JAMES BIKRAM DHOJ JOSHI

706A IS Building
135 N. Bellefield Avenue, PA 15260
Office: (412) 624-9982

227 MacDuff Court
Gibsonia, PA 15044
Cell: (412) 523-5112 (Preferred)

EDUCATION

- **PhD**, Electrical and Computer Engineering, Purdue University (August, 2003).
- **MS**, Computer Science, Purdue University, (May, 1998).
- **BE**, Computer Science & Engineering, Motilal Nehru NIT, India (1993) (formerly known as Motilal Nehru Regional Engineering College)
- ***Certificates***:
  - *Certificate* in ***Executive Presence and Influence: Persuasive Leadership Development*** Nov, 2023, The Wharton School, University of Pennsylvania,
  - *Certificate* in ***Leadership and Management Skills for Non-Managers*** (2022); 24 – hour training at the National Science Foundation (CPE Credits)
  - *Certificate* in ***Applied Management Principles***; 60 in-class hour mini-MBA, Krannert School of Management, Purdue University (May 15- June 2, 2000)

AREAS OF SPECIALIZATION/INTEREST

- Cybersecurity, Trust and Privacy areas: e.g., Advanced Access Control, Insider Threats, Security and Privacy in Distributed systems - Edge/Cloud/Social Networks; Privacy in AI/ML

PROFESSIONAL EXPERIENCE

- **Professor**, Department of Informatics and Networked Systems, School of Computing and Information, University of Pittsburgh (2016 – current)
- **Expert,** US National Science Foundation, Directorate of Technology, Innovation and Partnership (TIP)/Emerging Technology Division (Sept, 2023 – present)
- **Program Director**, US National Science Foundation, CNS Division, SaTC Program – on loan from University of Pittsburgh as IPA (Sept, 2019 – Aug, 2023)
- **Affiliate Scholar**, Pitt's Institute of Cyber Law, Policy, and Security
- **Associate Professor**, University of Pittsburgh (September, 2008 – 2015)
  - Graduate program in Information Science and Technology, and Telecommunications and Networking (also served in joint appointment capacity in Departments of Computer Science and Health Information Management for several years).
- **Assistant Professor**, University of Pittsburgh, (August, 2003 – August 2008)
  - Graduate program in Information Science and Technology, and Telecommunications and Networking (School of Information Science, before SCI was created)
- **Research Assistant**, Distributed Multimedia Systems Lab, ECE, Purdue University

- Involved in Center of Education and Research in Information Assurance and Security (CERIAS) projects (1998-2003).

- **Research Assistant**, Purdue University (1997-1999)
  - National Water Quality Database Project, Agricultural/Biological Engineering,
- **Research Assistant**, Purdue University (1996-97)
  - Crystal Visualization lab, Veterinary Medicine Dept.,
- **Lecturer**, Computer Science and Engineering, Kathmandu University, Nepal (1993-1996)

HIGHLIGHTS - NSF RELATED ACTIVITIES

- **NSF Awards**:
  - NSF Director's Award for Superior Accomplishment (**Individual Category, 2023**)

    For "*exemplary public service and leadership in advancing privacy-preserving capabilities within data and analytics learning, showcasing nationally and internationally NSF's core values for scientific leadership, public service, innovation and collaboration*"
  - NSF Director's Award for Superior Accomplishment (**Group Category, 2022**)

    For *contribution in the creation of the* ***Resilient and Intelligent Next-G Systems*** program
- **Expert** (Program Director) US National Science Foundation, Directorate of Technology, Innovation and Partnerships (Sept, 2023 – present)
  - Led the development of the **NSF Privacy-preserving Data Sharing in Practice** (PDaSP) program. I led all efforts related to its conception and building partnership with Industry and Agencies. Also contributed/contributing to other AI, Digital Assets & Cybersecurity initiatives (e.g., DCL on AI-Ready testbed).
  - Contributing to ongoing writing of **National Privacy Research Strategy**
- **Program Director**, NSF, CNS Division, SaTC Program (Sept, 2019 – Aug, 2023)
  - Leadership/Management of ***Privacy, and Applied Crypto R&D*** portfolio, and supporting many other SaTC areas (e.g., Systems / Network Security; Hardware Security; SaTC Education)
  - Leading / Coordinating COVID RAPID Grants funding activities for SaTC (in 2020).
  - Led CISE-wide effort to conceptualize, and initiate a ***Virtual Organization*** for ***Computing Research for Pandemic Preparedness and Resilience*** – the project is now called **PREPARE VO** (was Cognizant Program Officer for this project): prepare-vo.org/ - this VO's goal was to to build/promote CISE researcher community collaboration to foster COVID focused research and road-mapping research challenges to prepare the nation for future pandemics.
  - On behalf of the NSF, participated in **sub-Interagency Policy Committees (sub-IPCs)** on: (a) Privacy-Preserving Machine Learning; (b) Digital Identity; (c) Digital Assets
  - Provided key inputs/responses related to Privacy areas as needed (e.g., draft Bills, Congressional inquiries, etc.)

- **Co-Chair** of *Privacy R&D Interagency Working Group* of the *Networking and Telecommunications Research and Development* (**NITRD**) Program (https://www.nitrd.gov) (March, 2021 – Aug, 2023)
  - Co-led various interaction with experts/researchers and stakeholders, and visioning activities

- **Co-Chair** of the *Fast-Track Action Committee for National Digital Assets R&D Agenda*, **NITRD** (Dec, 2022 – Aug, 2023)
  - Co-led the publication of the ***National Objectives for Digital Assets R&D*** in March, 2023
  - Provided key technical leadership in various discussions and co-led the writing of the ***National Strategy for Digital Assets R&D*** (not public)

- **Co-Chair** of the *Fast-Track Action Committee on Advancing Privacy Preserving Data Sharing and Analytics* **(PPDSA), NITRD** (Feb, 2022 – March, 2023)
  - Co-led many meetings, roundtables towards gathering inputs for the ***National Strategy to Advance PPDSA*** which was published in March, 2023. NSF PDaSP program addresses this National Strategy and the EO on Safe, Secure and Trustworthy Development and Use of Artificial Intelligence.

- **Co-lead** of ***US-UK Privacy Enhancing Technology Prize Challenge*** (US leading team from White House OSTP, NSF, and NIST)
  - Provided technical leadership in exploring the Challenge concept by convening many inter-agency meetings, and public meetings.
  - Provide leadership in driving the synthetic dataset creation activity in collaboration with University of Virginia (for Pandemic/healthcare use case) and Swift (of financial crime use case). Provided overall oversight of the Challenge process spanning dataset development, testing/assessment environments, and final assessments and award decisions.

- **Member**, NITRD *Cybersecurity and Information Assurance* (CSIA) *R&D Strategy* Task Force (May, 2023 – Dec, 2023)
  - Contributed in the writing of the *2023 Federal Cybersecurity* R&D (*published*)

- **Member**, NITRD *National Privacy Research Strategy* writing group (2023)
  - Contributing in the writing of the *2024 National Privacy Research Strategy (ongoing)*
- **Other NSF activities while at SaTC**
  - Co-Led, initiation of ***Workshop*** on Secure and Privacy-preserving Federal Data Sharing & another ***Workshop*** to explore Security, Privacy and Ethical issues in Health/Biomedical research to create research (Cognizant Program Officer for both)
  - Help/Support formation of **NSF Internet Measurement Research** (IMR)
  - NSF DCL engagements: (i) AI-Cybersecurity Education (through Dear Colleague Letter solicitation); (ii) EU-US NGI partnership
  - Exploring collaborative funding opportunities in Cybersecurity and Privacy with international partners (3 countries)

HIGHLIGHTS - NON-NSF RELATED ACTIVITIES

- **Chair, School of Information Sciences (SIS) Council** (2014 – 2017); Member (2012 – 2014)
  - Leadership in addressing School-wide issues related to all the programs and school governance

- Provided SIS leadership in transitioning to the new School of Computing and Information that integrated SIS with Computer Science department, which was earlier housed in School of Arts and Sciences.

- **Developed** the **first BE degree program in *Computer Science & Engineering* in Nepal** in 1994 at Kathmandu University; Top 2 program in Nepal now
  - **Currently the CS program ranks 2nd in Nepal as per https://edurank.org/cs/np/**

- **Leadership in Conference activities** –
  - Editor-In-Chief of IEEE TSC (2017-2022)
  - Founding steering chair of IEEE CS conferences: (1) IEEE Collaboration and Internet Computing; (2) IEEE Cognitive Machine Intelligence; and (3) IEEE Trust, Privacy and Security in Intelligent Systems, and Applications.

- **Director** and co-founder of *Laboratory of Education and Research on Security Assured Information Systems* (LERSAIS)
  - Provided leadership in creation of LERSAIS as Pitt's center of Cybersecurity education and research activities in 2003/2004 right after joining Pitt
  - Within few years, Led the faculty team to get the University designated as a *National Center of Academic Excellence in Information Assurance Education* as well as *Research* (NCAE/IAE) by the NSA and DHS. The Cybersecurity program was ranked in top 10 in US in HP Ponenom report in 2014.
  - Led efforts to establish and manage two rounds of NSF SFS scholarship programs.

AWARDS / HONORS

1. NSF Director's Award for Superior Accomplishment (**Individual Category, 2023**)

   For "*exemplary public service and leadership in advancing privacy-preserving capabilities within data and analytics learning, showcasing nationally and internationally NSF's core values for scientific leadership, public service, innovation and collaboration*"
2. NSF Director's Award for Superior Accomplishment (**Group Category, 2022**)

   For *contribution in the creation of the **Resilient and Intelligent Next-G Systems*** program
3. Elected to IEEE Fellow on Jan 1, 2023 for "***Contributions in Access Control and Privacy***"
4. Elected to Fellow of *Artificial Intelligence Industry Academy within the International AI Industry Alliance* (2024)
5. Elected Fellow of the *Asia-Pacific Artificial Intelligence Association* (AAIA) (2024)
6. IEEE Computer Society ***Golden Core*** member since 2022
7. Research Leadership Award of the Society of Information Reuse and Integration (SIRI) – 2018 for "*Research and Mentoring on Security and Assured Information Systems*" (Jul 8, 2018)
8. Elected as ACM Distinguished Member of ACM in Nov, 2017
9. Best Paper Award, IEEE BigData Congress, 2017
10. Fellow of Society of Information Reuse and Integration – Elected in Aug, 2013

11. Elected to ACM Senior Membership in Oct, 2013
12. Elevated to IEEE Senior Membership in July, 2013
13. Best Student Paper Award in ACM SPRINGL, 2011
14. Best Paper Award in ACM CODASPY 2011
15. NSF-CAREER Award, 2006
16. Service Award, IEEE Conference on Information Reuse and Integration, 2006, 2007, 2011, 2012
17. Honored for faculty accomplishments in 2004, & 2006 Honors Convocation of the University of Pittsburgh.
18. Student Author Travel Award, International Conference on Multimedia and Expo, August 2000, New York
19. Colombo Plan Scholarship for pursuing BE Computer Science & Engineering degree at MNNIT, India

EXTERNAL GRANTS

- Summer Honors Undergraduate Research Experience in Electric Grid (SHURE-Grid) at the University of Pittsburgh (funded for Summer, 2024; as a Co-PI/Participant
- NSF Federal Cyber Service: *A Curriculum in Security Assured Information Systems* (2004-2006); Amount: $ $283640. (as Co-PI)
- NSF-CAREER: *A Trust-based Access Control Management Framework for Secure Information Sharing and Multimedia Workflows in Heterogeneous Environments* (2006-2011); Amount: $416,419.00. (as PI)
- NSF Federal Cyber Service: *A Scholarship Program for Security Assured Information Systems Track* (2006-2011); Amount: $1,055,553.00; Period. (as PI)
- NSF CNS Division: *CSR: SGER: Dynamic Data Driven Defense Mechanisms for Cybersecurity* (2007-2009); Amount: $104,537.00. (as Co-PI)
- NSF-IIS (CPATH Program): *CPATH-1: Health Computing: Integrating Computational Thinking into Health Science Education* (2007-2009); Amount: $283,640. (as Co-PI)
- NSF Federal Cyber Service: *A Scholarship Program for Security Assured Information Systems Track* (2011-2014); Amount: $ $1,326,071.00. (as PI)
- NIST: *Standards: People, Process, Products and Productivity Focus on Information Technology Standards* (2013-20014); Amount: $99,535. (as Co-PI)
- NSA CAE Cybersecurity Grant: *Towards Insider Threat Assessment and Mitigation* (2014 – 2015); Amount: $264,553. (as PI)
- NSF CMMI – RAPID: *RAPID: Scalability and Sustainability in Uncertain Environments: Recovery from the Nepal Earthquakes of April 25 and May 12, 2015*; Amount: $46,327 (as Co-PI)
- NSF-DGE Award (SFS - Capacity): *A Curriculum for Security Assured Health Informatics*, NSF-DGE Award (2014 – 2017/2018(Ext)); Amount: $897,055.00. (as PI)
- NSF-CICI: *SAC-PA: Towards Security Assured Cyberinfrastructure in Pennsylvania* (2016 – 2018); Amount: $499,951.00. (as PI)

- NSF OAC: CyberTraining: *CDL: Security-Assured Data Science Workforce Development in Pennsylvania* (2017 – 2020); Amount: $499,952. (as Co-PI)
- CISCO Grant: *DiCoTraM: Towards a Distributed Collaborative Traffic Monitoring System* (2012-2013); Amount: $54,034; Period. (as PI)
- DoD IASP proposal: *Capacity Building* (*Research + Equipment*) *and IRMC Partnership* (2006-2007) (Capacity Building only); Amount: ~$55,000 (as PI)
- DoD IA Scholarship Program: *Program Partnership with the Information Resource Management College* (IRMC) *of the National Defense University* (NDU) (For IRMC Partnership and Capacity Building) (2005); Amount: $273,660, (approved overall budget); 2005; (as PI)
- CISCO CIAG Equipment Grant: *A Proposal for Cisco CIAG Equipment Grant*; Spring 2005; Amount: ~$130,000. (as PI)

INTERNAL GRANTS (as PI)

- University of Pittsburgh Institute for Cyber Law, Policy and Policy: *Distinguished Seminar Series* (PittCyber, $10,000)
- University of Pittsburgh CRDF: *An Adaptive Framework for Security-Assured Survivable Information Systems* (2004-2006)*;* Amount: $19,988;
- Research Interest Group (RIG) – Phase I Funding from the Dean (through internal Competitive) --*Security Assured Information Systems* (SAIS) RIG (2006-2007); Amount: $20,000; Year
- Dean's Entrepreneurial Initiatives: *LERSAIS Seminar and Student Research Groups* (2005-2006) Amount: $15,000.
- Dean's Entrepreneurial Initiatives: *Laboratory of Education and Research on Security Assured Information Systems*; (2004-05) Amount: $12,000

PUBLICATIONS

Book

1. James B. D. Joshi et al. "Network Security: Know It All," May, 2008 (Contributor).
2. Co-Editor of Book titled: “Information Assurance: Survivability and Security in Networked Systems,”, Published in 2007 by Elsevier, Inc. Editors: Yi Qian, James Joshi, David Tipper, Prashant Krishnamurthy.
3. James B. D. Joshi, “A Generalized Temporal Role Based Access Control Model for Developing Secure Applications”, PhD Thesis, Purdue University, August, 2003.

Book Chapter

1. Nuray Baltaci Akhuseyinoglu, James Joshi, “Access Control Approaches for Smart Cities,” In: Al-Turjman F, Imran M, Editors. *IoT Technologies in Smart-Cities*: *From sensors to big data, security and trust*. UK: The Institution of Engineering and Technology (IET); 2019
2. Xuelian Long, Lei Jin, James Joshi, “Information Privacy,” Innovation in Information Security (Vol 4), World Scientific Publishing Co. Pte. Ltd, 2018.

3. H. Takabi, S.T. Zargar, and J. Joshi, "Mobile Cloud Computing and Its Security, Privacy and Trust Management Challenges," *in Security, Privacy, Trust, and Resource Management in Mobile and Wireless Communications, D. B. Rawat, B.B. Bista, and G. Yan Ed. IGI Global, 2014. doi:10.4018/978-1-4666-4691-9, 2014*

4. Hassan Takabi and James B. D. Joshi. Policy Management in Cloud Computing Environment: Challenges and Approaches. *in Security Engineering for Cloud Computing: Approaches and Tools, Editors: D. G. Rosado, D. Mellado, E. Fernandez-Medina, and M. Piattini, IGI Global, September 2012*.

5. Hassan Takabi and James B. D. Joshi, Gail-Joon Ahn, Security and Privacy in Cloud Computing: Towards a Comprehensive FrameworkService-Oriented Methodology and Technologies for Cloud Computing", *in Principles, Methods and Service-oriented Approaches for Cloud Computing, Editors: X. Yang and L. Liu, IGI Global, January 2013.*

6. Mohd Anwar, Amirreza Masoumzadeh and James Joshi, "Security and Privacy in Location Based Services," *Location Based Services*; Advanced Location-Based Technologies and Services, H. A. Karimi, Ed. CRC Press, 2013, pp. 235–264.

7. Yue Zhang, James Joshi, "Access Control and Trust Management for Emerging Multidomain Environments," in *Annals of Emerging Research in Information Assurance*, Security and Privacy Services, Editors: S. Upadhyaya, R. O. Rao 2009.

8. Yue Zhang, James Joshi, "Temporal Access Control," *Encyclopedia of Database Systems*, Editors-in-Chief: Ling Liu, M. Tamer Özsu, Springer, 2009.

9. Yue Zhang, James Joshi, "Role based Access Control", *Encyclopedia of Database Systems*, Editors-in-Chief: Ling Liu, M. Tamer Özsu Springer, 2009.

10. Yue Zhang, James B. D. Joshi, "ANSI/INCITS RBAC Standard." *Encyclopedia of Database Systems*, Editors-in-Chief: Ling Liu, M. Tamer Özsu, Springer, 2009

11. Yue Zhang, James B. D. Joshi, "GEO-RBAC Model," *Encyclopedia of Database Systems*, Editors-in-Chief: Ling Liu, M. Tamer Özsu, Springer, 2009

12. Yue Zhang, James B. D. Joshi, "Administration Model for RBAC," *Encyclopedia of Database Systems*, Editors-in-Chief: Ling Liu, M. Tamer Özsu, Springer, 2009

13. James B. D. Joshi, Mei-Ling Shyu, Shu-Ching Chen, Walid Aref, Arif Ghafoor, "A Multimedia-Based Threat Management and Information Security Framework," in *Multimedia Technologies: Concepts, Methodologies, Tools, and Applications* (3 Volumes) Edited By: Mahbubur Rahman Syed, Minnesota State University, Mankato, USA, June, 2008

14. James B. D. Joshi, Siqing Du, Saubhagya R Joshi, "A Trust Based Access Control Management Framework for a Secure Grid Environment" in Book titled: *Security in Distributed, Grid, and Pervasive Computing*, Edited by Dr. Yang Xiao, to be published by Auerbach Publications, CRC Press 2007.

15. James B. D. Joshi, S. R. Joshi, and S. M. Chandran, "Information Security Issues and Challenges," in *Encyclopedia of Digital Government,* 2006.

16. James B. D. Joshi, S. R. Joshi, and S. M. Chandran, "Identity Management and Privacy Issues," in *Encyclopedia of Digital Government*, 2006.

17. James B. D. Joshi, S. M. Chandran, A. Ghafoor, and W. G. Aref, "Survivability Issues and Challenges," in *Encyclopedia of Digital Government*, 2006.

18. James B.D. Joshi, Mei-Ling Shyu, Shu-Ching Chen, Walid Aref, Arif Ghafoor, "A Multimedia-Based Threat Management and Information Security Framework," *Web and Information Security* (editors: Elena Ferrari, Bhavani Thuraisingham), IDEA Group, 2005.

19. James B. D. Joshi, Arif Ghafoor, Walid Aref, Eugene H. Spafford, “Digital Government Security and Privacy Challenges,” William J. McIver, Jr. & Ahmed K. Elmagarmid (eds) *Advances in Digital Government*: *Technology*, *Human Factors*, *& Policy*. Boston, Kluwer, 2002, Chapter 7, pp. 121-136.

Special Issue Guest Editor

1. Mei-Ling Shyu, Surya Nepal, Valerie Issarny, James Joshi; “Special Issue on Services Computing for COVID-19 and Future Pandemics,” IEEE Transactions on Services Computing, 06/17/2022
2. Schahram Dustdar, Surya Nepal, James Joshi. Special Section on Advances in Internet-based Collaborative Technologies, ACM Transactions on Internet Technology, Vol. 19, No. 3, Article 37e., November 2019.
3. Mei-Ling Shyu, James Joshi, Qiong Liu: Guest Editors'. Int. J. Semantic Computing 9(2): 139-142 (2015)
4. Chengcui Zhang, Elisa Bertino, Bhavani M. Thuraisingham, James B. D. Joshi: Guest editorial: Information reuse, integration, and reusable systems. Information Systems Frontiers 16(5): November 2014, Volume 16, Issue 5, pp 749-752
5. Lakshmish Ramaswamy, Barbara Carminati, James B. D. Joshi, Calton Pu: Editorial: Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom 2012). MONET 19(5): October 2014, Volume 19, Issue 5, p 634
6. Barbara Carminati, Lakshmish Ramaswamy, Anna Cinzia Squicciarini, James Joshi, Calton Pu: Preface. Int. J. Cooperative Inf. Syst. 23(2) (2014)
7. Lakshmish Ramaswamy, Barbara Carminati, Lujo Bauer, Dongwan Shin, James Joshi, Calton Pu, Dimitris Gritzalis: Editorial. Computers & Security 41: 1-2 (June, 2014)
8. James Caverlee, Calton Pu, Dimitrios Georgakopoulos, James Joshi: Editorial for CollaborateCom 2011 Special Issue. MONET 18 (2): 235-236 (2013)
9. Weisong Shi, James Joshi, Tao Zhang, Eun K. Park, Juan Quemada: ACM/Springer Mobile Networks and Applications (MONET) Special Issue on "Collaborative Computing: Networking, Applications and Worksharing". MONET 17(3): 376-377 (2012)
10. James Joshi, Elisa Bertino, Calton Pu, Heri Ramampiaro: ACM/Springer Mobile Networks and Applications (MONET) Special Issue on "Collaborative Computing: Networking, Applications and Worksharing". MONET 17(3): 325-326 (2012)
11. Songqing Chen, Le Gruenwald, James Joshi, Karl Aberer: ACM/Springer Mobile Networks and Applications (MONET) Special Issue on “Collaborative Computing: Networking, Applications and Worksharing”. Mobile Networks and Applications, 17 (4). pp. 506-507; (2012)
12. James Joshi, Barbara Carminati: Guest Editorial SACMAT 2009 and 2010. *ACM Transactions on Information Systems Security,* 14(3): 22 (2011).
13. Dimitris Gritzalis and James Joshi (Editors); Special Issue on Access Control Methods and Technologies, Computer and Security, Volume 30, Issues 2–3, Pages 89-170 (March–May 2011)
14. Mehmet Kaya, James B. D. Joshi, Mei-Ling Shyu: Guest Editorial - Introduction to the *Special Issue on Information Reuse and Integration*. JIKM 10(3): (2011)

Refereed Journal /Articles

1. Runhua Xu, Bo Li, Chao Li, James Joshi, Shuai Ma, and Jianxin Li. "TAPFed: Threshold Secure Aggregation for Privacy-Preserving Federated Learning." IEEE Transactions on Dependable and Secure Computing (IEEE TDSC); 2024

2. Runhua Xu, Chao Li, James Joshi, "Blockchain-based Transparency Framework for Privacy Preserving Third-party Services," IEEE TDSC, June, 2022
3. Runhua Xu, James Joshi, Chao Li, "*NN-EMD*: Efficiently Training Neural Network Using Encrypted Multi-sourced Datasets," IEEE TDSC; April, 2021
4. Leila Karimi, Maryam Aldairi; James Joshi, Mai Abdelhakim, "An Automatic Attribute Based Access Control Policy Extraction from Access Logs," *IEEE Transactions on Dependable and Secure Computing*, Jan 25, 2021
5. Runhua Xu, James Joshi, "Trustworthy and Transparent Third-Party Authority," *ACM Transactions on Internet Technology* (TOIT), 2020.
6. Nuray Baltaci Akhuseyinoglu, James Joshi, "A Constraint and Risk-aware Approach to Attribute-based Access Control for Cyber-Physical Systems," *Springer Computers & Security*, 2020.
7. Runhua Xu, James Joshi, Prashant Krishnamurthy, "An Integrated Privacy Preserving Attribute Based Access Control Framework Supporting Secure Deduplication," *IEEE Transactions on Dependable and Secure Computing*, 2019
8. Nathalie Baracaldo, Balaji Palanisamy, James Joshi, "*G-SIR*: An Insider Attack Resilient Geo-Social Access Control Framework," *IEEE Transactions on Dependable and Secure Computing,* 16(1): 84-98 (2019)
9. Leming Zhou, Bambang Parmanto, James Joshi, "Development and Evaluation of a New Security and Privacy Track in a Health Informatics Graduate Program: Multidisciplinary Collaboration in Education," JMIR Medical Education, 2018;4(2):e19
10. Lei Jin, Chao Li, Balaji Palanisamy, James Joshi, "*k-Trustee*: Location Injection Attack-resilient Anonymization for Location Privacy" Elsevier Computer & Security, Volume 78, September 2018, Pages 212-230
11. Louise K. Comfort and James Joshi (2017) Scalability and Sustainability in Uncertain Environments: Transition to Recovery from the 2015 Gorkha, Nepal, Earthquakes. Earthquake Spectra: December 2017, Vol. 33, No. S1, pp. S385-S401.
12. Mohd Anwar, James Joshi, Joseph Tan, "Anytime, anywhere access to secure, Privacy-aware Healthcare Services: Issues, Approaches & Challenges," *Elsevier Health Policy and Technology journal*.
13. Rose E. Constantino, Betty Braxter, Dianxu Ren, Joseph David Burroughs, Willa Marlene Doswell, Linden Wu, Juhae Grace Hwang, Mary Lou Klem, James B D Joshi, W. Brian Greene "Comparing Online with Face-to-Face HELPP Intervention in Women Experiencing Intimate Partner Violence," *Issues in Mental Health Nursing* 00:1–9, 2015
14. Jianfeng Lu, James B. D. Joshi, Lei Jin, Yiding Liu, "Towards Complexity Analysis of User Authorization Query Problem in RBAC" *Elsevier Computer & Security*, Volume 48, February 2015, Pages 116–130.
15. Lei Jin, Xuelian Long, Ke Zhang, Yu-Ru Lin, James B.D. Joshi, "Characterizing Users' Check-in Activities Using Their Scores in a Location-based Social Network," Springer Multimedia Systems, 2014.
16. Youna Jung, James B. D. Joshi: CPBAC: Property-based access control model for secure cooperation in online social networks. Computers & Security 41: 19-39 (2014)
17. Nathalie Baracaldo, James Joshi: An adaptive risk management and access control framework to mitigate insider threats. Computers & Security 39: 237-254 (2013)

18. S.T. Zargar, J. Joshi, and D. Tipper, "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks," *IEEE Communications Surveys & Tutorials*, vol. PP, no. 99, pp. 1-24. (Published Nov 12, 2013) (Early Access-online Mar. 28, 2013)
19. Lei Jin, James B. D. Joshi, Mohd Anwar, "Mutual-friend based attacks in social network systems," Computers & Security 37: 15-30 (2013)
20. Amirreza Masoumzadeh and James Joshi, "Top Location Anonymization for Geosocial Network Datasets," Transactions on Data Privacy, vol. 6, no. 1, pp. 107-126, 2013.
21. Hassan Takabi, James B. D. Joshi, "Semantic-based Policy Management for Cloud Computing Environments," *International Journal of Cloud Comuting* 1(2/3): 119-144 (2012)
22. Amirreza Masoumzadeh and James Joshi, "Preserving Structural Properties in Edge-Perturbing Anonymization Techniques for Social Networks," *IEEE Transactions on Secure and Dependable Computing* 9(6): 877-889 (2012) [Amirreza received ***Catherine Ofiesh Orner Award*** for this paper at School of Information Sciences, University of Pittsburgh]
23. Youna Jung and James B.D. Joshi, "CRiBAC: Community based Role interaction Access Control Model", *Computers & Security*, Elsevier, 31(4): 497-523 (2012)
24. Youna Jung, Minsoo Kim, Amirreza Masoumzadeh, James B.D Joshi, "A Survey of Security for Multiagent Systems", *Artificial Intelligence Review*, Springer Netherlands, Doi: 10.1007/s10462-011-9228-8
25. Lei Jin, Hassan Takabi, James B. D. Joshi, "Analyzing Security and Privacy Issues of Using E-mail Address as Identity" *International Journal Information Privacy, Security and Integrity,* Vol. 1, No. 1, 2011
26. Amirreza Masoumzadeh and James Joshi, "Ontology-Based Access Control for Social Network Systems," , *International Journal Information Privacy, Security and Integrity,* Vol. 1, No. 1, 2011
27. Xuelian Long, James Joshi, "BaRMS: A Bayesian Reputation Management Approach for P2P Systems, *Journal of Information & Knowledge Management*, Vol: 10, No: 3, pp 273-283 (2011)
28. Hassan Takabi, James Joshi, Gail-Joon Ahn, "Security and Privacy Challenges in Cloud Computing Environments," IEEE Security and Privacy, Jan-Feb, 2011.
29. Carlos E. Caicedo, James Joshi, Summit Tuladhar, "IPv6 Security Challenges," Vol(42), Issue(2), (Feb, 2009), IEEE Computer, Page(s): 36-42.
30. Yue Zhang, James Joshi, "SRBAC07: A Scoped Administration Model for RBAC with Hybrid Hierarchy," *Journal of Information Assurance and Security* 2007 (Volume 2, issue 4)
31. James, B.D. Joshi, Elisa Bertino, Arif Ghafoor and Yue Zhang, "Formal Foundations for hybrid hierarchies in GTRBAC", *ACM Transactions on Information and System Security* (TISSEC), Vol. 10, No. 4, Jan, 2008, pp. 1-39.
32. Basit Shafiq, James B. D. Joshi, Elisa Bertino, Arif Ghafoor, "Secure Interoperation in a Multi-Domain Environment Employing RBAC Policies," *IEEE Transactions on Knowledge and Data Engineering*. Vol. 17, No. 11, Pages 1557 - 1577, Nov. 2005.
33. Rafae Bhatti, James B. D. Joshi, Basit Shafiq, Elisa Bertino, Arif Ghafoor, "X-GTRBAC Admin: A Decentralized Administration Model for Enterprise Wide Access Control," *ACM Transactions on Information and System Security (TISSEC),* Vol. 8 No. 4, Nov, 2005.
34. James B. D. Joshi, Elisa Bertino, Arif Ghafoor, "Analysis of Expressiveness and Design Issues for a Temporal Role Based Access Control Model," *IEEE Transactions on Dependable and Secure Computing,* April, 2005.

35. James B. D. Joshi, Elisa Bertino, Usman Latif, Arif Ghafoor, "Generalized Temporal Role Based Access Control Model," *IEEE Transactions on Knowledge and Data Engineering*, Vol 17, No. 1 pages 4-23, Jan, 2005.
36. Rafae Bhatti, James B. D. Joshi, Elisa Bertino, Arif Ghafoor, "X-GTRBAC: An XML-based Policy Specification Framework and Architecture for Enterprise-Wide Access Control," *ACM Transactions on Information and System Security* Vol. 8, No. 2, Pages 187-227, May 2005.
37. Rafae Bhatti, James B. D. Joshi, Elisa Bertino, Arif Ghafoor, "XML-based Specification for Web-Services Document Security", *IEEE Computer*, Vol. 37, No. 4, April, 2004.
38. James B. D. Joshi, Rafae Bhatti, Elisa Bertino, Arif Ghafoor, "An Access Control Language for Multidomain Environments," *IEEE Internet Computing,* Nov-Dec 2004, pages 40-50.
39. James B. D. Joshi, Kevin Li, Husni Fahmi, Basit Shafiq, Arif Ghafoor, "A Model for Secure Multimedia Document Database System in a Distributed Environment," *IEEE Transactions on Multimedia: Special Issue on Multimedia Databases*, Vol. 4, No. 2, June, 2002, pp. 215-234.
40. James B. D. Joshi, Arif Ghafoor, Walid Aref, Eugene H. Spafford, "Digital Government Security Infrastructure Design Challenges," *IEEE Computer*, Vol. 34, No. 2, February, 2001, pp 66-72.
41. James B. D. Joshi, Walid G. Aref, Arif Ghafoor and Eugene H. Spafford, "Security Models for Web-Based Applications," *Communications of the ACM*, Vol. 44, No. 2, February, 2001, pp. 38-44.

Submitted/Under Preparation/arXiv

1. Leila Karimi, Mai Abdelhakim, James Joshi, "Adaptive ABAC Policy Learning: A Reinforcement Learning Approach," IEEE TDSC (**Major Revision**);
2. Runhua Xu,Nathalie Baracaldo, James Joshi, "Privacy-Preserving Machine Learning System: Methods, Challenges and Directions," arXiv,
3. Maryam Aldairi1, Laila Karimi, James Joshi, "Multi-Dimensional Trust Modeling for Unsupervised Insider Threat Detection" to be submitted.

Refereed Symposium/Conferences/Workshop

Under review/being submitted:

- Runhua Xu, Shiqi Gao, Chao Li, James Joshi, Jianxin Li, "Dual Defense: Enhancing Privacy and Mitigating Poisoning Attacks in Federated Learning," NeurIPS 2024
- Liou Tang, James Joshi, "Attacking Machine Unlearning, or Attacking with Machine Unlearning? A Taxonomy," (being submitted)
- Peilin He, James Joshi, "FL-RDSN: A Novel Framework for Privacy-Preserving Lossy Image Reconstruction," (being submitted)
- Liou Tang, James Joshi, Ashish Kundu; "Attacking Machine Unlearning, or Attacking with Machine Learning? A Taxonomy," (**being submitted**)
- Runhua Xu, James Joshi, "Dual Defense: Enhancing Privacy and Mitigating Poisoning Attacks in Federated Learning," NeuIPS 2024 (**submitted**)

Published

1. Maryam Aldairi, James Joshi, "Towards Assessing Integrated Differential Privacy and Fairness Mechanisms in Supervised Learning," IEEE TPS 2024

2. Galen Harrison, Przemyslaw Porebski, Jiangzhuo Chen, Mandy Wilson, Henning Mortveit, Parantapa Bhattacharya, Dawen Xie, Stefan Hoops, Anil Vullikanti, Li Xiong, James Joshi, Madhav Marathe; "Synthetic Information and Digital Twins for Pandemic Science: Challenges and Opportunities," 2023 5th IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA), 2023/11/1
3. Runhua Xu, Nathalie Baracaldo, Yi Zhou, Ali Anwar, James Joshi, Heiko Ludwig, "FedV: Privacy-Preserving Federated Learning over Vertically Partitioned Data," AISec2021 Workshop at ACM CCS, Nov, 2021
4. Runhua Xu, James Joshi, "Revisiting Secure Computation Using Functional Encryption: Opportunities and Research Directions," 2020 Second IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA), Oct, 2020.
5. Maryam Aldairi, Leila Karimi, James Joshi, "A Trust Aware Unsupervised Learning Approach for Insider Threat Detection," 2019 IEEE 20th International Conference on Information Reuse and Integration, 2019.
6. Runhua Xu, James Joshi and Chao Li, "*CryptoNN*: Training Neural Networks over Encrypted Data," IEEE ICDCS 2019 in Dallas, Texas, US, July 7th – July 10th, 2019.
7. LeRoy Carr III, Anthony Newtson, James Joshi, "Towards modernizing the Future of American Voting," (Vision paper – Invited), IEEE CIC 2018, Philadelphia, PA, USA.
8. Leila Karimi, James Joshi, "An Unsupervised Learning Based Approach for Mining Attribute Based Access Control Policies," IEEE BigData, Dec 10-13, 2018, Seattle, WA, USA,
9. Runhua Xu, Balaji Palanisamy and James Joshi. QueryGuard: Privacy-preserving Latency-aware Query Optimization for Edge Computing," IEEE TrustCom 2018 (August), New York, USA.
10. Maryam Karimi, Prashant Krishnamurthy, James Joshi, David Tipper, "Mining Historical Data towards Interference Management in Wireless Proceedings," of the 13th ACM Symposium on QoS and Security for Wireless and Mobile Networks: 81-88, November 21 - 25, 2017
11. Nuray Baltaci Akhuseyinoglu, James Joshi: "A Risk-Aware Access Control Framework for Cyber-Physical Systems." CIC 2017 (Oct, 2017): 349-358.
12. Leila Karimi, James Joshi: "Multi-Owner Multi-Stakeholder Access Control Model for a Healthcare Environment." CIC 2017 (Oct, 2017): 359-368
13. Chao Li, Balaji Palanisamy, James Joshi, "Differentially Private Trajectory Analysis for Points-of-Interest Recommendation, IEEE BigData Congress," 2017 (June) **BEST PAPER AWARD**
14. Runhua, Xu, James Joshi, Prashant Krishnamurthy, David Tipper, "Insider Threat Mitigation in Attribute Based Encrytion", National Cyber Summit 2017.
15. Runhua Xu, James B. D. Joshi: Enabling Attribute Based Encryption as an Internet Service. IEEE CIC 2016: 417-425 (Nov, 2016)
16. Leila Karimi, James Joshi: Multi-Owner Multi-Stakeholder Access Control Model for a Healthcare Environment. CIC 2017: 359-368.
17. Yue Su, Ziyi Lan, Yu-Ru Lin, Louise K. Comfort, James Joshi: Tracking Disaster Response and Relief Following the 2015 Nepal Earthquake. CBig Workshop, IEEE CIC 2016: 495-499
18. Chao Li, Balaji Palanisamy, James Joshi, SocialMix: Supporting Privacy-Aware Trusted Social Networking Services. *IEEE ICWS 2016*: San Francisco, CA: 115-122
19. Runhua Xu, James B. D. Joshi: An Integrated Privacy Preserving Attribute Based Access Control Framework. *IEEE CLOUD* 2016, San Francisco, CA: 68-76.

20. Runhua Xu, James B. D. Joshi: Enabling Attribute Based Encryption as an Internet Service. *IEEE CIC 2016*: 417-425, Pittsburgh, USA (Invited), November 2-4, 2016.
21. Y. Su, Z. Lan, Y-R Lin, L.K. Comfort and J. Joshi, Tracking Disaster Response and Relief Efforts following the 2015 Nepal Earthquake International Workshop on Collaborative Internet Computing for Disaster Management (CIC-DM), Pittsburgh, PA, November 2-4, 2016.
22. Leila Karimi, Balaji Palanisamy, James Joshi: A Dynamic Privacy Aware Access Control Model for Location Based Services. Workshop in IEEE CIC 2016: 554-557, Pittsburgh, PA, November 2-4, 2016.
23. L. K. Comfort, J. B. D. Joshi, F, Yuldashev, Scalability and Sustainability in Uncertain Environments: Recovery from the Nepal Earthquakes, April 25 and May 12, 2015, presented by L.K. Comfort at the 2015 American Geophysical Union (AGU) conference in San Francisco, CA December 14-18, 2015. [**Poster**]
24. Nathalie Baracaldo, Balaji Palanisamy, James Joshi "Geo-Social-RBAC: A Location-based Socially Aware Access Control Framework" The 8th International Conference on Network and System Security (NSS 2014). Lecture Notes in Computer Science Volume 8792, 2014, pp 501-509
25. Lei Jin, Hassan Takabi, Xuelian Long, James B.D. Joshi, "Exploiting Users' Inconsistent Preferences in a Social Network System to Discover Private Friendship Links," 2014 Workshop on Privacy in the Electronic Society (WPES), Held in conjunction with CCS 2014, Nov 3-7, 2014
26. Lei Jin, Balaji Palanisamy, James B.D. Joshi, "Compromising Cloaking-based Location Privacy Preserving Mechanisms with Location Injection Attacks," 21st ACM Conference on Computer and Communications Security (Poster), Nov 3-7, 2014.
27. Balaji Palanisamy, Sheldon Sensenig, James B. D. Joshi, Rose Constantino, LEAF: A privacy-conscious social network-based intervention tool for IPV survivors. IEEE IRI 2014 (Aug, 2014): 138-146
28. Saman Taghavi Zargar, James B. D. Joshi, David Tipper, DiCoTraM: A distributed and coordinated DDoS flooding attack tailored traffic monitoring. IRI 2014 (Aug, 2014): 120-129
29. Xuelian Long, Lei Jin and James Joshi, "Towards Understanding Traveler Behavior in Location-Based Social Networks," IEEE GlobeCom 2013, Dec, Atlanta, USA
30. Xuelian Long and James Joshi, "A HITS-based POI Recommendation Algorithm in Location-Based Social Networks," (Short Paper) The 2013 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM 2013) Niagara Falls, Canada, August 25-28, 2013
31. Xuelian Long, Lei Jin, James Joshi: Understanding venue popularity in Foursquare. CollaborateCom 2013: 409-418
32. Nathalie Baracaldo, James Joshi, "Beyond Accountability: Using Obligations to Reduce Risk Exposure and Deter Insider Attacks. ACM SACMAT 2013: June, 2013, 213-224
33. A. Masoumzadeh and J. Joshi, "Privacy Settings in Social Networking Systems: What You Cannot Control," in Proc. 8th ACM Symposium on Information, Computer and Communications Security (ASIACCS 2013), May, 2013
34. A. Masoumzadeh, L. Jin, J. Joshi, and R. Constantino, "HELPP Zone: Towards Protecting College Students from Dating Violence," in iConference 2013 Proceedings, 2013, pp. 925-928.

35. S.T. Zargar, and J. Joshi, "DiCoDefense: Distributed Collaborative Defense against DDoS flooding attacks," the 34th IEEE Symposium on Security & Privacy (S&P'13)(Poster), May 19-22, 2013, San Francisco, CA.
36. Rose Constantino, Amirreza Masoumzadeh, Lei Jin, James Joshi, Joseph Burroughs, Dominique de la Cruz, "HELPP Zone App and TMI: Disrupting Intimate Partner Violence in College Students" 2013 International Nursing High-end Forum (INHF), China, 22nd - 23rd June, 2013.
37. Youna Jung, Minsoo Kim, James B. D. Joshi: Towards secure cooperation in online social networks. CollaborateCom 2012: October, 2012, 80-88
38. Lei Jin, Xuelian Long and Joshi B.D. Joshi, Towards understanding Residential Privacy by Analyzing User' Activities in Foursquare, In Proceedings of the 2012 Workshop on Building Analysis Datasets and Gathering Experience Returns for Security (BADGERS'12), Held in conjunction with CCS 2012, Raleigh, NC, USA.
39. Xuelian Long, Lei Jin, James Joshi, "Exploring Trajectory-Driven Local Geographic Topics in Foursquare," *in the 4th International Workshop on Location-Based Social Networks* (LBSN 2012), Sept 8, 2012 - Pittsburgh, Pennsylvania, USA (Held in conjunction with Ubicomp 2012).
40. Lei Jin, Xuelian Long, Mohd Anwar, James Joshi, "Analysis of Access Control Mechanisms for Users' Check-ins in Location-based Social Network Systems," 2nd International *Workshop on Issues and Challenges on Social Computing (WICSOC)*, 2012 (with IEEE IRI2012).
41. Nathalie Baracaldo, James Joshi, "A Trust-and-Risk Aware RBAC Framework: Tackling Insider Threat," *ACM SACMAT* 2012: 167-176
42. Hassan Takabi and James B. D. Joshi. Policy Management as a Service: An Approach to Manage Policy Heterogeneity in Cloud Computing Environment. In Proc. 45th *Hawaii International Conference on System Sciences* (HICSS), Hawaii, USA, January 4-7, 2012.
43. Hassan Takabi and James B. D. Joshi. Toward a Semantic Based Policy Management Framework for Interoperable Cloud Environments. *In Proc. 1st International IBM Cloud Academy Conference* (ICA CON 2012), Research Triangle Park (RTP), North Carolina, USA, April 19-20, 2012.
44. Jesus M. Gonzalez, Mohd Anwar, James B. D. Joshi, "Trust-Based Approaches to Solve Routing Issues in Ad-Hoc Wireless Networks: A Survey," IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2011, vol., no., pp.556,563, 16-18 Nov. 2011
45. Jesus M. Gonzalez, Mohd Anwar, James B. D. Joshi, "A Trust-based Approach Against IP-spoofing Attacks." *Ninth Annual Conference on Privacy, Security and Trust* (PST 2011), 19-21 July, 2011, Montreal, Québec, Canada.(pg 63-70)
46. Jesus M. Gonzalez, Mohd Anwar, James B. D. Joshi, "A Trust-based Approach to Mitigate Rerouting Attacks," *CollaborateCom*, poster version, International Conference on, 15-18 October 2011.
47. Amirreza Masoumzadeh, James Joshi, "Anonymizing Geo-Social Network Datasets*, 4th ACM SIGSPATIAL International Workshop on Security and Privacy in GIS and LBS,* November 1st, 2011, Chicago, IL, USA (***Best Student Paper Award***)
48. Hassan Takabi and James Joshi, "An Approach to manage Policy Heterogeneity in Cloud Computing Environment," Poster,*The 27th Annual Computer Security Applications Conference* (ACSAC 2011), Orlando, FL, USA, December 5-9, 2011.

49. Hassan Takabi and James B. D. Joshi, "Policy Management as a Service: An Approach to Manage Policy Heterogeneity in Cloud Computing Environment," In Proc. 45th *Hawaii International Conference on System Sciences* (HICSS), Hawaii, USA, January 4-7, 2012.

50. Amirreza Masoumzadeh, James Joshi, "An Alternative Approach to k-Anonymity for Location-Based Services," *The 8th International Conference on Mobile Web Information Systems* (MobiWIS 2011), Procedia CS Vol:5: 522-530 (2011)

51. Baracaldo, Nathalie; Masoumzadeh, Amirreza; Joshi, James; "A Secure, Constraint-aware Role-based Access Control Interoperation Framework," T*he 5th International Conference on Network and System Security* (NSS), Italy, 2011

52. Saman Taghavi Zargar, Hassan Takabi, and James B. D. Joshi, "DCDIDP: A Distributed, Collaborative, and Data-driven Intrusion Detection and Prevention Framework for Cloud Computing Environments.", the 7th *Intl Conference on Collaborative Computing: Networking, Applications and Worksharing* (CollaborateCom 2011), October 15-18, 2011, Orlando, FL.

53. Saman Taghavi Zargar, Hassan Takabi, and James B. D. Joshi, "DCDIDP: A Distributed, Collaborative, and Data-driven IDP Framework for Cloud", the 14th *International Symposium on Recent Advances in Intrusion Detection* (RAID'11)(Poster), September 20-21, 2011, Menlo Park, CA.

54. Youna Jung, Minsoo Kim, James B. D. Joshi, "DRiBAC: Context-Aware Dynamic Role Interaction Access Control", In Proc. of 12th *International Conference of Information Reuse and Integration*, pp. 88 – 93, USA, 2011

55. Lei Jin, Hassan Takabi, and James B.D Joshi, "Towards Active Detection of Identity Clone Attacks on Online Social Networks", *In Proc. of the ACM Conference on Data and Application Security and Privacy* (CODASPY 2011), San Antonio, TX, USA, 21-23 February 2011. (***Best Paper Award***)

56. Saman Taghavi Zargar, and James B. D. Joshi, "A Collaborative Approach to Facilitate Intrusion Detection and Response against DDoS Attacks", *the 6th Int'l Conference on Collaborative Computing: Networking, Applications and Worksharing* (CollaborateCom 2010), October 9-12, 2010, Chicago, IL.

57. Amirreza Masoumzadeh and James Joshi, "Preserving Structural Properties in Anonymization of Social Networks," *in Proc. 6th International Conference on Collaborative Computing: Networking, Applications and Worksharing* (CollaborateCom 2010), Chicago, IL, USA, Oct. 9-12, 2010.

58. Amirreza Masoumzadeh and James Joshi, "OSNAC: An Ontology-Based Access Control Model for Social Networking Systems," *in Proc. 2nd IEEE Int'l Conference on Social Computing Information* (SocialCom 2010), Minneapolis, MN, USA, Aug. 20-22, 2010.

59. Hassan Takabi, James B. D. Joshi, and Gail-Joon Ahn, "SecureCloud: Towards a Comprehensive Security Framework for Cloud Computing Environments", *In Proc. of the First IEEE International Workshop on Emerging Applications for Cloud Computing* (CloudApp2010). Held in conjunction (COMPSAC 2010), Seoul, Korea, July 19-23, 2010.

60. Lei Jin, Hassan Takabi, and James B.D Joshi, "Security and Privacy Risks: Using Email Address as Identity", *In Proc. of the Second IEEE International Conference on Information Privacy, Security, Risk and Trust* (PASSAT2010), Minneapolis, USA, August 20-22, 2010.

61. Xuelian Long and James Joshi. "Enhanced One-Pass IP Multimedia Subsystem Authentication Protocol for UMTS." *International Communications Conference* (ICC2010), South Africa, May 23-27, 2010

62. Hassan Takabi and James Joshi. "StateMiner: An Efficient Similarity-Based Approach for Optimal Mining of Role Hierarchy." *In Proc. ACM Symposium on Access Control Models and Technologies* (SACMAT), Pittsburgh, June 9-11, 2010. (Hassan Takabi received ***Korfhage Best Paper Award, School of Information Sciences, University of Pittsburgh***)
63. Guo, Yanhui & Joshi, James. "Topic-based Personalized recommendation for Collaborative Tagging System," *ACM Hypertext-2011*, Toronto, Canada, June 13-16, 2010
64. Yue Zhang and James B.D. Joshi, "An Implementation Architecture of the GTRBAC Model", 2010 *International Conference on Computer Design and Applications* (ICCDA-10), Jun. 2010, Qinghuangdao, Hebei, China
65. Yue Zhang and James B.D. Joshi, "Understanding Access Control Challenges in Loosely-Coupled Multidomain Environment", *12th International Conference on Enterprise Information Systems* (ICEIS-10), Jun. 2010, Funchal, Madeira, Portugal
66. Yue Zhang and James B.D. Joshi, "Role Based Domain Discovery in Decentralized Secure Interoperations", *2010 International Symposium on Collaborative Technologies and Systems* (CTS-10), May. 2010, Chicago, IL
67. Amirreza Masoumzadeh, James Joshi, and Hassan A. Karimi, "LBS (k,T)-Anonymity: A Spatio-Temporal Approach to Anonymity for Location-Based Service Users," *in Proc. 17th ACM SIGSPATIAL GIS*, Seattle, WA, USA, Nov. 4-6 2009.
68. Hassan Takabi, James B. D. Joshi, and Hassan A. Karimi. A Collaborative K-anonymity Approach for Location Privacy in Location-Based Services. In *Proc. the 5th Int'l Conference on Collaborative Computing: Networking, Applications and Worksharing* (CollaborateCom 2009), Crystal City, Washington D.C., USA, November 11-14, 2009.
69. Hassan Takabi, Minsoo Kim, James B. D. Joshi, and Michael B. Spring. An Architecture for Specification and Enforcement of Temporal Access Control Constraints using OWL. *In Proc. 2009 ACM Workshop on Secure Web Services (SWS 2009), Held in conjunction with the 16th ACM Conference on Computer and Communications Security* (CCS 2009), pages 21–28. Chicago, IL, USA, November 13, 2009.
70. Hassan Takabi and James B. D. Joshi. An Efficient Similarity-Based Approach for Optimal Mining of Role Hierarchy. *In Proc. 16th ACM Conference on Computer and Communications Security* (CCS 2009)(Poster), Chicago, IL, USA, November 9-13, 2009.
71. Saman Taghavi Zargar, Martin B.H. Weiss, and James B. D. Joshi, "Security Issues in Dynamic Spectrum Access", the *37th Research Conference on Communication, Information and Internet Policy* (TPRC '09), September 25-27, 2009, Arlington, VA.
72. Saman Taghavi Zargar, M. Amir Moulavi, Rajkumar Buyya, Mahmoud Naghibzadeh, and James B. D. Joshi, "RRNA: Reliable Soft Real-Time Network Aware Grid Scheduling Algorithm Using Round Trip Time", *12th Communications and Networking Simulation Symposium* (CNS'09), March22 -27, 2009, San Diego, CA.
73. Amirreza Masoumzadeh and James B. D. Joshi, "PuRBAC: Purpose-aware role-based access control," *in Proc. 3rd Int'l Symposium on Information Security*, Lecture Notes in Computer Science. Springer, Nov. 10-11 2008.
74. Yue Zhang and James B.D. Joshi, "Temporal UAS: Supporting Efficient RBAC Authorization in Presence of the Temporal Role Hierarchy", *IEEE/IFIP International Symposium on Trust, Security and Privacy for Pervasive Applications* (TSP-08), Dec. 2008, ShangHai, China
75. Youna Jung, Amirreza Masoumzadeh, James B.D. Joshi, Minkoo Kim, " RiBAC: Role Interaction based Access Control Model for Community Computing", *The 4th International*

Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom2008), Nov.13-16, 2008, Orlando, FL, USA.

76. Minsoo Kim, James B.D. Joshi, Minkoo Kim, " Access Control for Cooperation Systems based on Group Situation", The *4th International Conference on Collaborative Computing: Networking, Applications and Worksharing* (CollaborateCom2008), Nov. 13-16, 2008, Orlando, FL, USA
77. Yue Zhang and James B.D. Joshi, "UAQ: A Framework for User Authorization Query Processing in RBAC extended with Hybrid Hierarchy and Constraints", *ACM symposium on access control models and technologies* (SACMAT), Jun. 2008, Estes Park, CO.
78. Yue Zhang and James B.D. Joshi, "A request-driven secure interoperation framework in loosely-coupled multi-domain environments employing RBAC policies," International Conference on Collaborative Computing: Networking, Applications and Worksharing, 2007. CollaborateCom 2007.; 12/2007
79. Yue Zhang, James Joshi, "SRBAC07: A Scoped Administration Model for RBAC with Hybrid Hierarchy," *The Third International Symposium on Information Assurance and Security*, August 29-31, 2007, Manchester, United Kingdom.
80. Yue Zhang, James Joshi, "ARBAC07: A Role-based Administration Model for RBAC with Hybrid Hierarchy," *IEEE Proceedings of the International Conference on Information Reuse and Integration*, Las Vegas, Aug13-15, 2007.
81. Summit R. Tuladhar, Carlos E. Caicedo, James B. D. Joshi, "Inter-Domain Authentication for Seamless Roaming in Heterogeneous Wireless Networks," *IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing*, June 11-13, 2008 Taichung, Taiwan.
82. Carlos E. Caicedo, James B. D. Joshi, "Security Issues in IPv6," ITERA-08, March 27-29, 2008
83. Kai Ouyang James B. D. Joshi, "CT-RBAC: A Temporal RBAC Model with Conditional Periodic Time," *Third International Workshop on Information Assurance*, New Orleans, April 2007.
84. Michael Chuang, Suronapee Phoomvuthisarn, James B. D. Joshi, "An Integrated Framework for Trust-Based Access Control for Open Systems," *CollaborateCom* 2006, GA, USA.
85. Jun-Hyung Park, Min-Soo Kim, Bong-Nam Noh, James B. D. Joshi, "A Similarity based Technique for Detecting Malicious Executable files," *IEEE Proceedings of the International Conference on Information Reuse and Integration*, Hawaii, 2006.
86. Siqing Du, James B. D. Joshi, "Supporting Authorization Query and Inter-domain Role Mapping in Presence of Hybrid Role Hierarchy," *The 11th ACM Symposium on Access Control Models and Technologies*, USA, June 2006.
87. James B. D. Joshi, Elisa Bertino, "Fine-grained Role-based Delegation in Presence of Hybrid Role Hierarchy," *The 11th ACM Symposium on Access Control Models and Technologies*, USA, June 2006.
88. Suroop M Chandran, Korporn Panyim, James B. D. Joshi, "A Requirements-Driven Trust Framework for Secure Interoperation in Open Environments", *The Fourth International Conference on Trust Management*, (iTrust-06), May 16-19, Italy, 2006.
89. Suroop M Chandran, James B. D. Joshi, "LoT RBAC: A Location and Time-based RBAC Model", *Proceedings of the 6th International Conference on Web Information Systems Engineering* (WISE 2005), New York, Nov 2005.

90. Suroop M Chandran, James B. D. Joshi, “Towards Administration of a Hybrid Role Hierarchy", *IEEE International Conference on Information Reuse and Integration*, Las Vegas, Aug 15-17, 2005.
91. Smithi Piromruen, James B. D. Joshi, “An RBAC Framework for Time Constrained Secure Interoperation in Multi-domain Environment,” *IEEE Workshop on Object-oriented Real-time Databases* (WORDS-2005), 2005.
92. Basit Shafiq, Ammar Masood, and Arif Ghafoor, James B. D. Joshi, "A Role-Based Access Control Policy Verification Framework for Real-Time Systems", *IEEE Workshop on Object-oriented Real-time Databases* (WORDS-2005), 2005.
93. Rafae Bhatti, James B. D. Joshi, Elisa Bertino, Arif Ghafoor, “X-GTRBAC Admin: A Decentralized Administration Model for Enterprise Wide Access Control”, *The 9th ACM Symposium on Access Control Models and Technologies*, New York, June 2004.
94. James B. D. Joshi, Elisa Bertino, Basit Shafiq, Arif Ghafoor, “Dependencies and Separation of Duty Constraints in GTRBAC”, *The 8th ACM Symposium on Access Control Models and Technologies*, Como, Italy, June 2003.
95. Rafae Bhatti, James B. D. Joshi, Elisa Bertino, Arif Ghafoor, “Access Control in Dynamic XML-based Web-Services with X-RBAC”, The *First International Conference in Web Services*, June 23-26, Las Vegas, Nevada, 2003.
96. James B. D. Joshi, Elisa Bertino, Arif Ghafoor, "Hybrid Role Hierarchy for Generalized Temporal Role Based Access Control Model,” *26th Annual International Computer Software and Applications Conference Workshop*, (COMPSAC 2002 Workshop), Oxford, England, 26-29th August, 2002, pp. 951-956.
97. James B. D. Joshi, Elisa Bertino, Arif Ghafoor, “Temporal Hierarchy and Inheritance Semantics for GTRBAC,” *The 7th ACM Symposium on Access Control Models and Technologies*, June 3-4, 2002, Moterey, CA, pp 74-83.
98. J. Joshi, A. Ghafoor, “A Petri-Net Based Multilevel Security Specification Mechanism for Multimedia Documents in a Multidomain Environment,” *The Second Annual Systems Security Engineering Conference*, February 28 – March 2, 2001, Orlando, FL.
99. J. Joshi, A. Ghafoor, “A Petri-Net Based Multilevel Security Specification Model for Multimedia Documents,” *IEEE International Conference on Multimedia and Expo*, New York, USA, July 30-August 2, 2000, pp 533-536.
100. S. Sedigh, J. Joshi, A. Bashandy, A. Ghafoor, “Quality Based Evaluation of Filtering Mechanisms in MPEG Video Communications,” *Proc. of 17th IEEE Symposium on Reliable and Distributed Computing*, West Lafayette, IN, USA, October 20-23, 1998, pp. 449-454.

Technical Reports

1. James Joshi, Rafae Bhatti, Elisa Bertino, Arif Ghafoor, “X-RBAC: An Access Control Language for Multi-domain Environments,” CERIAS TR 2004-46.
2. Basit Shafiq, James B. D. Joshi, Arif Ghafoor “A Petri-net Model for Verification of RBAC Policies,” *CERIAS Technical Report* TR 2002-33, Purdue University, 2003.
3. Joshi, J., Bhatti, R., Bertino, E., Ghafoor, A., “X- RBAC : An Access Control Language for Multi-domain Environments,” CERIAS, School of Electrical and Computer Engineering, Purdue University, Technical Report CERIAS TR 2004-46
4. Bhatti, R., Bertino, E., Ghafoor, A., Joshi, J., “XML-Based Specification for Web Services Document Security” CERIAS, School of Electrical and Computer Engineering, Purdue University, Technical Report CERIAS TR 2004-65

5. Bhatti, R., Joshi, J, Bertino, E., Ghafoor, A, "X-GTRBAC Admin: A Decentralized Administration Model for EnterpriseWide Access Control," CERIAS, School of Electrical and Computer Engineering, Purdue University, Technical Report CERIAS TR 2004-04
6. Bhatii, R., Joshi, J., Bertino, E, Ghafoor, A., "Access Control in Dynamic XML-based Web-Services with X-RBAC" CERIAS, School of Electrical and Computer Engineering, Purdue University, Technical Report CERIAS TR 2003-26
7. Joshi, J., "Generalized Temporal Role Based Access Control Model for Developing Secure Systems" CERIAS, School of Electrical and Computer Engineering, Purdue University, Technical Report CERIAS TR 2003-23
8. Shafiq, B. Joshi, J., Bertino, E., Ghafoor, A., "Optimal Secure Interoperation in a Multi-Domain Environment Employing RBAC Policies" CERIAS, School of Electrical and Computer Engineering, Purdue University, Technical Report CERIAS TR 2003-24
9. Joshi, J., Bertino, E., Shafiq, Ghafoor, A., "Dependencies and Separation of Duty Constraints In GTRBAC" CERIAS, School of Electrical and Computer Engineering, Purdue University, Technical Report CERIAS TR 2003-04
10. Joshi, J., Bertino, E., Latif, U., Ghafoor, A., "Generalized Temporal Role Based Access Control Model (GTRBAC) (Part I) - Specification and Modeling" CERIAS, School of Electrical and Computer Engineering, Purdue University, Technical Report CERIAS TR 2001-47
11. Joshi, J., Bertino, E., Shafiq, B., Latif, U., Ghafoor, A., "Generalized Temporal Role Based Access Control Model (GTRBAC) (Part II) - Expressiveness and Design Issues" CERIAS, School of Electrical and Computer Engineering, Purdue University, Technical Report CERIAS TR 2003-01
12. Shafiq, B., Joshi, J. B. D., and Ghafoor, A., "A Petri-Net Model for Verification of RBAC Policies," CERIAS, Purdue University, Technical Report TR 2002-33, 2002.
13. Shafiq, B., Joshi, J., Bertino, E., and Ghafoor, A., "Optimal Secure Interoperation in a Multi-Domain Environment Employing RBAC Policies," CERIAS, School of Electrical and Computer Engineering, Purdue University, Technical Report CERIAS TR 2003-24, 2003.
14. Joshi, J. Bertino, E. Ghafoor, A., "Temporal Hierarchy and Inheritance Semantics for GTRBAC" CERIAS, School of Electrical and Computer Engineering, Purdue University, Technical Report CERIAS TR 2001-52
15. Joshi, J. Ghafoor, A., Aref, W. G., Spafford, E., "Digital Government Security Infrastructure Design Challenges" CERIAS, School of Electrical and Computer Engineering, Purdue University, Technical Report CERIAS TR 2001-31
16. Joshi, J., Ghafoor, A., "A Petri-net Based Multilevel Security Specification Model for Multimedia Documents" CERIAS, School of Electrical and Computer Engineering, Purdue University, Technical Report CERIAS TR 2000-09
17. Joshi, J., Ghafoor, A, "A Petri-net Based Multilevel Security Specification Model for Multimedia Documents" CERIAS, School of Electrical and Computer Engineering, Purdue University, Technical Report CERIAS TR 2000-09

KEYNOTES/TALKS & PANELS

KEYNOTE / TALKS

1. **Keynote** at University of South Dakota's 4th annual Artificial Intelligence Symposium, sponsored by IEEE, April 11, 2024
    - Title: "*Privacy, Ethics and Responsible AI: Challenges and Road ahead*"

2. **Keynote** at TDK Corporation, Tokyo Headquarters (Kick-off meeting of corporate leadership), March 27, 2024
    - **Title**: "Cybersecurity, Privacy and Trustworthy AI: Opportunities for Global Leadership in Digital Transformation and Societal Impact"
3. **Invited Talks on** "NSF SaTC Transition to Practice"
    - DHS Workshop on Privacy Enhancing Technology, June 21, 2022
    - US-Japan PETs Workshop, June 16, 2022
4. **Keynote**: "Overview of SaTC & Privacy: Challenges and road ahead," Third Annual Workshop on Emerging Data Science Methods for Complex Biomedical and Cyber Data, March 16-17, 2023
5. **Keynote**: "*Privacy in the Age of AI/ML*" @ CSIRO's Data61 & DST Cyber security Summer School, Feb 21-23, 2022, Australia (Virtual)
6. **Keynote**: "*Privacy in the AI-Enabled World*" @ The 22nd International Conference on Web Information Systems Engineering Oct 26-29, 2021, Melbourne, Australia (Virtual)
7. **Keynote**: "*Privacy – Challenges and Directions*" @ Inter International Conference on Secure Knowledge Management in the AI Era Oct 8-9, 2021, San Antonio, TX, USA (Virtual)
8. **Talk at Cybersecurity Faculty Development Workshop**, University of Tennessee @ Chattabooga; Title: "*Cybersecurity and Privacy: NSF Programs and Funding Opportunities*," June 28-30, 2021
9. **Distinguished Speaker** at IUPUI: Title: "*Towards Secure and Privacy-Aware Cloud Environments,"* (*followed by SaTC overview*), March 12, 2021
10. **Invited Talk** at *Missouri University of S&T*, Rolla; Title 1: "*Towards Privacy-Preserving Access Control and Authority Transparency*"; Title 2: "*SaTC and related opportunities*" (Dec 14, 2020):
11. **Visionary Talk** at the Fourth *Workshop for Women in Hardware & Systems Security* (WISE); Title: "*Overview of NSF SaTC and related Programs and Opportunities*." (Dec 14, 2020);
12. **Invited Speaker** at the 13th Annual Cyber Security Day at Indiana University of Pennsylvania; Title: "*Cybersecurity and Privacy: Challenges Ahead*" (Oct 20, 2020)
13. **Keynote** at ACM CODASPY 2020; Title: "*Towards Privacy-Preserving Access Control and Authority Transparency,*" (Aug 3, 2020)
14. **Keynote** at "Intelligent and Resilient Power Grid Infrastructure" Workshop at the (March 9, 2020) – University of Pittsburgh; Title: "Computer & Information Science & Engineering (CISE)/SaTC and Other Programs"
15. **Talk** at US NSF; Title: "NSF and My Vision for Secure and Trustworthy Computing", Spring, 2019
16. **Invited Speaker** at the 10th Annual Cyber Security Day at Indiana University of Pennsylvania; Title: "*Insider Threats: Challenges and Mitigation Approaches*" (Oct 26, 2017)
17. **Invited Talk** at *Emory University*; Title: "*Towards Preservation of Structural Properties in Anonymized Social Networks*," Spring, 2012
18. **Invited Talk** at *Kathmandu University*, Nepal; Title: "*Towards Defending Against Identity Clone Attacks on Online Social Network*s" at, Summer, 2011
19. **Invited Talk** at *Siam University*, Thailand "GTRBAC and Expressiveness Design Issues in Advanced RBAC models," Summer, 2011

20. **Invited Talk** at CERAIS, Purdue; Title: "GTRBAC: A Generalized Temporal Role based Access Control Model", (Fall, 2004);

PANELS

1. **Panelist** in **Panel**: Cybersecurity and Privacy: Closing the Gap Between Theory and Practice
   - SaTC PI Meeting, Sept 4-5, 2024, Pittsburgh
2. **Panelist** in **Panel**: Public and private sector initiatives to foster PET adoption
   - Singapore-OECD Expert Workshop on Privacy Enhancing Technologies, Jul 16, 2024
3. **Panel Moderator/organizer** for the following panels:
   - AI Impact and Challenges in Industry and Government @IEEE CIC 2023
   - Grand Challenges in Cybersecurity and Privacy @IEEE TPS 2023
4. **Panel Moderator**/organizer: "Data Privacy Research in US," Privacy Symposium, April 5-6, 2022
5. **Panelist** in session on "International Cooperation for Research on Privacy and Data Protection" Privacy Symposium, April 17-21, 2023 (Venice)
6. **Panelists** - Third Annual Workshop on Emerging Data Science Methods for Complex Biomedical and Cyber Data, March 16-17, 2023
7. **Panel Talk** "Privacy and AI," Veteran's Affairs NAII Brain Summit, Sept 7, 2022

PhD COMMITTEES

Committee Chair

Current

1. Maryam Aldairi (started in Fall, 2017), Dissertation proposal done
2. Peilin He (Current PhD student), Started in 2023
3. Liou Tang, (Current PhD student), Started in 2024

Graduated

4. Yue Zhang, (**Graduated** in 2010), Current: Senior Software Engineer, Yahoo; Previous: Google, Inc (Interned at IBM Watson)
5. Daniel Takabi (**Graduated** in Summer 2013), Director of School of Cybersecurity, Old Dominion University; Previous: University of North Texas and Georgia State University (Interned at Cisco); Interned at Cisco
6. Amirreza Masoumzadeh (**Graduated** in Summer, 2014) – Associate Professor, CS, SUNY, Albany
7. Saman Taghavi Zargar (**Graduated** in Summer, 2014) - Software Development Manager at Amazon EMR Spark; Previous: Cisco, Salesforce (Interned at Cisco twice; first job at Cisco)
8. Xuelian Long (**Graduated** in Summer, 2015), Facebook, Inc (Interned at TripAdvisor)
9. Nathalie Baracaldo (**Graduated** in Spring, 2016), Technical Manager of AI Security and Privacy Solutions; senior Research Scientist & Master Inventor, IBM Almaden Research (Interned at IBM Almaden Research two times)

10. Runhua Xu (**Graduated**, Summer 2020), Current: Professor, Beihang University; Previous: Research Staff at IBM Almaden Research (Interned at IBM Almaden Research)
11. Leila Karimi (**Graduated** in Summer, 2021), Current: Meta (Software Engineer); Previous: Datometry Inc. (Research Scientist in Cybersecurity)

PhD Committee Member

1. Ajesh Koyatan Chathoth, (CS, SCI, University of Pittsburgh)
2. Jingzhe Wang (DINS, SCI, University of Pittsburgh)
3. Kuheli Sai (DINS, SCI, University of Pittsburgh)
4. Faris Alotibi (DINS, SCI, University of Pittsburgh)
5. Xiaoyu Liang (CS, SCI, University of Pittsburgh) (Status: Graduated)
6. Chao Li, (DINS, SCI, University of Pittsburgh) (Status: Graduated)
7. Jinlai Xu (DINS, SCI, University of Pittsburgh (Status: Graduated)
8. Farhod Yuldashev, (PhD in GSPIA, University of Pittsburgh) (Status: Graduated)
9. Tanapat Anusas-Amornkul (Tel, University of Pittsburgh), "On detection mechanisms and their performance for packet dropping attack in ad hoc networks" (Status: Graduated)
10. Saowaphak Sasanus (Tel, University of Pittsburgh), "Adaptive Multi-class Signaling Overload Control for Cellular Networks," (Status: Dissertation Proposal)
11. Haidong Xia (CS, University of Pittsburgh), "Using Secure CoProcessor to Enforce Network Access Policies in Enterprise and Ad Hoc Networks, (Graduated)
12. Phongsak Kiratiwintakorn (Telcom, University of Pittsburgh), "Energy Efficient Security Framework For Wireless Local Area Networks, (Status: Graduated)
13. Siqing Du (IS, University of Pittsburgh), 2007
14. Jiang Zheng (CS, University of Pittsburgh), 2008
15. Ricardo Villamarin-Salomon (CS, University of Pittsburgh), 2008

External Reviewer

1. Harsha Pussewalage, Agder University, Norway (Summer, 2019) – as an Opponent.
2. Sadhana Jha, IIT Kharagpur, India (Summer, 2018)
3. Cuneyt Gurcan Akcora, "Profiling User Interactions on Online Social Networks," (Advisor: Elena Ferrari and Barbara Carminati), Universitàdegli Studi dell'Insubria – Varese (2013)
4. Igor Nai Fovino, "Privacy Preserving Data Mining - Concepts, Techniques and evaluation Methodologies," Universitàdegli Studi di Milano (Main Advisor: Elisa Bertino; graduated.
5. Giovanni Mella, "Disitributed and Cooperative Updates of XML Documents," Università degli Studi di Milano (Main Advisor: Elisa Bertino; graduated).
6. Stefano Franzoni (CS, PhD Candidate), University of Milan, graduating in 2007.

PROFESSIONAL ACTIVITIES

Editor-in-Chief

1. IEEE Transactions on Services Computing (Jan, 2017 – Dec, 2021)
2. EAI Endorsed Transactions on Collaborative Computing (**Founding co-EiC**: 2014 – 2015)

Associate Editor / Editorial Review Board

1. Associate Editor, ACM Transactions on Privacy and Security (2023 – present)
2. EB Member of ACM Transactions on Digital Threats: Research and Practice (Since 2018)
3. EB Member of Springer's Journal of BigData (Since 2013)
4. Associate Editor Associate Editor of IEEE Transactions on Services Computing (Since Jan 2013 - 2016)
5. EB Member of International Journal of Multimedia and Ubiquitous Engineering (Since 2007; few years)
6. EB Member of International Journal of E-Business Research (Since Jan, 2005 till 2011)
7. EB Member of International Journal of Network Security (June, 2005 – June, 2007)

Steering Committees

1. **Founding Chair** of Steering Committee of International Conference on Trust, Privacy and Security of Intelligent Systems, and Applications (IEEE TPS) (2019 – current)
2. **Founding Chair** of Steering Committee of IEEE International Conference on Cognition Machine Intelligence and (IEEE CogMI) (2019 – current)
3. **Founding Chair** of Steering Committee of IEEE International Conference on Collaboration and Internet Computing (IEEE CIC) (2015 – current)
4. Co-Chair of CollaborateCom Steering Committee (Nov 2012 - 2014)
5. Member of IEEE IRI Steering committee (2014 – current)
6. Member of ACM SACMAT Steering Committee (2011 – 2017)
7. Member of Steering Committee of IEEE International Conference on Multimedia & Expo (IEEE ICME) – IEEE CS representative (2013 - 2015)

IEEE/ACM Committee Memberships

1. ACM Provenance Working Group – part of ACM US Technology Policy Committee (2024-)
2. IEEE Fellows Committee membership (2023, 2024)
3. Member 2022 IEEE Computer Society Pubs Board ad hoc committee on new topic areas (2023)
4. 2020 - 2023 IEEE Innovation in Societal Infrastructure Award Committee (**Chair: 2020-2022; member 2023**)
5. 2019 IEEE Innovation in Societal Infrastructure Award Committee (Member)
6. EiC Search Committee for ACM Transactions on Internet Computing (June, 2018)
7. EiC Search Committee for IEEE Internet Computing (Done in May, 2018)
8. EIC Search Committee for IEEE Transactions on Dependable and Secure Computing (Done in Fall, 2017)
9. EIC Search Committee for IEEE Transactions on Multimedia (Done in Summer, 2017)

10. 2014 & 2015 IEEE CS Technical Achievement Award Committee
11. IEEE Technical Committee on Multimedia (TCMC) SIG on Multimedia Security and Privacy; (**Chair**; 2016 -present)
    a. Member of TCMC Special Issue Evaluation Committee (Spring, 2016)
12. Nomination Committee of IEEE CS Technical Committee on Semantic Computing for TC Chair Election (2014)

General (Co) Chair

1. ACM CODSAPY 2025, Pittsburgh, PA
2. The 4th International IEEE Conference on Collaboration and Internet Computing (CIC 2018), Philadelphia, Oct 18-20, 2018, PA, USA
3. The 8th International Conference on Collaborative Computing: Networking, Applications and Worksharing (*CollaborateCom-2011*), USA, 2012
4. The 7th International Conference on Collaborative Computing: Networking, Applications and Worksharing (*CollaborateCom-2011*), USA, 2011
5. The 15th ACM Symposium on Access Control Models and Technologies, SACMAT2010, USA, 2010.
6. The 6th International Conference on Collaborative Computing: Networking, Applications and Worksharing (*CollaborateCom-2010*), USA, 2010
7. The 5th International Conference on Collaborative Computing: Networking, Applications and Worksharing (*CollaborateCom-2009*), USA, 2009

[Workshop]

8. The 9th International Workshop on Trusted Collaboration *(Aug, TrustCol 2014)*
9. The 8th International Workshop on Trusted Collaboration (TrustCol 2013)
10. The 7th International Workshop on Trusted Collaboration (TrustCol 2012)
11. The 6th International Workshop on Trusted Collaboration (TrustCol 2011)
12. The 5th International Workshop on Trusted Collaboration (TrustCol 2010)

Program Chair or Track Chair

1. 11th International Conference on Mathematics and Computing, Jan 9-11, 2025, India
2. IEEE 25th International Conference on Information Reuse and Integration for Data Science, San Jose, CA, USA, Aug 7-9, 2024
3. IEEE International Conference on Edge Computing (IEEE EDGE part of IEEE SERIVICES), July 8-13, Milan, Italy, 2019,
4. IEEE Information Reuse & Integration (IEEE IRI) in Data Science, 2019, (Jul-Aug, 2019)
5. International Conference on Blockchain (ICBN; part of SCF SERVICES), 2019
6. IEEE Big Data 2016, Washington D.C., USA
7. The IEEE International Conference on Information Reuse and Integration, USA, 2016 (IRI2016), Pittsburgh, USA

8. The First International Conference on Collaboration and Internet Computing (IEEE CIC 2015), Hangzhao, China, 2015
9. The IEEE International Conference on Information Reuse and Integration, USA, 2015 (IRI2015), San Francisco, USA
10. **Area-Lead** of Cloud Security at IEEE CLOUD 2015
11. IEEE ISM 2014: IEEE International Symposium on Multimedia (Dec, 2014)
12. The IEEE International Conference on Information Reuse and Integration, USA, 2014 (IRI2014)
13. The IEEE International Conference on Information Reuse and Integration, USA, 2013 (IRI2013)
14. SafeConfig 2013: IEEE 6th Symposium on Security Analytics and Automation (Collocated with IEEE Conference on Communications and Network Security)
15. The IEEE International Conference on Information Reuse and Integration, Las Vegas, 2012 (IRI2012)
16. The IEEE International Conference on Information Reuse and Integration, Las Vegas, 2011 (IRI2011)
17. IEEE COMPSAC 2010 (**Track: Security**)
18. The IEEE International Conference on Information Reuse and Integration, Las Vegas, 2010 (IRI2010)
19. The 14th ACM Symposium on Access Control Models and Technologies, SACMAT09, Italy, 2009.
20. The 4rd International Conference on Collaborative Computing: Networking, Applications and Worksharing (*CollaborateCom-2008*), Florida, USA, 2008
21. IEEE COMPSAC 2009 (Track: Social and Collaborative Networks)
22. The IEEE International Conference on Information Reuse and Integration, Las Vegas, 2007
23. The IEEE International Conference on Information Reuse and Integration, Hawaii, 2006
24. **Program Vice Co-chair** of Multimedia Security Track at 2007 IEEE International Symposium on Multimedia (ISM'07), Taiwan, December, 2007.

[Workshop]

25. IEEE C-Big: Workshop on Collaborative BigData (Oct, 2014)
26. 2009 International Workshop on Network Assurance and Security Services in Ubiquitous Environments (NASSUE-2009)
27. IEEE International Workshop on Trusted Collaboration (TrustCol-07), New York, 2007.
28. IEEE International Workshop on Trusted Collaboration (TrustCol-06), Georgia, 2006.
29. IEEE International Workshop on Information Assurance, (with IPCCC-07), New Orleans, 2007.
30. IEEE International Workshop on Information Assurance, (with IPCCC-06), Phoenix, 2006.
31. IEEE International Workshop on Information Assurance, (with IPCCC-04), Phoenix, 2004.

Test of Time Best Paper Awards Chair

1. ACM SACMAT 2019

Finance Co-Chair

2. The Third International Conference on Collaboration and Internet Computing (IEEE CIC 2017), San Jose, USA, 2017.
3. The Second International Conference on Collaboration and Internet Computing (IEEE CIC 2016), Pittsburgh, USA, 2016.

Sponsorship Co-Chair;

1. IEEE IRI 2017, Salt Lake City, USA, Jul 7-9, 2018

Panels Co-Chair

1. The 6th International Conference on Collaborative Computing: Networking, Applications and Worksharing (*CollaborateCom-2010*), USA, 2010
2. The 13th ACM Symposium on Access Control Models and Technologies, SACMAT08, USA, 2008.

Workshop Chair

1. Very Large Databases 2012 (*VLDB2012*), Turkey, 2012
2. Workshop on Cooperative Autonomous Resilient Defenses in Cyberspace *(CyberCARD 2011),* DC. USA, Jan 2011
3. The 3rd International Conference on Collaborative Computing: Networking, Applications and Worksharing (*CollaborateCom-2007*), New York, USA, 2007
4. The 2nd International Conference on Collaborative Computing: Networking, Applications and Worksharing (*CollaborateCom-2006*), Georgia, USA, 2006

Publicity Chair

1. IEEE CIC 2018, Philadelphia, USA, Oct 18-20, 2018
2. The First International Workshop on Research Challenges in Next Generation Networks for First Responders and Critical Infrastructures, in conjunction (with IEEE IPCCC), New Orleans, Louisiana, April 11-13, 2007.
3. The IEEE International Conference on Information Reuse and Integration, Las Vegas, 2005.

Panelist/Panel Moderator

1. IEEE BigData 2016 "Big Data Security and Privacy" panelist.
2. CollaborateCom 2014 (Panel Moderator): BigData – Challenges and Opportunities
3. The 9th ACM Symposium on Access Control Models and Technologies, SACMAT 2004, New York; Panel title: Security for Grid-based Computing Systems Issues and Challenges.

Session Chair

1. The 9th ACM Symposium on Access Control Models and Technologies, SACMAT 2004, New York
2. The IEEE International Conference on Information Reuse and Integration, Las Vegas, 2005
3. The IEEE International Conference on Information Reuse and Integration, Hawaii, 2006
4. The IEEE International Conference on Information Reuse and Integration, Las Vegas, 2007
5. The 2nd International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom-2006), Georgia, USA, 2006
6. International Workshop on Information Assurance, (with IPCCC-07), New Orleans, 2007.
7. International Workshop on Information Assurance, (with IPCCC-06), Phoenix, 2006.

8. International Workshop on Information Assurance, (with IPCCC-04), Phoenix, 2004.

Technical Program Committee Membership

1. The International Symposium on Cyber Security, Cryptology and Machine Learning (CSCML) - 2023
2. ACM SACMAT, 2023
3. ACM SACMAT 2022, ICML 2022 Workshop on Machine Learning for Cybersecurity
4. IEEE BigData 2022 PC; Osaka, Japan, Dec 17-20
5. ACM SACMAT 2022, 2021, SACMAT 2020, SACMAT2019, SACMAT2018, SACMAT2013, SACMAT2012, SACMAT 2011, SACMAT2008, SACMAT07, SACMAT06, SACMAT2005, SACMAT2004, SACMAT2003
6. IFIPTM'20 (IFIP WG 11.11 international Conference on Trust Management), IFIPTM 2019, IFIPTM2010, IFIPTM2009,
7. 2019 IEEE Conference on Dependable and Secure Computing - DSC 2019, China
8. ICDCS 2019: 39th IEEE International Conference on Distributed Computing System, TX, 2019 (Security, Privacy, and Trust in Distributed Systems)
9. The 5th IEEE International Conference on Multimedia Big Data (BigMM) – Singapore, 2019
10. Workshop on Distributed Analytics Infrastructure and Algorithms for Multi-Organization Federations (DAIS), 2019 (@SMARTCOMP 2019)
11. Workshop on Research for Insider Threat - WRIT 2018, WRIT 2014
12. IEEE International Conference on Services Computing (IEEE SCC) – SCC2019, SCC2018,
13. ACM Conference on Data and Applications Security and Privacy (ACM CODASPY) – CODASPY 2017, CODASPY 2016, CODASPY 2015
14. The 25th ACM International Conference on Information and Knowledge Management (CIKM 2016)
15. International Conference on Network and System Security: NSS 2018 NSS2013, NSS2012
16. 1st IEEE International Conference on Multimedia Big Data BigMM 2015
17. Fourth International Workshop on Privacy, Security and Trust in Mobile and Wireless Systems – MobiPST 2014
18. Annual International Computers, Software & Applications Conference – COMPSAC 2014, COMPSAC 2011
19. ACM Cloud and Autonomic Computing Conference – CAC 2013
20. International Conference on Social Informatics -- SoCInfo2012, SoCInfo2011,
21. IEEE/EAI International Conference on Collaborative Computing: Networking, Applications and Worksharing: CollaborateCom2013, CollaborateCom2012, CollaborateCom2011, CollaborateCom2010, CollaborateCom2007, CollaborateCom2006
22. ASE/IEEE International Conference on Privacy, Security, Risk and Trust - PASSAT2012
23. LBSN2012, PST2011, MobiWIS2011, WSRAS2012
24. ACM Workshop on Security and Privacy in GIS and LBS -- SPRING11, SPRINGL10, SPRINGL09,
25. SSC09, SSC09, WWW2009Posters, WWW2011Posters
26. ICC'08 - Wireless Networking Symposium, Beijing, China, 2008.

27. The 14th International MultiMedia Modeling (MMM), Kyoto, Japan, Jan, 2008.
28. ICIW 2007 committee, Peter Kiewit Institute, University of Nebraska Omaha, USA on the 24-25 April 2008
29. 2nd International Conference on Information Warfare and Security, Naval Postgraduate School, Monterey, California, USA, 8-9 March 2007
30. The 8th IFIP Working Conference on Virtual Enterprises (PRO-VE'07), Guimaraes, Portugal, 10-12 Sept, 2007
31. The Third IEEE International Workshop on Multimedia Information Processing and Retrieval (IEEE-MIPR 2007) will take place in Taichung, Taiwan, R.O.C. on December 10-12, 2007.
32. 3rd international workshop on security in systems and networks (SSN 2007), to be held in conjunction with 21st IEEE IPDPS March 26-30, 2007, Long Beach, California, USA.
33. The Second IEEE International Workshop on Multimedia Information Processing and Retrieval (MIPR'06), in conjunction with IEEE International Symposium on Multimedia (ISM2006), San Diego, California, USA, December 11-13, 2006.
34. 3rd IEEE Workshop on Situation Management (SIMA 2007) at MILCOM 2007, Orlando, Florida, Oct 29-31, 2007
35. Workshop on Parallel and Distributed Multimedia Computing (ParDMCom-06) held in conjunction with ISPA-06: The International Symposium on Parallel and Distributed Processing and Application, Sorrento, Italy, December 1 -4, 2006
36. The Second IEEE LCN Workshop on Network Security (WNS 2006) Tampa, Florida, U.S.A. 14 November 2006
37. The 2007 International Conference on Genetic and Evolutionary Methods (GEM'07) (*Honorary*)
38. The 2007 International Conference on Bioinformatics and Computational Biology (BIOCOMP'07) (*Honorary*)
39. The 8th IFIP Working Conference on Virtual Enterprises (PRO-VE'07), Guimaraes, Portugal, 10-12 Sept, 2007
40. The First International Workshop on Research Challenges in Next Generation Networks for First Responders and Critical Infrastructures, in conjunction (with IEEE IPCCC), New Orleans, Louisiana, April 11-13, 2007.
41. International Conference on E-business (ICE-B), 28-31 July, Barcelona, Spain.
42. First International Workshop on Trust and Reputation Management in Massively Distributed Computing Systems (TRAM 2007), to be held in conjunction withThe 27th International Conference on Distributed Computing Systems (ICDCS 2007), Toronto, Canada, June 25-29, 2007.
43. Second International Workshop "Dependability Aspects on Data WArehousing and Mining applications" DAWAM 2007, in conjunction with The Second International Conference on Availability, Reliability and Security- ARES 2007.
44. The Second IEEE International Workshop on Multimedia Databases and Data Management (MDDM'07), in conjunction with 2007 IEEE 23rd International Conference on Data Engineering (ICDE 2007), April 16-20, 2007, The Marmara Hotel, Istanbul, Turkey.
45. 3rd international workshop on security in systems and networks (SSN 2007), to be held in conjunction with 21st IEEE IPDPS March 26-30, Long Beach, California, USA.

46. The 3rd International Workshop on Visualization for Computer Security (VizSec06), held in conjunction with the 13th ACM Conference on Computer and Communications Security (CCS 2006)
47. 2006 IEEE International Workshop on Multimedia Databases and Data Management (MDDM'06), in conjunction with The 22nd IEEE International Conference on Data Engineering (ICDE2006), 4/3/2006 - 4/7/2006, Atlanta, Georgia, USA.
48. International Conference on e-Business (ICE-B) (Spronsored by IEEE and ACM-SIGMIS), 2006,
49. The 10th Colloquium for Information Systems Security Education, MD, June, 2006.
50. Workshop on Parallel and Distributed Multimedia Computing (ParDMCom-06), to be held in conjunction with ISPA-06: The International Symposium on Parallel and Distributed Processing and Application, Sorrento, Italy, December 1 -4, 2006.
51. International MultiMedia Modeling Conference (MMM) 2007, Singapore, January 9-12, 2007.
52. 2007 International Conference on Multimedia and Ubiquitous Engineering (MUE 07), April 26th - 28th, 2007, Seoul Olympic Parktel, Seoul, Korea.
53. The 2nd IEEE LCN Workshop on Network Security, (WNS 206), Tampa, Florida, U.S.A. 14 November 2006.
54. International Conference on Privacy, Security and Trust (PST 2006). Theme: Bridge the Gap between PST Technologies and Business Services, Ontario, Canada, Oct 30 - Nov 1, 2006
55. The IEEE GLOBECOM 2006 Computer and Network Security Systems Symposium, San Francisco, CA, USA, 27 November - 1 December 2006 (reviewer)
56. The IEEE International Workshop on Multimedia Technology and Ubiquitous Computing (MTUC 2006) in conjunction with The IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC 2006)
57. 10th Colloquium for Information Systems Security Education (CISSE), Maryland, June, 2006
58. The 4th European Conference on Information Warfare and Security (ECIW 2006), University Of Glamorgan, UK, 2006
59. The 2nd international workshop on Security in systems and Networks (SSN'2006), to be held in conjunction with 20th IEEE IPDPS, April 25-29, Rhode Island, Greece.
60. The 5th European Conference on Information Warfare and Security (ECIW 2006), University Of Glamorgan,
61. 2005 IEEE International Workshop on Multimedia Information Processing and Retrieval (MIPR'05), in conjunction with IEEE International Symposium on Multimedia (ISM2005), Irvine, CA, December 12-14, 2005.
62. The 8th IEEE International Symposium on Object-oriented Real-time distributed Computing, May 18-20, 2005, Seattle, Washington
63. The 2005 IEEE International Conference on Information Reuse and Integration, Las Vegas, 2005
64. The International Workshop on Frontiers of Information Technology (FIT), being held on Dec. 20-21, 2004 in Islamabad, Pakistan.
65. The 4th European Conference on Information Warfare and Security (ECIW 2005), University Of Glamorgan, UK, 11-12 July 2004
66. The 1st International Workshop on Systems and Network Security (SNS 2005) Denver, Colorado, USA, April 8, 2005 (to be held in conjunction with in conjunction with the IEEE 19th IPDPS)

67. Workshop on Information Assurance, 2004, April 14-17, Phoenix, *Session Chair* and *Program Co-Chair*,
68. The 6th International Symposium on Multimedia Software Engineering (IEEE MSE'04), Florida International University, Miami, FL, USA December 13-15, 2004.
69. The Second ACM Workshop on Multimedia Databases (ACM MMDB'04) to be held in conjunction with the 13th International Conference on Information and Knowledge Management (ACM CIKM 2004).
70. The First Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services, August 22-26, 2004 - Boston, Massachusetts, USA

SERVICE AT US NATIONAL SCIENCE FOUNDATION

Program Director, SaTC (Sept, 2019 – Aug, 2023); PD Expert (Sept, 2023 – current)

[**Highlights provided earlier**]

1. Contribution to DCL on AI-Ready Testbed.
2. Lead for the development of the new NSF Program Privacy-Preserving Data Sharing in Practice (PDaSP) – launched on June 26, 2024
3. Co-Chair of Networking and Information Technology Research and Development (NITRD) - Privacy Interagency Working Group (Privacy IWG); Spring, 2021 – Aug, 2023
4. Co-Chair of NITRD Fast Track Action Committee for Advancing Privacy-Preserving Data Sharing and Analytics (developing National Strategy for PPDSA) – till Aug, 2023
5. Co-Chair of NITRD Fast Track Action Committee for developing National Digital Assets R&D Agenda (currently in progress) – till Aug, 2023
6. Member, CSIA R&D Strategic Priority Task Force, (currently ongoing)
7. NSF representative for National Security Council (NSC) Interagency Policy Subcommittee (IPC-Sub) on Digital Identity; NSC IPC-Sub on Digital Assets; NSC IPC-Sub on Privacy Preserving Machine Learning (May, 2021 – Sec, 2021)
8. Managing Panels/Proposals: that falls within *Privacy and Applied Crypto* portfolio; assist in *Systems Security* panels. Proposal categories: *Small*, *Medium* and *Frontier*/Large projects
9. Contribution in the following projects/activities (in collaboration with others)
    - Co-led US-UK PETs Prize Challenge
    - Contribution to NSF RINGS program
    - Co-Led initiation of ***Workshop*** on Secure and Privacy-preserving Federal Data Sharing (May 21, 26) (Cognizant Program Office for this project)
    - Co-led initiation of ***Workshop*** to explore Security, Privacy and Ethical issues in Health/Biomedical research to create research roadmap (May-June) (Cognizant Program Office for this project)
    - Co-led initiation of a ***Virtual Organization*** for ***Computing Research for Pandemic Preparedness and Resilience*** – the project is now called **PREPARE VO** (Cognizant Program Officer for this project): prepare-vo.org/

- NSF DCL engagements: (i) AI-Cybersecurity Education (through Dear Colleague Letter solicitation); (ii) EU-US NGI partnership
- Exploring collaborative funding opportunities with Japan and Australia

ADVISORY BOARDS

1. Member, External Advisor of Cyber Security Research Coordination Center, Australia (Dec, 2019 – 2021)
2. Member, External Advisory Board of Robert Morris University – Computer and Information Systems program (2018 – 2021)
3. CAE Advisory Board of Robert Morris University (2018-2019)

UNIVERSITY & EDUCATIONAL SERVICES

University of Pittsburgh, USA (since Fall, 2003)

1. SCI Planning and Budgeting Committee (PBC) (2023 – present)
2. University Council on Graduate Studies (UCGS) (2023 – present)
3. IPA Policy Committee (2022)
4. SCI Academic Council (2017 -2019)
5. University of Pittsburgh Executive Export Control Committee (2018 -2020)
6. SIS Council (elected)
    i. Chair (Elected 2014 – 2017)
    ii. Member (2012 – 2014)
7. *Faculty Search Committee* (2013, of two faculty members recruited)
8. *Curriculum Committee*, Graduate program in Information Science and Technology
    i. Chair in 2013 academic year
    ii. Member since 2004
9. *Chair* of the *Departmental Colloquium* Committee
    - Organizer for the Departmental Colloquium (2005 – 2006).
10. *Director* and *co-founder* of *Laboratory of Education and Research on Security Assured Information Systems* (LERSAIS)
    - Led the faculty team to get the University designated as a *National Center of Academic Excellence in Information Assurance Education* (NCAE/IAE) by the NSA and DHS.
        i. Oversaw the entire application process for original as well as the redesignation
    - Currently the *Point of Contact* for the NCAE/IAE program.
    - Established the state-of-the-art lab facility with CISCO equipment grant and DoD capacity building grant (as PI)
11. Developed Security Curriculum and formalized Security Track
    - Developed the first Certificate of Advanced Studies in SAIS Track
        i. Post-bac as well as Post-grad CAS
        ii. Preparation of online course offering in security track – starting in Spring, 2015

- Formalized the Security Assured Information Systems (SAIS) Track at SIS – first track that set the example for other tracks.
- Led the LERSAIS team towards receiving the certification for the SAIS track courses for all the five national IA standards CNSS - 4011, 4012, 4013, 4014 and 4015. Pitt was one of only about a dozen institutions with all the five certifications at that time.
- Established and currently manage the prestigious NSF-Cyber Corp SFS Scholarship Program
    i. Since 2006: two rounds of funding
    ii. Director of the SFS program
        Oversee all aspect of SFS program management including: recruitment, student evaluation, student mentoring, and students' activity planning
- *Leader* of the *Information Assurance Research Interest Group* (currently nine members) in the School of Information Sciences (SIS) (Summer, 2006-2007).
- Developed and taught three new security courses for the security track and revised over the years
    i. *Introduction to Security* (Mapped to about 85% of CNSS 4011, 4012 and 4013 standards)
    ii. *Security Management* (Mapped to CNSS 4014 and 4015)
    iii. *Developing Secure Systems*

12. External Partnerships
    - Information Resource Management College partnership for DoD IA Scholarship Program to facilitate transfer of students with IRMC certificates to pursue MSIS/MST degree programs at DIST (passed by the department)
13. Organizing Workshop/Training
    - Microsoft Onsite Security Training, Dec 2-3, 2004 – attended by 32 (students and some University personnel)
    - Cisco Professors Security Boot Camp, July 6-9, 2005

Kathmandu University, Nepal (1993 - 1996)

- Developed the first Undergraduate Computer Science and Engineering curriculum in Nepal in 1993-1994.
- Designed and taught several courses for the first time at KU (*Computer Foundation Course; Introduction to Structured Programming; Data Structures and Algorithms, Communications and Networking, Hardware and System Maintenance, and Software Lab*)
- Managed the procurement, setting-up and maintenance of KU's computer centers in the schools of Engineering, and Management