PERSONAL INFORMATION

Name: Guowen Xu (IEEE/CCF Senior Member)

Date of Birth： June 5,1991

E-Mail: guowen.xu@uestc.edu.cn

Homepage: https://guowen-xu.github.io/

Address: University of Electronic Science and Technology of China, P.R. China

EDUCATION BACKGROUND

- Ph.D. of Cyberspace Security **2015/09-2020/12**
  (Supervisor: Prof. **Hongwei Li: IEEE Fellow**)
  School of Computer Science and Engineering
  University of Electronic Science and Technology of China (UESTC)
- Visiting Ph.D. in Cyberspace Security **2019/08-2020/08**
  (Supervisor: Prof**. Robert H. Deng: IEEE Fellow)**
  School of Information of Systems
  Singapore Management University
- Bachelor of Information and Computing Science **2010/09-2014/06**
  School of Mathematical and Physical Science
  Anhui Jianzhu University (AHJZU)

PROFESSIONAL EXPERIENCE

- Research Fellow **2021/03-2023/05**
  School of Computer Science and Engineering
  Nanyang Technological University, Singapore
- Research Fellow **2023/05-2024/08**
  Department of Computer Science
  City University of Hong Kong
- Professor **2024/08-present**
  School of Computer Science and Engineering
  University of Electronic Science and Technology of China

RESEARCH INTERESTS

AI Security and Privacy, Data Security

AWARDS AND HONORS

- 2025 IEEE Signal Processing Society Best Paper Award, IEEE Signal Processing Society
- 2025 R10 Young Professionals Outstanding Volunteer in Academic Award, IEEE Region 10 Young Professionals
- 2025 IEEE TCHS Young Researcher Award, IEEE Systems, Man, and Cybernetics Society
- 2024 Computing’s Top 30 Early Career Professionals, IEEE Computer Society
- 2024 IEEE Early Career Speaker, IEEE Computer Society
- 2024 Outstanding Youth Editor Award, Cybersecurity journal (Springer)
- 2023 IEEE BigDataSecurity Best Paper Award
- 2022-2024 Distinguished Reviewer of ACM Transactions on the Web
- 2022 Huawei Genius Young Talent Program, Huawei.
- 2021 Wu Wenjun First Prize of Artificial Intelligence Science and Technology Progress
- 2020 IEEE ICPADS Best Paper Award

SELECTED PUBLICATIONS (CCF A papers: 68; Google Citations**:** 6132; **2026/01/06)**

[1] [**USENIX Security 2026**] Jiayimei Wang, Tao Ni, **Guowen Xu**, Qingchuan Zha7o, Cong Wang. Adversarial Patch EXterminator: Zero-Shot and Patch-Agnostic Defense Framework Against Adversarial Patch Attacks[C]. *The 35th USENIX Security Symposium*, 2026 (**CCF A**)

[2] [**AAAI 2026**] Xinyuan Qian, Haoyong wang, Hangcheng Cao, Shuai Yuan, Senkang Hu, Qingchuan Zhao, Hongwei Li, **Guowen Xu*(Corresponding Author)**. MartDE: A Privacy-Preserving and Cost-Efficient Evaluation Framework for Data Marketplaces[C]. *The Fortieth AAAI Conference on Artificial Intelligence*, 2025. (**CCF A**)

[3] [**AAAI 2026**] Zihan Wang, Rui Zhang, Yu Liu, Wenshu Fan, Wenbo Jiang, Qingchuan Zhao, Hongwei Li, **Guowen Xu*(Corresponding Author)**. MPMA: Preference Manipulation Attack Against Model Context Protocol[C]. *The Fortieth AAAI Conference on Artificial Intelligence*, 2025. (**CCF A, Oral**)

[4] [**AAAI 2026**] Zihan Wang, Rui Zhang, Hongwei Li, Wenshu Fan, Wenbo Jiang, Qingchuan Zhao, **Guowen Xu*(Corresponding Author)**. ConfGuard: A Simple and Effective Backdoor Detection for Large Language M odels[C]. *The Fortieth AAAI Conference on Artificial Intelligence*, 2025. (**CCF A**)

[5] [**AAAI 2026**] Haonan An, Guang Hua, Hangcheng Cao, Zhengru Fang, **Guowen Xu**, Susanto Rahardja, Yuguang Fang. Removing Box-Free Watermarks for Image-to-Image Models via Query-Based Reverse Engineering[C]. *The Fortieth AAAI Conference on Artificial Intelligence*, 2025. (**CCF A**)

[6] **[TMC 2026]** Senkang Hu, Yihang Tao, Guowen Xu, Xinyuan Qian, Yiqin Deng, Xianhao Chen, Sam Tak Wu Kwong, Yuguang Fang. CP-uniGuard: A Unified, Probability-Agnostic, and Adaptive Framework for Malicious Agent Detection and Defense in Multi-Agent Embodied Perception Systems[J]. *IEEE Transactions on Mobile Computing*, 2026. (**CCF A**)

[7] **[TDSC 2026]** Haonan An，Guang Hua, Wei Du, Hangcheng Cao, Yihang Tao, Guowen Xu, Susanto Rahardja, Yuguang Fang. [J]. *IEEE Transactions on Dependable and Secure Computing*, 2026. (**CCF A**)

[8] [**TDSC 2025**] **Guowen Xu**, Shengmin Xu, Jianting Ning, Xinyi Huang, Hongwei Li, Rongxing Lu. New Secure Sparse Inner Product with Applications to Machine Learning[J]. *IEEE Transactions on Dependable and Secure Computing*, 2025. (**CCF A**)

[9] [**TDSC 2025**] Jianfei Sun, **Guowen Xu*(Corresponding Author)**, Hongwei Li, Tianwei Zhang, Cong Wu, Xuehuan Yang, Robert H. Deng. Sanitizable Cross-domain Access Control with Policy-driven Dynamic Authorization[J]. *IEEE Transactions on Dependable and Secure Computing*, 2025. (**CCF A**)

[10] [**TDSC 2025**] Jianfei Sun, **Guowen Xu*(Corresponding Author)**, Yang Yang, Xuehuan Yang, Cong Wu, Zhen Liu, Guomin Yang, Robert H. Deng. Forward-Secure Hierarchical Delegable Signature for Smart Homes[J]. *IEEE Transactions on Information Forensics and Security*, 2025. (**CCF A**)

[11] **[NeurIPS 2025]** Shuai Yuan, Xingshuo Han, Hongwei Li, **Guowen Xu*(Corresponding Author)**, Wenbo Jiang, Tao Ni, Qingchuan Zhao, Yuguang Fang. The Fluorescent Veil: A Stealthy and Effective Physical Adversarial Patch Against Traffic Sign Recognition[C]. *The Thirty-Ninth Annual Conference on Neural Information Processing Systems*, 2025. (**CCF A**)

[12] [**ICML 2025**] Rui Zhang, Yun Shen, Hongwei Li, Wenbo Jiang, Hanxiao Chen, Yuan Zhang, **Guowen Xu*(Corresponding Author)**, Yang Zhang. The Ripple Effect: On Unforeseen Complications of Backdoor Attacks[C]. *International Conference on Machine Learning*, 2025. (**CCF A**)

[13] [**ICML 2025**] Shuai Yuan, Hongwei Li, Rui Zhang, Hangcheng Cao, Wenbo Jiang, Tao Ni, Wenshu Fan, Qingchuan Zhao, **Guowen Xu*(Corresponding Author)**. Omni-Angle Assault: An Invisible and Powerful Physical Adversarial Attack on Face Recognition [C]. *International Conference on Machine Learning*, 2025. (**CCF A**)

[14] [**TDSC 2025**] Xiaoyuan Liu, Hongwei Li, **Guowen Xu*(Corresponding Author)**, Shengmin Xu, Xinyi Huang, Tianwei Zhang, Yijing Lin, Jianying Zhou. Antelope: Fast and Secure Neural Network Inference[J]. *IEEE Transactions on Dependable and Secure Computing*, 2025. (**CCF A**)

[15] [**TDSC 2025]** Shuai Yuan, **Guowen Xu*(Corresponding Author)**, Hongwei Li, Rui Zhang, Hangcheng Cao, Xinyuan Qian, Tao Ni, Qingchuan Zhao, Yuguang Fang. No Trespassing: Ground-view Adversarial Patches for Privacy-aware Management in COTS Robot Vacuum Cleaner[J]. *IEEE Transactions on Dependable and Secure Computing (TDSC)*, 2025. (**CCF A**)

[16] [**ASIACCS 2025**] Hangcheng Cao, **Guowen Xu*(Corresponding Author)**, Wenbing Huang, Hongwei Li. Can Small-scale Evaluation Reflect Real Ability? A Performance Study of Emerging Biometric Authentication[C]. in *Proceedings of ACM ASIACCS*, Ha Noi, Vietnam, 2025.

[17] [**ACSAC 2025**] Yuan Zhang, Yali Wang, **Guowen Xu*(Corresponding Author)**, Yaqing Song, Hongwei Li. Belt and Braces! Fight against Key Compromising in Single Sign-On Systems [C]. in *Proceedings of Annual Computer Security Applications Conference (ACSAC)*, Honolulu, Hawaii, USA, 2025. (**CCF B**)

[18] **[TDSC 2025]** Wenbo Jiang, Hongwei Li, Jiaming He, Rui Zhang, **Guowen Xu**, Tianwei Zhang, Rongxing Lu. I2I Backdoor: Backdoor Attacks against Image-to-Image Tasks[J]. *IEEE Transactions on Dependable and Secure Computing (TDSC)*, 2025. (**CCF A**)

[19] **[TDSC 2025]** Jiayin Li, Shengmin Xu, Xingshuo Han, Jianting Ning, Xinlei He, **Guowen Xu.** Verifiable and Lightweight Multi-Round Secure Federated Learning[J]. *IEEE Transactions on Dependable and Secure Computing (TDSC)*, 2025. (**CCF A**)

[20] **[TIFS 2025]** Hangcheng Cao, **Guowen Xu**, Ziyang He, Xuan Zhang, Shengmin Xu, Xinyuan Qian, Anjia Yang, Jianting Ning. The Lives of Others: Snooping on Smartphone Usage Behaviors via Attention-enabled Multi-channel Spatiotemporal Information Fusion[J]. *IEEE Transactions on Information Forensics and Security (TIFS)*, 2025. (**CCF A**)

[21] **[TIFS 2025]** Hanxiao Chen, Hongwei Li, Meng Hao, Pengzhi Xing, Jia Hu, Wenbo Jiang, Tianwei Zhang, **Guowen Xu**. Conan: Secure and Reliable Machine Learning Inference against Malicious Service Providers[J]. *IEEE Transactions on Information Forensics and Security (TIFS)*, 2025. (**CCF A**)

[22] **[TIFS 2025**] Cong Wu, Hangcheng Cao, Jing Chen, **Guowen Xu**, Ziming Zhao, Yang Liu, Hongbo Jiang. RUGSCREENER: Leveraging Temporal Graph Neural Network for Rugpull Detection in DeFi[J]. *IEEE Transactions on Information Forensics and Security*, 2025. (**CCF A**)

[23] **[TMC 2025]** Yongzhao Zhang, Yuqiao Yang, Zhiwei Chen, Zhongjie Wu, Ting Chen, Jun Li, Jie Yang, Guowen Xu, Wenhao Liu, Xiaosong Zhang, Jingwei Li, Yu Jiang, Zhou Su. A Practical Dos Attack on Commercial UWB Ranging Systems[J]. *IEEE Transactions on Mobile Computing*, 2025. (**CCF A**)

[24] **[TMC 2025]** Ming Li, Jian Weng, Jiasi Weng, Yi Li, Yongdong Wu, Dingcheng Li, **Guowen Xu**, Robert H. Deng. IvyCross: A Privacy-Preserving and Concurrency Control Framework for Blockchain Interoperability[J]. *IEEE Transactions on Mobile Computing*, 2025. (**CCF A**)

[25] **[CVPR 2025]** Haonan An, Guang Hua, Zhengru Fang, **Guowen Xu**, Susanto Rahardja, Yuguang Fang. Decoder Gradient Shield: Provable and High-Fidelity Prevention of Gradient-Based Box-Free Watermark Removal [J]. *IEEE / CVF Computer Vision and Pattern Recognition Conference*, 2025. (**CCF A**)

[26] **[TIFS 2025]** Hangcheng Cao, **Guowen Xu,** Ziyang He, Shaoqing Shi, Shengmin Xu, Cong Wu, Jianting Ning. Unveiling the Superiority of Unsupervised Learning on GPU Cryptojacking Detection: Practice on Magnetic Side Channel-based Mechanism[J]. *IEEE Transactions on Information Forensics and Security*, 2025. (**CCF A**)

[27] **[AAAI 2025]** Senkang Hu, Yihang Tao, **Guowen Xu**, Yiqin Deng, Xianhao Chen, Yuguang Fang, Sam Kwong. CP-Guard: Malicious Agent Detection and Defense in Collaborative Bird's Eye View Perception[C]. *Thirty-Ninth AAAI Conference on Artificial Intelligence*, 2025. (**Oral**, **CCF A**)

[28] **[AAAI 2025]** Yang Wei, Jingyu Tan, **Guowen Xu**, Zhuoran Ma, Zhuo Ma, Bin Xiao. Power of Diversity: Enhancing Data-Free Black-Box Attack with Domain-Augmented Learning[C]. *Thirty-Ninth AAAI Conference on Artificial Intelligence,* 2025. (**CCF A**)

[29] **[CCS 2024]** Cong Wu, Jing Chen, Ziming Zhao, Kun He, **Guowen Xu**, Yueming Wu, Haijun Wang, Honggwei Li, Yang Liu, Yang Xiang. TokenScout: Early Detection of Ethereum Scam Tokens via Temporal Graph Learning[C]. in *Proceedings of ACM Conference on Computer and Communications Security*, 2024. (**CCF A**)

[30] **[S&P 2024]** Xingshuo Han, Yutong Wu, Qingjie Zhang, Yuan Zhou, Yuan Xu, Han Qiu, **Guowen Xu**, and Tianwei Zhang. Backdooring Multimodal Learning[C]. in *IEEE Symposium on Security and Privacy*, 2024. (**CCF A**)

[31] **[TDSC 2024]** Wenbo Jiang, Hongwei Li, **Guowen Xu**, Hao Ren, Haomiao Yang, Tianwei Zhang. Rethinking the Design of Backdoor Triggers and Adversarial Perturbations: A Color Space Perspective[J]. *IEEE Transactions on Dependable and Secure Computing*, 2024. (**CCF A**)

[32] **[TDSC 2024]** Hao Ren, **Guowen Xu*(Corresponding Author)**, Tianwei Zhang, Jianting Ning, Xinyi Huang, Honggwei Li, Rongxing Lu. Efficiency Boosting of Secure Cross-platform Recommender Systems over Sparse Data. *IEEE Transactions on Dependable and Secure Computing*, 2024. (**CCF A**)

[33] **[TIFS 2024]** Wenfeng Huang, Axin Wu, Shengmin Xu, **Guowen Xu**, Wei Wu. EASNs: Efficient Anonymous Social Networks with Enhanced Security and High Scalability [J]. *IEEE Transactions on Information Forensics and Security*, 2024. (**CCF A**)

[34] **[INFOCOM 2024]** Xinyuan Qian, Hongwei Li, **Guowen Xu**, Haoyong Wang, Tianwei Zhang, Xianhao Chen, Yuguang Fang. Privacy-Preserving Data Evaluation via Functional Encryption, Revisited [C]. in *Proceedings of IEEE International Conference on Computer Communications*, 2024. (**CCF A**)

[35] **[TIFS 2024]** Cong Wu, Jing Chen, Kun He, Ziming Zhao, Qianru Fang, Hao Ren, **Guowen Xu**, Yang Liu, Yang Xiang. Rethinking Membership Inference Attacks Against Transfer Learning[J]. *IEEE Transactions on Information Forensics and Security*, 2024. (**CCF A**)

[36] **[TIFS 2024]** Xiaoyuan Liu, Hongwei Li, **Guowen Xu**, Xilin Zhang, Tianwei Zhang, JIanying Zhou. Secure and Lightweight Feature Selection for Horizontal Federated Learning [J]. *IEEE Transactions on Information Forensics and Security*, 2024. (**CCF A**)

[37] **[TIFS 2024]** Hanxiao Chen, Hongwei Li, Meng Hao, Jia Hu, **Guowen Xu**, Xilin Zhang, Tianwei Zhang.SecBNN, Efficient Secure Inference on Binary Neural Network. *IEEE Transactions on Information Forensics and Security*, 2024. (**CCF A**)

[38] **[TMC 2024]** Cong Wu, Hangcheng Cao, **Guowen Xu**, et al. It's All in the Touch: Authenticating Users with HOST Gestures on Multi-Touch Screen Devices [J]. *IEEE Transactions on Mobile Computing*, 2024. (**CCF A**)

[39] [**TIFS 2024**] Zhirui Zeng, Tao Xiang, Shangwei Guo, Jialing He, Qiao Zhang, **Guowen Xu**, Tianwei Zhang. Contrast-then-Approximate: Analyzing Keyword Leakage of Generative Language Models[J]. *IEEE Transactions on Information Forensics and Security*, 2024. **(CCF A)**

[40] [**TDSC 2024**] Xinyuan Qian, Hongwei Li, Meng Hao, **Guowen Xu**, Haoyong Wang, Yuguang Fang. Decentralized Multi-Client Functional Encryption for Inner Product with Applications to Federated Learning [J]. *IEEE Transactions on Dependable and Secure Computing*, 2024. **(CCF A)**

[41] [**TDSC 2024**] Haomiao Yang, Dongyun Xue, Mengyyu Ge, Jingwei Li, **Guowen Xu**, Hongwei Li, Rongxing Lu. Fast Generation-Based Gradient Leakage Attacks: An Approach to Generate Training Data Directly from The Gradient [J]. *IEEE Transactions on Dependable and Secure Computing*, 2024. **(CCF A)**

[42] [**TSC 2024**] Shuai Yuan, Hongwei Li, Xinyuan Qian, Meng Hao, Yixiao Zhai, **Guowen Xu**. Efficient and Privacy-preserving Outsourcing of Gradient Boosting Decision Tree Inference [J]. *IEEE Transactions on Services Computing*, 2024. **(CCF A)**

[43] [**DSN 2024**] Xiaoxuan Lou, Kangjie Chen, **Guowen Xu*(Corresponding Author)**, Han Qiu, Shangwei Guo, Tianwei Zhang. Protecting Confidential Virtual Machines from Hardware Performance Counter Side Channels[C]. *The 54th Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, 2024. (**CCF B**)

[44] [**EuroS&P 2024**] Guanlin Li, **Guowen Xu*（Corresponding Author）**, Han Qiu, Shangwei Guo, Run Wang, Jiwei Li, Tianwei Zhang, Rongxing Lu. Fingerprinting Image-to-Image Generative Adversarial Networks[C]. *IEEE European Symposium on Security and Privacy*, 2024.

[45] [**ICRA 2024**] Yuang Zhang, Haonan An, Zhengru Fang, **Guowen Xu,** Yuan Zhou, Xianhao Chen, Yuguang Fang. SmartCooper: Vehicle Collaborative Perception under Adaptive Fusion and Judger Mechanism[C]. *IEEE International Conference on Robotics and Automation*, 2024. (**CCF B**)

[46] [**ICDCS 2024**] Xinyuan Qian, Hongwei Li, Haoyong Wang, **Guowen Xu**, Shengmin Xu, Ju Ren. SecSCS: A User-Centric Secure Smart Camera System Based on Blockchain [C]. *The 44th IEEE International Conference on Distributed Computing Systems*, 2024. (**CCF B**)

[47] [**TDSC 2023**] **Guowen Xu**, Xingshuo Han, Tianwei Zhang, Shengmin Xu, Jianting Ning, Xinyi Huang, Hongwei Li, Robert H.Deng. SIMC 2.0: Improved Secure ML Inference Against Malicious Clients [J]. *IEEE Transactions on Dependable and Secure Computing*, 2023. (**CCF A**)

[48] [**TDSC 2023**] **Guowen Xu**, Xingshuo Han, Gelei Deng, Tianwei Zhang, Shengmin Xu, Jianting Ning, Anjia Yang, Hongwei Li. VerifyML: Obliviously Checking Model Fairness Resilient to Malicious Model Holder [J]. *IEEE Transactions on Dependable and Secure Computing*, 2023. (**CCF A**)

[49] [**TIFS 2023**] **Guowen Xu**, Shengmin Xu, Jinhua Ma, Jianting Ning, and Xinyi Huang. An Adaptively Secure and Efficient Data Sharing System for Dynamic User Groups in Cloud [J]. *IEEE Transactions on Information Forensics and Security,* 2023. (**CCF A**)

[50] [**TIFS 2023**] Jianfei Sun, **Guowen Xu*(Corresponding Author)**, Tianwei Zhang, Xuehuan Yang, Mamoun Alazab, Robert H. Deng. Privacy-aware and Security-enhanced Efficient Matchmaking Encryption [J]. *IEEE Transactions on Information Forensics and Security*, 2023, to appear. (**CCF A**)

[51] [**TKDE 2023**] Zhuoran Ma, Jianfeng Ma, Yinbin Miao, **Guowen Xu**, Yang Liu, Ximeng Liu, Robert H. Deng. FLGAN: GAN-Based Unbiased Federated Learning under Non-IID Settings[J]. *IEEE Transactions on Knowledge and Data Engineering*, 2023. (**CCF A**)

[52] **[ICML 2023]** Haoxiao Chen, Hongwei Li, Meng Hao, Kangjie Chen, **Guowen Xu**, Tianwei Zhang, Xilin Zhang [C]. GuardHFL: Privacy Guardian for Heterogeneous Federated Learning. in *International Conference on Machine Learning*, 2023. (**CCF A**)

[53] **[ICLR 2023]** Guanlin Li, **Guowen Xu***(**Corresponding Author)**, Shangwei Guo, Han Qiu, Jiwei Li, Tianwei Zhang. Extracting Robust Models with Uncertain Examples[C]. in *International Conference on Learning Representations.* 2023.

[54] **[ICLR 2023]** Kangjie Chen, Xiaoxuan Lou, **Guowen Xu**, Jiwei Li, Tianwei Zhang. Clean-image Backdoor: Attacking Multi-label Models with Poisoned Labels Only[C]. in *International Conference on Learning Representations,* 2023. (**Notable-top-5%**)

[55] [**TDSC 2023**] Wenbo Jiang, Hongwei Li, **Guowen Xu**, Tianwei Zhang, Rongxing Lu. A Comprehensive Defense Framework against Model Extraction Attacks [J]. *IEEE Transactions on Dependable and Secure Computing*, 2023. (**CCF A**)

[56] [**CVPR 2023**] Wenbo Jiang, Hongwei Li, **Guowen Xu**, Tianwei Zhang. Color Backdoor: A Robust Poisoning Attack in Color Space [C]. in *Proceedings of IEEE / CVF Computer Vision and Pattern Recognition Conference*, 2023. (**CCF A**)

[57] [**INFOCOM 2023**] Dongyun Xue, Haomiao Yang, Mengyu Ge, Jingwei Li, **Guowen Xu**, Hongwei Li. Fast Generation-Based Gradient Leakage Attacks against Highly Compressed Gradients [C]. in *Proceedings of IEEE International Conference on Computer Communications*, 2023. (**CCF A**)

[58] **[TSC 2023]** Shengmin Xu, Xingshuo Han, **Guowen Xu**, Jianting Ning, Xinyi Huang, Robert H. Deng. An Adaptive Secure and Practical Data Sharing System with Verifiable Outsourced Decryption [J]. *IEEE Transactions on Services Computing*, 2023, to appear. **(CCF A)**

[59] **[TCSVT 2023]** **Guowen Xu**, Guanlin Li, Shangwei Guo, Tianwei Zhang, Hongwei Li. Secure Decentralized Image Classification with Multiparty Homomorphic Encryption[J]. *IEEE Transactions on Circuits and Systems for Video Technology*, 2023. (**CCF B**)

[60] **[CCS 2022]** Gelei Deng, **Guowen Xu***(**Corresponding Author**), Yuan Zhou, Tianwei Zhang, Yang Liu. On the (In) Security of Secure ROS2[C]. in *Proceedings of ACM Conference on Computer and Communications Security*, 2022. **(CCF A)**

[61] [**TDSC 2022**] **Guowen Xu**, Xingshuo Han, Shengmin Xu, Tianwei Zhang, Hongwei Li, Xinyi Huang, Robert H Deng. Hercules: Boosting the Performance of Privacy-preserving Federated Learning[J], *IEEE Transactions on Dependable and Secure Computing*, 2022. **(CCF A)**

[62] [**TIFS 2022**] Jianfei Sun, **Guowen Xu***(**Corresponding Author)**, Xuehuan Yang, Tianwei Zhang, Mamoun Alazab, Robert H. Deng. Verifiable, Fair and Privacy-preserving Broadcast Authorization for Flexible Data Sharing in Clouds [J]. *IEEE Transactions on Information Forensics and Security*. 2022. (**CCF A**)

[63] [**TIFS 2022**] Jianfei Sun, **Guowen Xu***(**Corresponding Author**), Tianwei Zhang, Mamoun Alazab, Robert H. Deng. A Practical Fog-based Privacy-preserving Online Car-hailing Service System [J]. *IEEE Transactions on Information Forensics and Security*, 2022. **(CCF A)**

[64] [**ECCV 2022**] Guanlin Li, **Guowen Xu***(**Corresponding Author**), Han Qiu, Ruan He, Jiwei Li, Tianwei Zhang. Improving Adversarial Robustness of 3D Point Cloud Classification Models[C]. in *Proceedings of European Conference on Computer Vision*. 2022. **(CCF B)**

[65] [**TITS 2022**] Jianfei Sun, **Guowen Xu*** (**Corresponding Author**) Tianwei Zhang, Xiaochun Cheng, Xingshuo Han, MingJian Tang. Secure Data Sharing with Flexible Cross-domain Authorization in Autonomous Vehicle Systems[J]. *IEEE Transactions on Intelligent Transportation Systems*, 2022. **(CCF B)**

[66] **[TIFS 2022]** Hanxiao Chen, Hongwei Li, Yingzhe Wang, Meng Hao, **Guowen Xu**, Tianwei Zhang. PriVDT: An Efficient Two-Party Cryptographic Framework for Vertical Decision Trees [J]. *IEEE Transactions on Information Forensics and Security*, 2022. **(CCF A)**

[67] [**TDSC 2022**] Wenbo Jiang, Tianwei Zhang, Han Qiu, Hongwei Li, **Guowen Xu**. Incremental Learning, Incremental Backdoor Threats[J]. *IEEE Transactions on Dependable and Secure Computing,*2022. **(CCF A)**

[68] [**NeurIPS 2022**] Meng Hao, Hongwei Li, Hanxiao Chen, Pengzhi Xing, **Guowen Xu**, Tianwei Zhang. Iron: Private Inference on Transformers [C]. in *Proceedings of Thirty-Sixth Conference on Neural Information Processing Systems*. 2022. **(CCF A)**

[69] [**MM 2022**] Xingshuo Han, **Guowen Xu**, Yuan Zhou, Xuehuan Yang, Jiwei Li, Tianwei Zhang. Physical Backdoor Attacks to Lane Detection Systems in Autonomous Driving [C]. in *Proceedings of ACM International Conference on Multimedia*. 2022. **(CCF A)**

[70] [**TSC 2022**] Jingwei Wang, Xinchun Yin, Jianting Ning, Shengmin Xu, **Guowen Xu**, and Xinyi Huang. Secure Updatable Storage Access Control System for EHRs in the Cloud [J]. *IEEE Transactions on Services Computing*, 2022, to appear. **(CCF A)**

[71] [**TCSVT 2022**] Shangwei Guo, Tianwei Zhang, **Guowen Xu**, Han Yu, Tao Xiang, Yang Liu. Topology-aware Differential Privacy for Decentralized Image Classification[J]. *IEEE Transactions on Circuits and Systems for Video Technology*, vol.32, no.6, pp.4016-4027, 2022. **(CCF B)**

[72] [**INFOCOM 2021**] Haoran Yuan, Xiaofeng Chen, **Guowen Xu***(**Corresponding Author**), Jianting Ning, Joseph Liu, Robert H Deng. Efficient and Verifiable Proof of Replication with Fast Fault Localization[C]. in *Proceedings of IEEE International Conference on Computer Communications,* 2021. **(CCF A)**

[73] [**TCC 2021**] Jianfei Sun, **Guowen Xu***(**Corresponding Author**), Tianwei Zhang, Hu Xiong, Hongwei Li, Robert H Deng. Share your data carefree: An efficient, scalable and privacy-preserving data sharing service in cloud computing[J]. *IEEE Transactions on Cloud Computing*, 2021.

[74] [**TDSC 2021**] Shengmin Xu, Jianting Ning, Xinyi Huang, Yingjiu Li, **Guowen Xu**. Untouchable Once Revoking: A Practical and Secure Dynamic EHR Sharing System via Cloud[J]. *IEEE Transactions on Dependable and Secure Computing*, 2021. **(CCF A)**

[75] [**TIFS 2021**] Xiaoyuan Liu, Hongwei Li, **Guowen Xu**, Zongqi Chen, Xiaoming Huang, and Rongxing Lu. Privacy-Enhanced Federated Learning against Poisoning Adversaries [J]. *IEEE Transactions on Information Forensics and Security*, 2021. **(CCF A)**

[76] [**TDSC 2021**] Shengmin Xu, Jianting Ning, Yingjiu Li, Yinghui Zhang, **Guowen Xu**, Xinyi Huang, Robert H. Deng. A Secure EMR Sharing System with Tamper Resistance and Expressive Access Con-

trol[J]. *IEEE Transactions on Dependable and Secure Computing*, 2021. **(CCF A)**

[77] **[ESORICS 2021]** Shengmin Xu, Jianting Ning, Jinhua Ma, **Guowen Xu**, Jiaming Yuan, Robert Deng. Revocable Policy-Based Chameleon Hash [C], in *Proceedings of European Symposium on Research in Computer Security*, 2021. **(CCF B)**

[78] [**ACSAC 2021**] Meng Hao, Hongwei Li, **Guowen Xu**, Hanxiao Chen, Tianwei Zhang. Efficient, Private and Robust Federated Learning[C]. in *Proceeding of Annual Computer Security Applications Conference*, online, 2021. **(CCF B)**

[79] **[TDSC 2020] Guowen Xu,** Hongwei Li, Yun Zhang, Shengmin Xu, Jianting Ning, Robert H. Deng. Privacy-preserving Federated Deep Learning with Irregular Users[J]. *IEEE Transactions on Dependable and Secure Computing*, 2020. **(CCF A)**

[80] [**ASIACCS 2020**] **Guowen Xu**, Hongwei Li, Shengmin Xu, Hao Ren, Kan Yang, Yinghui Zhang, Jianfei Sun, Robert H. Deng. Catch You If You Deceive Me: Verifiable and Privacy-aware Truth Discovery in Crowd Sensing Systems[C]. in *Proceedings of ACM ASIA Conference on Computer and Communications Security,* Taipei, Taiwan, China, 2020.

[81] [**ACSAC 2020**] **Guowen Xu**, Hongwei Li, Hao Ren, Jianfei Sun, Shengmin Xu, Jianting Ning, Haomiao Yang, Kan Yang, Robert H. Deng. Secure and Verifiable Inference in Deep Neural Networks[C]. in *Proceeding of Annual Computer Security Applications Conference*, 2020. (**CCF B**)

[82] [**TCC 2020**] **Guowen Xu**, Hongwei Li, Hao Ren, Xiaodong Lin, Xuemin (Sherman) Shen. DNA Similarity Search with Access Control over Encrypted Cloud Data[J]. *IEEE Transactions on Cloud Computing*, 2019.

[83] [**ICPADS 2020**] **Guowen Xu**, Hongwei Li, Yuan Zhang, Xiaodong Lin, Robert H Deng, Xuemin (Sherman) Shen. A Deep Learning Framework Supporting Model Ownership Protection and Traitor Tracing[C]. in *Proceedings of IEEE International Conference on Parallel and Distributed Systems*, 2020. (**Best Paper Award**)

[84] **[TDSC 2020]** Shengmin Xu, Jianting Ning, Yingjiu Li, Yinghui zhang, **Guowen Xu**, Xinyi Huang, Robert H Deng. Match in My Way: Fine-Grained Bilateral Access Control for Secure Cloud-Fog Computing[J]. *IEEE Transactions on Dependable and Secure Computing*, 2020. **(CCF A)**

[85] [**TIFS 2019**] **Guowen Xu**, Hongwei Li, Sen Liu, Kan Yang, Xiaodong Lin. VerifyNet: Secure and Verifiable Federated Learning[J]. *IEEE Transactions on Information Forensics and Security,* 2019. (**CCF A**)

[86] [**TVT 2019**] **Guowen Xu**, Hongwei Li, Sen Liu, Mi Wen, Rongxing Lu. Efficient and Privacy-preserving Truth Discovery in Mobile Crowd Sensing Systems[J]. *IEEE Transactions on Vehicular Technology,* 2019.

[87] **[IEEE Commun Mag 2019] Guowen Xu**, Hongwei Li, Hao Ren, Kan Yang，Robert H. Deng. Data Privacy and Security in Deep Learning: Attacks, Solutions and Opportunities[J]. *IEEE Communications Magazine*, 2019.

[88] [**TIFS 2018**] **Guowen Xu**, Hongwei Li, Yuanshun Dai, Kan Yang, Xiaodong Lin. Enabling Efficient and Geometric Range Query with Access Control over Encrypted Spatial Data[J]. *IEEE Transactions on Information Forensics and Security,* 2018. (**CCF A**)

[89] [**CCS 2018**] **Guowen Xu**, Hongwei Li, Rongxing Lu. Poster: Practical and Privacy-Aware Truth Discovery in Mobile Crowd Sensing Systems[C]. in *Proceedings of ACM Conference on Computer and Communications Security*, Toronto, Canada. 2018. (**CCF A**)

[90] [**Comput Secur 2017**] **Guowen Xu**, Hongwei Li, Chen Tan, Dongxiao Liu, Yuanshun Dai, Kan Yang. Achieving Efficient and Privacy-Preserving Truth Discovery in Crowd Sensing Systems[J]. *Computers & Security*, 2017. (**CCF B**)

PROJECT EXPERIENCES

[1] [2026.01-2028.12] Research on Security-Critical Technologies for Autonomous Driving Based on Multimodal Large Models, National Science Fund Program for Young Scientists of China, **PI**, Amount: **￥300K**.

[2] [2026.01-2029.12] XXX Platform Design and Implementation. Key R&D Project of JKW. **PI**, Amount: **￥9.6 million**.

[3] [2026.01-2027.12] Research on Key Technologies for Integrated Attack-Defense of Multimodal Large Models for Autonomous Driving. General Program of the Sichuan Provincial Natural Science Foundation. **PI**, Amount: **￥200K.**

[4] [2025.01-2027.12] Data Security, National Science Fund Program for Excellent Young Scientists (Overseas) of China, **PI**, Amount: **￥2 million**.

[5] [2024.09-2027.09] Key Security and Privacy Issues on Machine Learning, **PI**, Start-up at UESTC, Amount: **￥2 million**.

ACADEMIC ACTIVITIES

➢ **Editorial Board**:

- IEEE Transactions on Pattern Analysis and Machine Intelligence, 2025-present
- IEEE Transactions on Dependable and Secure Computing, 2025-present
- IEEE Transactions on Information Forensics and Security, 2024-present
- IEEE/ACM Transactions on Audio, Speech, and Language Processing, 2025-present
- IEEE Transactions on Circuits and Systems for Video Technology, 2024-present
- IEEE Transactions on Network and Service Management, 2023-2025
- IEEE Open Journal of Signal Processing (OJSP), 2023-2025
- ACM Digital Threats: Research and Practice, 2023-2025
- Pattern Recognition (Elsevier), 2024-2025
- Information Fusion (Elsevier), 2024-2025
- Cybersecurity (Springer), 2024-2025
- IET Information Security, 2023-2025
- Lead Guest Editor of ACM Transactions on Autonomous and Adaptive Systems （TAAS）, Special Issue on Trustworthy Security and Privacy-AI Powered Autonomous Driving, 2024-2025

➢ **Technical Committee**:

- 2026-2028 Member of IEEE Region 10 Young Professionals Committee (YPC)
- 2026 **Area Chair** of International Conference on Machine Learning (ICML)
- 2026 **Area Chair** of IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)
- 2026 **Area Chair** of International Conference on Learning Representations (ICLR)
- 2026 **Area Chair** of ACM Conference on Knowledge Discovery and Data Mining (KDD)
- 2026 **Senior Program Committee** of AAAI Conference Artificial Intelligence (AAAI)
- 2026 The ACM Conference on Computer and Communications Security (CCS’ 26)
- 2026 The 35th USENIX Security Symposium (USENIX Security'26)
- 2025 **Area Chair** of ACM Conference on Knowledge Discovery and Data Mining (KDD)
- 2025 **Area Chair** of International Conference on Machine Learning (ICML)

- 2025 **Associate Chair** of 28th ACM SIGCHI Conference on Computer-Supported Cooperative Work & Social Computing (CSCW)
- 2025 **Area Chair** of International Conference on Learning Representations (ICLR)
- 2025 **Senior Program Committee** of AAAI Conference Artificial Intelligence (AAAI)
- 2025 **Area Chair** of International Joint Conference on Neural Networks (IJCNN)
- 2025 The 35-th IEEE Visualization and Visual Analytics Conference (VIS)
- 2025 The 37th International Conference on Computer Aided Verification (CAV)
- 2025 The 32nd IEEE Conference on Virtual Reality (VR)
- 2025 International Conference on Autonomous Agents&Multiagent Systems (AAMAS)
- 2025 The 30th Annual ACM Conference on Intelligent User Interfaces (IUI)
- 2025 The 29th Financial Cryptography and Data Security Conference (FC)
- 2024 **Area Chair** of International Conference on Machine Learning (ICML)
- 2024 Thirty-eighth Conference on Neural Information Processing Systems (NeurIPS)
- 2024 Annual Computer Security Applications Conference (ACSAC)
- 2023 The ACM Web Conference
- 2023-2024 Thirty-Seventh AAAI Conference on Artificial Intelligence (AAAI)
- 2022 Thirty-sixth Conference on Neural Information Processing Systems (NeurIPS)

➢ **Technical Community Member**:

- IEEE Computer Society Technical Community on Data Engineering
- IEEE Computer Society Technical Community on Dependable Computing and Fault Tolerance
- IEEE Digital Privacy Community
- IEEE Computer Society Technical Community on High Performance Computing
- IEEE Computer Society Technical Community on Intelligent Informatics
- IEEE Internet of Things Community
- IEEE Computer Society Technical Community on Pattern Analysis and Machine Intelligence
- IEEE Computer Society Technical Community on Multimedia Computing
- IEEE Computer Society Technical Community on Security and Privacy
- IEEE Computer Society Technical Community on Services Computing
- IEEE Signal Processing Society Technical Community on Computational Imaging
- IEEE Signal Processing Society Technical Community on Image, Video, and Multidimensional Signal Processing
- IEEE Robotics and Automation Technical Committee on Energy, Environment, and Safety Issues
- IEEE Robotics and Automation Technical Committee on Verification of Autonomous Systems
- IEEE Consumer Technology Society's Technical Committees on Security and Privacy in Consumer Technology

➢ **Others**:

- Technical Review Board of IEEE Transactions on Parallel and Distributed Systems (TPDS), 2025-present
- Distinguished Reviewers Board of ACM Transactions on the Web, 2022-present
- Mentor of IEEE Signal Processing Mentorship Academy (SigMA), 2025-present