ARTIFICIAL INTELLIGENCE AND CYBERSECURITY

DIVISION FOR RESEARCH
UNIVERSITY AT ALBANY
State University of New York

ALBANY.EDU/RESEARCH

ACKNOWLEDGEMENTS

Assistance in the production of this document by the following individuals is greatly appreciated:

Elisa Lopez, Thecla Philip, and Jennifer Krausnick
DIVISION FOR RESEARCH

Jill Reid
OFFICE OF COMMUNICATIONS & MARKETING

Arion James
UALBANY STUDENT

Featured AICS Researchers

MESSAGE FROM THE DIVISION FOR RESEARCH

The University at Albany (UAlbany) is a comprehensive Research 1 (R1) institution under the Carnegie Classification and one of four research-focused "University Centers" in the State University of New York system. UAlbany is widely recognized for its cutting-edge research programs, student-centered academic and research experiences, and opportunities for research collaboration and industry partnership. UAlbany has a demonstrated history of service to New York's Capital Region and has been recognized by the Carnegie Foundation's Community Engagement Classification.

UAlbany offers significant expertise in two rapidly growing and closely related research areas: Artificial Intelligence (AI) and Cybersecurity (CS). AI technologies automate many tasks traditionally performed by humans, such as image or speech recognition, robot-assisted surgery, analysis of large data sets, and simulations of complex social problems. Cybersecurity is a rapidly evolving field dedicated to protecting information systems from intrusion, disruption, or damage by bad actors.

Our AI and CS faculty work across a wide range of disciplines and departments, including Computer Science, Information Security, Mathematics, Electrical Engineering, and Emergency Preparedness. Their research projects are supported by grants from the Department of Defense, the National Science Foundation, the National Institute of Justice, the Department of Energy, Global 500 corporations, and private foundations. We hope that you will be inspired by the many research opportunities available to our students and research partners.

JAMES A. DIAS, PH.D.
VICE PRESIDENT FOR RESEARCH

SATYENDRA KUMAR, PH.D.
ASSOCIATE VICE PRESIDENT FOR RESEARCH

Dr. Chang's lab is using computer vision and artificial intelligence to develop "smarter" technologies with a wide range of applications. Video analytics can be deployed to identify "fake" media, automate industrial site monitoring, enhance the situational awareness of robots, improve traffic management, and facilitate online learning.

MING-CHING CHANG

ASSISTANT PROFESSOR
COMPUTER SCIENCE

PHD, BROWN UNIVERSITY
MCHANG2@ALBANY.EDU

EXPERTISE

Computer vision, artificial intelligence, video analytics, machine learning

ACHIEVEMENTS

- Developed a deep neural network model for multi-people visual detection and human pose estimation
- Applied state-of-the-art deep neural network and AI techniques to smart transportation for vehicle detection, tracking, counting and re-identification
- Developed deepfake detection algorithms to identify forgery images for media forensics

PUBLICATIONS

- *3D Single-Person Concurrent Activity Detection Using Stacked Relation Network*, Y. Wei, W. Li, Y. Fan, L. Xu, M.-C. Chang and S. Lyu, Thirty-Fourth AAAI Conference on Artificial Intelligence, New York, NY (February 2020).
- *Multi-Scale Structure-Aware Network for Human Pose Estimation*, L. Ke, M.-C. Chang, H. Qi and S. Lyu, 15th European Conference on Computer Vision, Munich, Germany (September 2018).
- *Adaptive RNN Tree for Large-Scale Human Action Recognition*, W. Li, L. Wen, M.-C. Chang, S. Lim and S. Lyu, IEEE International Conference on Computer Vision, Venice, Italy (October 2017).

Dr. Ekenna's team is working on robust motion planning algorithms that use machine learning techniques to improve the speed and accuracy of autonomous robots and reduce the opportunity for cyber-attacks that exploit situational awareness vulnerabilities. Another project focuses on a metering system to identify weak components in internet of things (IoT) frameworks prior to deployment.

CHINWE EKENNA

ASSISTANT PROFESSOR
COMPUTER SCIENCE

PHD, TEXAS A&M UNIVERSITY
CEKENNA@ALBANY.EDU

EXPERTISE

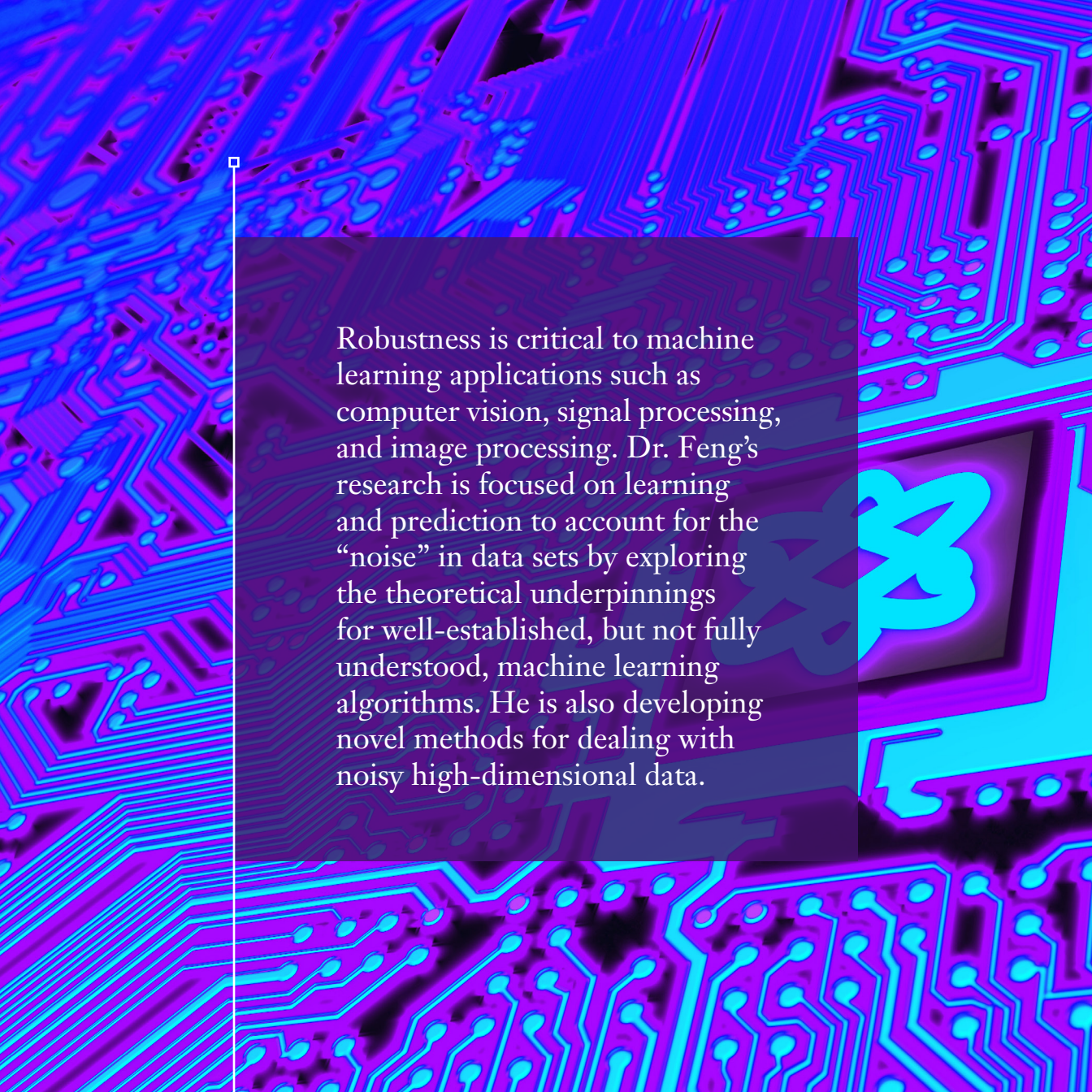
Internet of things (IoT) ecology, anomaly detection, reinforcement learning

ACHIEVEMENTS

- Applied reinforcement learning techniques to improve motion planning algorithms for autonomous robot applications in cybersecurity
- Combined cybersecurity research with AI techniques, such as anomaly detection and reinforcement learning, to create a measure of vulnerability to IoT players
- Developed IoT applications to smart city infrastructures

PUBLICATIONS

- *Attentional Adversarial Variational Video Generation via Decomposing Motion and Content*, S. Talafha, B. Rekabdar, C.P. Ekenna and C. Mousas, 2020 IEEE 14th International Conference on Semantic Computing, San Diego, CA, 45-52 (2020).
- *Smart city in crisis: Technology and policy concerns*, T. Soyata, H. Habibzadeh, C. Ekenna, B. Nussbaum and J. Lozano, Sustainable Cities and Society **50** 101566 (2019).
- *Investigating Heterogeneous Planning Spaces*, A. Upadhyay and C. Ekenna, 2018 IEEE International Conference on Simulation, Modeling, and Programming for Autonomous Robots 108-115 (2018).



Robustness is critical to machine learning applications such as computer vision, signal processing, and image processing. Dr. Feng's research is focused on learning and prediction to account for the "noise" in data sets by exploring the theoretical underpinnings for well-established, but not fully understood, machine learning algorithms. He is also developing novel methods for dealing with noisy high-dimensional data.

YUNLONG FENG

ASSISTANT PROFESSOR
MATHEMATICS AND STATISTICS

PHD, CITY UNIVERSITY OF HONG KONG
YLFENG@ALBANY.EDU

EXPERTISE

Robust machine learning, statistical learning theory

ACHIEVEMENTS

- Established systematic theoretical foundations for supervised learning paradigms associated with the information-theoretic criteria
- Developed a statistical learning framework to enable modal regression on high-dimensional data
- Made progress toward the theory and methodologies of robust machine learning

PUBLICATIONS

- *A statistical learning approach to modal regression*, Y. Feng, J. Fang and J.A.K. Suykens, Journal of Machine Learning Research **21** 1 (2020).
- *Kernel density estimation for dynamical systems*, H. Hang, I. Steinwart, Y. Feng and J.A.K. Suykens, Journal of Machine Learning Research **19** 1260 (2018).
- *Learning with the maximum correntropy criterion induced losses for regression*, Y. Feng, X. Huang, L. Shi, Y. Yang and J.A.K. Suykens, Journal of Machine Learning Research **16** 993 (2015).

The internet of things (IoT) has enabled rapid adoption of smart devices and cloud computing, which has created new security and privacy concerns. Dr. Majumdar is applying a type of artificial intelligence called natural language processing to learning-based security auditing. The results have numerous industrial and governmental applications to both IoT products, such as autonomous vehicles and smart health devices, and cloud computing platforms.

SURYADIPTA MAJUMDAR

ASSISTANT PROFESSOR
INFORMATION SECURITY AND DIGITAL FORENSICS

PHD, CONCORDIA UNIVERSITY
SMAJUMDAR@ALBANY.EDU

EXPERTISE

Internet of things (IoT) security, cloud computing security, network security

ACHIEVEMENTS

- Authored book, *Cloud Security Auditing*, on AI-aided security auditing methods
- Developed a learning-based proactive security auditing framework for cloud computing platforms
- Built a proactive security framework for Internet of Things (IoT) based on natural language processing (NLP) techniques

PUBLICATIONS

- *Cloud Security Auditing*, Suryadipta Majumdar, Taous Madi, Yushun Wang, Azadeh Tabiban, Momen Oqaily, Amir Alimohammadifar, Yosr Jarraya, Makan Pourzandi, Lingyu Wang and Mourad Debbabi, Springer International Publishing (2019).
- *Proactivizer: Transforming Existing Verification Tools into Efficient Solutions for Runtime Security Enforcement*, Suryadipta Majumdar, Azadeh Tabiban, Meisam Mohammady, Alaa Oqaily, Yosr Jarraya, Makan Pourzandi, Lingyu Wang and Mourad Debbabi, 24th European Symposium on Research in Computer Security **2** 239 (2019).
- *Learning Probabilistic Dependencies among Events for Proactive Security Auditing in Clouds*, Suryadipta Majumdar, Azadeh Tabiban, Yosr Jarraya, Momen Oqaily, Amir Alimohammadifar, Makan Pourzandi, Lingyu Wang and Mourad Debbabi, Journal of Computer Security **27** 165 (2019)


Threat assessment and cybersecurity are becoming increasingly critical to the public sector. As a former government intelligence analyst, Dr. Nussbaum is particularly interested in assessing cyber risks and threats at the level of states, regions and municipalities - national security problems at the sub-national level.

BRIAN NUSSBAUM

ASSISTANT PROFESSOR
EMERGENCY PREPAREDNESS, HOMELAND SECURITY AND CYBERSECURITY

PHD, UNIVERSITY AT ALBANY
BNUSSBAUM@ALBANY.EDU

EXPERTISE

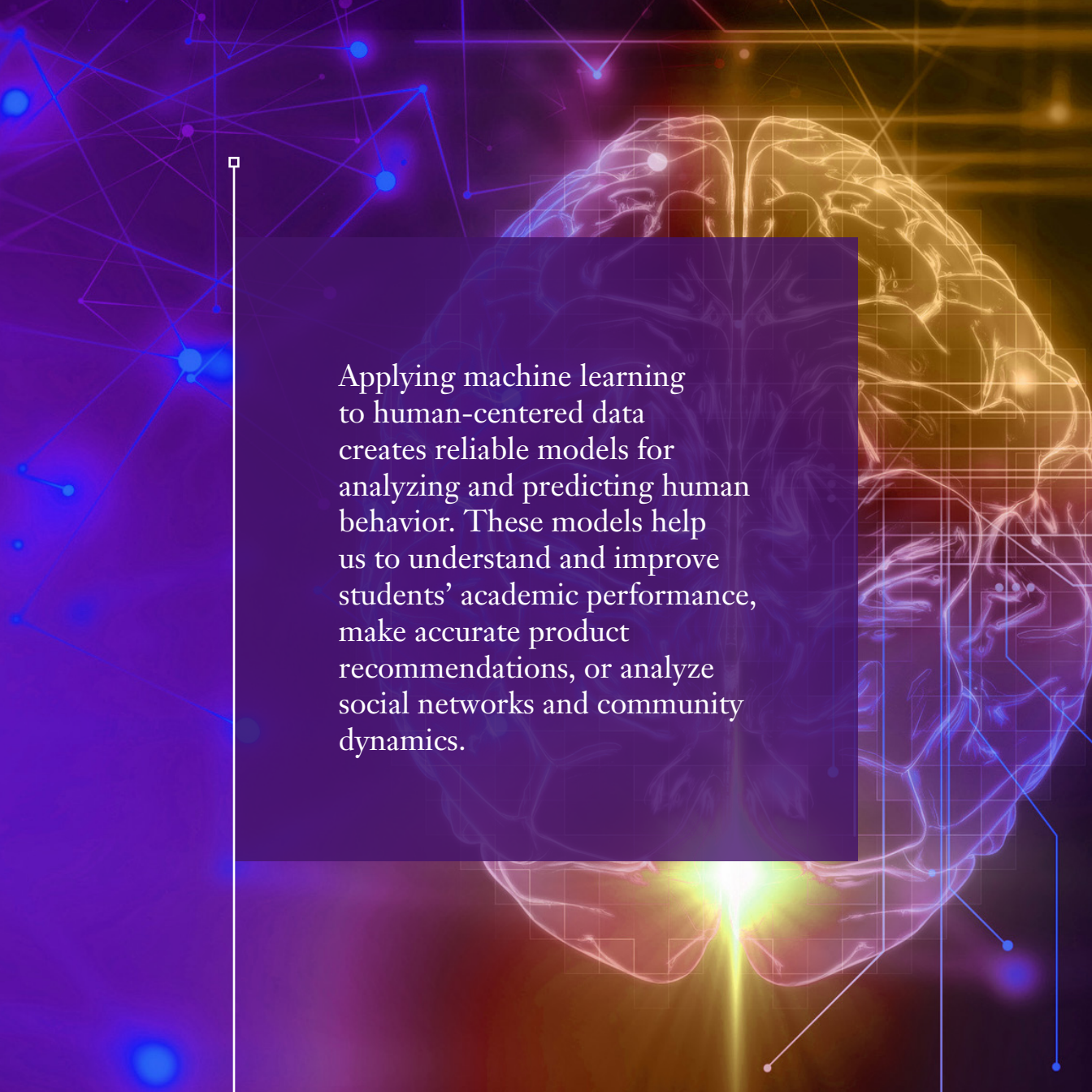
Cybersecurity and critical infrastructure, smart cities, state and local government

ACHIEVEMENTS

- Articulated social, political, and organizational hurdles to smart city implementation in a paper that was cited in Congressional testimony
- Illustrated potential uses for excess capacity of smart city devices for information collection, communication, and analysis during public emergencies
- Collaborated on a privacy and security survey on technical and socio-organizational vulnerabilities in smart cities

PUBLICATIONS

- *A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities*, H. Habibzadeh, B.H. Nussbaum, F. Anjomshoa, B. Kantarci and T. Soyata, Sustainable Cities and Society **50** 101660 (2019).
- *Smart city in crisis: Technology and policy concerns*, T. Soyata, H. Habibzadeh, C. Ekenna, B. Nussbaum and J. Lozano, Sustainable Cities and Society **50** 101566 (2019).
- *Communicating cyber intelligence to non-technical customers*, B. H. Nussbaum, International Journal of Intelligence and Counter-Intelligence **30** 743 (2017).



Applying machine learning to human-centered data creates reliable models for analyzing and predicting human behavior. These models help us to understand and improve students' academic performance, make accurate product recommendations, or analyze social networks and community dynamics.

SHAGHAYEGH SAHEBI

ASSISTANT PROFESSOR
COMPUTER SCIENCE

PHD, UNIVERSITY OF PITTSBURGH
SSAHEBI@ALBANY.EDU

EXPERTISE

Machine learning in human-centered applications with multi-view and sparse data, personalization, recommender systems, and educational data mining

ACHIEVEMENTS

- Developed matrix and tensor factorization models and algorithms to capture learner knowledge gain and forgetting, estimate learning material's domain knowledge map, and predict students' future performance
- Developed transfer learning and domain adaptation approaches to model user interests across multiple domains and systems for high quality learner recommendations
- Created factorization and process models to distinguish between efficient and inefficient online learning behaviors, detect procrastination, and study the effects on learning gain and performance

PUBLICATIONS

- *Detecting Trait vs. Performance Student Behavioral Patterns Using Discriminative Non-Negative Matrix Factorization*, M. Mirzaei and S. Sahebi, Proceedings of the Thirty-Third International Florida Artificial Intelligence Research Society Conference, North Miami Beach, FL (May 2020).
- *Review-Based Cross-Domain Collaborative Filtering: A Neural Framework*, T.N. Doan and S. Sahebi, Workshop on Recommendation in Complex Scenarios 23-28 (2019).
- *Rank-Based Tensor Factorization for Student Performance Prediction*, T. N. Doan and S. Sahebi, 12th International Conference on Educational Data Mining 288-293 (2019).

The rapid proliferation of “fake news” demands sophisticated methods to mitigate misinformation. Tools for analyzing and authenticating the source and content of news items include natural language processing, machine learning, fusion algorithms, and component and page ranking. Dr. Atrey is combining them in a robust tool that analyzes credibility and provides a “truthfulness score” to consumers.

PRADEEP ATREY

ASSOCIATE PROFESSOR
COMPUTER SCIENCE

PHD, NATIONAL UNIVERSITY OF SINGAPORE
PATREY@ALBANY.EDU

EXPERTISE

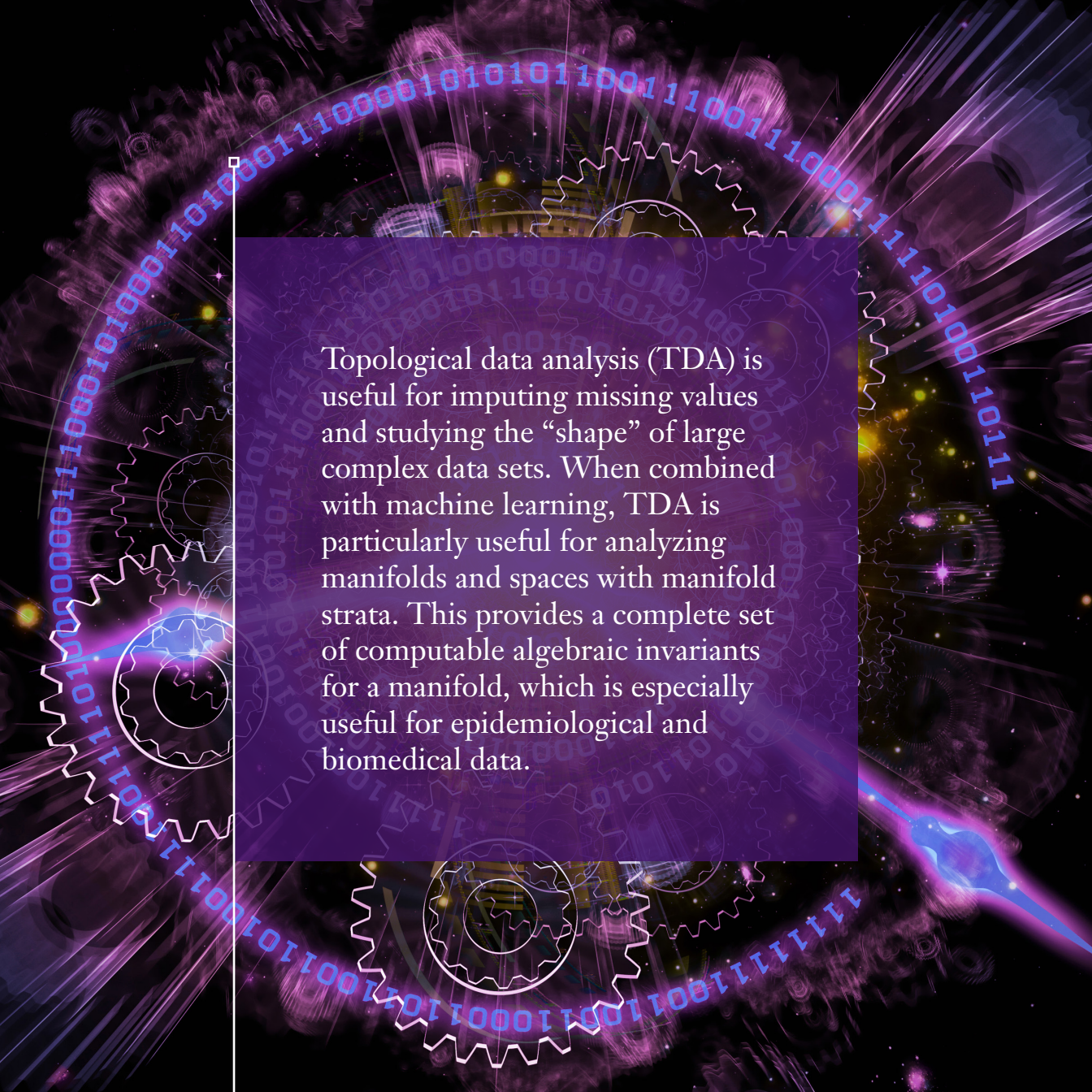
Fake news detection, secure computing, privacy-enabled location-based services, memory forensics, phishing detection

ACHIEVEMENTS

- Adopted hybrid approach for fake news detection that leverages both content and context
- Designed and developed SecureCSuite framework that enables secure cloud-based editing, deduplication and searching of encrypted documents
- Developed method for social and textual feature-based cyberbully detection
- Developed privacy-enabled location-based services using secure GPS data

PUBLICATIONS

- *A framework to detect fake tweet images on social media*, S. Parikh, S. Khedia and P.K. Atrey, The Fifth IEEE International Conference on Multimedia Big Data, Singapore (2019).
- *On the origin, proliferation and tone of fake news*, S. Parikh, V. Patil and P.K. Atrey, 2nd IEEE International Conference on Multimedia Information Processing and Retrieval, San Jose, CA, USA, 135-140 (2019).
- *On cyberbullying incidents and underlying online social relationships*, Q. Huang, V.K. Singh and P.K. Atrey, Springer Journal of Computational Social Science **1** 241 (2018).



Topological data analysis (TDA) is useful for imputing missing values and studying the “shape” of large complex data sets. When combined with machine learning, TDA is particularly useful for analyzing manifolds and spaces with manifold strata. This provides a complete set of computable algebraic invariants for a manifold, which is especially useful for epidemiological and biomedical data.

BORIS GOLDFARB

ASSOCIATE PROFESSOR
MATHEMATICS
AND STATISTICS

PHD, CORNELL UNIVERSITY
BGOLDFARB@ALBANY.EDU

EXPERTISE

Topological data analysis (TDA), explainable learning, artificial intelligence

ACHIEVEMENTS

- Parallelization of persistent homology computation
- Stratification learning using density-based TDA Mappers
- Missing data imputation methods based on the TDA Mapper algorithm
- Parallelization of discrete Morse theory algorithms

PUBLICATIONS

- *Singular persistent homology with geometrically parallelizable computation*, B. Goldfarb, Topology Proceedings **55** 273 (2020).
- *A new missing data imputation method based on the Mapper algorithm*, B. Goldfarb and R. Moag, preprint (2020).
- *Stratification learning using density-based TDA Mappers, I: the general approach and the case of graphs*, B. Goldfarb and D. Goldfarb, preprint (2020).

The proliferation of social media has also given rise to online harassment. Machine learning enables fast, accurate detection of cyberbullying, both by alerting offenders to potentially offensive content and by allowing their victims to limit inappropriate contact. This creates safer online communities, particularly for young people who are the frequent targets of cyberbullies.

DAPHNEY STAVROULA ZOIS

ASSISTANT PROFESSOR
ELECTRICAL AND COMPUTER ENGINEERING

PHD, UNIVERSITY OF SOUTHERN CALIFORNIA
DZOIS@ALBANY.EDU

EXPERTISE

Decision making under uncertainty, machine learning, detection and estimation theory, intelligent systems design, signal processing

ACHIEVEMENTS

- Devised on-the-fly instance-wise feature selection and classification algorithm
- Devised algorithm for detection of changes in spatio-temporal data
- Devised algorithm for heterogeneous sensor selection in energy-constrained sensor networks

PUBLICATIONS

- *On-the-fly Feature Selection and Classification with Application to Civic Engagement Platforms*, Y. Liyanage, D.-S. Zois and C. Chelmis, 45th International Conference on Acoustics, Speech, and Signal Processing, Barcelona, Spain (May 2020).
- *Robust Freeway Accident Detection: A Two-Stage Approach*, Y. Liyanage, D.-S. Zois and C. Chelmis, 44th International Conference on Acoustics, Speech, and Signal Processing, Brighton, UK (May 2019).
- *Cyberbullying Ends Here: Towards Robust Detection of Cyberbullying in Social Media*, M. Yao, C. Chelmis and D.-S. Zois, The Web Conference, San Francisco, CA (May 2019).

Intelligent security and privacy analysis are critical to thwarting social engineering attacks. Dr. Masoumzadeh is using automated techniques to analyze the security and privacy behavior of applications without accessing the code. He and his team are also developing a platform that detects social engineering attacks and engages the perpetrators in conversation with the goal of investigating them.

AMIR MASOUMZADEH

ASSISTANT PROFESSOR
COMPUTER SCIENCE

PHD, UNIVERSITY OF PITTSBURGH
AMASOUMZADEH@ALBANY.EDU

EXPERTISE

Modeling, testing and verification of security policies; privacy control, privacy enhancing technologies and data anonymization; machine learning in cybersecurity

ACHIEVEMENTS

- Developed machine learning approaches for detecting impersonation and social engineering attacks based on stylometric and communication behaviors
- Proposed machine learning approach for learning access control behavior of web applications without access to application's code
- Developed machine learning algorithms for constructing high-level access control policies from low-level authorization information in systems
- Proposed a computational model of information exposure in online social networks that can be used for privacy awareness and control
- Developed efficient algorithms for anonymizing social and geo-social network datasets

PUBLICATIONS

- *Active Learning of Relationship-Based Access Control Policies*, P. Iyer and A. Masoumzadeh, Proceedings of the 25th ACM Symposium on Access Control Models and Technologies 155-166 (2020).
- *Security Analysis of Relationship-Based Access Control Policies*, A. Masoumzadeh, Eighth ACM Conference on Data and Application Security and Privacy 186–195 (2018).
- *Modeling Exposure in Online Social Networks*, A. Cortese and A. Masoumzadeh, 15th Annual Conference on Privacy, Security and Trust 327 (2017).

Risk analysis is an effective tool for anticipating and mitigating the consequences of cybersecurity incidents. Impact modeling that considers both internal and external dependencies transforms cyber risk management from a narrow technical issue to a broader business security strategy. This approach creates a common language for technical experts and executive decision makers to collaborate on business continuity planning.

UNAL TATAR

ASSISTANT PROFESSOR
EMERGENCY PREPAREDNESS, HOMELAND SECURITY AND CYBERSECURITY

PHD, OLD DOMINION UNIVERSITY
UTATAR@ALBANY.EDU

EXPERTISE

Cybersecurity risk analysis, cyber resiliency, cyber insurance, privacy by design, critical infrastructure protection, cybersecurity education

ACHIEVEMENTS

- Created an economics-based cyber risk assessment method for acquisition decisions
- Developed a cyber risk quantification method for actuaries and insurance sector
- Assessed cybersecurity risks of maritime critical infrastructure through a novel risk analysis method for the NATO Combined Joint Operations from the Sea Centre of Excellence (CJOS COE)
- Developed cyberterrorism and security research and education program for NATO Defense Against Terrorism Centre of Excellence (DAT COE)

PUBLICATIONS

- *A complex structure representation of the US critical infrastructure protection program based on the Zachman framework*, U. Tatar, B. Karabacak, P.F. Katina and A. Igonor, International Journal of System of Systems Engineering 9 221 (2019).
- *Agent-Based Model of Sand Supply Governance Employing Blockchain Technology*, F. Sabz Ali Pour, U. Tatar and A. Gheorghe, Annual Simulation Symposium 14 1-11 (2018).
- *Impact Assessment of Cyber Attacks: A Quantification Study on Power Generation Systems*, U. Tatar, B. Bahsi and A. Gheorghe, 11th System of Systems Engineering Conference 1-6 (2016).

User compliance to security policies is a critical component of managing security risks. A good risk management program should have a clearly defined plan for enforcing policy compliance, detecting non-compliance, and addressing non-compliance.

VICTORIA KISEKKA

ASSISTANT PROFESSOR
INFORMATION SECURITY AND DIGITAL FORENSICS

PHD, UNIVERSITY AT BUFFALO SCHOOL OF MANAGEMENT
VKISEKKA@ALBANY.EDU

EXPERTISE

Cybersecurity risk analysis, security policies, user security and privacy behaviors, cybersecurity education.

ACHIEVEMENTS

- Conceptualization and design of moving target defense system
- Design of two-person authentication proof of concept
- Development of cybersecurity and digital forensics training materials

SELECTED PUBLICATIONS

- Mitigating E-Services Avoidance: The Role of Government Cybersecurity Preparedness, Abdelhamid, M., Kisekka, V., & Samonas, S., Information and Computer Security, 27(1), 26-46 (2019).
- The Effectiveness of Health Care Information Technologies: Evaluation of Trust, Security Beliefs, and Privacy as Determinants of Health Care Outcomes, Kisekka, V., & Giboney, J. S., Journal of medical Internet research, 20(4), e107 (2018).
- An Agile Methodology for the Disaster Recovery of Information Systems Under Catastrophic Scenarios, Baham, C., Hirschheim, R., Calderon, A. A., & Kisekka, V., Journal of Management Information Systems, 34(3), 633-663 (2017).

Cybersecurity is critical to our society's functioning. Organizations need to recognize the importance of cybersecurity and must understand their responsibilities in securing their assets. As a former Application and Security Manager, Critical Care Information Systems, Dr. Yankson is interested in developing privacy and security conscious solutions and teaching the next generation of students who can help organizations build reliable cybersecurity programs and prevent attacks.

BENJAMIN YANKSON

ASSISTANT PROFESSOR
SECURITY

PHD, ONTARIO TECH UNIVERSITY
BYANKSON@ALBANY.EDU

EXPERTISE

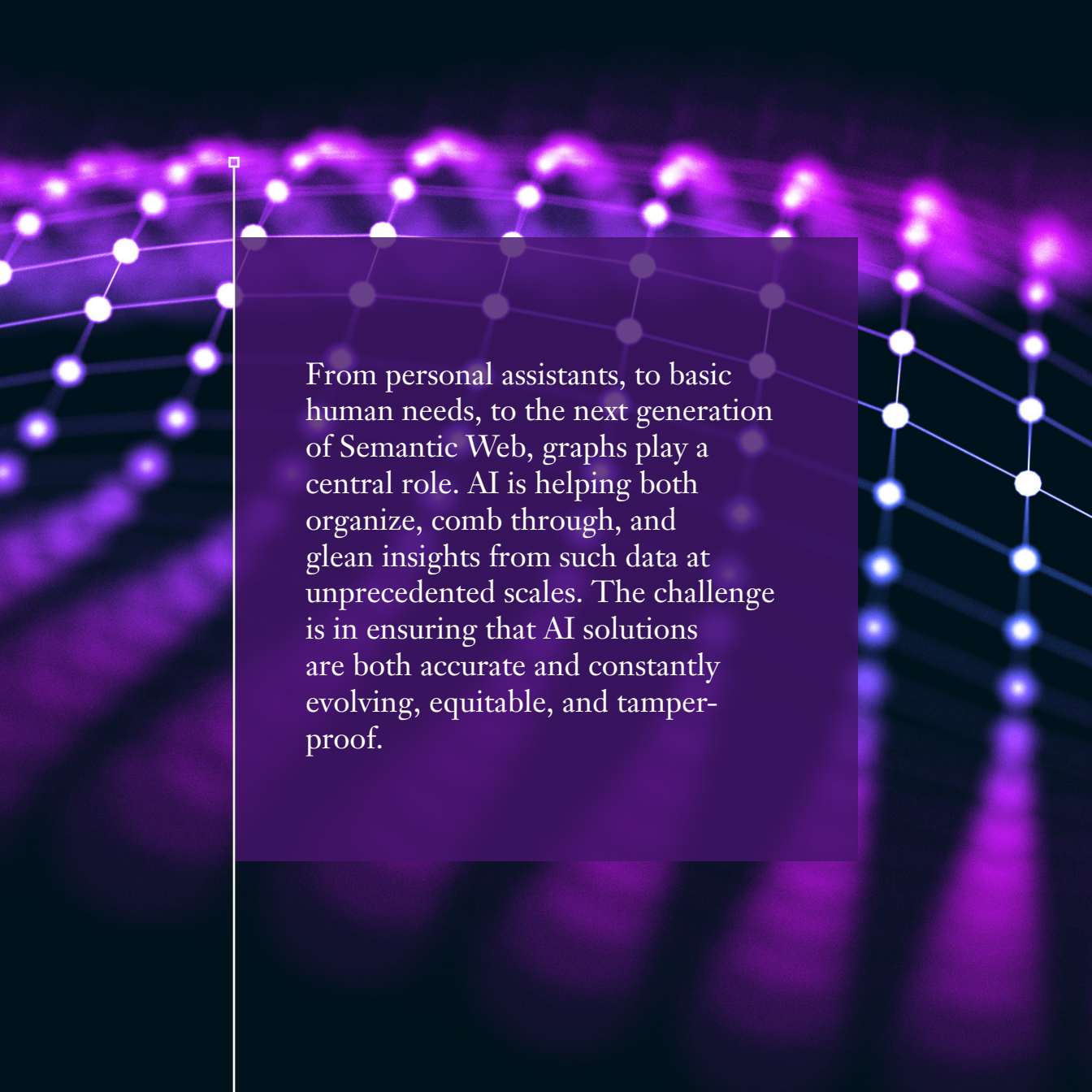
Privacy and Security IoT toys; Cybersecurity Risk and Information Assurance; Security Auditing and Compliance, and Digital Forensics

ACHIEVEMENTS

- Developed a conceptual "Privacy Preservation Framework for IoT toys" cited in UNICEFs' Human Rights Centre executive report on "Artificial Intelligence and Children's rights.
- Managed several critical security projects, including Critical Care Information Systems.
- Collaborated internationally on various initiatives on developing privacy and security solutions for IoT Toys.

SELECTED PUBLICATIONS

- Yankson B, Iqbal F. & Hung P.C.K. (2020). 4P Based Forensics Investigation Framework for Smart Connected Toys. In Proceedings of the 15th International Conference on Availability, Reliability, and Security (ARES '20). Association for Computing Machinery, New York, NY, USA, Article 44, 1–9. DOI: https://doi.org/10.1145/3407023.3409213
- Yankson B., Iqbal F., Aleem S., Shah B., Hung P.C.K, & Albuquerque A.P. (2019). A Privacy-Preserving Context Ontology (PPCO) for Smart Connected Toys. 12th CMI Conference on Cybersecurity and Privacy, Nov 28 – 30, 2019, Copenhagen SV, Denmark. pp. 1-6
- Yankson, B. (2020). Space Infrastructure Security Through the Lens of Plan-Do-Check-Act (PDCA) Cybersecurity Framework. NATO Science for Peace and Security Series – D: Information and Communication Security, 57(Space Infrastructures: From Risk to Resilience Governance), 109–119. https://doi.org/10.3233/NICSP200012


From personal assistants, to basic human needs, to the next generation of Semantic Web, graphs play a central role. AI is helping both organize, comb through, and glean insights from such data at unprecedented scales. The challenge is in ensuring that AI solutions are both accurate and constantly evolving, equitable, and tamper-proof.

CHARALAMPOS CHELMIS

ASSISTANT PROFESSOR
COMPUTER SCIENCE

PHD, UNIVERSITY OF SOUTHERN CALIFORNIA
CCELMIS@ALBANY.EDU

EXPERTISE

Socially important data science, semantic web, machine learning

ACHIEVEMENTS

- Algorithmic solutions for the detection and anticipation of cyberbullying
- Computational models of influence and information dissemination in online social media
- Large-scale graph analytics on commodity hardware

PUBLICATIONS

- Mengfan Yao, Charalampos Chelmis, and Daphney-Stavroula Zois. “Cyberbullying ends here: Towards robust detection of cyberbullying in social media.” The World Wide Web Conference. 2019.
- Saeed, Muhammad Rizwan, Charalampos Chelmis, and Viktor K. Prasanna. “Extracting entity-specific substructures for RDF graph embeddings.” Semantic Web 10.6 (2019): 1087-1108.
- Srivastava, Ajitesh, Charalampos Chelmis, and Viktor K. Prasanna. “Computing competing cascades on signed networks.” Social Network Analysis and Mining 6.1 (2016): 82.

Dr. Ying's research group explores the design of new risk measures and efficient optimization algorithms from the novel interaction of statistics, applied mathematics, and machine learning. He and his group have developed robust and efficient ML algorithms for various application domains, such as face verification, anomaly detection, prediction of tumor growth, prediction of wildfires, and privacy protection.

YIMING YING

ASSOCIATE PROFESSOR
MATHEMATICS AND STATISTICS

PHD, ZHEJIANG UNIVERSITY
YYING@ALBANY.EDU

EXPERTISE

Machine learning, statistical learning theory, mathematical data science, optimization for big data

ACHIEVEMENTS

- Developed efficient optimization algorithms for analyzing big imbalanced data
- Established statistical and mathematical foundations for various machine learning algorithms
- Designed privacy-preserving machine learning algorithms for complex and nonstandard learning problems with theoretical guarantees

PUBLICATIONS

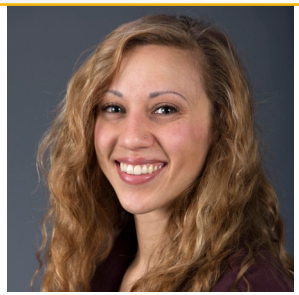
- Differential privacy of SGD with non-smooth loss. P. Wang, Y. Lei, Y. Ying and H. Zhang. Preprint (2020).
- Fine-Grained analysis of stability and generalization for SGD. *International Conference on Machine Learning (ICML)*, Y. Lei and Y. Ying (June 2020).
- Stochastic online AUC maximization. *Advances in Neural Information Processing Systems* (Oral presentation). Y. Ying, L. Wen and S. Lyu (December 2016)

In a rapidly changing world, it is critical that we integrate cutting-edge technologies into our research. Atmospheric Science, in particular, is a prime example of “big data,” and Dr. Sulia is striving to exploit advanced computational techniques, such as data analytics and machine learning and push weather research and development into new frontiers.

KARA SULIA

RESEARCH FACULTY
ATMOSPHERIC SCIENCES RESEARCH CENTER

PHD, PENN STATE UNIVERSITY
KSULIA@ALBANY.EDU



EXPERTISE

Implementation of novel computational techniques to advance research and development in the Atmospheric Sciences

ACHIEVEMENTS

- Development of advanced visualization software platforms and associated APIs including (1) a mobile app for real-time New York State Mesonet data, (2) web-based interface displaying multi-source air quality measurements and forecasts, and (3) web-based interface for multi-source electrical outage information.
- Determination of the impacts of weather on utility grid outages; development of load, outage, and photovoltaic generation forecasts.
- Development of a database containing millions of type-categorized cloud particle images to characterize weather event microphysics.

PUBLICATIONS

- *A new method for ice-ice aggregation in the Adaptive Habit Model*, K. J. Sulia, Z. J. Lebo, V. Przybylo, and C. G. Schmitt, J. Atmospheric Sciences, **78**, 133-154, 10.1175/JAS-D-20-0020.1 (2021).
- *The Ice Particle and Aggregate Simulator (IPAS). Part I: Extracting dimensional properties of ice-ice aggregates for microphysical parameterization*, V. Przybylo, K. J. Sulia, C G. Schmitt, and Z. Lebo, J. Atmospheric Sciences., **76**, 1661-1676, 10.1175/JAS-D-18-0187.1 (2019).
- *Simulated Polarimetric Fields of Ice Vapor Growth Using the Adaptive Habit Model. Part II: A Case Study from the FROST Experiment*, K. J. Sulia and M. R. Kumjian, Monthly Weather Review, **145**, 2303-2323, 10.1175/MWR-D-16-0062.1 (2017).

Dr. Goel is currently engaged in cyber security and warfare research and computer security threats such as botnets and malware, risk analysis, security policy development and evaluation, security modeling, and self-organized complex systems. He is leading an effort, launched by IEEE Communications Society and the IEEE Standards Association, to create a vision for the Smart Grid 15 years into the future.

SANJAY GOEL

PROFESSOR
INFORMATION SECURITY & DIGITAL FORENSICS

PHD, RENSSELAER POLYTECHNIC INSTITUTE
GOEL@ALBANY.EDU

EXPERTISE

Cyber Security, Digital Forensics, Cyber Warfare, Artificial Intelligence, Machine Learning, Optimization, and Smart Grid

ACHIEVEMENTS

- Established FACETS (Forensics, Analytics, Complexity, Energy and Transportation Security Center), a research center on security and forensics.
- Established an Economic Development Administration supported University Center for Cyber Innovation and Research, and the Blackstone Launchpad for mentoring students in business development.
- Started the BS and MS programs in Digital Forensics and obtained the NSA Center of Excellence Designation.

PUBLICATIONS

- *National Cyber Security Strategy and the Emergence of Strong Digital Borders*, Sanjay Goel, Connections: The Quarterly Journal **19**, no. 1 (2020): 73-86.
- *Got Phished? Internet Security and Human Vulnerability*, Sanjay Goel, Kevin Williams, and Ersin Dincelli, J. Association for Information Systems: **18**:1(2) (2017).
- *How vulnerable are international financial markets to terrorism? An empirical study based on terrorist incidents worldwide*, Sanjay Goel, Seth Cagle, Hany Shawky, J. Financial Stability, Elsevier, **33**(C), 120-132 (2017).


DIVISION FOR RESEARCH
UNIVERSITY AT ALBANY
State University of New York
ALBANY.EDU/RESEARCH