SHASHANK ARORA

43 Tampa Ave , Albany, NY 12203

(518) · 502 · 8562 , shashankarora105@gmail.com

EDUCATION

University at Albany, State University of New York *August 2017 - Present*
Ph.D., Computer Science

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

PUBLICATIONS

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

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, USA, August 2022 (To Appear)

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

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

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), Tapei, Taiwan, December 2020

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, Canada, October 2017

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

EXTERNAL REVIEWER

ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM)

Signal Processing: Image Communication Journal

Electronics and Telecommunications Research Institute (ETRI) Journal

IEEE International Workshop on Information Forensics and Security (WIFS)

International Symposium on Foundations & Practice of Security (FPS)

Journal of Information Security and Applications (JISA)

International Conference on Acoustics, Speech, and Signal Processing (ICASSP)

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

PROFESSIONAL EXPERIENCE

Student Research Assistant   January 2016 - May 2017
SUNY Albany

· **Bluetooth Based Authentication for Anti Phishing**   August 2016 - May 2017
· Worked on implementation of Multi-factor authentication scheme using Bluetooth-enabled smartphone devices
· Gained a deep understanding of authentication schemes and browser extension APIs.

· **SecureCEdit**   January 2016 - August 2016
· Worked on implementing a Secure Cloud Document Editing Tool.
· Developed an asynchronous key distribution algorithm.
· Gained a deep understanding of AES, key generation algorithms, and Google APIs.

Software Engineer   September 2012 - July 2015
Wipro Technologies   *Hyderabad, India*

· **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.

ACADEMIC PROJECTS

Research Projects

· **Selecting Gaze-Aware Representative Group Image**   February 2022 - June 2022
· Developed and implemented an algorithm for determining gaze uniformity in live images
· Developed and implemented an algorithm for selecting a representative image from frames of a live image
· Project involved using Python and Machine Learning techniques

· **SecureC2Edit with Secret Sharing**   Feb 2021 - December 2021
· 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

· **Cryptanalysis of PBKDF2**   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.

· **SecureC2Edit: Secure Collaborative and Concurrent Editing**   January 2018 - May 2021
· 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

· **Gaze Uniformity in Group Images**   January 2020 - August 2020
· Developed an algorithm for determining gaze uniformity in group images
· Project involved using Python

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

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.
· Learned 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.

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