MURTUZA S. JADLIWALA

CONTACT INFORMATION

San Pedro 1 (SP1) 310E,
The University of Texas at San Antonio,
506 Dolorosa St.,
San Antonio, TX 78204, USA.

Phone: +1-210-458-5693
Fax: +1-210-458-4437
E-mail: murtuza.jadliwala@utsa.edu
WWW: https://sprite.utsa.edu/people/mjadliwala/

EMPLOYMENT HISTORY

The University of Texas at San Antonio (UTSA), San Antonio, TX, USA

- *Associate Professor in the Department of Computer Science* **September 2021 - current**
- *Assistant Professor in the Department of Computer Science* **January 2018 - August 2021**

Wichita State University (WSU), Wichita, KS, USA

- *Assistant Professor in the Electrical Engg. and Computer Science Dept.* **January 2012 - December 2017**

Swiss Federal Institute of Technology (EPFL), Lausanne, Switzerland

- *Lecturer in the School of Computer and Communication Sciences* **September, 2011 - December, 2011**
- *Research Scientist in the School of Computer and Communication Sciences* **September, 2008 - September, 2011**

State University of New York at Buffalo (SUNY Buffalo), Buffalo, NY, USA

- *Graduate Assistant in the Dept. of Computer Science and Engg.* **August, 2003 - May 2008**

Investment Research and Information Services Ltd., Mumbai, India

- *Software Engineer and Technical Leader* **June, 2000 - June 2002**

EDUCATION

State University of New York at Buffalo, Buffalo, NY, USA

- Ph.D., Computer Science & Engineering, September 2008.
- M.S., Computer Science, June 2004.

Mumbai University, Mumbai, India

- B.E., Computer Engineering, June 2000.

HONORS AND AWARDS

- **UTSA Cloud Technology Endowed Fellowship**, 2022-2023.
- **UTSA CS Department Annual Faculty Research Award**, 2022.
- **NSF CAREER Award**, 2020.
- **Dwane and Velma Wallace Excellence in Teaching Award**, 2017.
- **Finalist for the Wichita State University Academy for Effective Teaching (AET) award -** This is a student nominated teaching award.
- **U.S. Air Force Office of Scientific Research Summer Faculty Fellowship**, 2015. Fellowship included a stipend of approximately $\$15K$ to perform research on wearable device security at the AFRL Information Institute in Rome, NY.
- **Wichita State University Award for Research/Creative Projects**, 2014. Award included a $\$4K$ seed grant for research in online social network security and privacy.
- **Nokia Invention Awards** in 2010 and 2011.
- **Graduate Student Research Award** for outstanding research activities, SUNY Buffalo, August 2005.

Research Interests

All aspects of cyber and cyber-physical systems security & user-privacy, with a special focus on the topics of Mobile & IoT Security, Distributed Systems Security, Privacy Enhancing Technologies, Incentive-based Mechanism Design for Security, Adversarial Machine Learning and Design of Mobile/Ubiquitous Sensing Algorithms, Systems and Applications.

Research Projects & Funding

- **PI**: "Collaborative Research: CISE-MSI: Active and Passive Internet Measurements for Inferring IoT Maliciousness at Scale", sponsored by National Science Foundation (NSF), PI Share: $12,500 (Project Total: $259,999) from October 2022 - September 2025. Through PI Transfer, Former PI: Elias Bou-Harb (Louisiana State Univeristy).
- **PI**: "OAC Core: Small: Devising Data-driven Methodologies by Employing Large-scale Empirical Data to Fingerprint, Attribute, Remediate and Analyze Internet-scale IoT Maliciousness", sponsored by National Science Foundation (NSF), PI Share: $51,990 (Project Total: $496,898) from August 2019 - July 2024. Through PI Transfer, Former PI: Elias Bou-Harb (Louisiana State Univeristy).
- **Co-PI**: "PARTNER: Neuro-Inspired AI for the Edge at UTSA (NAIAD)", sponsored by National Science Foundation (NSF), UTSA Share: $2,080,000 (Project Total: $2,800,000) from October 2023 - September 2026. Lead-PI: Dhireesha Kudithipudi (UTSA), Co-PIs: Fidel Santamaria and Panagiotis Markopoulos (UTSA), Hai Li (Duke).
- **PI (UTSA)**: "Organization of a Summer School on Modern Trends in Cybersecurity and Privacy", sponsored by the German Academic Exchange Service (DAAD), Project Total: 25,000 Euros from December 2022 - December 2023. Co-PI: Ahmad Reza-Sadeghi (TU-Darmstadt, Germany).
- **PI (UTSA)**: "Collaborative Research: CISE-MSI: DP: CNS: Multi-Modal User-Centric Mobility Scooter Driving Safety Assessment System", sponsored by National Science Foundation (NSF), UTSA Share: $125,771 (Project Total: $600,000) from October 2023 - September 2026. Lead-PI: Tingting Chen (Cal Poly Pomona), Co-PIs: Amar Raheja and Mai Jara (Cal Poly Pomona).
- **Lead PI**: "Collaborative Research: CCRI: New: ScooterLab - A Programmable and Participatory Sensing Testbed using Micromobility Vehicles", sponsored by National Science Foundation (NSF), UTSA Share: $1,713,162 (Project Total: $1,919,062) from March 2023 - February 2026. Co-PIs: Greg Griffin, Sushil Prasad (University of Texas at San Antonio) and Anindya Maiti (University of Oklahoma).
- **Co-PI**: "EAGER: DCL: SaTC: Enabling Interdisciplinary Collaboration: Studying Social Engineering Attacks Targeting Vulnerable Refugee Populations", sponsored by National Science Foundation (NSF), $296,470 from July 2022 - June 2024. PI: Mythili Menon (Wichita State University).
- **Co-PI**: "Joint Cyber Command & Control (JCC2)", MITRE Corporation, $50,000 from May 2021 - September 2021. PI: John Huggins (University of Texas at San Antonio), Co-PI: Heena Rathore (University of Texas at San Antonio).
- **PI**: "Addressing Security and Privacy Challenges in Visual Augmented Reality (VAR)", Grant for Research Advancement and Transformation (GREAT) sponsored by UTSA Vice President for Research, Economic Development, and Knowledge Enterprise (VPREDKE), $20,000 from October 2021 - July 2022. Co-PI: Xiaoyin Wang (University of Texas at San Antonio).
- **PI**: "CCRI: Planning: ScooterLab: Development of a Programmable and Participatory e-Scooter Testbed to Enable CISE-focused Micromobility Research", sponsored by National Science Foundation (NSF), $100,000 from August 2020 - February 2022. Co-PIs: Greg Griffin, Sushil Prasad (University of Texas at San Antonio) and Anindya Maiti (University of Oklahoma).
- **PI**: "CAREER: A Holistic Context-based Approach for Security and Privacy in the Era of Ubiquitous Sensing and Computing", sponsored by National Science Foundation (NSF), $499,512 from June 2020 - May 2025.
- **PI**: "CSR: Small: Surviving Cybersecurity and Privacy Threats in Wearable Mobile Cyber-Physical Systems", sponsored by National Science Foundation (NSF), $419,044 from October 2015 - October 2020. Co-PI: Jibo He (Wichita State University).
- **PI**: "ROBOT: Rules Oriented Blockchain Operations Transactor, sponsored by NASA STTR and subcontracted by Emergent Space Technologies, $35,000 from September 2019 - August 2020. Co-PI: Raymond Choo (University of Texas at San Antonio).
- **PI**: "EAGER: A Cloud-assisted Framework for Improving Pedestrian Safety in Urban Communities using Crowd-sourced Mobile and Wearable Device Data", sponsored by National Science

Foundation (NSF), $179,843 from July 2016 - July 2019. Co-PI: Jibo He (Wichita State University).
- **PI**: "Surviving Cybersecurity Threats in the Era of Modern Wearable Cyber-Physical Systems", Summer Extension Grant sponsored by Information Institute, US Air Force Research Lab (AFRL), $9833 from September - October 2015.
- **PI**: "Social Puzzles: Context-Based Access Control in Online Social Networks", Award for Research/Creative Projects in Summer sponsored by Office of Research and Technology Transfer, Wichita State University, $4000 from May - July 2014.
- **Co-PI**: "Towards a Privacy-Aware Information-Sharing Framework for Advanced Metering Infrastructures", sponsored by Power Systems Energy Research Cener (PSERC), an NSF Industry-University Cooperative Research Center, $220,000 from June 2013 - August 31, 2015. PI: Vinod Namboodiri (Wichita State University), Co-PIs: Murtuza Jadliwala, Visvakumar Aravinthan (Wichita State University) and Lalitha Sankar (Arizona State University).

Research Experience

The University of Texas at San Antonio and Wichita State University

- *Director of Security, Privacy, Trust and Ethics in Computing Research Lab (SPriTELab)* **January, 2012 - current**
  Current research projects can be found at: http://sprite.utsa.edu/
- *Machine Learning & Deployment Thrust Lead, MATRIX - UTSA AI Consortium for Human Well-Being* **July, 2020 - current**
  More details at: http://ai.utsa.edu/

Swiss Federal Institute of Technology, Lausanne, Switzerland

- *Postdoctoral Research Fellow* **September, 2008 - December, 2011**
  Projects undertaken can be found at: http://lca.epfl.ch/projects/privacy-mobile-pervasive/

State University of New York at Buffalo, Buffalo, NY, USA

- *Research Assistant at the Center of Excellence in Information Systems Assurance Research and Education (Dept. of CSE, SUNY Buffalo)* **August, 2004 - 08**

Publications

Refereed Journal and Magazine Articles
(† indicates solely supervised students, ‡ indicates co-supervised students)

- Shah, D., Huang, R., Vinayaga-Sureshkanth, N., Chen, T., Jadliwala, M., "ScooterID: Posture-based Continuous User Identification from Mobility Scooter Rides", in IEEE Transactions on Mobile Computing, 2024.
- Rajabi, T., Khalil, A A., Manshaei, M H., Rahman, M A., Dakhilalian, M., Ngouen, M., Jadliwala, M., and Uluagac, S., "Feasibility Analysis for Sybil Attacks in Shard-Based Permissionless Blockchains", in ACM Distributed Ledger Technology: Research and Practice (DLT), 2023.
- Wijewickrama, R., Dohadwalla, S., Maiti, A., Jadliwala, M., and Narain, S., "SkinSense: Efficient Vibration-based Communications Over Human Body Using Motion Sensors", in Elsevier Internet of Things, 2023.
- Rathore, H., Samant, A., Jadliwala, M., "TangleCV: A Distributed Ledger Technique for Secure Message Sharing in Connected Vehicles", in ACM Transactions on Cyber-Physical Systems (TCPS), 2020.
- Maiti, A.†, and Jadliwala, M., "Smart Light-based Information Leakage Attacks", in ACM GetMobile: Mobile Comp. and Comm. 24, 1 (March 2020), 28-32, 2020. Invited Magazine Article for the ACM IMWUT (UbiComp 2019) Paper.
- Zhu, A., Cao, S., Yao, H., Jadliwala, M., and He, J., "Can Wearable Devices Facilitate a Driver's Brake Response Time in a Classic Car-Following Task?", in IEEE Access, 2020.
- Maiti, A.†, and Jadliwala, M., Light Ears: Information Leakage via Smart Lights, in the Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT), Volume 3, Number 3, Article 98, pp. 98:01-98:27, 2019 (presented at ACM UbiComp 2019).
- Vinayaga-Sureshkanth, N.†, Maiti, A.†, Jadliwala, M., Crager, K.‡, He, J., and Rathore, H., A Practical Framework for Preventing Distracted Pedestrian-related Incidents using Wrist Wearables, in IEEE Access, 2018.

- Manshaei, M.H., Jadliwala, M., Maiti, A.†, and Fooladgar, M., A Game-Theoretic Analysis of Shard-Based Permissionless Blockchains, in IEEE Access, 2018.
- Maiti, A.†, Jadliwala, M., He, J., and Bilogrevic, I., "Side-Channel Inference Attacks on Mobile Keypads using Smartwatches", in the IEEE Transactions on Mobile Computing (TMC), 2018.
- He, J., McCarley, J., Crager, K.‡, Jadliwala, M., and Hua, L., "Do Wearable Devices Bring Distraction Closer to Drivers? Comparing Smartphones and Google Glass", in Applied Ergonomics, 2018.
- Bagai, R., Malik, N.‡, and Jadliwala, M., "Measuring Anonymity of Pseudonymized Data after Probabilistic Background Attacks", in the IEEE Transactions on Information Forensics and Security (TIFS), Vol. 12, Nr. 5, pp. 1156-1169, May 2017.
- Boustani, A.†, Maiti, A.†, Yousefian Jazi, S., Jadliwala, M., and Namboodiri, V., "Seer Grid: Privacy and Utility Implications of Two-Level Load Prediction in Smart Grids", in the IEEE Transactions on Parallel and Distributed Systems (TPDS), 2017.
- Bilogrevic, I., Huguenin, K., Agir, B., Jadliwala, M., Gazaki, M., and Hubaux, J-P., "A Machine-Learning Based Approach to Privacy-Aware Information-Sharing in Mobile Social Networks", in Pervasive and Mobile Computing (PMC), Elsevier, 2016.
- Karimi, B., Namboodiri, V., and Jadliwala, M., "Scalable Meter Data Collection in Smart Grids through Message Concatenation", in the IEEE Transactions on Smart Grids (TSG), 2015.
- Bilogrevic, I., Jadliwala, M., Joneja, V., Kalkan, K., Hubaux, J.-P. and Aad, I., "Privacy-Preserving Optimal Meeting Location Determination on Mobile Devices", accepted in IEEE Transactions on Information Forensics and Security (TIFS), 2014.
- Jadliwala, M., Bilogrevic, I. and Hubaux, J-P., "Optimizing Mix-zone Coverage in Pervasive Wireless Networks", in the Journal of Computer Security (JCS), Vol. 21, No. 3, pp. 317-346, IOS Press, 2013.
- Freudiger, J., Jadliwala, M., Hubaux, J-P., Niemi, V., and Ginzboorg, P., Privacy of Community Pseudonyms in Wireless Peer-to-Peer Networks, ACM/Springer Mobile Networks and Applications (MONET): Special Issue on Context-Awareness of Mobile Systems, Vol. 18, No. 3, pp. 413-428, Springer-Verlag, 2012.
- Bilogrevic, I., Jadliwala, M., Kumar, P., Walia, SS., Hubaux, J-P., Aad, I. and Niemi, V., "Meetings through the Cloud: Privacy-Preserving Scheduling on Mobile Devices", Elsevier Journal of Systems and Software, Special Issue on 'Mobile Applications: Status and Trends', Vol. 84, pp. 1910-1927, 2011.
- Jadliwala, M., Zhong, S., Upadhyaya, S., Qiao, C. and Hubaux, J-P., "Secure Distance-Based Localization in the Presence of Cheating Beacon Nodes", IEEE Transactions on Mobile Computing (TMC), Vol. 9, Nr. 6, pp. 810-823, 2010.
- Jadliwala, M., Duan, Q., Xu, J. and Upadhyaya, S. (2007) "On Extracting Consistent Graphs in Wireless Sensor Networks", International Journal of Sensor Networks (IJSNET): Special Issue on Theoretical and Algorithmic Aspects in Sensor Networks, Vol. 2, Nos. 3/4, pp.149-162, 2007.

Refereed Conference Proceedings

(† indicates solely supervised students, ‡ indicates co-supervised students, * indicates equally contributing authors)

- Kumari, K.†, Abbasihafshejani, M.†, Pegoraro, A., Rieger, P., Arshi, K., Jadliwala, M., Sadeghi, A-R., "Voice Deepfake Detection using Micro-Frequency and Compositional Analysis", Network & Distributed System Security Symposium (NDSS), 2025.
- Kumari, K.†, Jadliwala, M., Jha, S., and Maiti, A., "Towards a Game-theoretic Understanding of Explanation-based Membership Inference Attacks", Conference on Game Theory and AI for Security (GameSec), 2024.
- Sabra, M.†, Vinayaga Sureshkanth, N.†, Sharma, A., Maiti, A., and Jadliwala, M., "De-anonymizing VR Avatars using Non-VR Motion Side-channels", ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec), 2024.
- Abdullah, S., Cheruvu, A., Kanchi, S., Chung, T., Gao, P., Jadliwala, M., and Viswanath, B., "An Analysis of Recent Advances in Deepfake Image Detection in an Evolving Threat Landscape", 45^{th} IEEE Symposium on Security and Privacy (S&P), 2024.
- Sendner, C., Stang, J., Dmitrienko, A., Wijewickrama, R.†, and Jadliwala, M., "MirageFlow: A New Bandwidth Inflation Attack on Tor", Network & Distributed System Security Symposium

(NDSS), 2024.

- Abbasi, M.†, Manshaei, M H., and Jadliwala, M., "Detecting and Punishing Selfish Behavior during Gossiping in Algorand Blockchain", IEEE Virtual Conference on Communications (VCC), 2023.
- Kumari, K.†, Rieger, P., Fereidooni, H., Jadliwala, M., and Sadeghi, A-R., "BayBFed: Bayesian Backdoor Defense for Federated Learning", to appear in the proceedings of the 44^{th} IEEE Symposium on Security and Privacy (S&P), 2023.
- Sabra, M.†, Maiti, A.†, and Jadliwala, M., "Background Buster: Peeking through Virtual Backgrounds in Online Video Calls", in the proceedings of the IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2022.
- Vinayaga-Sureshkanth, N.†, Wijewickrama, R.†, Maiti, A.†, and Jadliwala, M., "An Investigative Study on the Privacy Implications of Mobile E-scooter Rental Apps", in the proceedings of the ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec), 2022.
- Abbasi, M., Manshaei, M.H., Rahman, M.A., Akkaya, K., and Jadliwala, M., "On Algorand Transaction Fee: Challenges and Mechanism Design", in the proceedings of the IEEE International Conference on Communications (ICC), 2022.
- Wijewickrama, R.†, Maiti, A.†, and Jadliwala, M., "Write to Know: On the Feasibility of Wrist Motion based User-Authentication from Handwriting", in the proceedings of the ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec), June 2021.
- Ramesh, S., Rui, X., Maiti, A.†, Lee, J.T., Ramprasad, H., Kumar, A., Jadliwala, M., and Han, J., "Acoustics to the Rescue: Physical Key Inference Attack Revisited", in the proceedings of the USENIX Security Symposium (SECURITY), 2021.
- Sabra, M.†, Maiti, A.†, and Jadliwala, M., "Zoom on the Keystrokes: Exploiting Video Calls for Keystroke Inference Attacks", in the proceedings of the Network & Distributed System Security Symposium (NDSS), 2021.
- Fooladgar, M., Manshaei, H., Jadliwala, M., and Rahman, MA., "On Incentive Compatible Role-based Reward Distribution in Algorand", in the proceedings of the 50^{th} IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), Valencia, Spain, June 2020.
- Kumari, K.†, Jadliwala, M., Maiti, A.†, and Manshaei, H., "Analyzing Defense Strategies Against Mobile Information Leakages: A Game-Theoretic Approach", in the proceedings of the 10^{th} Conference on Decision and Game Theory for Security (GameSec), Stockholm, Sweden, October 2019.
- Wijewickrama, R.†, Maiti, A.†, and Jadliwala, M., "deWristified: Handwriting Inference Using Wrist-Based Motion Sensors Revisited", in the proceedings of the 12^{th} ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec), Miami, Florida, USA, May 2019.
- Maiti, A.†, Heard, R.†, Sabra, M.†, and Jadliwala, M., "Towards Inferring Mechanical Lock Combinations using Wrist-Wearables as a Side-Channel", in the proceedings of the 11^{th} ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec), Stockholm, Sweden, June 2018.
- Maiti, A.†, Armbruster, O.†, Jadliwala, M., and He, J., "Smartwatch-Based Keystroke Inference Attacks and Context-Aware Protection Mechanisms", in the proceedings of the 11^{th} ACM Asia Conference on Computer and Communications Security (ASIACCS), Xi'an, China, May-June 2016.
- Maiti, A.†, Jadliwala, M., He, J., and Bilogrevic, I., "(Smart)Watch Your Taps: Side-Channel Keystroke Inference Attacks using Smartwatches", in the proceedings of the 19^{th} Annual International Symposium on Wearable Computers (ISWC), Osaka, Japan, 2015.
- Boustani, A.†, Jadliwala, M. Kwon, H.and Alamatsaz, N.†, "Optimal Resource Allocation in Cognitive Smart Grid Network", in the proceedings of the 12^{th} Annual IEEE Consumer Communications and Networking Conference (CCNC 2015), Las Vegas, Nevada, 2015.
- Jadliwala, M., Maiti, A.† and Namboodiri, V., "Social Puzzles: Context-Based Access Control in Online Social Networks", in the proceedings of the 44^{th} Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), Atlanta, Georgia, USA, 2014.
- Alamatsaz, N.†, Boustani, A.†, Jadliwala, M. and Namboodiri, V., AgSec: Secure and Efficient CDMA-based Aggregation for Smart Metering Systems. in the proceedings of the 11^{th} Annual IEEE Consumer Communications and Networking Conference (CCNC 2014), Las Vegas, Nevada, 2014.

- Boustani, A.†, Alamatsaz, N.†, Jadliwala, M. and Namboodiri, V., LocJam: A Novel Jamming-based Approach to Secure Localization in Wireless Networks. in the proceedings of the 11^{th} Annual IEEE Consumer Communications and Networking Conference (CCNC 2014), Las Vegas, Nevada, 2014.
- Karimi, B., Namboodiri, V. and Jadliwala, M., "On the Scalable Collection of Metering Data in Smart Grids through Message Concatenation", in the proceedings of the IEEE International Conference on Smart Grid Communications - Symposium on Communication Networks for Smart Grids and Smart Metering (SmartGridComm 2013), Vancouver, Canada, 2013.
- Bilogrevic, I., Huguenin, K., Agir, B., Jadliwala, M. and Hubaux, J-P., "Adaptive Information-Sharing for Privacy-Aware Mobile Social Networks", in the proceedings of the 2013 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp 2013), Zurich, Switzerland, 2013.
- Badruddoza, A., Namboodiri, V. and Jadliwala, M., "On the Energy Efficiency of Dynamic Spectrum Access under Dynamic Channel Conditions", in the proceedings of the 2013 International Conference on Cognitive Radio Oriented Wireless Networks (CROWNCOM 2013), Washington DC, 2013.
- Bilogrevic, I., Jadliwala, M., Lam, I., Aad, I., Ginzboorg, P., Niemi, V., Bindschaedler, L., and Hubaux, J-P., "Big Brother Knows Your Friends: on Privacy of Social Communities in Pervasive Networks", in the Proceedings of the 10th International Conference on Pervasive Computing (PERVASIVE 2012), Newcastle, UK, 2012.
- Bindschaedler, L.*,‡, Jadliwala, M.*, Bilogrevic, I., Aad, I., Ginzboorg, P., Niemi, V. and Hubaux, J-P., "Track Me If You Can: On the Effectiveness of Context-based Identifier Changes in Deployed Mobile Networks", in the Proceedings of the 19^{th} Annual Network & Distributed System Security Symposium (NDSS 2012), San Diego, USA, 2012.
- Jadliwala, M., Bilogrevic, I. and Hubaux, J-P., "Optimizing Mixing in Pervasive Networks: A Graph-Theoretic Perspective", in the Proceedings of the 16^{th} European Symposium on Research in Computer Security (ESORICS 2011), Leuven, Belgium, 2011.
- Bilogrevic, I., Jadliwala, M., Kalkan, K., Hubaux, J-P. and Aad, I., "Privacy in Mobile Computing for Location-Sharing-Based Services", in the Proceedings of the 11^{th} Privacy Enhancing Technologies Symposium (PETS 2011), Waterloo, Ontario, 2011.
- Bilogrevic, I., Jadliwala, M., Hubaux, J-P., Aad, I. and Niemi, V., "Privacy-Preserving Activity Scheduling on Mobile Devices", in the Proceedings of the 1^{st} ACM Conference on Data and Application Security and Privacy (CODASPY 2011), San Antonio, Texas, 2011.
- Jadliwala, M., Duan, Q., Upadhyaya, S. and Xu, J., "Towards a Theory for Securing Time Synchronization in Wireless Sensor Networks", in the Proceedings of the 2^{nd} ACM Conference on Wireless Network Security (WiSec 2009), pages: 201-212, Zurich, Switzerland, 2009.
- Zhong, S., Jadliwala, M., Upadhyaya, S. and Qiao, C., "Towards a Theory of Robust Localization against Malicious Beacon Nodes", in the Proceedings of The 27^{th} IEEE International Conference on Computer Communication (INFOCOM 2008), pages: 1391-1399, Phoenix, Arizona, April 15-17, 2008.
- Jadliwala, M., Upadhyaya, S. and Taneja, M., "ASFALT: A Simple Fault-Tolerant Signature-based Localization Technique for Emergency Sensor Networks", in the Proceedings of The 26^{th} IEEE International Symposium on Reliable Distributed Systems (SRDS 2007), pages: 3-12, Beijing, CHINA, October 10-12, 2007.
- Virendra M., Jadliwala M., Chandrasekaran M., Upadhyaya S., "Quantifying Trust in Mobile Ad-Hoc Networks", In Proceedings of the IEEE International Conference on Integration of Knowledge Intensive Multi-agent Systems (KIMAS'05), Waltham, MA, Apr 2005, pp. 65-71.
- Braynov, S. and Jadliwala, M. 2004. "Detecting Malicious Groups of Agents", in proceedings of the 1^{st} IEEE Symposium on Multi-agent Security and Survivability, Drexel University, Philadelphia, PA, USA, 2004.

Refereed Workshop Proceedings

(† indicates solely supervised students, ‡ indicates co-supervised students, * indicates equally contributing authors)

- Maiti, A.*,‡, Vinayaga-Sureshkanth, N.*,‡, Jadliwala, M., Wijewickrama, R., and Griffin, G., "Impact of E-Scooters on Pedestrian Safety: A Field Study Using Pedestrian Crowd-Sensing",

IEEE PerCom Workshop on Sensing Systems and Applications using Wrist Worn Smart Devices (WristSense), 2022.

- Vinayaga-Sureshkanth, N.†, Wijewickrama, R.†, Maiti, A.†, and Jadliwala, M., "Security and Privacy Challenges in Upcoming Intelligent Urban Micromobility Transportation Systems", in the proceedings of the 2nd ACM Workshop on Automotive and Aerial Vehicle Security (AutoSec), colocated with ACM CODSPY, 2020.
- Rathore, H., Samant, A., Jadliwala, M., and Mohamed, A., "TangleCV: Decentralized Technique for Secure Message Sharing in Connected Vehicles", in the proceedings of the ACM Workshop on Automotive Cybersecurity (AutoSec), In conjuction with ACM CODASPY 2019, Dallas, Texas, March 2019.
- Sabra, M.†, Maiti, A.†, and Jadliwala, M., "Keystroke Inference Using Ambient Light Sensor on Wrist-Wearables: A Feasibility Study", in proceedings of the 4^{th} Workshop on Wearable Systems and Applications (WearSys), colocated with ACM MobiSys, Munich, Germany, June 2018.
- Vinayaga-Sureshkanth, N.†, Maiti, A.†, Jadliwala, M., Crager, K., He, J., and Rathore, H., "Towards a Practical Pedestrian Distraction Detection Framework using Wearables", in the Proceedings of the Workshop on Sensing Systems and Applications Using Wrist Worn Smart Devices (WristSense), colocated with IEEE PerCom, 2018. – ***Best Paper Award***
- Crager, K.‡, Maiti, A.†, Jadliwala, M., He, J., Information Leakage through Mobile Motion Sensors: User Awareness and Concerns, in the Proceedings of the 2^{nd} European Workshop on Usable Security (EuroUSec), colocated with Euro S&P, 2017.
- Maiti, A.†, Crager, K.‡, Jadliwala, M., He, J., Kwiat, K., Kamhoua, C., "RandomPad: Usability of Randomized Mobile Keypads for Defeating Inference Attacks", in the Proceedings of the 2^{nd} International Workshop on Innovations in Mobile Privacy and Security (IMPS), colocated with Euro S&P, 2017.
- Maiti, A.†, Jadliwala, M., Weber, C.†, "Preventing Shoulder Surfing using Randomized Augmented Reality Keyboards", in the Proceedings of the 2^{nd} IEEE PerCom Workshop on Security, Privacy and Trust in the Internet of Things (SPT-IOT), 2017.
- Bilogrevic, I., Huguenin, K., Jadliwala, M., Lopez, F., Hubaux, J-P., Ginzboorg, P. and Niemi, V., "Inferring Social Ties in Academic Networks Using Short-Range Wireless Communications", Accepted for publication in the Proceedings of the 2013 ACM Workshop on Privacy in the Electronic Society (WPES 2013), Berlin, Germany, 2013.
- Jadliwala, M., Freudiger, J., Aad, I., Hubaux, J-P. and Niemi, V., "Privacy-Triggered Communications in Pervasive Social Networks", in the Proceedings of the 5^{th} IEEE WoWMoM Workshop on Autonomic and Opportunistic Communications (AOC 2011), Lucca, Italy, 2011.
- Shokri, R., Freudiger, J., Jadliwala, M. and Hubaux, J-P., "A Distortion-based Metric for Location Privacy", in the Proceedings of the ACM Workshop on Privacy in the Electronic Society (WPES), Chicago, USA, 2009.
- Jadliwala, M., Upadhyaya, S., Rao, H.R. and Sharman, R. "Security and Dependability Issues in Location Estimation for Emergency Sensor Networks", The Fourth Workshop on e-Business (WeB 2005), Venetian, Las Vegas, Nevada, USA, 2005.
- Braynov, S. and Jadliwala, M. "Representation and Analysis of Coordinated Attacks", in the Proceedings of The ACM Workshop on Formal Methods in Security Engineering (FMSE), pp. 43-51, Washington D.C., USA, 2003.

Posters/Demos

- Spracklen, J., Wijewickrama, R., Sakib, AHM., Maiti, A., and Jadliwala, M., "Special Delivery! Investigating the Prevalence, Causes, and Mitigation Methods of Package Hallucinations in Code Generating LLMs. ", at the 33^{rd} USENIX Security Symposium (SECURITY), 2024.
- Shah, D., Huang, R., Chen, T., and Jadliwala, M., "Rider Posture-based Continuous Authentication with Few-Shot learning for Mobility Scooters", at the 38^{th} AAAI Conference on Artificial Intelligence (AAAI), 2024.
- Bilogrevic, I., Huguenin, K., Jadliwala, M., Florent Lopez, Hubaux, J-P., Ginzboorg, P. and Niemi, V.,"Poster and Extended Abstract: Inferring Social Ties in Pervasive Networks: An On-campus Comparative Study", at the 2013 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp), 2013.
- Jadliwala, M., Freudiger, J., Aad, I., Hubaux, J-P. and Niemi, V., "Demo: Privacy-Triggered

Communications in Pervasive Social Networks", at the 8^{th} Annual International Conference on Mobile Systems, Applications and Services (MobiSys), 2010.
– Bilogrevic, I., Jadliwala, M. and Hubaux, J-P., "Security Issues in Next Generation Mobile Networks: LTE and Femtocells", at the 2nd International Femtocell Workshop, 2010.

Patents

– Jadliwala, M., Maiti, A., "Blockchain Game", Provisional patent granted by USPTO, Full patent application filed on 4/23/2020. Serial Number: 16/856,782.
– Aad, I., Bilogrevic, I., Cristofaro, E., Durussel, A., Hubaux, J-P., Jadliwala, M., Niemi, V., "Method and apparatus for preserving privacy for appointment scheduling", Granted by USPTO, Publication number: US8667062 B2.
– Aad, I., Freudiger, J., Jadliwala, M., Hubaux, J-P. and Raya, M., "Method and apparatus for triggering user communications based on privacy information", 12/718521, 2010 (Date filed: 05-Mar-2010).

Teaching Experience

Teaching Highlights

– Led the successful proposal preparation, curriculum design and Fall 2020 launch of the new Masters (MS) degree in Cybersecurity Science at the University of Texas at San Antonio.
– Received Wichita State University's Dwayne and Velma Wallace Excellence in Teaching Award (2017) and finalist for the student nominated Academy for Effective Teaching (AET) award (2017).
– Instrumental in developing the computer security and information assurance curricula at Wichita State University. This includes significantly improving the existing courses, and developing many new undergraduate and graduate level courses and labs in this area.
– Voted as one of the top three teachers in the EECS department in the IEEE-HKN (Wichita State University chapter) Nikola Tesla Award.
– Lead the development and deployment of WuMesh, a wireless, software-defined, mesh network testbed, currently being used for various teaching and research-related activities in the computer networking area at Wichita State University.

The University of Texas at San Antonio, San Antonio, TX, USA

– *CS 5713* - Practical Attack & Defense Techniques* **Fall 2020,21,22,23,24**
– *CS 4473/6393* - Cryptocurrencies & Bitcoins* **Spring 2018, Fall 2020,21**
– *CS 3873 - Computer Networks* **Fall 2018,19**
– *CS 5323 - Principles of Computer & Information Security* **Spring 2019,20,21,23**

∗ - newly designed courses taught for the first time at University of Texas at San Antonio

Wichita State University, Wichita, KS, USA

– *CS 898AT* - Bitcoins and Cryptocurrencies* **Fall 2017**
– *CS 797G - Mathematical Foundations of Computer Networking* **Fall 2015**
– *CS 898AD* - Security and Cooperation in Wireless Networks* **Fall 2014**
– *CS 898AB* - Privacy Enhancing Technologies* **Fall 2013, Spring 2015,16,17**
– *CS 767* - Foundations of Network Security* **Spring 2013,14,15,16,17**
– *CS 736 - Data Communication Networks* **Spring 2013**
– *CS 766* - Information Assurance & Security* **Fall 2012,13,14,15,16**
– *CS 464 - Computer Networks* **Spring 2012, Fall 2016**
– *CS 560 - Data Structures and Algorithms II* **Spring 2012**

∗ - newly designed courses taught for the first time at Wichita State University

Swiss Federal Institute of Technology, Lausanne, Switzerland

– *Co-taught Computer Networks with Prof. Jean-Pierre Hubaux* **Fall, 2011**
– *Guest Lecturer for Computer Networks* **Fall, 2010**

Student Supervision and Committees

Current and Past Graduate Students

- Ms. Nisha Vinayaga Sureshkanth, PhD, expected Fall 2024, University of Texas at San Antonio.
- Mr. Joe Spracklen, PhD, expected Summer 2026, University of Texas at San Antonio.
- Ms. Maryam Abbasi, PhD, expected Summer 2026, University of Texas at San Antonio.
- Mr. Aaditya Khant, PhD, expected Summer 2027, University of Texas at San Antonio.
- Mr. A.H.M Nazmus Sakib, PhD, expected Summer 2028, University of Texas at San Antonio.
- Mr. Mahsin Bin Akram, PhD, expected Spring 2029, University of Texas at San Antonio.
- Mr. Sahan Kalutarage, PhD, expected Spring 2029, University of Texas at San Antonio.
- Ms. Kimia Razani, PhD, expected Spring 2029, University of Texas at San Antonio.
- Mr. Andrew Laramore, MS Thesis, expected Fall 2025, University of Texas at San Antonio.
- Dr. Raveen Wijewickrama, PhD, Summer 2024, University of Texas at San Antonio.
- Dr. Mohd Amjad Sabra, PhD, Spring 2023, University of Texas at San Antonio.
- Dr. Kavita Kumari, PhD, August 2022, University of Texas at San Antonio.
- Ms. Comfort Olorunlero, MS Thesis, August 2021, University of Texas at San Antonio.
- Mr. Aaron Bray , MS Project, December 2019, University of Texas at San Antonio.
- Dr. Anindya Maiti, PhD, June 2018, Wichita State University.
- Mr. Raveen Wijewickrama, MS Project, December 2017, Wichita State University.
- Ms. Suhasini Neppalli, MS Project, July 2017, Wichita State University.
- Dr. Arash Boustani, PhD, December 2016, Wichita State University.
- Ms. Zoya Khan, MS Thesis, December 2015, Wichita State University.
- Mr. Anindya Maiti, MS Thesis, September 2014, Wichita State University.
- Mr. Navid Alamatsaz, MS Thesis, June 2014, Wichita State University.
- Mr. Cheng Jiang, MS Thesis, June 2014, Wichita State University.
- Mr. Laurent Bindschaedler, MS Thesis, June 2011, EPFL.

Honors to Graduate Students

- Ms. Nisha Vinayaga Sureshkanth received the Apple Student Travel Scholarship and Apple Best Paper Award for her research paper "Towards a Practical Pedestrian Distraction Detection Framework using Wearables" at the Workshop on Sensing Systems and Applications Using Wrist Worn Smart Devices (WristSense) – colocated with IEEE PerCom, 2018.
- Mr. Anindya Maiti received the Wichita State University's 2015 Dora Wallace Hodgson Outstanding Thesis award for his MS Thesis work.
- Ms. Zoya Khan won the People's Choice Award at the Google Hackathon 2014, held Oct. 24-25 at the national convention of the Society of Women Engineers, in Los Angeles, USA.

Thesis and Dissertation Supervision and Committees

- "Static and Binary Source Code Vulnerability Analysis with Transformer-based Generative Models", by Nafis Tanveer Islam (PhD Dissertation Committee Member, Summer 2024), University of Texas at San Antonio.
- "Friend or Foe: Evaluating Sensor-based Information Side-Channels and Covert Communication Channels on Modern Wearable Devices" by Raveen Wijewickrama (PhD Dissertation Committee Chair, Summer 2024), University of Texas at San Antonio.
- "Addressing Privacy Challenges in Modern Audio-Video Communication Systems & Applications" by Mohd A Sabra (PhD Dissertation Committee Chair, Spring 2023), University of Texas at San Antonio.
- "When and How to Protect? Modeling Repeated Interactions with Computing Services under Uncertainty" by Kavita Kumari (PhD Dissertation Committee Chair, Summer 2022), University of Texas at San Antonio.
- "Evaluating the Privacy and Security Implications of Ambient Light Sensors on Modern Mobile Devices" by Comfort Olorunlero (Masters Thesis Committee Chair, Summer 2021), University of Texas at San Antonio.
- "SPRM: Source Path Routing Model for Software Defined Networks", by Sharvari Komajwar (PhD Dissertation Committee Member, Summer 2021), University of Texas at San Antonio.
- "Inferring Malware Detector Metrics in the Absence of Ground Truth" by John Charlton (PhD Dissertation Committee Member, Spring 2021), University of Texas at San Antonio.
- "Secure Cloud Assisted Smart Cars and Big Data: Access Control Models and Implementation"

by Maanak Gupta (PhD Dissertation Committee Member, Fall 2018), University of Texas at San Antonio.
- "Attribute-Based Access and Communication Control Models for Cloud and Cloud-enabled Internet of Things" by Smriti Bhatt (PhD Dissertation Committee Member, Fall 2018), University of Texas at San Antonio.
- "Security and Privacy of Cyber and Physical User Interactions in the Age of Wearable Computing" by Anindya Maiti (PhD Dissertation Committee Chair, Spring 2018), Wichita State University.
- "On Automatically Classifying Software Code Review Feedback in the Context of Internal Quality" by Janani Raghunathan (Masters Thesis Committee Member, Summer 2017), Wichita State University.
- "Security and Privacy in Critical Infrastructure Cyber-Physical Systems: Recent Challenges and Solutions" by Arash Boustani (PhD Dissertation Committee Chair, Fall 2016), Wichita State University.
- "An Evaluation of the Effectiveness of Smart Meter Data Perturbation Mechanisms using a Unified Stochastic Framework" by Zoya Khan (Masters Thesis Committee Chair, Fall 2015), Wichita State University.
- "Online Privacy Preservation Using Packet Padding" by Kirankumar Chandrashekar (Masters Thesis Committee Member, Fall 2015), Wichita State University.
- "Innovation in Software Defined Networking and Throughput Stable Scheduling Algorithm" by Fahad Khan (Masters Thesis Committee Member, Fall 2014), Wichita State University.
- "Capacity Analysis and Data Concentration for Smart Grid Communication Networks at the Power Distribution Level" by Babak Karimi (PhD Dissertation Committee Member, Summer 2014), Wichita State University.
- "Disclosure Risk Measurement of Anonymized Datasets after Probabilistic Attacks" by Nafia Malik (Masters Thesis Committee Member, Summer 2014), Wichita State University.
- "Context-Aware Access Control: An Alternate Privacy Protection Mechanism for Online Social Networks " by Anindya Maiti (Masters Thesis Committee Chair, Summer 2014), Wichita State University.
- "Towards an Analytical Framework for Privacy Preserving Aggregation in Smart Grid" by Navid Reza Alamatsaz (Masters Thesis Committee Chair, Spring 2014), Wichita State University.
- "Preserving Query Privacy with a Query-based Memorizing Algorithm" by Jiang Cheng (Masters Thesis Committee Chair, Spring 2014), Wichita State University.
- "Mining Evolutionary Couplings from Developer Interactions and Commits" by Fasil T. Bantelay (Masters Thesis Committee Member, Summer 2013), Wichita State University.
- "On the Energy Efficiency of Dynamic Sprectrum Access in the Ad-hoc wireless LAN scenario" by Anm Badruddoza (PhD Dissertation Committee Member, Spring 2013), Wichita State University.
- "Effect of Data Caching on System-wide Anonymity with Users Sending and Receiving Multiple Messages" by Ahsan Ahmad Khan (Masters Thesis Committee Member, Spring 2012), Wichita State University.
- "Measuring Anonymity while Sending and Receiving Multiple Messages" by Abdus Samad (Masters Thesis Committee Member, Spring 2012), Wichita State University.
- "Track Me If You Can!: Measuring Effectiveness of Context-based Pseudonym-Changes against Coordinated Tracking Attacks in Pervasive Social Networks" by Laurent Bindschaedler (Masters Thesis Committee Chair, Spring 2011), EPFL.
- "From Privacy Protection to Service Optimization in Pervasive Networks" by Anthony Durussel (Masters Thesis Committee Member, Spring 2010), EPFL.

Project Supervision

- "Obfuscated Binary Analysis Across Architectures" by Aaron Bray (Masters Project Committee Chair, December 2019), The University of Texas at San Antonio.
- "Inferring Private Handwritten Information Using Smart Wrist-Wearables" by Raveen Wijewickrama (Masters Project Committee Chair, December 2017), Wichita State University.
- "Analysis of Zero Permission Sensors in Existing Android Applications" by Suhasini Neppalli (Masters Project Committee Chair, Summer 2017), Wichita State University.
- "Energy Consumption of Commercial UAV under Variable Payload" by Matthew Krehbiel (Masters Project Committee, Fall 2016), Wichita State University.

– "The Impact of Communication Frequency on the Energy-Efficiency of Cognitive Radios" by Farid Al Zoubi (Masters Project Committee, Spring 2012), Wichita State University.
– "Where do we Meet? A Privacy-Preserving Meeting Location System for Mobile Devices" by Igor Bilogrevic (EPFL Doctoral school project, Fall 2011), EPFL.
– "Nokia Instant Community Trial: Usage Reports and Data Visualization" by Stefan Lazarevic (Masters semester project, Spring 2011), EPFL.
– "A Tool for Efficient Storage and Retrieval of User Mobility and Application Data in Experimental Systems" by Dimitrije Pesic (Masters semester project, Spring 2011), EPFL.
– "The Security of QR-Codes for Mobile Advertising" by Arbuzova Natalya (Masters semester project, Spring 2011), EPFL.
– "Familiar Stranger Applications for Pervasive Social Networks" by Juyuan Liu (Masters semester project, Spring 2011), EPFL.
– "Catch Me If You Can: Femtocell-based IMSI/TMSI Catcher for UMTS Cellular Networks" by Dominique Bongard (Doctoral semester project, Fall 2010), EPFL.
– "UMTS and Femtocell security: Hands-on Experience with Real Cellular Networks" by Carl Hedari and Charles-Edmond Renouard (Masters semester project, Fall 2010), EPFL.
– "Pseudonym Change Algorithm for Nokia Instant Community" by Andreea-Simona Anghel (Masters semester project, Fall 2010), EPFL.
– "Privacy-Preserving Optimal Meeting Location Scheduling on Mobile Devices" by Vishal Joneja (Masters semester project, Fall 2010), EPFL.
– "Privacy-Preserving Optimal Meeting Location Scheduling on Mobile Devices" by Kubra Kalkan (Internship, Summer 2010), EPFL.
– "Implementation and Analysis of Privacy-Preserving Scheduling Protocols" by Praveen Kumar and Sudeep Singh Walia (Internship, Summer 2010), EPFL.
– "Measuring Privacy in Pervasive Social Networks" by Sabrina Pérez (SeCoWinet course project, Fall 2009), EPFL.
– "Data-centric Trust Mechanisms in Real-Time Context-Aware Data Sharing" by Tingting Chen (Internship, Summer 2009), EPFL.
– "Quantifying and Visualizing Privacy in Pervasive Social Networking Applications" by Laurent Bindschaedler and Avital Gutman (Internship, Summer 2009), EPFL.
– "Secure Short Messaging Service (SSMS) on Mobile Devices" by Marc Bailly and Laurent Bindschaedler (Bachelor Semester Project, Spring 2009), EPFL.
– "Secure Messaging Between Mobile Devices in Ad-Hoc Mode" by Nawfal Cherqui (Masters Semester Project, Spring 2009), EPFL.
– "Best-Effort Secure Positioning in Wireless Networks" by Loïc Etienne and Aristidis Papaioannou (SeCoWinet course project, Fall 2008), EPFL.
– "Best Effort Secure Time Synchronization in Low Duty-cycle Wireless Sensor Networks" by Mitko Tanevski (SeCoWinet course project, Fall 2008), EPFL.

Institutional Service

University & College Service

– Member, Faculty Search Committee, 2022. (in ISCS Department, UTSA)
– Member, CS Department Chair Search Committee, 2022. (in CoS, UTSA)
– Member, College Faculty Review and Advisory Committee, 2022. (in CoS, UTSA)
– Peer Mentor, University-wide NSF CAREER Peer Mentoring Team, 2020. (in UTSA)
– Member, Boeing Fellowship committee, College of Engineering, January 2015 - December 2017. (in CoE, WSU)
– Member, College of Engineering Scholarship and Awards Committee, August 2013 – December 2017. (in CoE, WSU)
– College of Engineering Curriculum and Pedagogy team, College of Engineering, August – December 2012. (in CoE, WSU)

Department Service

– Program Director and Graduate Advisor of Record, MS in Cybersecurity Science Degree program, 2021 – Present. (in CS department, UTSA)
– Organized and delivered the first department-wide NSF CAREER workshop, 2020. (in CS department, UTSA)

- Led development of the CS/ECE Department Broadening Participation Plan (BPC), 2020. (in CS department, UTSA)
- Committee Member, Department Faculty Advisory Committee (DFAC), 2019 – Present. (in CS department, UTSA)
- Committee Chair, Department Lab and Facilities Committee, 2019 – Present. (in CS department, UTSA)
- Committee Member, Graduate Student Committee, 2019 – Present. (in CS department, UTSA)
- Committee Chair, Cyber Security Concentration, 2018 – Present. (in CS department, UTSA)
- Committee Lead, New MS Cyber Security Science degree proposal and implementation committee, 2018- Present. (in CS department, UTSA)
- Committee Member, Lab & Facilities, 2018 - 2019. (in CS department, UTSA)
- Committee Member, Colloquium Committee, 2018. (in CS department, UTSA)
- Founded the WSU cybersecurity student association. (in EECS department, WSU)
- Chair, Ad-hoc committee to review GTA policies, January – May 2016. (in EECS department, WSU)
- Member, Faculty hiring committee for open software engineering faculty position, October 2015 – May 2016. (in EECS department, WSU)
- Member, Faculty hiring committee for open software engineering faculty position, October 2014 – May 2015. (in EECS department, WSU)
- Member, Faculty hiring committee for open networking faculty position, October 2014 – May 2015. (in EECS department, WSU)
- Chair, Faculty hiring committee for two open networking faculty position, January – May 2013. (in EECS department, WSU)
- Member, Awards committee, August 2012 – May 2013. (in EECS department, WSU)
- Member, Graduate committee, January 2012 - December 2017. (in EECS department, WSU)
- Member, Faculty hiring committee for networking, January – May 2012. (in EECS department, WSU)

Professional Service

Conference Organization

- General Chair, UTSA Cyber-AI Winter School (`https://sprite.utsa.edu/cyberaiwinterschool/`), San Antonio, Texas, 2023.
- General Chair, ACM WiSec 2022, San Antonio, Texas, 2022.
- Publication Chair, ACM CODASPY 2022, Baltimore-Washington DC Area, 2022.
- Publication Chair, ACM CODASPY 2021, Virtual (Online), 2021.
- Publication Chair, ACM CODASPY 2020, New Orleans, USA, 2020.
- Program Co-Chair, SKM 2019, Goa, India, 2019.
- Poster Chair, ACM SACMAT 2019, Toronto, Canada, 2019.
- Publication Chair, ACM CODASPY 2019, Dallas, USA, 2019.
- Worshop Chair, HotWiSec 2013 (co-located with ACM WiSec 2013), Budapest, Hungary, April 2013.
- Program Co-Chair, HotWiSec 2011 (co-located with IPCCC 2011), Orlando, Florida, November 2011.
- Workshop Co-Chair, IEEE SRDS 2010, New Delhi, India, November 2010.
- Publicity Co-Chair, IEEE SRDS 2009, Niagara Falls, NY, September 2009.
- General Chair, 21^{st} Annual Computer Science and Engineering Graduate Research Conference, Dept. of CSE, SUNY Buffalo, March 2008.

Technical Program Committees

- NDSS 2025, ACNS 2024-25, IEEE S&P 2023 - 25, PoPETS 2023-2025, WiSec 2022, NAS 2022, SecureComm 2019-20, IEEE DSC 2019, IEEE ISM 2015-16, 4th International Symposium on Forensic Science and Security (SDFS 2016), ACM ASIACCS Security in Cloud Computing Workshop 2016, IEEE SmartGridComm 2015, ACM WiSec 2014-2015, ANT 2013-2014, CCNC 2014, Annual Symposium on Information Assurance 2012-2015, Nokia Mobile Data Challenge Workshop (MDC) 2012, PILATES 2012, ICCCN 2011,2012,2016,2017, UIC 2010, IEEE ISDPE 2010, IEEE IPCCC 2009 - 2017, Workshop on Secure Knowledge Management (SKM 2008, 2010).

Reviewer

- **Federal Funding Agencies:** Panelist (Proposal Reviewer) for several programs/divisions within the NSF Computer and Information Science and Engineering directorate.
- **Journals:** ACM Transactions on Privacy and Security (TOPS), ACM Transactions on Sensor Networks, IEEE Transactions on Dependable and Secure Computing (TDSC), IEEE Transactions on Spatial Algorithms and Systems, IEEE Transactions on Wireless Communications, IEEE Transaction in Mobile Computing (TMC), IEEE Transactions in Parallel and Distributed Systems (TPDS), IEEE Transactions on Information Forensics and Security (T-IFS), IEEE Transactions on Vehicular Technology (TVT), IEEE Transactions on Network and Service Management (TNSM), IEEE Journal on Selected Topics in Signal Processing, IEEE Transactions on Industrial Informatics, IEEE Wireless Communications Magazine, IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans, Elsevier Pervasive and Mobile Computing, Elsevier Computer Communications, Elsevier Information Sciences journal, EURASIP Journal on Wireless Communications and Networking, International Journal of Distributed Sensor Networks.
- **Conferences:** CCS, PETS, INFOCOM, MILCOM, SRDS, Wi-Opt, WiSec, Financial Crypto.

Editor

- ACM Distributed Ledger Technologies: Research and Practice (Associate Editor).
- Springer Information Systems Frontier Journal (Guest Editor).

Presentations and Seminar Talks

- "Reality Check: Seeing Through the Lies and Deceit of Generative AI Models", Invited Guest Lecture, TU Darmstadt, Darmstadt, Germany, August 2024.
- "Datasets for Security and Privacy Research in IoT: What Do We Have and Where Do We Go?", Invited Talk at Schloss Dagstuhl Seminar on Security and Privacy of Current and Emerging IoT Devices and Systems, Dagstuhl, Germany, July 2024.
- "Backdoor Attacks in Federated Learning", Invited Tutorial at the NSF AI Spring School hosted by UTSA AI Consortium for Human Well-Being (MATRIX), San Antonio, Texas, March 2024.
- "Friend or Foe? An Era of Fun and Games (.. and Mischief) with IoT Sensors.", Keynote at the Cyber-Physical Systems Security Workshop, IEEE Conference on Communications and Network Security (CNS), Austin, Texas, October 2022.
- "Friend or Foe? An Era of Fun, Games and Mischief with IoT Sensors.", at University of Oklahoma as part of Presidential Dream Course Series, November 2021 (invited talk).
- "Friend or Foe? ML Meets Privacy", at UTSA MATRIX AI Institute Seminar Series, October 2020 (invited talk).
- "Friend or Foe? Security and Privacy Pitfalls in the Internet-of-Things Era", at Indian Institute of Technology Mumbai, 11th March 2019 (invited talk).
- "Towards Inferring Mechanical Lock Combinations using Wrist-Wearables as a Side-Channel", at 2018 UTSA College of Sciences Research Conference, 5th October 2018 (invited research seminar).
- "Privacy Threats in the Era of Wearables", at the Wichita Cyber Security Forum, 4th October 2017 (invited talk).
- "Smartwatch-Based Inference Attacks and Context-Aware Protection Mechanisms", at the Wichita State University Industrial and Manufacturing Engineering Seminar Series, March 2016 (invited research seminar).
- "Surviving Cybersecurity Threats in the Era of Modern Wearable Cyber-Physical Systems", at the US Air Force Research Lab - Information Institute, Rome, NY, July, 2015.
- "Contextual Privacy in Pervasive and Mobile Networking Environments", at the University of New Hampshire, Computer Science Department, Durham, NH, April, 2013.
- "Track Me If You Can: On the Effectiveness of Context-based Identifier Changes in Deployed Mobile Networks", at the Kansas Telecommunications Industry Association (KTIA) Spring Meeting, Wichita, USA, May 10, 2012.
- "Track Me If You Can: On the Effectiveness of Context-based Identifier Changes in Deployed Mobile Networks", at the IEEE Wichita Chapter Meeting, Wichita, USA, April 26, 2012.
- "Optimizing Mixing in Pervasive Networks: A Graph-Theoretic Perspective", at the 16th European Symposium on Research in Computer Security (ESORICS 2011), Leuven, Belgium, September 14, 2011.
- "Security and Privacy of Context Determination Services for Wireless Mobile Networks", at

College of Arts and Sciences, University of Illinois at Springfield, Springfield, USA, April 18, 2011.
- "Security and Privacy of Context Determination Services for Wireless Mobile Networks", at College of Engineering, Wichita State University, Wichita, USA, April 6, 2011.
- "Privacy-Preserving Activity Scheduling on Mobile Devices", Invited Talk at Nokia Research Center, Helsinki, Finland, September 21, 2010.
- "Security and Privacy Issues in Pervasive Social Networks", at the Nokia Workshop, Lausanne, Switzerland, December 2009.
- "Towards a Theory for Securing Time Synchronization in Wireless Sensor Networks", at the 2^{nd} ACM Conference on Wireless Network Security (WiSec 2009), Zurich, Switzerland, March 17, 2009.
- "Towards a Theory of Robust Distance-based Localization in the Presence of Cheating Beacon Nodes", Invited Talk at the Swiss Federal Institute of Technology (ETHZ), Zurich, Switzerland, September 11, 2008.
- "Towards a Theory of Robust Localization against Malicious Beacon Nodes", at the 27th IEEE International Conference on Computer Communication (INFOCOM 2008), Phoenix, Arizona, April 17, 2008.
- "Security and Robustness of Localization Techniques in Emergency Sensor Networks", Invited Talk at the Swiss Federal Institute of Technology (EPFL), Lausanne, Switzerland, March 6, 2008.
- "Multi-agent Real-Time A* Search using Replacement", at the 16^{th} Annual Computer Science and Engineering Graduate Research Conference, SUNY Buffalo, Buffalo, NY, March 2003.

References

Available on request.