SHASHANK ARORA

43 Tampa Ave, Albany, NY 12203
(518) · 502 · 8562 , shashankarora105@gmail.com , https://shashankarora.github.io/home/

EDUCATION

University at Albany, State University of New York *August 2017 - December 2022*
Ph.D., Computer Science
Thesis Title: *Frameworks for Secure Collaborative and Concurrent Editing*
Advisor: Dr. Pradeep K. Atrey

University at Albany, State University of New York *August 2015 - December 2016*
Master of Science, Computer Science
GPA: 4.00

Amity University, Uttar Pradesh, India *August 2008 - May 2012*
Bachelor of Technology, Computer Science
GPA: 6.33/ 10

RESEARCH INTERESTS AND LAB

Research Lab

· Albany Lab for Privacy and Security (ALPS), http://www.cs.albany.edu/ALPS/

Research Interests

· My research interests include Security and Privacy, Applied Cryptography, Cloud Security, Cyber Security, Multimedia Computing and Forensics.
· My current research focus is on issues related to i) security and privacy of user data stored over cloud, ii) multimedia computing in general. In particular, I am interested in the following areas:
· **Secure Computations:** Encrypted domain processing of user data over cloud systems.
· **Cyber Security:** Detection and prevention of Denial of Service, Distributed Denial of Service, Ransomware, Cryptojacking attacks.
· **Multimedia Computing:** Auditing, analysis, and correction of bias in machine learning algorithms for multimedia data.

PUBLICATIONS

[**J1**]: S Arora and PK Atrey. *SecureC2Edit: A Framework for Secure Collaborative and Concurrent Document Editing,* IEEE Transactions on Dependable and Secure Computing (TSDC)

[**C1**]: O Kulkarni, S Arora, A Mishra, VK Singh and PK Atrey. *A Multi-stage Bias Reduction Framework for Eye Gaze Detection,* The 6th IEEE International Conference on Multimedia Information Processing and Retrieval (MIPR), Singapore, September 2023

[**C2**]: O Kulkarni, S Arora and PK Atrey. *GARGI: Selecting Gaze-Aware Representative Group Image from a Live Photo,* The 5th IEEE International Conference on Multimedia Information Processing and Retrieval (MIPR), San Jose, CA, USA, August 2022

[**C3**]: S Arora and PK Atrey. *Secure Collaborative Editing Using Secret Sharing,* IEEE International Workshop on Information Forensics and Security (WIFS), Montpellier, France, December 2021

[**C4**]: G Kodwani, S Arora and PK Atrey. *On Security of Key Derivation Functions in Password-based Cryptography,* IEEE International Conference on Cyber Security and Resilience (CSR), Virtual, July 2021

[**C5]:** O Kulkarni, V Patil, SB Parikh, S Arora and PK Atrey. *Can You All Look Here? Towards Determining Gaze Uniformity In Group Images,* IEEE International Symposium on Multimedia (ISM), Taipei, Taiwan, December 2020

[**C6]:** P Singh, S Arora, K Williamson and PK Atrey. *S3Email: A Method for Securing Emails from Service Providers,* IEEE International Conference on Systems, Man, and Cybernetics (SMC), Banff, AB, Canada, October 2017

[**C7]:** S Arora, G Varshney, PK Atrey and M Misra. *SecureCEdit: An Approach for Secure Cloud-based Document Editing,* IEEE Conference on Communications and Network Security (CNS), Philadelphia, PA, USA, October 2016

WORK EXPERIENCE

Faculty August 2023 - Present
University at Albany, SUNY, USA

Research Assistant October 2022 - July 2023
University at Albany, SUNY, USA

Student Research Assistant January 2016 - May 2017
University at Albany, SUNY, USA

Software Engineer September 2012 - June 2015
Wipro Technologies, Hyderabad, India

PROJECTS

Research Projects

· **SecureC2Edit: Secure Collaborative and Concurrent Editing** January 2018 - Present
· Project developed as a part of Ph.D. Thesis. Comprised of three sub-projects:

· *SecureC2Edit: A structured peer-to-peer framework for secure collaborative and concurrent editing [J1]*
· Developed a structured peer-to-peer Hybrid Differential Synchronization (HDS) algorithm for secure collaborative and concurrent editing
· Developed an asynchronous key distribution algorithm to facilitate encryption
· Proof of concept implemented as a P2P Java Swing application

· *SecureC2Edit with Secret Sharing [C3]*
· Developed a framework for secure collaborative and concurrent editing that uses Shamir's Secret Sharing for security
· Proof of concept implemented as a P2P Java Swing application

· *SecureCEdit: A client-server framework for secure collaborative editing [C7]*
· Developed a client-server secure cloud document editing framework.
· Developed an asynchronous key distribution algorithm.
· Gained a deep understanding of applied cryptography, specifically, AES, key generation algorithms, and Google OAuth APIs.

· **GARGI: Selecting Gaze-Aware Representative Group Image from a Live Photo** February 2022 - Present

- Research track comprised of three projects:

- *Auditing and Reducing Bias in Gaze Detection Algorithm [C1]*
- Developed algorithms for auditing gender bias in eye center detection, pupil detection, and gaze detection
- Formulated metrics and tuning parameters to optimize the trade-off between fairness and accuracy/precision

- *Selecting Gaze-Aware Representative Group Image [C2]*
- Developed an algorithm for determining gaze uniformity in live images
- Developed an algorithm for selecting a representative image from frames of a live image
- Project developed in Python

- *Gaze Uniformity in Group Images [C5]*
- Developed an algorithm for determining gaze uniformity in group images
- Project developed in Python

- **Cryptanalysis of PBKDF2 [C4]** August 2019 - January 2021
- Analysis of reduction in security when using password-based equivalents of popular symmetric encryption schemes.
- Developing a theoretical analysis framework for password-based encryption frameworks.

- **S3Email: A method for securing emails from service providers [C6]** January 2017 - October 2017
- Developed a secure email communication scheme using Shamir's Secret Sharing
- Proof concept implemented as a Java Swing application.

- **Bluetooth Based Authentication for Anti Phishing** August 2016 - May 2017
- Implemented Multi-factor authentication scheme using Bluetooth-enabled smartphone devices
- Developed a mastery of authentication schemes and browser extension APIs.

Course Projects

- **Video Stabilization using Affine Transforms** August 2017- December 2017
- Course: Computer Vision
- MATLAB application to stabilize a video using Feature Extraction and Affine Transformation
- Learned MATLAB, developed an understanding of Digital Image Processing

- **Detecting DoS attacks using Multivariate Correlation Analysis** August 2016- December 2016
- Course: Information Security
- Java and Python-based console application used to detect Denial-Of-Service attacks by analyzing network traffic.
- Implemented a research paper as part of coursework.

- Gained proficiency in Python, developed an understanding of Multivariate Correlation Analysis

- **Project Management System** August 2015- December 2015
- Course: Software Engineering
- Web application used to create projects, user stories, teams and task lists to manage projects.
- Developed business logic and designed user interface for creating tasks lists.
- Developed an understanding of Agile methodology.

Industry Projects

- **Logistics Planning Tool** April 2013 - July 2015
- Intranet application to generate shipment plan and distribution plan for natural rubber.
- Developed and implemented business logic and designed user interface.
- Gained a deep understanding of J2EE framework.

- **Paperless Invoice** December 2012 - March 2013
- Intranet application to search and extract sales reports and generate invoices.
- Developed business logic and designed user interface.
- Gained an understanding of J2EE framework.

TEACHING

Teaching August 2023 - Present

CSI 409/509: Automata and Formal Languages (Fall 2023)

CSI 518: Software Engineering (Fall 2023)

Teaching Assistant August 2017 - July 2022

CSI 201: Introduction to Computer Science (Fall 2017, Fall 2019, Fall 2021, Summer 2022)

CSI 210: Discrete Structures (Fall 2020)

CSI 213: Data Structures (Summer 2021)

CSI 311: Principles of Programming Languages (Spring 2018, Fall 2018)

CSI 404: Computer Organization (Spring 2019, Fall 2020, Spring 2022)

CSI 409: Automata and Formal Languages (Spring 2020)

CSI 412: Operating Systems (Fall 2020)

CSI 426/526: Cryptography (Spring 2018, Spring 2019, Spring 2020, Spring 2021)

CSI 433/533: Multimedia Computing (Fall 2019)

CSI 499: Capstone Project in Computer Science (Spring 2020, Spring 2021, Fall 2021, Spring 2022)

PROFESSIONAL ACTIVITIES

External Reviewer

- Conferences: IEEE WIFS, IEEE ICASSP, and FPS.
- Journals: ACM TOMM, Elsevier Image Comm., Elsevier JISA, and Wiley ETRI.

Conference Presentations

- *SecureCEdit: An Approach for Secure Cloud-based Document Editing,* IEEE Conference on Communications and Network Security (CNS), Philadelphia, PA, USA, October 2016
- *Secure Collaborative Editing Using Secret Sharing,* IEEE International Workshop on Information Forensics and Security (WIFS), Montpellier, France, December 2021

Session Chair

- *Cyber 6-Cybernetics for Informatics*, 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC), Banff, AB, Canada, October 2017

TECHNICAL SKILLS

Programming Languages	Java/J2EE, Python, MATLAB, R
Protocols and APIs	Java Swing, JDBC, Jama, Numpy, Pandas
Web Development	HTML, CSS, Javascript, JSF 2 (Primefaces), EJB 3, JPA 2
Database	Oracle, MySQL, SQL, PL-SQL
Tools	IBM RAD 8, IBM WAS 7, SQL Developer, Eclipse, MySQL Workbench, Spyder, Visual Studio Code
Operating Systems	Linux, Windows, Android
SDLC	Agile

REFERENCES

Prof. Dr. Pradeep K. Atrey
University at Albany, State University of New York
patrey@albany.edu

Prof. Dr. Paliath Narendran
University at Albany, State University of New York
pnarendran@albany.edu

Prof. Michael Phipps
University at Albany, State University of New York
mphipps@albany.edu