Jianbing Ni, PhD

Contact   Department of Electrical and Computer Engineering
Smith Faculty of Engineering
Queen's University, Kingston, Ontario, Canada K7L 3N6
Phone: (613) 533-6000 ext. 79428
Mobile: (226) 989-2170
Email: jianbing.ni@queensu.ca
https://nisp-q.github.io/

Education
09/2014-10/2018   PhD in Electrical and Computer Engineering, University of Waterloo, Canada
09/2011-07/2014   MSc in Computer Engineering, University of Electronic Science and Technology of China, Chengdu, China
09/2007-07/2011   BSc in Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu, China

Employment Experience
2024-   Assistant Professor (Cross-appointed), School of Computing, Queen's University
2019-   Assistant Professor, Department of Electrical and Computer Engineering, Queen's University
2018-2019   Post-Doctoral Fellow, Department of Electrical and Computer Engineering, University of Waterloo
2018   Part-time Lecturer, Department of Physics and Computer Science, Wilfrid Laurier University

Research Interests
- Artificial Intelligence (AI) Security and Ethics: Adversarial Machine Learning, Privacy-Preserving Federated Learning, Ethical AI, and Trustworthy AI.
- Security and Privacy in Vehicular Communication Systems, Mobile Networks, Edge-Cloud Computing, and Cyber-Physical Systems.
- Blockchain Technology: Secure Decentralized Finance, Digital Cryptocurrency, and Secure Blockchain Applications.

Summary

Peer-reviewed Journal Papers	Peer-reviewed Conference Papers	Papers Under Review	Journal Editorship	Invited Research Seminars	Research Fundings
78	45	5	10	26	9

- Citation number (Google Scholar): 6,400+; H - index: 42
- 25 first-author papers in journals and conferences
- 8 ESI highly cited papers (top 1% cited in Web of Science for the field and year)
- 3 ESI hot papers (top 0.1% cited in Web of Science for the field and year)
- 9 Best/Outstanding Paper Awards from international conferences and journals
- 1.2 M research funds from federal institutions and industrial partners
- Nominated for Tier 2 Canada Research Chair in Intelligent System Security and Privacy

Prizes and Awards

2024 Smith Engineering Innovation in Teaching Award, Queen's University
2023 IEEE Technical Committee on Scalable Computing (TCSC) Award for Excellence in Scalable Computing (Early Career Researchers)
2023 Outbound International Faculty Mobility Award, Smith Engineering, Queen's University
2022 IEEE Vehicular Technology Society Early Career Award
2022 IEEE Outstanding Leadership Award on IEEE Int. Conf. Computational Science and Engineering, Wuhan, China
2022 Outstanding Paper Award on IEEE Int. Conf. High Performance Computing and Communications, Chengdu, China
2022 Best Paper Award for IEEE Transactions on Mobile Computing
2020 Best Paper Award on IEEE/CIC Int. Conf. Communications in China, Chongqing, China
2018 Best Paper Award on IEEE Int. Conf. Mobile Ad Hoc and Sensor Systems, Chengdu, China
2018 Best Paper Award on IEEE Int. Conf. Communications, Kansas City, MO, USA
2017 Best Paper Award on IEEE Global Communications Conf., Singapore
2017 Best Paper Award on IEEE Int. Conf. Wireless Communications and Signal Processing, Nanjing, China
2017 Jon W. Mark Graduate Scholarship Award, University of Waterloo
2016 Best Paper Award on EAI Int. Conf. Security and Privacy in Communication Networks, Guangzhou, China
2016 Faculty of Engineering Graduate Scholarship Award, University of Waterloo
2015 Best Paper Award on Int. Conf. Broadband and Wireless Computing, Communication and Applications, Krakow, Poland

Awarded Research Funding

2024-2028 M. Zulkernine, J. Ni (Co-supervisor), "Creating Inclusive Digital Society: Online Violence and Cyberbullying Detection and Mitigation," $140,000, Bruce Mitchell Research Program - Doctoral Trainees fund, Queen's University.
2024-2027 M. Zulkernine, **J. Ni** (Co-PI), "Mitigating Security, Privacy, and Ethical Impacts in Advanced Driver Assistance Systems," $300,000, National Cybersecurity Consortium, Cyber Security Innovation Network program.
2023-2024 **J. Ni** (PI), S. Yam, N. Lu, M. Greeff, F. Chan, "Exploiting AI to Build Secure, Reliable, and Trusted Human-Autonomy Teaming for Attack Detection and Recognition," $199,000, IDEaS Program, Canada.
2023-2024 M. Greeff, S. Yam, **J. Ni** (Investigator), N. Lu, F. Chan, "Safe Autonomous Arctic Ship-To-Shore Transit with Zero GHG Emissions," $197,250, IDEaS Program, Canada.
2022-2023 **J. Ni** (PI), S. Yam, M. Greeff, F. Chan, "Enhancing 5G and Beyond Infrastructure for Secure, Flexible, and Smart Military Communications," $199,800, IDEaS Program, Canada.
2022-2023 S. Yam, **J. Ni** (Investigator), M. Greeff, F. Chan, "Power, Network, and Sensor Management System with Machine Learning Analytics for 24/7 Arctic infrastructure monitoring," $200,000, IDEaS Program, Canada.
2022-2023 **J. Ni** (PI), "Digital Wallet Integration with Multiple Blockchain Networks," $15,000, MITACS Business Strategy Internship (BSI) Program, Canada.
2022-2023 **J. Ni** (PI), "Proof of Erasure: Secure Personal Data Deletion with Public Verifiability," $50,000, Office of the Privacy Commissioner of Canada Contributions program, Canada.

2020-2022   **J. Ni** (PI), "A Secure and Privacy-Preserving Edge Caching Framework in Next-Generation Mobile Networks," $125,000, CFI John R. Evans Leaders Fund, Canada.

2020-2025   **J. Ni** (PI), "Secure and Privacy-Preserving Edge Caching in Next-Generation Mobile Networks," $165,000 ($33,000/year), NSERC Discovery Grant, Canada.

2020-2021   **J. Ni** (PI), "Secure and Privacy-Preserving Edge Caching in Next-Generation Mobile Networks," $12,500, NSERC DGECR - Discovery Launch Supplement, Canada.

2019-2099   **J. Ni** (PI), $60,000, Research Initiation Grant (RIG), Queen's University, Canada.

Awarded Teaching Funding

2021   T. Dean, **J. Ni**, J. Marshall, N. Zhang, and D. Zhao, "Ethics Module for Artificial Intelligence Engineering," $40,000, eCampusOntario Open Educational Resource – Collaboration, Ontario.

I. Professional Services, Leadership, and Editorships

2024-   Member, Queen's Center for Security and Privacy, Queen's University

2023   Queen's Advancing Leadership Program

2022-   IEEE Senior Member

2021-   Member, Ingenuity Labs Research Institute, Queen's University

2021- Co-Chair of the IEEE Blockchain Canada Chapter in IEEE Technology and Engineering Management Society (TEMS)

2019-   Member of National Cybersecurity Consortium (NCC), Canada

Technical Journal Editorships

2021-   Associate Editor, ACM Distributed Ledger Technologies: Research and Practice

2021-   Associate Editor, Security and Safety

2020-   Associate Editor, IEEE Systems Journal

2024   Guest Editor, Journal of Surveillance, Security and Safety, Special Issue on "Security, Privacy, and Trust in Intelligent Cyber-Physical Systems and Internet of Things: Trends, Issues, and Challenges".

2023   Guest Editor, Computer Communications (Elsevier), Special Issue on "Security and Reliability in Future Intelligent Mobile Communication".

2023   Guest Editor, Journal of Information and Intelligence (Elsevier), Special Issue on "Data Security and Privacy Computing in Artificial Intelligence".

2021   Guest Editor, IEEE Open Journal of the Communications Society, Special Issue on "Security and Privacy for the Transformative Technologies in 5G and Beyond".

2020   Guest Editor, IEEE Internet of Things Journal, Special Issue on "Cybertwin-driven 6G: Architectures, Methods and Applications".

2020   Guest Editor, Computer Communications (Elsevier), Special Issue on "Security and Privacy in Space-Ground Integrated Network".

2020   Guest Editor, Concurrency and Computation Practice and Experience, Special Issue on "Federated learning in Mobile Edge Computing and Internet of Things".

Leadership Roles in International Conferences

2025   Symposium Co-chair, Multimedia Computing and Communications, International Conference on Computing, Networking and Communications (ICNC 2025), February 17-20, Honolulu, Hawaii, USA

2024   Symposium Co-chair, Communication and Information System Security, IEEE International Conference on Communications, June 9–13, 2024, Denver, CO, United States

2024 Track Chair, Communications, Networking, and Signal Processing Track, IEEE Canada Conf. ECE 2024, Kingston, Ontario, Canada

2024 Track Chair, Privacy Track, The 21st Annual International Conference on Privacy, Security, and Trust (PST2024), Sydney, Australia

2023 General Co-Chair, The Sixth International Conference on Frontiers in Cyber Security Aug.17-19, 2023, Chengdu, China

2023 Registration & Finance Co-Chair, IEEE ComSoc Frontier Networking Symposium, Sept. 5, 2023, Toronto, Canada

2023 Co-Chair, IEEE Int. Conf. Communications in China 2023 Workshop on Emerging Radio Access Network Technologies for B5G/6G (eRAN), Dalian, China

2022 Program Vice-Chair, IEEE Int. Conf. Computational Science and Engineering (CSE), Dec. 9-22, 2022, Wuhan, China

2022 Publicity Chair, EAI Int. Conf. Security and Privacy in New Computing Environments (SPANCE) December 30-31, 2022, Qinhuangdao, China

2022 Co-Chair, IEEE Int. Conf. Communications in China 2022 Workshop on Emerging Radio Access Network Technologies for B5G/6G (eRAN), Foshan City, China

2021 Session Chair, Int. Conf. Privacy, Security and Trust (PST) 2021, Auckland, New Zealand

2021 Track Chair, IEEE Int. Symposium Systems Engineering 2021, Virtual Conference

2021 Co-Chair, IEEE Int. Conf. Communications in China 2021 Workshop on Emerging Radio Access Network Technologies for B5G/6G (eRAN), Xiamen, China

2021 Track Chair, IEEE Canada Conf. ECE 2021, London, Ontario, Canada

2017 Publicity Co-Chair, Int. Conf. Provable Security, Xi'an, China

Technical Program Committee Member of International Conferences

2024 The sixth International Conference on Communications, Signal Processing, and their Applications (ICCSPA), Istanbul, Türkiye.

2024 International Conference on Computing and Communication Networks (ICCCN), Big Island, Hawaii, USA

2024 The 29th Australasian Conference on Information Security and Privacy (ACISP), Sydney, Australia

2024 Int. Conf. Information and Communications Security (ICICS) 2024, Mytilene, Greece

2024 IEEE Global Communications Conf. (GLOBECOM) 2024, Cape Town · South Africa

2024 IEEE Vehicular Technology Conf. (VTC) - Spring 2024, Singapore

2024 IEEE Int. Conf. Communications (ICC) 2024, Denver, Colorado, United States

2024 IEEE Canada Conf. ECE 2024, Kingston, ON, Canada

2024 Int. Conf. Privacy, Security and Trust (PST) 2024, Sydney, Australia

2023 IEEE Int. Conf. Communications in China 2023, Dalian, China

2023 IEEE Global Communications Conf. (GLOBECOM) 2023, Kuala Lumpur, Malaysia

2023 Int. Conf. Information and Communications Security (ICICS) 2023, Tianjin, China

2023 IEEE Vehicular Technology Conf. (VTC) - Spring 2023, Florence, Italy

2023 IEEE Int. Conf. Communications (ICC) 2023, Rome, Italy

2023 IEEE Canada Conf. ECE 2023, Regina, SK, Canada

2023 Int. Conf. Privacy, Security and Trust (PST) 2023, Copenhagen, Denmark

2023 IEEE INFOCOM 2023 International Workshop on AI-Driven Trustworthy, Secure, and Privacy-Preserving Computing (AidTSP 2023), New York, United States

2022 IEEE Global Communications Conf. (GLOBECOM) 2022, Rio de Janeiro, Brazil

2022 Int. Conf. Information and Communications Security (ICICS) 2022, Canterbury, UK

2022 IEEE Vehicular Technology Conf. (VTC) - Spring 2022 Helsinki, Finland

2022   IEEE Int. Conf. Communications (ICC) 2022, Seoul, South Korea
2022   IEEE Inte. Conf. on Trust, Security and Privacy in Computing and Communications (TrustCom 2022), Wuhan, China
2021   IEEE Global Communications Conf. (GLOBECOM) 2021, Madrid, Spain
2021   Int. Conf. Information and Communications Security (ICICS) 2021, Chongqing, China
2021   Int. Conf. Privacy, Security and Trust (PST) 2021, Auckland, New Zealand
2021   EAI Int. Conf. Mobile Multimedia Communications (Mobimedia) 2021, Guiyang, China
2021   IEEE Vehicular Technology Conf. (VTC) - Spring 2021, Virtual conference
2021   IEEE Int. Conf. Communications (ICC) 2021, Montreal QC, Canada
2020   IEEE Global Communications Conf. (GLOBECOM) 2020, Taipei, Taiwan
2020   IEEE Int. Conf. Parallel and Distributed Systems (ICPADS) 2020, Hong Kong
2020   IEEE Vehicular Technology Conf. (VTC) - Spring 2020, Helsinki, Finland
2020   IEEE Vehicular Technology Conf. (VTC) - Fall 2020, Victoria, Canada
2020   Int. Conf. Information and Communications Security (ICICS) 2020, Copenhagen, Danmark
2020   Int. Conf. Privacy, Security and Trust (PST) 2020, Hangzhou, China
2019   IEEE Global Communications Conf. (GLOBECOM) 2019, Hawaii, United States
2019   Int. Conf. Information and Communications Security (ICICS) 2019, Beijing, China
2018   Int. Conf. Provable Security (ProvSec) 2018, Jeju, South Korea
2018   IEEE Global Communications Conf. (GLOBECOM) 2018, Abu Dhabi, United Arab Emirates
2017   Int. Conf. Provable Security (ProvSec) 2017, Xi'an, China
2017   IEEE Global Communications Conf. (GLOBECOM) 2017, Marina Bay Sands, Singapore
2016   IEEE Global Communications Conf. (GLOBECOM) 2016, Washington, D.C., United States
2015   IEEE Global Communications Conf. (GLOBECOM) 2015, San Diego, Unite States

Administration and Committee Memberships (Queen's University)

2024-2025   Chair, UCC Subcommittee on CMPE direct entry curriculum
2023-2025   Chair of Undergraduate Studies - Computer Engineering
2023-2025   CEAB Report Committee
2022-2023   Coordinator, Graduate Affairs-PhD Comprehensive Exam
2022-2023   Space and Facilities Committee
2022-2023   Coordinator, Computer and Software Engineering Research Group
2022   Member, ECE Graduate Student Scholarship Committee
2021-2022   Member, ECE Appointment Committee
2021-2022   Coordinator, Graduate Affairs-PhD Comprehensive Exam
2021   Member, ECE Graduate Student Scholarship Committee
2021   Member, ECE EDI Working Group
2020-2021   Member, ECE Appointment Committee 2
2020-2021   Counselor, Queen's IEEE Student Branch

II. Student Training, Supervision, and Advisory Committee Membership

Current Students

Dr. Ni is currently supervising 2 PhD students, co-supervising 1 PhD student and 1 MSc student, and 2 new PhD students and 2 new MASc will join our group in September 2024.

05/2022-   **X. Li**, PhD student in Accelerated Master's Degree Program and promoted to PhD program, "Privacy and Robustness in Federated Unlearning".

[1] **X. Li**, Y. Liu, J. Ni, and Y. He, "Securing E-Petition: A Privacy-Preserving Fine-Grained Electronic Petition System for Health and Political Petitions," *Proc. of IEEE ICC 2022*, Seoul, South Korea, 16–20 May 2022.

[2] M. He, **X. Li**, J. Ni, and H. Yang, "Balancing Efficiency and Security for Network Access Control in Space-Air-Ground Integrated Networks," *Proc. of PST 2021*, Auckland, New Zealand, Dec. 13-15, 2021.

[3] M. He, **X. Li**, and J. Ni, "Physical Layer Security for mmWave Communications: Challenges and Solutions," *ZTE Communications*, vol. 20, no. 4, pp. 41--51, 2022.

[4] J. Zhao, **X. Li**, and J. Ni, "'Privacy-Preserving Model Aggregation for Asynchronous Federated Learning" *The 12th IEEE/CIC ICCC 2023*, Dalian, China, August 10-12, 2023.

[5] **X. Li**, M. He, and J. Ni, "Secure and Privacy-preserving Network Slicing in 3GPP 5G System Architecture," *The 12th IEEE/CIC ICCC 2023*, Dalian, China, August 10-12, 2023.

[6] B. Mosher, **X. Li**, Y. He, and J. Ni, "Verifiable and Privacy-preserving Ad Exchange for Targeted Advertising," *The 20th Annual International Conference on Privacy, Security & Trust*, Copenhagen, Denmark, 21-23 August 2023.

[7] X. Wu, **X. Li**, J. Ni and R. Lu, "Evaluating Security and Robustness for Split Federated Learning against Poisoning," *IEEE Transactions on Information Forensics & Security*, major revision.

[8] **X. Li**, X. Wu, and J. Ni, "Accelerating Secure and Verifiable Data Deletion in Cloud Storage via SGX and Blockchain," *IEEE GLOBECOM 2024*, Cape Town, South Africa, December 8-12, 2024, under review.

01/2023- **X. Wu,** PhD student, "Adversarial Attacks and Detection in Split Federated Learning".

[1] **X. Wu**, R. Duan, and J. Ni, "Unveiling Security, Privacy, and Ethical Concerns of ChatGPT," *Journal of Information and Intelligence*, accepted.

[2] **X. Wu**, X. Li, J. Ni, and R. Lu, "Evaluating Security and Robustness for Split Federated Learning against Poisoning," *IEEE Transactions on Information Forensics & Security*, major revision.

[3] **X. Wu**, Y. Han, H. Dahrouj, J. Ni, Z. Liang, and X. Zhang, Manipulating Predictions over Discrete Inputs in Machine Teaching, arXiv preprint arXiv:2401.17865, January 2024.

[4] X. Li, **X. Wu**, and J. Ni, "Accelerating Secure and Verifiable Data Deletion in Cloud Storage via SGX and Blockchain," *IEEE GLOBECOM 2024*, Cape Town, South Africa, December 8-12, 2024, under review.

09/2023- N. Rubaiyat, MSc student, co-supervising with Prof. M. Zulkernine. "Mitigating Security, Issues in Advanced Driver Assistant Systems".

01/2024- R. Abbasi, PhD student, co-supervising with Prof. M. Zulkernine. "Unsupervised Anomaly Detection in Advanced Driver Assistant Systems".

05/2024- Junxuan Wu, MEng student, Project Title: "Mitigating AI Hallucination With Knowledge Graphs."

05/2024- Tianyi Tang, MEng student, Project Title: "Watermark Detection for AI Generated Images."

05/2024- Junze Yan, MEng student, Project Title: "Assessing and Mitigating Vulnerabilities in AI-Generated Smart Contracts."

Previously Supervised Graduate Students

01/2020-12/2023   **M. He**, PhD, "Physical-Layer Security for Millimeter-Wave Communication".

09/2020-01/2023 **J. Zhao**, MASc, **Vector Scholarship in AI**. "Privacy Preservation and Verifiability for Federated Learning". Software Engineer, Theia, Ottawa

09/2020-08/2022 **Y. Liu**, MASc, co-supervised with Prof. M. Zulkernine, **MITACS Business Strategy Internship at MyLaminin Inc.**, "Privacy and Regulatory Compliance for Central Bank Digital Currency."

09/2020-08/2022 **B. Mosher**, MASc, **NSERC USRA Summer 2020 Award**, "Privacy and Fairness for Online Targeted Advertising," (Optable Inc., Montreal)

05/2020-08/2020 **R. Duan**, MEng student, "Fake Image Generation and Detection based on Generative Adversarial Network (GAN)."

05/2023-08/2023 **R. Li**, MEng student, "Adversarial Attack and Mitigation of Object Identification on Satellite Images".

05/2023-08/2023 **Y. Liang**, MEng student, "Attacks and Defence of Object Detection on SAR Images".

Supervised Capstone Projects of Undergraduate Students

2023-24 T. Kirton, P. Ortiz, T. Stephney, and T. Wade, ELEC 490 project, "Voice to ChatGPT."

2023-24 F. Clark, K. Dillon, and T. Hamilton, ELEC 490 project, "Physical Attacks on Self-Driving Systems".

2022-23 E. Li, L. Wu, J. Wu, and X. Wang, ELEC 490 project, "Facial Payment."

2022-23 A. Jones, A. Gregoire, C Gauthier, and O. Gurevich, ELEC 490 project, "Hacking Contactless Payment."

2022-23 B. Soutter, G. Palfrey, H. Grieve, and M. Passler, ELEC 490 project, "Blockchain-based Package Tracking and Management System."

2022-23 A. Kochhar, D. Gunda, G. Anderson, and W. Kennedy, ELEC 490 project, "Blockchain-based Document Sharing Platform."

2022-23 Y. Li, W. Hou, H. Xu. Z. Liu, and Y. Zheng, CISC 498 Graduate Project, "Web-based Real-time Data Explorer."

2021-22 E. Gibbons, G. Brydon, E. Duffy, and H. Yeatman, ELEC 490 project, "Privacy Preserving Online Advertisement System." (**Students' Choice Award**)

2021-22 T. Lampen, J. Dowker, E. Bibas, and D.-A. Edwards, ELEC 490 project, "Blockchain-based Mobile Online Election."

2021-22 E. Phimister, A. Moskalewicz, L. Shrago, and G. Bratkov, ELEC 490 project, "Hardware-based Password Manager." (**2nd Place Award in Electrical + Computer Engineering**)

2021-22 D. Tavernese, H. Haider, H. Sherik, ELEC 490 project, "Freelancing for Students."

2020-21 B. Caron, A. Pan, and C. Gritter, ELEC 490 project "FacialPC: PC Facial Controller." (Co-supervised with Dr. S. Gazor)

2020-21 A. Farley, S. Dobrowolski, and C. Masloub, ELEC 490 project, "NewsEye: Fake New Detection."

2020-21 Q. Roy-Foster, J. Cheung, X. Sirois, and M. Thompson, ELEC 490 project, "An Anti-peeping Application on Smartphones." (Co-supervised with Dr. T. Dean)

2020-21 B. Kitor, R. Kalkhoran, M. Crompton, and J. Wiederick, ELEC 490 project, "Blockchain Auction."

Supervised Research Projects of Undergraduate Students

2021-22 X. Li, ELEC 497 Research Project, "Transparent and Privacy-preserving Electronic Petition atop Blockchain."

2020-21 B. Mosher, NSERC USRA Summer 2020 Award, "Protecting Customer Privacy on Social Networks."

PhD Advisory Committee Membership

2024   External Examiner, Soosan Naderi Mighan, Toronto Metropolitan University, ON, Canada.
2023- Internal Examiner, P. Fathollahzadeh
2023- Internal Examiner, S. Shokrolahi.
2022- Internal Examiner, B. Schonewille.
2022   External Examiner, C. Zhang, Western University, ON, Canada.
2021- Internal Examiner, S. Matsui.
2021- Internal Examiner, Y. Youssef.
2021- Department Representative, H. Damirchi.
2020- Int/Ext. Examiner, S. Azmy.
2020- Department Representative, A. Laha.
2020- Department Representative, A. Tessier.
2020- Internal Examiner, O. Ehsan.
2019- Internal Examiner, L. H. Tanyani.

Graduate Thesis Defence Committee Membership

2024   Int. Examiner, S. Debaditya, MASc Thesis Defense.
2024   Int.Ext. Examiner, S. Zheng, MSc Thesis Defense.
2024   Int. Examiner, E. Duffy, MASc Thesis Defense.
2023   Int/Ext. Examiner, B. Chawky, PhD Thesis Defense.
2023   Int/Ext. Examiner, I. Pepin, MSc Thesis Defense
2023   Int/Ext. Examiner, M. Kantardjian, MSc Thesis Defense
2023   Int. Examiner, S. Soltanieh, MASc Thesis Defence.
2023   Chair, Y. Zhou, MASc Thesis Defense.
2023   Int/Ext. Examiner, A. Anwar, PhD Thesis Defense.
2023   Int/Ext. Examiner, D. Kamath, MSc Thesis Defense.
2023   Int/Ext. Examiner J. Banks, MSc Thesis Defense.
2023   Int/Ext. Examiner, A. Carthy, MSc Thesis Defense.
2023   Int. Examiner, Q. Bader, MASc Thesis Defence.
2023   Int. Examiner, B. Kitor, MASc Thesis Defence.
2023   Int. Examiner, D. Mays, MASc Thesis Defence.
2022   Chair, J. Guo, MSc Thesis Defence.
2022   Chair, A. Bhatti, MSc Thesis Defence.
2022   Int. Examiner, B. Mahdi, MASc Thesis Defence
2022   Int. Examiner S. R. Taghanaki, MASc Thesis Defence.
2022   Int/Ext. Examiner, B. Rombaut, MSc Thesis Defence
2022   Int/Ext. Examiner, F. Faghihi, PhD Thesis Defence
2022   Int/Ext. Examiner, M. S. Allaham, MSc Thesis Defence.
2022   Int/Ext. Examiner, Z. Khaled, MSc Thesis Defence.
2022   Int/Ext. Examiner, S. Shafieian, PhD Thesis Defence.
2021   Int/Ext. Examiner, A. Chaudhry, MSc Thesis Defence.
2021   Int/Ext. Examiner, L. Moukahal, PhD Thesis Defence.
2021   Int/Ext. Examiner, T. A. M. Ghaleb, PhD Thesis Defence.
2021   Int/Ext. Examiner, A. Tagra, MSc Thesis Defence.
2021   Internal Examiner, Y. Temucin, MASc Thesis Defence.
2021   Int/Ext. Examiner, L. J. Moukahal, PhD Thesis Defence.
2021   Int/Ext. Examiner, M. Alharthi, PhD Thesis Defence.

2020   Chair, H. Banting, MASc Thesis Defence.
2020   Internal Examiner, J. Kaur, MASc Thesis Defence.
2020   Internal Examiner, S. Azmy, MASc Thesis Defence.
2020   Internal Examiner, A. C. D. Araujo, MASc Thesis Defence.
2020   Chair, J. Mazumder, MASc Thesis Defence.
2020   Int/Ext. Examiner, H. Zhang, PhD Thesis Defence.
2020   Chair, F. R. Cogo, MASc Thesis Defence.
2020   Chair, K. Ross, MASc Thesis Defence.
2020   Chair, W. A. Mueller, MASc Thesis Defence.
2020   Internal Examiner, X. Lin, MASc Thesis Defence.
2020   Internal Examiner, B. Mahdy, MASc Thesis Defence.
2020   Chair, H. Elsherbiny, MASc Thesis Defence.
2020   Head Delegate, W. Liu, PhD Thesis Defence.
2020   Chair, A. Kumar, MASc Thesis Defence.
2019   Int/Ext. Examiner, A. Rahman, PhD Thesis Defence.
2019   Int/Ext. Examiner, A. A. Zarir, M. Sc Thesis Defence
2019   Chair, A. Awasthi, MASc Thesis Defence.
2019   Internal Examiner, M. B. Salloum, MASc Thesis Defence.

III. Knowledge Translation

2023   Solution of private 5G network for building broadband connectivity in remote and communications-denied environments, Department of National Defense, Canada.

We extended 5G and beyond technologies to connect the public 5G mobile platforms that are fielded by the various branches of the armed services for enabling secure and prioritized information exchange for ground forces, Intelligence, Surveillance, and Reconnaissance (ISR) sensors, tactical operational centers, and military satellites. The developed 5G network provides the infrastructure with soldiers for information exchange at any time, and the operators can share critical C4ISR information in a degraded or denied area of network coverage. This was funded by Department of National Defense. We developed a demo and presented it on IEEE PIMRC 2023, Toronto, Ontario, Sept 5-8, 2023.

2022   Solution of secure document sharing system with cross blockchain mobile wallet, MyLaminin Inc., Canada.

We developed a new blockchain-enabled document sharing and verification service platform that enables individuals, organizations, and governments to securely share important personal and business documents using blockchain or distributed ledger technology. The blockchain-enabled document sharing and verification service platform is extended to support different blockchain networks that issue their credentials securely to a single digital wallet. This platform was developed with MyLaminin Inc. and has received SOC2 certification.

2021   Solution of blockchain-based secure data sharing on the Mr. Ray blockchain platform in health monitoring, Mr. Ray Co., China.

We developed a blockchain-based secure data sharing platform over the Mr. Ray blockchain platform to enable secure sharing of medical records and images among hospitals, patients, and doctors. This platform provides fine-grained access control over the medical data and supports distributed data storage for data security. This platform was deployed at Sichuan Provincial People's Hospital, China, and is managing the medical records of over 12 million patients.

IV. Significant Contributions to Research

Books and Monographs

B1.   X. Lin, **J. Ni**, and X. Shen, "Privacy-Enhancing Fog Computing and its Applications," SpringerBriefs in Electrical and Computer Engineering, Springer Verlag, 2018.

Technical Papers Under Review

P1.   X. Wu[*], X. Li[*], **J. Ni**, and R. Lu, "Evaluating Security and Robustness for Split Federated Learning against Poisoning," *IEEE Transactions on Information Forensics & Security*, major revision.

P2.   J. Zhou, J. Wu, **J. Ni**, Y. Wang, Y. Pan, and Z. Su, "Protecting Your Attention during Distributed Graph Learning: Privacy-preserving Federated Graph Attention Network," *IEEE Transactions on Information Forensics & Security*, under review.

P3.   C. Yu, Z. Meng, W. Zhang, L. Lei, **J. Ni**, K. Zhang, and H. Zhao, "Secure and Efficient Federated Learning Against Model Poisoning Attacks in Horizontal and Vertical Data Partitioning," *IEEE Transactions on Neural Networks and Learning Systems*, under review.

P4.   M. Hu, Y. He, Z. Peng, **J. Ni**, Z. Sun, F. Suya, Open Sesame: The Spell of Bypassing Speaker Verification System through Backdoor Attack, *IEEE Transactions on Audio, Speech and Language Processing*, under review.

P5.   Q. Le*, J. Ni, S. S.-H. Yam, F. Chan, and N. Lu, "Enhancing Robustness Against Adversarial Attacks with High-Intensity Perturbation: The Robust Swin Transformer Approach," *The 27th European Conference on Artificial Intelligence (ECAI-2024),* under review.

Refereed Journal Papers

J1.   M. He[*] and **J. Ni**, "On the Quantization of Phase Shifters for Physical Layer Secure Millimeter-Wave Communication Systems," *IEEE Transactions on Vehicular Technology*, to appear.

J2.   Y. Pan, Z. Su, Zhou, **J. Ni**, Y. Wang, and J. Zhou, "Privacy-Preserving Heterogeneous Personalized Federated Learning with Knowledge," *IEEE Transactions on Network Science and Engineering*, to appear.

J3.   L. Liu, C. Huang, D. Zhu, D. Liu, **J. Ni**, and X. Shen, "Enabling Efficient and Distributed Access Control for Pervasive Edge Computing Services," *IEEE Transactions on Mobile Computing*, to appear.

J4.   Y. He, P. Li, **J. Ni**, X. Deng, H. Lu, J. Zhang, and L. Yang, "RSAM: Byzantine-Robust and Secure Model Aggregation in Federated Learning for Internet of Vehicles using Private Approximate Median," *IEEE Transactions on Vehicular Technology*, to appear.

J5.   M. Zhao, C. Zhang, T. Wu, **J. Ni**, X. Liu, and L. Zhu, "Revocable and Privacy-Preserving Bilateral Access Control for Cloud Data Sharing," *IEEE Transactions on Information Forensics & Security*, to appear.

J6.   M. He[*], and **J. Ni**, "A Secret Multiuser Transmission Scheme with Dual-Phase-Shifter Structure for mmWave Wireless Communication," *IEEE Communications Letters*, vol, 28, no. 4, pp. 778-782, 2024.

J7.   X. Wu[*], R. Duan, and **J. Ni**, "Unveiling Security, Privacy, and Ethical Concerns of ChatGPT," *Journal of Information and Intelligence*, vol, 2, no. 2, pp. 102-115, 2024.

J8.   M. He[*], **J. Ni**, M. Li, A. Brighente, and M. Conti, "Enabling Low Sidelobe Secret Multicast Transmission for mmWave Communication: An Integrated Oblique Projection approach," *IEEE Transactions on Wireless Communications*, vol, 23, no. 1, pp. 276-289, 2024.

J9.   C. Zhang, M. Zhao, W. Zhang, Q. Fan, **J. Ni**, and L. Zhu, "Privacy-preserving Identity-based Data Rights Governance for Blockchain-empowered Human-centric Metaverse

Communication," *IEEE Journal on Selected Areas in Communications*, vol, 42, no. 4, pp. 963-977, 2024.

J10. L. Xue, **J. Ni**, D. Liu, X. Lin, and X. Shen, "Blockchain-based Fair and Fine-grained Data Trading with Privacy Preservation," *IEEE Transactions on Computers*, vol. 72, no. 9, pp. 2440-2453, 2023.

J11. Q. Xu, Z. Su, and **J. Ni**, "Incentivizing Secure Edge Caching for Scalable Coded Videos in Heterogeneous Networks," *IEEE Transactions on Information Forensics & Security*, vol. 18, pp. 2480--2492, 2023.

J12. L. Xue, D. Liu, **J. Ni**, X. Lin, and X. Shen, "Enabling Regulatory Compliance and Enforcement in Decentralized Anonymous Payment," *IEEE Transactions on Dependable and Secure Computing*, vol. 20, no. 2, pp. 931-943, 2023.

J13. M. Li, Y. Chen, L. Zhu, **J. Ni**, C. Lal, and M. Conti, "Astraea: Anonymous and Secure Auditing based on Private Smart Contracts for Donation Systems," *IEEE Transactions on Dependable and Secure Computing*, vol. 20, no. 4, pp. 3002--3018, 2023.

J14. **J. Ni**, M. H. Au, W. Wu, X. Luo, X. Lin, and X. Shen, "Dual-Anonymous Off-Line Electronic Cash for Mobile Payment," *IEEE Transactions on Mobile Computing*, vol. 22, pp. 3303-3317, 2023.

J15. M. He[*], X. Li[*], and **J. Ni**, "Physical Layer Security for mmWave Communications: Challenges and Solutions," *ZTE Communications*, vol. 20, no. 4, pp. 41--51, 2022.

J16. Y. He, X. Tan, **J. Ni**, L. T. Yang, and X. Deng, "Differentially Private Set Intersection for Asymmetrical ID Alignment," *IEEE Transactions on Information Forensics & Security*, vol. 17, pp. 3479--3494, 2022.

J17. C. Zhang, M. Zhao, Y. Xu, L. Zhu, W. Zhang, T. Wu, and **J. Ni**, "FRUIT: A Blockchain-based Efficient and Privacy-preserving Quality-aware Incentive Scheme", *IEEE Journal on Selected Areas in Communications*, vol. 40, no. 12, pp. 3343--3357, 2022.

J18. X. Yuan, J. Chen, N. Zhang, **J. Ni**, R. Yu, and V. Leung, "Digital Twin-Driven Vehicular Task Offloading and IRS Configuration on the Internet of Vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vo. 23, no. 12, pp. 24290--24304, 2022.

J19. M. He[*], **J. Ni**, Y. He, and N. Zhang, "Low-Complexity Phased-Array Physical Layer Security in Millimeter-Wave Communication for Cybertwin-Driven V2X Applications," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 5, pp. 4573-4583, 2022.

J20. **J. Ni**, K. Zhang, Y. Yu, and T. Yang, "Identity-based Provable Data Possession from RSA Assumption for Secure Cloud Storage," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 3, pp. 1753--1769, 2022.

J21. Y. He, **J. Ni**, L. T. Yang, W. Wei, X. Deng, D. Zou, and S. H. Ahmed, "Differentially Private Tripartite Intelligent Matching Against Inference Attacks in Ride-Sharing Services," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 11, pp. 22583--22595, 2022.

J22. D. Liu, H. Wu, C. Huang, **J. Ni**, and X. Shen, "Blockchain-based Collaborative Credential Management for Anonymous AKA in SAGVN," *IEEE Journal on Selected Areas in Communications*, vol. 40, no. 10, pp. 3104-3116, 2022.

J23. D. Liu, C. Huang, **J. Ni**, X. Lin, and X. Shen, "Blockchain-Cloud Transparent Data Marketing: Consortium Regulation and Executable Fairness," *IEEE Transactions on Computers*, vol. 71, pp. 3322--3335, 2022.

J24. C. Zhang, L. Zhu, C. Xu, **J. Ni**, C. Huang, and X. Shen, "Location Privacy-Preserving Task Recommendation with Geometric Range Query in Mobile Crowdsensing," *IEEE Transactions on Mobile Computing*, vol. 21, no. 12, pp. 4410--4425, 2022.

J25.   F. Tian, Z. Wu, X. Gui, **J. Ni**, and X. Shen, "Fine-grained Query Authorization with Integrity Verification over Encrypted Spatial Data in Cloud Storage," *IEEE Transactions on Cloud Computing*, vol. 10, no. 3, pp. 1831--1847, 2022.

J26.   D. Liu, H. Wu, **J. Ni**, and X. Shen, "Efficient and Anonymous Authentication with Succinct Multi-subscription Credential in SAGVN," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 3, pp. 2863--2873, 2022.

J27.   Y. Wang, Z. Su, **J. Ni**, N. Zhang, and X. Shen, "Blockchain-Empowered Space-Air-Ground Integrated Networks: Opportunities, Challenges, and Solutions," *IEEE Communications Surveys and Tutorials*, vol. 24, no. 1, pp. 160--209, 2022.

J28.   **J. Ni**, K. Zhang, and A. V. Vasilakos, "Security and Privacy for Mobile Edge Caching: Challenges and Solutions," *IEEE Wireless Communications*, vol. 8, no. 3, pp. 77--83, 2021.

J29.   S. Shen, C. Yu, K. Zhang, **J. Ni**, and S. Ci, "Adaptive and Dynamic Security in AI-empowered 6G: From an Energy Efficiency Perspective," *IEEE Communications Standards Magazine*, vol. 5, no. 3, pp. 80--88, 2021.

J30.   D. Liu, C. Huang, **J. Ni**, X. Lin, and X. Shen, "Blockchain-based Smart Advertising Network with Privacy-preserving Accountability," *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 3, pp. 2118--2130, 2021.

J31.   J. Liang, Z. Qin, **J. Ni**, X. Lin, and X. Shen, "Practical and Secure SVM Classification for Cloud-based Remote Clinical Decision Services," *IEEE Transactions on Computers*, vol. 70, no. 10, pp. 1612--1625, 2021.

J32.   Y. Zhang, C. Xu, **J. Ni**, H. Li, and X. Shen, "Blockchain-assisted Public-key Encryption with Keyword Search against Keyword Guessing Attacks for Cloud Storage," *IEEE Transactions on Cloud Computing*, vol. 9, no. 4, pp. 1335--1348, 2021. (**ESI Highly Cited Paper**[1])

J33.   **J. Ni**, K. Zhang, Q. Xia, X. Lin, and X. Shen, "Enabling Strong Privacy Preservation and Accurate Task Allocation for Mobile Crowdsensing," *IEEE Transactions on Mobile Computing*, vol. 19, no. 6, pp. 1317--1331, 2020. (**Best Paper Award**)

J34.   **J. Ni**, K. Zhang, Y. Yu, X. Lin, and X. Shen, "Providing Task Allocation and Secure Deduplication for Mobile Crowdsensing via Fog Computing," *IEEE Transactions on Dependable and Secure Computing*, vol. 17, no. 3, pp. 581--594, 2020. (**ESI Highly Cited Paper**[1])

J35.   R. Lu, L. Zhang, **J. Ni**, and Y. Fang, "5G Vehicle-to-Everything (V2X) Services: Gearing Up for Security and Privacy," *Proceedings of the IEEE*, vol. 108, no. 2, pp. 373-389, 2020. (**Invited Paper**)

J36.   Q. Jiang, N. Zhang, **J. Ni**, J. Ma, X. Ma, and K.-K. R. Choo, "Unified Biometric Privacy Preserving Three-factor Authentication and Key Agreement for Cloud-assisted Autonomous Vehicles," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 9, pp. 9390-9401, 2020. (**ESI Highly Cited Paper**[1])

J37.   D. Liu, **J. Ni**, X. Lin, and X. Shen, "Transparent and Accountable Vehicular Local Advertising with Practical Blockchain Designs," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 12, pp. 15694--15705, 2020.

J38.   H. Yang, Q. Zhou, **J. Ni**, H. Li, and X. Shen, "Accurate Image-based Pedestrian Detection with Privacy Preservation," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 12, pp. 14494--14509, 2020.

J39.   C. Zhang, L. Zhu, **J. Ni**, C. Huang, and X. Shen, "Verifiable and Privacy-Preserving Traffic Flow Statistics for Advanced Traffic Management Systems," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 9, pp. 11336--11347, 2020.

---

[1] ESI Highly Cited Paper - top 1% cited in Web of Science for the field and year

J40. H. Yang, S. Liang, **J. Ni**, H. Li, and X. Shen, "Secure and Efficient kNN Classification for Industrial Internet of Things," *IEEE Internet of Things Journal*, vol. 7, no. 11, pp. 10945-10954, 2020.

J41. C. Huang, **J. Ni**, R. Lu, and X. Shen, "Achieving Accountable and Efficient Data Sharing in Industrial Internet of Things," *IEEE Transactions on Information Informatics*, vol. 17, no. 2, pp. 1416-1427, 2020.

J42. D. Liu, C. Huang, **J. Ni**, X. Lin, and X. Shen, "Secure and Efficient Distributed Network Provenance: A Blockchain-based Approach," *IEEE Internet of Things Journal*, vol. 7, no. 8, pp. 7564--7574, 2020.

J43. M. Dai, Z. Su, R. Li, Y. Wang, **J. Ni**, and D. Fang, "An Edge-Driven Security Framework for Intelligent Internet of Things," *IEEE Network*, vol. 34, no. 5, pp. 39--45, 2020.

J44. J. Li, N. Zhang, **J. Ni**, J. Chen, and R. Du, "Secure and Lightweight Authentication with Key Agreement for Smart Wearable Systems," *IEEE Internet of Things Journal*, vol. 7, no. 8, pp. 7334--7344, 2020.

J45. C. Huang, R. Lu, **J. Ni**, and X. Shen, "DAPA: A Decentralized, Accountable, and Privacy-preserving Architecture for Car Sharing Services," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 5, pp. 4869--4882, 2020.

J46. Y. He, **J. Ni**, B. Niu, F. Li, and X. Shen, "Privbus: A Privacy-Enhanced Crowdsourced Bus Service via Fog Computing," *Journal of Parallel and Distributed Computing*, vol. 135, pp. 156-168, 2020.

J47. L. Xue, D. Liu, **J. Ni**, X. Lin, and X. Shen, "Balancing Privacy and Accountability for Industrial Mortgage Management," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4260--4269, 2020.

J48. **J. Ni**, X. Lin, and X. Shen, "Toward Privacy-preserving Valet Parking in Autonomous Driving Era," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 2, pp. 2893-2905, 2019.

J49. **J. Ni**, X. Lin, and X. Shen, "Toward Edge-assisted Internet of Things: From Security and Efficiency Perspectives," *IEEE Network Magazine*, vol. 33, no. 2, pp. 50-57, 2019.

J50. **J. Ni**, K. Zhang, X. Lin, and X. Shen, "Balancing Security and Efficiency for Smart Metering against Misbehaving Collectors," *IEEE Transactions on Smart Grid*, vol. 10, no. 2, pp. 1225-1236, 2019.

J51. D. Liu, **J. Ni**, A. Alahmadi, X. Lin, and X. Shen, "Anonymous Reputation System for Industrial IoT-enabled Retail Marketing atop PoS Blockchain," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3527-3537, 2019.

J52. A. Yang, J. Weng, N. Cheng, **J. Ni**, X. Lin, and X. Shen, "DeQoS Attack: Degrading Quality of Service in VANETs and its Mitigation," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 5, pp. 4834-4845, 2019.

J53. Y. Li, Y. Yu, G. Min, W. Susilo, **J. Ni**, and K.-K. R. Choo, "Fuzzy Identity-based Data Integrity Auditing for Reliable Cloud Storage Systems," *IEEE Transactions on Dependable and Secure Computing*, vol. 16, no. 1, pp. 72-83, 2019. (**ESI Highly Cited Paper**[1], **ESI Hot Paper**[2])

J54. **J. Ni**, K. Zhang, X. Lin, and X. Shen, "Securing Fog Computing for Internet of Things Applications: Challenges and Solutions," *IEEE Communications Surveys and Tutorials*, vol. 20, no. 1, pp. 601--628, 2018. (**ESI Highly Cited Paper**[1], **ESI Hot Paper**[2])

---

[1] ESI Highly Cited Paper - top 1% cited in Web of Science for the field and year
[2] ESI Hot Paper - top 0.1% cited in Web of Science for the field and year

J55.   **J. Ni**, X. Lin, and X. Shen, "Efficient and Secure Service-oriented Authentication Supporting Network Slicing for 5G-enabled IoT," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 3, pp. 644--657, 2018. (**ESI Highly Cited Paper[1]**)

J56.   **J. Ni**, K. Zhang, Y. Yu, X. Lin, and X. Shen, "Privacy-preserving Smart Parking Navigation Supporting Efficient Driving Guidance Retrieval," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 7, pp. 6504--6517, 2018.

J57.   D. Liu, **J. Ni**, X. Lin, and X. Shen, "Anonymous Group Message Authentication Protocol for LTE-based V2X Communications," *Internet Technology Letters*, vol. 1, no. 2, pp. e25, 2018. (**Invited Paper**)

J58.   K. Zhang, **J. Ni**, K. Yang, X. Liang, J. Ren, and X. Shen, "Security and Privacy for Smart City Applications: Challenges and Solutions," *IEEE Communications Magazine*, vol. 55, no. 1, pp. 122--129, Jan. 2017. (**ESI Highly Cited Paper[1], ESI Hot Paper[2]**)

J59.   Q. Jiang, **J. Ni**, J. Ma, L. Yang, and X. Shen, "Integrated Authentication and Key Agreement Framework for Vehicular Cloud Computing," *IEEE Network*, vol. 32, no. 3, pp. 28--35, 2018.

J60.   Y. He, **J. Ni**, X. Wang, B. Niu, F. Li, and X. Shen, "Privacy-preserving Partner Selection for Ride-sharing Services," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 7, pp. 5994--6005, 2018.

J61.   K. Zhang, X. Liang, **J. Ni**, K. Yang, and X. Shen, "Exploiting Social Network to Enhance Human-to-Human Infection Analysis without Privacy Leakage," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 4, pp. 607--620, 2018.

J62.   Y. Wang, X. Tao, **J. Ni**, Y. Yu, "Data Integrity Checking with Reliable Data Transfer for Secure Cloud Storage," *International Journal of Web and Grid Services*, vol. 14, no. 1, pp.106--121, 2018.

J63.   **J. Ni**, K. Zhang, K. Klharbi, X. Lin, N. Zhang, and X. Shen, "Differentially Private Smart Metering with Fault Tolerance and Range-based Filtering," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2483--2493, Sept. 2017.

J64.   **J. Ni**, A. Zhang, X. Lin, and X. Shen, "Security, Privacy and Fairness in Fog-based Vehicular Crowdsensing," *IEEE Communications Magazine*, vol. 55, no. 6, pp. 146--152, Jun. 2017.

J65.   L. Xue, **J. Ni**, Y. Li, and J. Shen, "Provable Data Transfer from Provable Data Possession and Deletion in Cloud Storage," *Computer Standards & Interfaces*, vol. 54, no. 1, pp. 46--54, Nov. 2017.

J66.   Y. Yu, Y. Li, **J. Ni**, G. Yang, Y. Mu, and W. Susilo, "Comments on Public Integrity Auditing for Dynamic Data Sharing with Multi-User Modification," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 3, pp. 658--659, Mar. 2016.

J67.   Y. Yu, **J. Ni**, Q. Xia, X. Wang, H. Yang, and X. Zhang, "SDIVIP2: Shared Data Integrity Verification with Identity Privacy Preserving in Mobile Clouds," *Concurrency and Computation: Practice and Experience*, vol. 28, no. 10, pp. 2877--2888, Jul. 2016.

J68.   Y. Zhang, **J. Ni**, X. Tao, Y. Wang, and Y. Yu, "Provable Multiple Replication Data Possession with Full Dynamics for Secure Cloud Storage," *Concurrency and Computation: Practice and Experience*, vol. 28, no. 4, pp. 1161--1173, Mar. 2016.

J69.   Y. Yu, L. Xue, M. H. Au, W. Susilo, **J. Ni**, Y. Zhang, A. V. Vasilakos, and J. Shen, "Cloud Data Integrity Checking with an Identity-based Auditing Mechanism from RSA," *Future Generation Computer System*, vol. 62, pp. 85--91, Sept. 2016.

J70.   Y. Yu, **J. Ni**, M. H. Au, Y. Mu, B. Wang, and H. Li, "Comments on a Public Auditing Mechanism for Shared Cloud Data Service," *IEEE Transactions on Services Computing*, vol. 8, no. 6, pp. 998--999, Nov.-Dec. 2015.

J71. Q. Xia, **J. Ni**, A. J. A. Kanpogninge, and J. C. Gee, "Searchable Public-key Encryption with Data Sharing in Dynamic Groups for Mobile Cloud Storage," *Journal of Universal Computer Science*, vol. 21, no. 3, pp. 440--453, 2015.

J72. Y. Yu, Y. Zhang, **J. Ni**, M. H. Au, L. Chen, and Y. Liu, "Remote Data Possession Checking with Enhanced Security for Cloud Storage," *Future Generation Computer Systems*, vol. 52, pp. 77--85, Nov. 2015.

J73. **J. Ni**, Y. Yu, Y. Mu, and Q. Xia, "On the Security of an Efficient Dynamic Auditing Protocol in Cloud Storage," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 10, pp. 2760--2761, Oct. 2014.

J74. Y. Yu, **J. Ni**, M. H. Au, H. Liu, H. Wang, and C. Xu, "Improved Security of a Dynamic Remote Data Possession Checking Protocol for Cloud Storage," *Expert System with Applications*, vol. 41, no. 17, pp. 7789--7796, Dec. 2014.

J75. Y. Yu, **J. Ni**, C. Xu, and L. Niu, "Cryptanalysis of a Secure and Efficient Identity-Based Signature Scheme," *Journal of Software*, vol. 25, no. 5, pp. 1125--1131, 2014.

J76. Y. Yu, **J. Ni**, H. Yang, Y. Mu, and W. Susilo, "Efficient Public Key Encryption with Revocable Keyword Search," *Security and Communication Networks*, vol. 7, no. 2, pp. 466--472, Feb. 2014.

J77. Y. Yu, **J. Ni**, and Y. Sun, "Security Analysis of a Distributed Reprogramming Protocol for Wireless Sensor Networks," *IEICE Transactions on Information and Systems*, vol. E96-D, no. 8, pp. 1875--1877, Aug. 2013.

J78. **J. Ni**, Y. Yu, Q. Xia, and L. Niu, "Cryptanalysis of Two Searchable Public Key Encryption Schemes with a Designated Tester," *Journal of Information and Computational Science*, vol. 9, no. 16, pp. 4819--4825, 2012.

Refereed Conference Papers

C1. N. Wang, J. Chen, **J. Ni**, L. Chen, and H. Zhou, "Leveraging Group Secret Sharing Technology for FD-RAN: A Lightweight AKA Mechanism," The IEEE 99th Vehicular Technology Conference (VTC 2024-Fall), Singapore, June 24-27, 2024.

C2. X. Li[*], M. He[*], and **J. Ni**, "Secure and Privacy-preserving Network Slicing in 3GPP 5G System Architecture," The 12th IEEE/CIC International Conference on Communications in China (ICCC 2023), Dalian, China, August 10-12, 2023.

C3. J. Zhao[*], X. Li[*], and **J. Ni**, "Privacy-Preserving Model Aggregation for Asynchronous Federated Learning" The 12th IEEE/CIC International Conference on Communications in China (ICCC 2023), Dalian, China, August 10-12, 2023.

C4. K. Khalafi, **J. Ni**, and N. Lu, "Online Convex Optimization for Dynamic RAN Slicing with Quality of Service," The 12th IEEE/CIC International Conference on Communications in China (ICCC 2023) Workshop on Edge Intelligence for 6G Networks, Dalian, China, August 10-12, 2023.

C5. B. Mosher[*], X. Li[*], Y. He, and **J. Ni**, "Verifiable and Privacy-preserving Ad Exchange for Targeted Advertising," The 20th Annual International Conference on Privacy, Security & Trust, Copenhagen, Denmark, 21-23 August 2023.

C6. B. Mosher[*] and **J. Ni**, "PAEEA: Privacy-Preserving Online Ad Exchange with Efficient Auction for Smart Advertising," Proc. of ICC 2023, Rome, Italy, 28 May-01 June 2023.

C7. Y. Liu[*], **J. Ni**, and M. Zulkernine, "AT-CBDC: Achieving Anonymity and Traceability in Central Bank Digital Currency," Proc. of ICC 2022, Seoul, South Korea, 16–20 May 2022.

C8.   Y. He, F. Wang, X. Deng, **J. Ni**, J. Feng, and S. Liu, "Ordinal Data Stream Collection with Condensed Local Differential Privacy," Proc. of HPCC, Chengdu, China, 18-20 December, 2022. (**Outstanding Paper Award**)

C9.   X. Li[*], Y. Liu[*], **J. Ni**, and Y. He, "Securing E-Petition: A Privacy-Preserving Fine-Grained Electronic Petition System for Health and Political Petitions," Proc. of ICC 2022, Seoul, South Korea, 16–20 May 2022.

C10.   J. Zhou, Z. Su, **J. Ni**，Y. Wang, Y. Pan, and R. Xin, "Personalized Privacy-Preserving Federated Learning: Optimized Trade-off Between Utility and Privacy," Proc. of GLOBECOM 2022, Rio de Janeiro, Brazil, 4-8 December 2022.

C11.   L. Liu, C. Huang, D. Zhu, D. Liu, **J. Ni**, and X. Shen, "Secure and Distributed Access Control for Dynamic Pervasive Edge Computing Services," Proc. of GLOBECOM 2022, Rio de Janeiro, Brazil, 4-8 December 2022.

C12.   Z. Peng, Y. He, Z. Sun, **J. Ni**, B. Niu, and X. Deng, "Crafting Text Adversarial Examples to Attack the Deep-Learning-based Malicious URL Detection," Proc. of ICC 2022, Seoul, South Korea, 16–20 May 2022.

C13.   M. He[*], X. Li[*], **J. Ni**, and H. Yang, "Balancing Efficiency and Security for Network Access Control in Space-Air-Ground Integrated Networks," Proc. of PST 2021, Auckland, New Zealand, Dec. 13-15, 2021.

C14.   Y. Pan, **J. Ni**, and Z. Su, "FL-PATE: Differentially Private Federated Learning with Knowledge Transfer," Proc. of IEEE GLOBECOM 2021, Madrid, Spain, Dec. 7-11, 2021.

C15.   M. He[*], **J. Ni**, D. Liu, H. Yang, and X. Shen, "Private, Fair, and Verifiable Aggregate Statistics for Mobile Crowdsensing in Blockchain Era," Proc. of IEEE/CIC ICCC 2020, Chongqing, China, Aug. 9-11, 2020. (**Best Paper Award**)

C16.   C. Zhang, L. Zhu, C. Xu, **J. Ni**, C. Huang, and X. Shen, "Efficient and Privacy-Preserving Non-Interactive Truth Discovery for Mobile Crowdsensing," Proc. of IEEE GLOBECOM 2020, Taipei, Taiwan, Dec. 7-11, 2020.

C17.   L. Xue, D. Liu, **J. Ni**, X. Lin, and X. Shen, "Consent-based Privacy-preserving Decision Tree Evaluation," Proc. of IEEE ICC 2020, Dublin, Ireland, June 7-11, 2020.

C18.   D. Liu, **J. Ni**, X. Lin, and X. Shen, "Towards Private and Efficient Ad Impression Aggregation in Mobile Advertising," Proc. of IEEE ICC 2019, Shanghai, China, May 20-24, 2019.

C19.   C. Huang, **J. Ni**, R. Lu, and X. Shen, "Online Advertising with Verifiable Fairness," Proc. of IEEE ICC 2019, Shanghai, China, May 20-24, 2019.

C20.   C. Huang, **J. Ni**, R. Lu, and X. Shen, "Exploring Anonymous User Review: Linkability Analysis with Machine Learning," Proc. of IEEE GLOBECOM 2019, Waikoloa, HI, USA, Dec. 9-13, 2019.

C21.   L. Xue, **J. Ni**, C. Huang, X. Lin, and X. Shen, "Forward Secure and Fine-grained Data Sharing for Mobile Crowdsensing," Proc. of PST 2019, Fredericton, NB, Canada, August 26-28, 2019.

C22.   J. Liang, Z. Qin, **J. Ni**, X. Lin, and X. Shen, "Efficient and Privacy-Preserving Outsourced SVM Classification in Public Cloud," Proc. of IEEE ICC 2019, Shanghai, China, May 20-24, 2019.

C23.   W. Wang, Z. Ying, **J. Ni**, X. Lin, and X. Shen, "Against Pilot Spoofing Attack with Double Channel Training in Massive MIMO NOMA Systems," Proc. of IEEE ICC 2019, Shanghai, China, May 20-24, 2019.

C24.   D. Liu, **J. Ni**, H. Li, X. Lin, and X. Shen, "Efficient and Privacy-preserving Ad Conversion for V2X-assisted Proximity Marketing," Proc. of IEEE MASS 2018, Chengdu, China, Oct. 9-12, 2018. (**Best Paper Award**)

C25. D. Liu, **J. Ni**, H. Li, and X. Shen, "Achieving Adaptive Linkability for Cellular V2X Group Communications in 5G," Proc. of IEEE GLOBECOM 2018, Abu Dhabi, UAE, Dec. 9-13, 2018.

C26. Y. He, **J. Ni**, B. Niu, F. Li, and X. Shen, "Privacy-preserving Ride Clustering for Customized-bus Sharing: A Fog-assisted Approach," Proc. of WiOpt 2018, Shanghai, China, May 7-11, 2018.

C27. C. Huang, D. Liu, **J. Ni**, R. Lu, and X. Shen, "Reliable and Privacy-Preserving Selective Data Aggregation for Fog-Based IoT," Proc. of IEEE ICC 2018, Kansas City, MO, USA, May 20-24, 2018. (**Best Paper Award**)

C28. **J. Ni**, X. Lin, and X. Shen, "Privacy-Preserving Data Forwarding in VANETs: A Personal-Social Behavior Based Approach," Proc. of IEEE GLOBECOM 2017, Singapore, Dec. 4--8, 2017. (**Best Paper Award**)

C29. **J. Ni**, X. Lin, Q. Xia, and X. Shen, "Dual-Anonymous Reward Distribution for Mobile Crowdsensing," Proc. of IEEE ICC 2017, Paris, France, May 21--25, 2017.

C30. **J. Ni**, K. Zhang, X. Lin, Q. Xia, and X. Shen, "Privacy-Preserving Mobile Crowdsensing for Location-Based Applications," Proc. of IEEE ICC 2017, Paris, France, May 21--25, 2017.

C31. A. Alamer, **J. Ni**, X. Lin, and X. Shen, "Location Privacy-Aware Task Recommendation for Spatial Crowdsourcing," Proc. of WCSP 2017, Nanjing, China, Oct. 11--13, 2017. (**Best Paper Award**)

C32. **J. Ni**, K. Zhang, X. Lin, Y. Yu, and X. Shen, "CPARN: Cloud-Based Privacy-Preserving Parking Navigation in Vehicular Ad Hoc Networks," Proc. of EAI SECURECOMM 2016, Guangzhou, China, Oct. 10--12, 2016. (**Best Paper Award**)

C33. **J. Ni**, X. Lin, K. Zhang, and Y. Yu, "Secure and Deduplicated Spatial Crowdsourcing: A Fog-Based Approach," Proc. of IEEE GLOBECOM 2016, Washington D.C., USA, Dec. 4--8, 2016.

C34. **J. Ni**, X. Lin, K. Zhang, and X. Shen, "Privacy-Preserving Real-Time Navigation System Using Vehicular Crowdsourcing," Proc. of IEEE VTC-Fall 2016, Montreal, Canada, Sept. 18--21, 2016. (**Invited Paper**)

C35. **J. Ni**, X. Lin, K. Zhang, Y. Yu, and X. Shen, "Secure Outsourced Data Transfer with Integrity Verification in Cloud Storage," Proc. of IEEE/CIC ICCC 2016, Chengdu, China, Jul. 27--29, 2016.

C36. **J. Ni**, K. Zhang, X. Lin, H. Yang, and X. Shen, "AMA: Anonymous Mutual Authentication with Traceability in Carpooling Systems," Proc. of IEEE ICC 2016, Kuala Lumpur, Malaysia, May 23--27, 2016.

C37. **J. Ni**, X. Lin, K. Zhang, Y. Yu, and X. Shen, "Device-Invisible Two-Factor Authenticated Key Agreement for BYOD," Proc. of IEEE/CIC ICCC 2016, Chengdu, China, Jul. 27--29, 2016.

C38. **J. Ni**, K. Zhang, X. Lin, and X. Shen, "EDAT: Efficient Data Aggregation without TTP for Privacy-Assured Smart Metering," Proc. of IEEE ICC 2016, Kuala Lumpur, Malaysia, May 23--27, 2016.

C39. Y. Yu, **J. Ni**, W. Wu, and Y. Wang, "Provable Data Possession Supporting Secure Data Transfer for Cloud Storage," Proc. of BWCCA 2015, Poland, Nov. 4--6, 2015. (**Best Paper Award**)

C40. **J. Ni**, K. Alharbi, X. Lin, and X. Shen, "Security-Enhanced Data Aggregation against Malicious Gateways in Smart Grid," Proc. of IEEE GLOBECOM 2015, San Diego, CA, USA, Dec. 6--10, 2015.

C41. Y. Yu, M. Yi, **J. Ni**, J. Deng, and K. Huang, "Identity Privacy-Preserving Public Auditing with Dynamic Group for Secure Mobile Cloud Storage," Proc. of NSS 2014, Xi'an, China, Oct. 15--17, 2014.

C42. Y. Yu, **J. Ni**, J. Ren, W. Wu, L. Chen, and Q. Xia, "Improvement of a Remote Data Possession Checking Protocol from Algebraic Signatures," Proc. of ISPEC 2014, Fuzhou, China, May 5--8, 2014.

C43. Y. Li, Q. Xia, **J. Ni**, and Y. Yu, "A New Construction of Proxy Signature Using Chameleon Hash Function," Proc. of IEEE INCoS 2013, Xi'an, China, Sept. 9--11, 2013.

C44. Y. Sun, J. Chai, H. Liang, **J. Ni**, and Y. Yu, "A Secure and Efficient E-Cheque Protocol from Chameleon Hash Function," Proc. of IEEE INCoS 2013, Xi'an, China, Sept. 9--11, 2013.

C45. L. Niu, Y. Yu, **J. Ni**, and Y. Sun, "Further Cryptanalysis of a Signature Scheme with Message Recovery," Proc. of IEEE INCoS 2012, Bucharest, Romania, Sept. 19--21, 2012.

Invited Research Seminars

S1. Privacy and Regulatory Compliance for Digital Currency, IEEE Communication Society CISTC Webinar Series, May 24, 2023.

S2. Secure and Distributed Access Control for Dynamic Pervasive Edge Computing Services, invited by Prof. Aiqing Zhang, Anhui Normal University, China, Tencent Meeting, December 05, 2022.

S3. Machine Learning in Cybersecurity, invited by Prof. Man Ho Au, Hong Kong University, Hong Kong, Zoom Meeting, Jan. 18, 2022.

S4. Security and Privacy in Mobile Edge Caching, invited by Prof. Chengcheng Zhao, Zhejiang University, Hangzhou, China, Jun. 20, 2021.

S5. Security and Privacy in Mobile Edge Caching, invited by Prof. Haibo Zhou, Nanjing University, Nanjing, China, Jul. 2, 2021.

S6. Security and Privacy in Mobile Edge Caching, invited by Prof. Feng Lyu, Central South University, Changsha, China, Jun. 18, 2021.

S7. Security and Privacy in Mobile Edge Caching, invited by Debiao He, Wuhan University, Wuhan, China, Jul. 8, 2021.

S8. Security and Privacy in Mobile Edge Caching, invited by Prof. Peng Yang, Huazhong University of Science and Technology, Wuhan, China, Jun. 15, 2021.

S9. Security and Privacy in Mobile Edge Caching, invited by Prof. Meng Li, Anhui University of Technology, Hefei, China, Jul. 3, 2021.

S10. Security and Privacy in Mobile Edge Caching, invited by Prof. Fei Ji, South China University of Technology, Guangzhou, China, Jul. 5, 2021.

S11. Security and Privacy for Mobile Edge Caching: Challenges and Solutions, invited by Prof. Nan Cheng, Xidian University, China, Tencent Meeting, Dec. 6, 2020.

S12. Security and Privacy for Mobile Edge Caching: Challenges and Solutions, invited by Prof. Aiqing Zhang, Anhui Normal University, China, Tencent Meeting, Nov. 23, 2020.

S13. Security and Privacy for Mobile Edge Caching: Challenges and Solutions, invited by Prof. Kai Fan, Xidian University, Xi'an, China, Tencent Meeting, May 14, 2020.

S14. Towards Privacy-preserving Valet Parking in Autonomous Driving Era, invited by Prof. Yong Yu, Shaanxi Normal University, Xi'an, China, Jun. 5, 2019.

S15. Towards Privacy-preserving Valet Parking in Autonomous Driving Era, invited by Prof. Qi Jiang, Xidian University, Xi'an, China, Jun. 4, 2019.

S16. Secure Data Analytics and User Privacy in Crowdsensing, invited by Prof. Li Yu, Huazhong University of Science and Technology, Wuhan, China, May 20, 2019.

S17. Secure Data Analytics and User Privacy in Crowdsensing, invited by Prof. Pu Xiao, Nanjing University of Posts & Telecommunications, Nanjing, China, May 16, 2019.

S18. Secure Data Analytics and User Privacy in Crowdsensing, invited by Prof. Rongxing Lu, University of New Brunswick, Canada, Jan. 10, 2019.

S19. Secure Data Analytics and User Privacy in Crowdsensing, invited by Prof. Ping Wang, York University, Canada, March. 15, 2019.

S20. Secure Data Analytics and User Privacy in Crowdsensing, invited by Prof. Lin Cai, University of Victoria, Canada, Nov. 19, 2018.

S21. Secure Data Analytics and User Privacy in Crowdsensing, invited by Prof. Man Ho Au, The Hong Kong Polytechnic University, Hong Kong, China, Nov. 30, 2018.

S22. Cloud-Based Privacy-Preserving and Trustworthy Parking Navigation, invited by Prof. Yong Yu, Shaanxi Normal University, Xi'an, China, Aug. 10, 2018.

S23. Security and Privacy Preservation for Mobile Crowdsensing, invited by Yong Yu, Shaanxi Normal University, Xi'an, China, Dec. 10, 2017.

S24. Security and Privacy Preservation for Mobile Crowdsensing, invited by Prof. Qi Jiang, Xidian University, Xi'an, China, Dec. 10, 2017.

S25. Secure and Deduplicated Spatial Crowdsourcing: A Fog-Based Approach, invited by Prof. Yuan Wu, Zhejiang University of Technology, Hangzhou, China, Nov. 30, 2017.

S26. Balancing Security and Efficiency for Smart Metering against Misbehaving Collectors, invited by Prof. Liping Qian, Zhejiang University of Technology, Hangzhou, China, July 27, 2016.

V. Course Development

<u>Undergraduate Course ELEC 473 Cryptography and Network Security</u>

Cryptography topics include: block ciphers, advanced encryption standard, public key encryption, hash functions, message authentication codes, digital signatures, key management and distribution, public-key infrastructure. Network security topics include: user authentication, network access control, Kerberos protocol, transport layer security (TLS), and IP security (IPsec).

<u>Graduate Course ELEC 877 AI for Cybersecurity</u>

This course covers the fundamentals of cybersecurity and machine learning, selected topics in machine learning for cybersecurity, including anomaly detection, malware analysis, network traffic analysis, and fake news defense, and the advanced topics in artificial intelligence (AI) security, including privacy-preserving AI, fairness in AI, and adversarial machine learning.

<u>eCampusOntario Open Educational Source</u>

The ethics module for artificial intelligence (AI) engineering targets specifically to undergraduate students in Electrical and Computer Engineering. The module includes introduction and professional ethics (lead by T. Dean), AI bias (lead by J. Ni), decision harm and radicalization (lead by J. Ni), privacy leakage in AI (lead by T. Dean), and AI misuse and mitigation (lead by T. Dean). This module is co-designed by the subject matter experts from Queen's University, University of Windsor, and McMaster University.

Record of Courses Taught

Term	Number	Title	Enrollment	Level	Course Notes
Fall18	CP460	Applied Cryptography	67	undergraduate	New
Win20	SOFT 423	Software Requirements	94	undergraduate	Updated
Fall20	ELEC 473	Cryptography and Network	73	undergraduate	New

		Security			
Win21	ELEC 877	AI for Cybersecurity	10	graduate	New
Fall21	ELEC 473	Cryptography and Network Security	71	undergraduate	
Win22	SOFT 423	Software Requirements	70	undergraduate	
Win22	ELEC 877	AI for Cybersecurity	15	graduate	
Fall22	ELEC 278 (001)	Fundamentals of Information Structures	189	undergraduate	Updated
Fall 22	ELEC 473	Cryptography and Network Security	73	undergraduate	
Win23	ELEC 877	AI for Cybersecurity	16	graduate	
Fall23	ELEC 278 (001)	Fundamentals of Information Structures	222	undergraduate	
Fall23	ELEC 473	Cryptography and Network Security	118	undergraduate	
Win24	ELEC 877	AI for Cybersecurity	16	graduate	