-Scale Private Data 海量数据查询中的双向隐私保护机制研究 (**PI**: National Natural Science Foundation of China 国家自然科学基金面上项目**负责人**, 61572413, 2016-2019, CNY 630,000)
- Incognito Browsing of Spatial-Temporal Data Using Computational Private Information Retrieval (**PI**: RGC/GRF, 12200914, 2015-2018, HK$ 692,894)
- Hybrid Geofencing Systems for Elderly and Child Care (**PI**: ITF/ITSP Tier 2, ITS/231/13FX, 2014-2016, **HK$2,378,200**)
- Authenticated Queries for Cloud-Assisted Multi-Source Data Collection (Co-I: RGC/GRF, 12202414, 2014-2017, PI: Prof. Xu Jianliang)
- Spatio-Temporal Attestation for Location-based Services Using Private Signatures (**PI**: RGC/GRF, HKBU 210612, 2012-2016, HK$ 690,000)
- iGPS: Privacy-Preserving Geo-Proximity Services in Location-based Social Networks (Co-I: RGC/GRF, HKBU 211512, 2012-2015, HK$ 700,000, PI: Prof. Xu Jianliang)
- Privacy-Conscious Query Authentication for Outsourced and Cloud Databases (**PI**: RGC/GRF, HKBU 210811, 2011-2014, HK$ 792,500)
- Semantic Location Modeling, Distance Browsing and Query Processing for Mobile Indoor Applications (Co-I: RGC/CERG HKUST6158/06E, 2006-2008, HK$ 688,000, PI: Prof. Dik Lun Lee)

External Consultancy Projects

- Penetration Test of Wireless Services for Pilot Multi-functional Smart Lampposts Scheme (Co-I, Office of The Government Chief Information Officer/Government of HKSAR, 2019, HK$ 270,000, PI: Prof. Francis Lau)
- Evaluation of Connectivity and Data Security of Different Telecommunication Technologies for a Public Lighting Remote Control and Monitoring System (Co-I, Highways Department/Government of HKSAR, 2018-2019, HK$1,170,000, PI: Prof. Francis Lau).

Awards/Honors

- Outstanding Researcher, Faculty Awards for Outstanding Achievement 2022, The Hong Kong Polytechnic University.
- Best Paper Award, International Workshop on Advanced Imaging Technology (IWAIT) 2021.
- Outstanding Reviewer Award, IEEE 36th International Conference on Data Engineering (ICDE), 2020.
- Research Grant Achievement Award, Faculty of Engineering, The Hong Kong Polytechnic University, 2020.
- Best Paper Award, 20th IEEE International Conference on Mobile Data Management (MDM' 2019).
- Best Theory Paper Award, FML'19, in conjunction with IJCAI'19.
- Research Grant Achievement Award, Faculty of Engineering, The Hong Kong Polytechnic University, 2018.
- Distinguished Reviewer Award, Very Large Data Bases (VLDB), 2018.
- Research Grant Achievement Award, Faculty of Engineering, The Hong Kong Polytechnic University, 2016.
- Distinguished Young Lecturer, 17th International Conference on Web-Age Information Management, 2016.
- 国家级科技项目奖先进个人，深圳市科技创新委员会，2015.
- Media Interview by Oriental Daily, a major Chinese newspaper in Hong Kong, Title: "幼童監察 App 追蹤位置防走失", October 5th, 2015.
- Bronze Award, Hong Kong U-21 Internet of Things Awards 2014, Capacity: Supervisor, Project Title: Intelligent Behaviour and Safety Tracker for Kids
- Best PhD Paper Award of the 6th ACM Postgraduate Research Day, 2005
- Team Leader of the Fourth Runner-up Winner of Microsoft Imagine Cup 2004, Hong Kong
  Project name: *i-surroud:* A Location-Aware Messenger Service
- Team Leader of the First Runner-up Winner of IBM Websphere National University Student Competition, 2000
- IBM Excellent University Student Award, 2000 (only 80 students nationwide were awarded)
- Exceptional Student Scholarship (for top 1% students), Shanghai Jiao Tong University, 1998 – 2001, 4 years in a row

Graduate Students

- Zi Liang (PhD), Principle Supervisor, "Fast Private Inference for Large Language Models", Dec 2026 (expected), The Hong Kong Polytechnic University.
- Xinwei Zhang (PhD), Principle Supervisor, "Safeguarding for On-device Machine Learning Systems", Aug 2026 (expected), The Hong Kong Polytechnic University.
- Liantong Yu (PhD), Co-Supervisor, "Towards Efficient OLAP Operations with Local Differential Privacy", Dec 2027 (expected), The Hong Kong Polytechnic University.
- Shiyu Zhang (PhD), Co-Supervisor, "CatIR: Category-Guided Candidate Item Retrieval for Multi-Interest Recommendation", Dec 2027 (expected), The Hong Kong Polytechnic University.

- Xinhao Yan (PhD), Co-Supervisor, "Secure Estimation for Unmanned Aerial Vehicles with Fast Encryption Approaches", Dec 2026 (expected), The Hong Kong Polytechnic University.
- Li Bai (PhD), Principle Supervisor, "Rethinking Recommendation Diversity on Fairness and Privacy Aspect", Aug 2025 (expected), The Hong Kong Polytechnic University.
- Haoyang Li (PhD), Principle Supervisor, "Model-based Poisoning Attack and Defense Schemes on Federated Learning", Aug 2026 (expected), The Hong Kong Polytechnic University.
- Yuemin Zhang (PhD), Co-Supervisor, "Trajectory Data Collection with Local Differential Privacy", Aug 2026 (expected), The Hong Kong Polytechnic University.
- Ronghua Li (PhD), Principle Supervisor, "Autonomous Penetration Testing Framework for Bluetooth Low Energy", Aug 2025 (expected), The Hong Kong Polytechnic University.
- Xun Ran (PhD), Co-Supervisor, " Differentially Private One-Class Collaborative Filtering for Recommender Systems", Dec 2025 (expected), The Hong Kong Polytechnic University.
- Yulian Mao (PhD), Principle Supervisor, "Local Differential Privacy in Artificial Intelligence of Things: Theory and Applications", Aug 2025 (expected), The Hong Kong Polytechnic University.
- Duan Jiawei (PhD), Principle Supervisor, "Privacy-Preserving Data Visualization and Exploration Techniques", August 2024 (expected), The Hong Kong Polytechnic University
- Yaxin Xiao (PhD, **HKPFS**), Principle Supervisor, "Machine Learning for Edge Computing", June 2024 (expected), The Hong Kong Polytechnic University.
- Chun Ho Kong (MPhil), Principle Supervisor, "Attacking IoT Wireless Protocols with Preamble Extraction and SDR." Aug 2024 (expected), The Hong Kong Polytechnic University.
- Rong Du (PhD), Principle Supervisor, "High Performance Hash-encoding in Local Differential Privacy Mechanisms", June 2024 (expected), The Hong Kong Polytechnic University.
- Yue Fu (PhD), Principle Supervisor, "By-product Computing of Useful Work in Blockchain Consensus", June 2024 (expected), The Hong Kong Polytechnic University.
- Haotian Yan (PhD), Principle Supervisor, "An Multiple Target on Message Authentication Code for the Data Integrity Problem in MLaaS", June 2024 (expected), The Hong Kong Polytechnic University.
- Li Tang (PhD), Principle Supervisor, thesis "Secure authentication and aggregation in large-scale data-driven systems", Dec 2023, The Hong Kong Polytechnic University.
- Ziyang Han (PhD), Principle Supervisor, "Access Pattern Hiding Based on Oblivious RAM in Crowd Data Exchange", Aug 2022, The Hong Kong Polytechnic University.
- Huadi Zheng (PhD), Principle Supervisor, "Handling Privacy-preserving Issues over Spatio-Temporal Information", Aug 2021, The Hong Kong Polytechnic University.
- Zhuo Chen (MPhil), Principle Supervisor, thesis "Towards Practical Location Systems with Privacy Protection." Sept 2015, Hong Kong Baptist University.
- Qian Chen (PhD), Co-Supervisor, thesis "Query authentication in data outsourcing and integration services." June 2015, Hong Kong Baptist University.

Last update: July 1, 2024