SAYANTON DIBBO

Current Position

Assistant Professor, Department of Computer Science
Hewson Faculty Fellow, Styslinger College of Engineering
Affiliate, Alabama Center for the Advancement of AI
Affiliate, Alabama Transportation Institute
Affiliate, Institute for Social Science Research
The University of Alabama

Contact Information

2111 Cyber Hall
Department of Computer Science
The University of Alabama
Box 870290
Tuscaloosa, AL 35487-0290

E-mail: sdibbo@ua.edu
Phone: 205-348-2166
Web-page: https://sayantondibbo.github.io/
LinkedIn: http://www.linkedin.com/svdibbo
Google Scholar: https://scholar.com/sdibbo

Education

Dartmouth College — Hanover, NH

Ph.D., Computer Science — June 2025
Area: Cybersecurity & AI/ML

University of California, Riverside — Riverside, CA

M.S., Computer Science — Spring 2019
Area: Data Science and ML

University of Dhaka — Dhaka, Bangladesh

B.Sc., Computer Science & Engineering — August 2016
Area: Computer Architecture

Research Interests

Trustworthy AI, Security/Privacy, AI/ML (Transparency, Fairness and Robustness), Biometric Authentication, IoT Security, Human-centered Computing, Health Informatics, Cyber-physical Systems, and Explainable Artificial Intelligence (XAI).

Appointments and Positions

Assistant Professor, Computer Science, **The University of Alabama**	2025-present
Hewson Faculty Fellow, Styslinger College of Engineering, **UA**	2025-2027
AI Assurance Intern, **Los Alamos National Laboratory (LANL)**	2024-2024
Cybersecurity Intern, **Los Alamos National Laboratory (LANL)**	2023-2023
Graduate Research Intern, **Financial Industry Regulatory Authority**	2022-2022
Graduate Assistant, Computer Science, **Dartmouth College**	2020-2025
Research Intern, Computer Science, **Dartmouth College**	2019-2020
Graduate Assistant, Computer Science & Eng, **UC Riverside**	2018-2019
Dean's Distinguished Fellow, **UC Riverside**	2017-2018

Professional Experience

The University of Alabama — Tuscaloosa, AL
Assistant Professor, Computer Science — August 2025-present

- Research and mentoring UG & Grad student research in AI/ML & Security/Privacy.
- Impactful teaching and learning in UG & Grad curriculum.
- Extramural research proposal development and collaboration.

Los Alamos National Laboratory (LANL) Los Alamos, NM
Graduate Research Intern, LLM & Multimodal Model Security/Privacy Summer 2024

- Investigate and compare LLMs (e.g., Bert, GPT) and multi-modal (e.g., CLIP) models' vulnerabilities.
- An empirical evaluation of the *robustness* of different convolutional and transformer-based networks in unimodal and multi-modal setups.
- Analyzing adversarial attack transferability in cross-modal setups, i.e., unimodal model to multimodal models.

Los Alamos National Laboratory (LANL) Los Alamos, NM
Graduate Research Intern, AI Assurance & Cybersecurity Summer 2023

- Design Robust Deep Learning Audio classification models to mitigate audio adversarial attacks.
- Generate audio features from continuous audio data and implement/design robust deep neural network models to prevent adversarial attacks against privacy-preserving audio models.
- Implement novel techniques to prevent privacy attacks against Computer Vision models by analyzing in-depth privacy attacks against the neural networks.

The Financial Industry Regulatory Authority (FINRA) Boston, MA
Graduate Research Intern, AI/ML & Cybersecurity Summer 2022

- Leverage Pre-trained models (NLP) and design fine-tuned Deep Learning models on financial market data (text) to analyze security threats (e.g., backdoor, evasion, inference) that might leak sensitive data and disrupt market integrity.
- Implement a framework to identify possible data privacy threats to the Deep Learning model and develop robust and effective defenses to safeguard and protect market data (financial institutions) and maintain financial market integrity.

Dartmouth College Hanover, NH
Research Assistant & Cybersecurity Fellow, CS Department Fall 2020 - Spring 2025

- Investigating how the *generalizability, memorization,* and *robustness* of Large Language Models (LLMs) can aid in the development of effective defenses against adversarial attacks.
- Exploring the concept of *disparate vulnerability* in the context of *Fairness* in Model Inversion Attribute Inference privacy attack and designing an ML model to predict disparate vulnerability based on features computed only from training data instances.
- Designing Model Inversion Attribute Inference Attacks to ML model handling tabular data,
- Developing phone-based implicit user authentication model. The goal is to design a framework based on implicit continuous biometrics to run the ML model on phones to authenticate IoT wearable users.
- Analyzing and visualizing college students' phone call data to identify potential contexts and geo-temporal patterns of student phone call behavior.
- Analyzing cough data and designing cough models to identify cough vs. other sounds, also investigating the impact of noise on generalized cough models.

Dartmouth College Hanover, NH
Research Intern, CS Department Fall 2019 - Summer 2020

- Developed smartphone application (Android) to collect diabetic patients' sensor data, including accelerometer, GPS, microphone, etc., data. This app also incorporates diabetic users' continuous glucose monitor (CGM) time-series data records from users' CGM portal with their permission. Finally, ML models and statistical methods will be applied to analyze factors affecting diabetes.
- Worked to (*develop digital tools for improved self-management of Diabetes*) to leverage smartphones and wearable technologies for identifying trends or behavioral patterns associated with diabetes, as well as develop data-driven ML models to ensure better self-management.

Instituto Superior Técnico Lisbon, Portugal
Participant, Lisbon ML School (LxMLS) July 21-29, 2020

- Learning and implementing different aspects of ML: classifiers, tools, optimization techniques, gradient descent, L-BFGS algorithm, loss function, batch normalization, regularization, etc on real-life datasets.

Cornell, Maryland, Max Planck Saarbrucken, Germany
Student Participant, Pre-Doctoral Research School, MPI-SWS August 6-11, 2019

- Learning emerging research topics in Computer Science and experiencing cutting-edge research in computer science, including computer systems/architecture, optimization, machine learning, deep learning model decision property, formal methods, AI, and data visualization.

University of California, Riverside Riverside, CA
Graduate Research & Teaching Assistant, CSE Department Spring 2018 - Spring 2019

- Design and Implement the K-Nearest Neighbor-based predictive model to predict six major Human Activities - three static (sitting, lying, and standing) and three dynamics (walking, walking down, and walking upstairs) as well as postural transitions (e.g., stand-to-sit, sit-to-lie, lie-to-sit, stand-to-lie) from the accelerometer and gyroscope data of Human Activity Recognition (HAR) public data set of the UCI Machine Learning Repository, collected by the smartphone sensors of the users.
- Analyzed different feature selection techniques and incorporated the Genetic and Simulated Annealing algorithms to select the most important features in an efficient way to improve the overall prediction accuracy of human activities compared to the existing techniques used so far.

University of Dhaka Dhaka, Bangladesh
Undergraduate Researcher, CSE Department Fall 2014 - Summer 2017

- Designed an improved and efficient division technique with reduced time complexity and introduced a new, compact tree-based quantum divider design algorithm to reduce the circuit depth and achieve better performance compared to the existing divider design techniques in area, power, depth, delay, and # of input lines.
- Developed an app for diabetic patients to facilitate their daily living by providing instructions (e.g., diet, exercise, and notification during emergency cases) according to their sugar level.

Relevant Projects

Vulnerability of LLM & Multimodal Models — Los Alamos, NM
Research Project (Individual Project) — Summer 2024

- Compare adversarial vulnerabilities of unimodal (LLMs) and multimodal models
- Assess transferability of attacks in cross-modal setups

Sparse-Guard: Sparse Coding based defense against privacy attacks — Los Alamos, NM
Research Project (Individual Project) — Summer 2023

- Incorporate Sparse Coding layer on neural network architecture
- Analyze the effectiveness of sparse coding layers against privacy attacks

Robust Audio Classification Modeling — Los Alamos, NM
Research Project (Individual Project) — Summer 2023

- Design ML models preventing adversarial attacks
- Introduce neuroscience-based techniques to design robust audio classifiers

Large Language Model (LLM) Generalizability — Hanover, NH
Research Project (Individual Project) — Winter-Spring 2023

- Leverage pre-trained large language models to analyze their robustness and generalizability
- Fine-tune language models for specific tasks to test their generalizability and memorization properties

Security for AI — Boston, MA
Research and Development Project (Team Project) — Summer 2022

- Design efficient data privacy and security threats (NLP) to Deep Learning Models
- Detect and mitigate Deep Learning Model security threats

Disparate Vulnerability in ML Model Inversion Attack — Hanover, NH
Research Project (Individual) — Winter 2022, Spring 2022

- Design model inversion attack against ML Models with the least adversarial capabilities
- Introduce disparity prediction model to analyze the *fairness* of ML models under adversarial and privacy attacks

Model Inversion Attribute Inference Attack (MIAI) on Tabular Data — Hanover, NH
Research Project (Individual) — Fall 2021

- Introduce novel black-box MIAI attack against ML Models
- Analyze efficacy of proposed attack and distributional privacy leakage

Biometric Authentication — Hanover, NH
Development Project (Team Project) — Winter 2021

- Design ML and DL models for user authentication
- Developing authentication models based on heart rate, breathing, and gait features

Phone Call Trend — Hanover, NH
Data Analytics Project (Team Project) — Winter 2021

- Predicting Geo-Temporal pattern of students' phone call behavior.
- Analyzing social and contextual impacts on communication pattern

HealthMine — Hanover, NH
Development Project (Team Project) — Spring 2020

- Design an Android app for collecting user sensor data.
- Develop a way to redirect to the 'Dexcom' CGM app from our own app to collect user blood glucose data from the CGM device after user authorization.
- Conducting user study to get feedback

Digital SMD — Hanover, NH
Research Intern Project (Individual) — Fall 2019

- Collecting and Analyzing Insulin Pump, Glucose Monitor Data.
- Applying ML models to detect elements affecting Diabetes self-management.
- Recommending diabetic patients based on the identified patterns.

Human Activity Recognition — Riverside, CA
Research Project (Team Project of two) — Spring 2018

- Predicting human activities based on smartphone sensor data set.
- Constructing data mining models to classify human activities.
- Demonstrating different feature selection techniques to test prediction accuracy.

Efficient Path Profiling in LLVM — Riverside, CA
Software Project (Team Project of two) — Spring 2018

- Implemented the Edge Profiling of any arbitrary code and constructed the Ball-Larus Path Profiling algorithm.
- Instrumenting the execution frequencies of different paths in any arbitrary code using the LLVM compiler infrastructure.

Mining Interesting Patterns from TSDB using Resampling — Riverside, CA
Research Project (Individual) — Fall 2017

- Proposed a new and effective approach to mine all types of interesting periodic patterns without having any predefined period value or type from the *Time Series Database* (TSDB).
- Detecting all types of periodic patterns, particularly by skipping intermediate events using the proposed algorithm.

Place Identification Using Augmented Reality — Dhaka, Bangladesh
Software Project (Team Project of ten) — Fall 2015

- Developed a system or application that facilitates users to find information about an unknown place.
- Identifying places by capturing the image of the place while directing the phone to that place.

Diabetic Monitor App — Dhaka, Bangladesh
Software Project (Team Project of ten) — Fall 2015

- Performed survey to collect data regarding diabetic patients.
- Developed an app to assist diabetic patients in getting information about foods, exercise, and other tips based on their sugar level.

Bank Management System — Dhaka, Bangladesh
Software Project (Individual) — Fall 2014

- Implemented customer accounts, deposits, and payment modules to ensure a secure and reliable banking system using JAVA.
- Ensured better management of data regarding customers bank account, transactions and history.

Cell-Phone Operated Land Rover — Dhaka, Bangladesh
Hardware Project (Team Project of three) — Spring 2014

- Applied phone calls to control a remote robot based on button press.
- Implemented using dual tone multiple frequency (DTMF) technique.

Result Processing System — Dhaka, Bangladesh
Software Project (Team Project of three) — Fall 2013

- Designed a secured and reliable result processing system for the university.
- Demonstrated the most efficient and reliable software design technique to implement the software.

Automatic Traffic Light Control — Dhaka, Bangladesh
Hardware Project (Team Project of three) — Spring 2013

- Implement a traffic light control system to control traffic lights consistently and accurately to maintain the proper flow of traffic.
- Used microcontroller and circuit chips to design the system with a timer IC to ensure the accuracy of traffic control.

Peer Reviewed Publications

C_1 Vhaduri, S., **Dibbo, S. V.**, Gomez, S., and Gajic, A. "Understanding Stability of Choices: Toward a Choice-Based Authentication in Cybersecurity." *IEEE SouthEastCon'26*, Huntsville, AL, March 2026. (* under review)

C_2 Jaiyeoba, O., **Dibbo, S. V.**, Vhaduri, S., and Springer, J., "RL-AC-WaveGAN: A Novel Reinforcement Learning-based Auxiliary Classifier WaveGAN for Fine-Grained Multi-Class Audio Synthesis." *INTERSPEECH Conference*, July 2025. (* under review)

C_3 Amebley, D.††, and **Dibbo, S. V.** "Are Neuro-Inspired Multi-Modal Vision-Language Models Resilient to Membership Inference Privacy Leakage?" *USENIX WOOT Conference on Offensive Technologies*, Bultimore, MD, August 2026 (* Top Security Conference, under review), Pre-print.

C_4 Gammon, R.†† , **Dibbo, S. V.**, Vhaduri, S., Teti, M. "Many Metrics, One Truth? Combining Heuristics to Detect Hallucinations in LLMs." *SPIE Defnse+Security Conference on Assurance and Security for AI-enabled Systems*, Washington D.C., April 2026. (* Just Accepted)

C_5 **Dibbo, S. V.**, Breuer, A., Moore, J. S., and Teti, M. A., "Improving Robustness to Model Inversion Attacks via Sparse Coding Architectures," *The 18th European Conference on Computer Vision (ECCV 2024)*, Milan, Italy, October 2024, pp. 117-136 [(**Acceptance rate 2395/8585 = 27.9%**)]

(ranked **3rd** journal/conference, with h5-index = 262, in Computer Vision & Pattern Recognition by Google Scholar).

C_6 **Dibbo, S. V.**, Moore, J. S., Kenyon, G. T., and Teti, M. A., "LCANets++: Robust Audio Classification using Multi-layer Neural Networks with Lateral Competitions," *IEEE International Conference on Acoustics, Speech, and Signal Processing Workshops (ICASSPW)*, Seoul, Korea, April 2024, pp. 129-133 (ranked **1st** journal/conference, with h5-index = 137, in Acoustics & Sound by Google Scholar).

C_7 **Dibbo, S. V.**, Mansingh S., Rego J., Kenyon G., Moore J., and Teti M., "How Can Neuroscience Help Us Build More Robust Deep Neural Networks?", *2nd AdvML Frontiers workshop at 40th International Conference On Machine Learning (ICML 2023)*, Honolulu, Hawaii, July 2023, Available.

C_8 **Dibbo, S. V.**, "SoK: Model Inversion Attack Landscape: Taxonomy, Threat Models, and Defenses," *36th IEEE Computer Security Foundations Symposium (IEEE CSF)*, Dubrovnik, Croatia, July 2023, pp. 408-425 (**Acceptance rate 38/187 = 20.3%**).

C_9 **Dibbo, S. V.**, Chung D. L., and Mehnaz S., "Model Inversion Attack with Least Information and an In-depth Analysis of its Disparate Vulnerability," *First IEEE Conference on Secure and Trustworthy Machine Learning (IEEE SaTML)*, Raleigh, USA (**Acceptance rate 40/152 = 26.3%**, *Similar to NeurIPS, ICML acceptance rate).

C_{10} Mehnaz S., **Dibbo, S. V.**, Kabir E., Li N., and Bertino E., "Are Your Sensitive Attributes Private? Novel Model Inversion Attribute Inference Attacks on Classification Models," *31st USENIX Security Symposium* (USENIX Security'22), Boston, USA. (**Acceptance rate 256/1492=17.2%**, *Highly Contributed as a Leading Student Author). (ranked **2nd** journal, with h5-index = 106, in Computer Security & Cryptography by Google Scholar).

C_{11} Vhaduri, S., **Dibbo, S. V.**, and Chen C., "Predicting a user's demographic identity from leaked samples of health-tracking wearables and understanding associated risks." *2022 IEEE 10th International Conference on Healthcare Informatics (ICHI)*, Rochester, MN, USA, June 2022, pp. 309-318.

C_{12} **Dibbo, S. V.**, Kim, Y., Vhaduri, S. "Effect of Noise on Generic Cough Models." *2021 IEEE 17th International Conference on Wearable and Implantable Body Sensor Networks (BSN)*, Virtual, July 2021, pp. 1-4.

C_{13} ****Dibbo, S. V.**, ** Vhaduri, S., Kim, Y., and C., and Pollabauer. "Visualizing college students' geo-temporal context-varying significant phone call patterns." *2021 IEEE 9th International Conference on Healthcare Informatics (ICHI)*, Victoria, Canada, August 2021, pp. 381-385.

C_{14} Vhaduri, S., **Dibbo, S. V.**, Chen, C., and Pollabauer, C."Predicting Next Phone-Call Duration: A Pathway To Promote Mental Health At the Age of Stay Home and Lockdown." *2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC)* Virtual, July 2021, pp. 804-811. [**Acceptance Rate: ≈ 27%**]

C_{15} **Dibbo, S. V.**, Cheung, W., and Vhaduri, S. "On-Phone CNN Model-based Implicit Authentication to Secure IoT Wearables." *EAI International Conference on Safety and Security in IoT* (EAI SaSeIoT), Cyberspace, April 2021. (* Best Community-voted Presentation)

C_{16} Muratyan, A., Cheung, W., **Dibbo, S. V.**, and Vhaduri, S. "Opportunistic Multi-Modal User Authentication for Health-Tracking IoT Wearables." *EAI International Conference on Safety and Security in IoT* (EAI SaSeIoT), Cyberspace, April 2021. (* Best Community-voted Presentation)

C_{17} Morton S., Li R., **Dibbo, S. V.**, and Prioleau T., "Data-Driven Insights on Behavioral Factors that Affect Diabetes Management," *42nd Annual International Conference of the IEEE Engineering in Medicine and Biology Society* (IEEE EMBC), Montreal, QC, Canada, July 2020.

C_{18} Babu, H. M. H., Jamal, L., **Dibbo, S. V.**, and Biswas A. K., "Area and Delay Efficient Design of a Quantum Bit String Comparator," *IEEE Computer Society Annual Symposium on VLSI* (IEEE ISVLSI), Bochum, Germany, July 2017.

C_{19} **Dibbo, S. V.**, Babu, H. M. H., and Jamal, L., "An Efficient Design Technique of a Quantum Divider Circuit," *IEEE International Symposium on Circuits & Systems* (IEEE ISCAS), Montreal, QC, Canada, May 2016 (ranked **15$^{\text{th}}$** journal, with h5-index = 39, in Computer Hardware Design by Google Scholar).

========== Journals ==========

J_1 **Dibbo, S. V.**, Lin, C-H., and Vhaduri, S., "Challenges and Opportunities of Generative AI Models in Audio/Acoustic." *Engineering Applications of Artificial Intelligence* Elsevier, August 2025. (* Impact Factor 8, Journal #16 in AI according to Google Scholar, Major Revision Submitted)

J_2 **Dibbo, S. V.**, Yoshimura, H., and Vhaduri, S. "Challenges and Opportunities of Federated Learning In the Age of IoT: A Multi-Domain Comprehensive Survey." *IEEE Access*, September 2025. (* under review)

J_3 Vhaduri, S., **Dibbo, S. V.**, Muratyan, A., and Cheung, W. "mWIoTAuth: Multi-wearable data-driven implicit IoT authentication." *Future Generation Computer Systems, Elsevier* (FGCS), May 2024. [**Impact Factor: 6.2, CiteScore: 21.1**] (ranked **2$^{\text{nd}}$** journal/conference, with h5-index = 146, in Computing Systems in Engineering & Computer Science by Google Scholar).

J_4 Lien, CW., Vhaduri, S., **Dibbo, S. V.**, and Shaheed, M. "Explaining vulnerabilities of heart rate biometric models securing IoT wearables." *Machine Learning with Applications, Elsevier* (MLA), May 2024.

J_5 Vhaduri, S., **Dibbo, S. V.**, and Cheung, W. "Implicit IoT Authentication Using On-Phone ANN Models and Breathing Data." *Elsevier Internet of Things* (IoT), Nov 2023. [**Impact Factor: 6, CiteScore: 12.1**] (ranked **6$^{\text{th}}$** journal/conference, with h5-index = 72, in Computing Systems in Engineering & Computer Science by Google Scholar).

J_6 Vhaduri, S., **Dibbo, S. V.**, and Kim, Y., "Environment Knowledge-Driven Generic Models to Detect Coughs from Audio Recordings," *IEEE Open Journal of Engineering in Medicine and Biology (IEEE OJEMB)*, April 2023. [**Impact Factor: 2.7, CiteScore: 9.5**]

J_7 Vhaduri, S., Cheung, W., and **Dibbo, S. V.**, "Bag of On-Phone ANNs to Secure IoT Objects Using Wearable and Smartphone Biometrics," *Transactions on Dependable and Secure Computing (IEEE TDSC)*, April 2023. [**Impact Factor: 7, CiteScore: 11.2**] (ranked **2$^{\text{nd}}$** journal, with h5-index = 70, in Computer Security & Cryptography in Engineering & Computer Science by Google Scholar).

J_8 Vhaduri, S., **Dibbo, S. V.**, and Cheung, W. "HIAuth: A Hierarchical Implicit Authentication System for IoT Wearables Using Multiple Biometrics." *IEEE Access*, volume 9, pp. 116395 – 116406, August 2021. [**Impact Factor: 3.9**] (ranked **1$^{\text{st}}$** journal/conference, with h5-index = 266, in Engineering & Computer Science (general) in Engineering & Computer Science by Google Scholar).

J_9 Vhaduri, S., **Dibbo, S. V.**, and Kim, Y. "Deriving College Students' Phone Call Patterns to Improve Student Life." *IEEE Access*, 2021. [**Impact Factor: 3.9**] (ranked **1st** journal/conference, with h5-index = 266, in Engineering & Computer Science (general) in Engineering & Computer Science by Google Scholar).

Poster Presentations

1. Gammon, R., and **Dibbo, S. V.**, "Many Metrics, One Truth? Combining Heuristics to Detect Hallucinations in LLMs," *Alabama Higher Education AI Exchange*, Tuscaloosa, October 2025.
2. Amebley, D., and **Dibbo, S. V.**, "VLMLeaks: Membership Inference Attacks against VLMs," *Alabama Higher Education AI Exchange*, Tuscaloosa, October 2025.
3. **Dibbo, S. V.**, Breuer, A., Moore, J. S., and Teti, M. A., "Improving Robustness to Model Inversion Attacks via Sparse Coding Architectures," *The 18th European Conference on Computer Vision (ECCV 2024)*, Milan, Italy, October 2024.
4. **Dibbo, S. V.**, Moore, J. S., Kenyon, G. T., and Teti, M. A., "LCANets++: Robust Audio Classification using Multi-layer Neural Networks with Lateral Competitions," *ACM International Conference on Neuromorphic Systems (ACM ICONS)*, Santa Fe, August 2023.

Doctoral Consortiums

1. **Dibbo, S. V.**, "Novel Privacy Attacks and Defenses Against Neural Networks," *ACM SIGSAC Conference on Computer and Communications Security (CCS)*, Salt Lake City, Utah, October 2024, pp. 5113-5115.
2. **Dibbo, S. V.**, Breuer, A., Moore, J. S., and Teti, M. A., "Improving Robustness to Model Inversion Attacks via Sparse Coding Architectures," *Doctoral Consortium, ECCV 2024* , Milano, Italy, October 2024.

Grants & Fundings

1. **PI** "Character Formation of STEM Students via AI-Driven Educational Frameworks: A Transferable Multi-Disciplinary Approach," *Spencer Foundation Education Research Grants*, \$50K, Dec 2025 (*Pending).
2. **PI** "ProvenanceShield: MIA-Resilient Tool for Disinformation Defense in VLMs," *Microsoft Research Faculty Fellowship*, \$47K, Dec 2025 (*Pending).
3. **PI** "Research Initiation: Fostering Trustworthy AI Competence Among Engineering Graduates through Interactive Cybersecurity-Focused Learning," *National Science Foundation (NSF)*, \$200K, Nov 2025 (*Pending).
4. **PI** "TFL: Generative AI Framework to Secure Training Data Leakage in Foundational Large Models," *Amazon Research Award*, \$120K, Nov 2025 (*Pending).
5. **PI** "A Novel Scalable Multi-Modal Fusion-based AI/ML Method for Better Prediction of Water Quality," *Cooperative Institute for Research to Operations in Hydrology (CIROH)* , \$250K, Oct 2025 (*Pending).
6. **PI** "Secure and Trustworthy Human-AI Teaming: Robust Privacy Defenses for Multi-Modal AI Systems," *Sloan Research Fellowships*, \$75K, Jul 2025 [UA IPF: 25-1252] (*Pending).
7. **PI:** "Google Cloud Research Program," *Google*, \$5K, Dec 2025.
8. **PI:** "Faculty Fellow, Styslinger College of Engineering," *Hewson Family Foundation*, \$15K, Nov 2025.

Invited Talks

1. West Alabama WVUA23 News Channel Interview on AI in Education — Fall 25
2. Knight Foundation School of Computing and Information Sciences, Florida International University — Spring 25
3. College of Emergency Preparedness, Homeland Security and Cybersecurity, University at Albany, State University of New York — Fall 24
4. Computer Science Department, University of Alabama — Fall 24
5. Computer Science Department, California State University, East Bay — Fall 24
6. Computer Science Department, Texas A&M Corpus Christi University — Fall 24
7. Center for Non-Linear Studies (CNLS), Los Alamos National Lab — Fall 23

Honors & Awards

- **Hewson Faculty Fellow, Styslinger College of Engineering**, prestigious Fellowship by the University of Alabama — November 2025
- **Inaugural Dartmouth Cybersecurity Research Cluster Pre-Doctoral Research Fellow**, prestigious Cybersecurity Research Fellowship by Dartmouth College — January 2024
- **National Science Foundation (NSF) Secure and Trustworthy Cyberspace (SaTC) Aspiring PI** Award to attend the PI Workshop organized by the NSF SaTC program — May 2023
- **Best Community-voted Presentation Award**, awarded by the EAI (SaSeIoT 2021) community for the best paper presentations — April 2021
- **Dartmouth Fellow**, Guarini Graduate School, Dartmouth College — September 2020
- **Dean's Award (Gold Medal)**, Faculty of Engineering & Technology, University of Dhaka (one of the top 2 institutions in Bangladesh) for securing **Second** merit position in the B.Sc. Examination in Computer Science & Engineering, held in Dec 2015 (awarded to top 3 students) — May 2018
- **Dean's Distinguished Fellow**, Bourns College of Engineering, University of California, Riverside — September 2017
- **Perfect Attendance Award**, Notre Dame College, Dhaka (best institution in Bangladesh) for maintaining 100% attendance during the two consecutive academic years of College (awarded to only 100% attendance holders) — August 2011
- **First Place Winner**, Notre Dame College, Dhaka, for securing the **First** merit position among the **1.7 million** secondary school certificate holders, participated in the competitive admission test across a country with **163 million** population (awarded to the top-most student) — July 2009

Teaching Experience

University of Alabama, Tuscaloosa — Tuscaloosa, AL
Course Instructor — Fall 2025-present
Department of Computer Science

- CS 690: Security and Privacy of Machine Learning — Spring 26
  (*class size: 20*)
  Tools: Blackboard
- CS 692: Mentored Research Experience — Fall 25, Spring 26
  (*class size: 5*)
  Tools: Blackboard
- CS 691: Independent Study — Spring 26
  (*class size: 5*)
  Tools: Slack, Blackboard
- CS 428: Computer Security — Fall 26
  (*class size: 50*)
  Tools: Ed Discussion, Canvas

Dartmouth College, Hanover — Hanover, NH
Graduate Teaching Assistant — Fall 2020-Winter 2025
Department of Computer Science

- COSC 61: Database Systems — Winter 25
  (*class size: 60; Undergraduate Class*)
  Tools: Ed Discussion, Canvas
- COSC 51: Computer Architecture — Fall 23, Fall 24
  (*class size: 50/60; Undergraduate Class*)
  Tools: Ed Discussion, Canvas
- COSC 89/189: Deep learning generalization and robustness — Spring 23
  (*class size: 20; Graduate/Undergraduate Class*)
  Tools: Piazza, Canvas
- COSC 78/278: Deep Learning — Winter 23
  (*class size: 60; Graduate Breadth Requirement*)
  Tools: Piazza, Canvas
- COSC 58/258: Operating Systems — Winter 22, Fall 22
  (*class size: 60, 58; Graduate Breadth Requirement*)
  Tools: Gitlab, Slack, Canvas
- COSC 59: Principles of Programming Languages — Summer 21
  (*class size: 40; Undergraduate class fulfills MSCS Requirement*)
  Tools: Slack, Codechef competition
- COSC 55: Security and Privacy — Winter 21, Fall 21
  (*class size: 35, 10; Undergraduate + MSCS Requirement*)
  Tools: Slack, Canvas
- COSC 10: Problem Solving using Object Oriented Programming — Fall 20, Spring 21, Spring 22
  (*class size: 110-120; Undergraduate Class*)
  Tools: Canvas, Slack

University of California, Riverside Riverside, CA
Graduate Teaching Assistant Fall 2018-Winter 2019
Department of Computer Science & Engineering

- CS 61: Machine Organization and Assembly Language Programming
  (*class size: 110*) Winter 19
  Tools: Github, Piazza, Gradescope
- CS 152: Compiler Design
  (*class size: 30*) Fall 18
  Tools: Piazza, Blackboard

Mentoring Experience

University of Alabama, Tuscaloosa Tuscaloosa, AL
Undergraduate & Graduate Faculty Mentor Fall 2025-present
Department of Computer Science

- Adebayo Keji, PhD Student, Computer Science, University of Alabama
- David Amebley, PhD Student, Computer Science, University of Alabama
- Collin Francel, Accelerated MS, Data Science Major, Randall Research Scholar, University of Alabama
  Mentored and supported/nominated for "The Barry Goldwater Scholarship and Excellence in Education Foundation Scholarship"
- Arsh Somani, Junior, Mechanical Engineering Major, University of Alabama
- Ryan Gammon, Sophomore, Data Science Major, University of Alabama
- Kevin Aharrah, Junior, Computer Science Major, Emerging Scholar, University of Alabama
- Foster Smith, Junior, Computer Science Major, University of Alabama
- Parker Patton, Freshman, Computer Science Major, University of Alabama
- Candace Barley, Sophomore, Computer Science Major, University of Alabama

Dartmouth College, Hanover Hanover, NH
Graduate Teaching Assistant Fall 2020-Winter 2025
Department of Computer Science

- Undergraduate Student Mentoring Experience:
  - Dae Lim Chung (currently an MS student in CS at Columbia University)
  - Darley Sackitey (currently a PhD student in CS at Georgia Institute of Technology)

- Arihant Chadda (senior UG)
- Sylvester E. Coch (senior UG)

University of Dhaka Dhaka, Bangladesh
Undergraduate Mentor Fall 2015
Department of Computer Science & Engineering

- Mentor and Section Leader:
  - Riaz Uddin (currently Maintenance Engineer, Ministry of Bangladesh)
- Research Collaborator & Coordinator:
  - Mubin Ul Haque (currently PhD Student in CS at the University of Adelaide)
  - Md. Solaiman Mia (currently Lecturer in CS at Green University of Bangladesh)

Fellowships

- Dartmouth Guarini Graduate School Travel Grant to attend ACM CCS Doctoral Consortium Attendance ($1000) Summer 24
- ACM CCS Doctorial Consortium Attendance Travel Grant ($1000) Summer 24
- NSF SaTC Aspiring PI Workshop attending travel grant ($2000) Summer 23
- Summer Research Fellowship, Center for Non-Linear Studies (CNLS), Los Alamos National Lab ($15000) Summer 23
- Dartmouth Graduate Student Council Conference Travel Grant ($500, $550) Fall 22, Winter 23
- Dartmouth College Fellowship ($30k/yr) Fall 2020-2025
- Higher Study Travel Grant, Bangladesh-Sweden Trust Fund, Ministry of Economic Relations, Bangladesh ($800) Fall 2018
- Dean's Distinguished Fellowship, Bourns College of Engineering, University of California, Riverside ($52,000 for 1 year) Fall 2017
- Dhaka University Alumni Association (DUAA) Scholarship, University of Dhaka ($400) Fall 2015
- Shamshul Haque Trust Fund Fellowship, University of Dhaka ($1200) Fall 2015
- Mitsubishi UFJ Foundation Scholarship, Mitsubishi Corporation, Tokyo, Japan ($3000) Fall 2015
- Higher Secondary School Scholarship, Education Board Dhaka ($500) Fall 2012
- Full-free Studentship, Notre Dame College, Dhaka ($400) Fall 2010
- Secondary School Scholarship, Education Board Dhaka ($300) Spring 2010
- The Scholar's Forum Scholarship, Scholars Forum, Dhaka ($200) Fall 2008
- Full-free Studentship, St. Gregory's High School & College ($400) Fall 2007
- Junior School Scholarship, Education Board Dhaka ($500) Spring 2007
- Gregorian Scholarship, St. Gregory's High School & College ($200) Fall 2007
- Primary School Scholarship, Education Board Dhaka ($100) Fall 2004

Leadership & Services

- Program Committee, *USENIX Security 2026* *2025-26*
- Program Committee, *ACM CCS 2026* *2025-26*
- Doctorial Consortium Presentation, ECCV Conference, Milano, Italy *2024*
- Research Poster Presentation, *International Conference on Neuromorphic Systems (ACM ICONS)*, Santa Fe, NM *2023*
- PC (Program Committee), *USENIX Security* Artifact Evaluation *2022-2023*
- Represent Dartmouth College Graduate Student Council (GSC) on new student orientation/the activities fair *Fall 2021*
- Co-chair of *Committee for Addressing Racism and Equity (CARE)*, Dartmouth College Graduate Student Council (GSC) *2021-2022*
- Participant of *Graduate Student Leadership Training*, Dartmouth College *2021*
- Volunteer at *ACM Ubicomp Conference* at London, UK *2019*
- Mentor at *BioHack 2019*, Hackathon of Biomedical Engineering Society Chapter, UC Riverside *2019*
- Participant of *'Leadership in Action Program'* at UC Riverside *2018*
- Volunteer, *'Tobacco Free Environment Campaign'* at UC Riverside *2018*
- Volunteer, *Martin Luther King Day* at UC Riverside *2018*
- Keynote speaker in *'Fresher's Reception Ceremony'* at Notre Dame College *2009*

Journal & Conference Paper Reviewer

1. Neural Information Processing Systems (NeurIPS) *2025*
2. Journal of Systems Architecture *2025*
3. Digital Signal Processing (DSP) Journal, Elsevier *2025*
4. ACM Transactions on Audio, Speech and Language Processing (T-ASL) *2025*
5. Journal of Neurocomputing, Elsevier *2024, 2025*
6. Women in Computer Vision Conference, ECCV *2024*
7. Neural Networks Journal, Elsevier *2024*
8. Computers and Security Journal, Elsevier *2024*
9. Internet of Things (IoT) Journal, Elsevier *2023*
10. IEEE Transactions on Neural Networks and Learning Systems *2023*
11. USENIX Security Symposium *2021*
12. NSysS Conference *2021*
13. Annual Computer Security Applications Conference (ACSAC) *2021*
14. IEEE Access *2024, 2018*
15. IEEE Transactions on Nanotechnology (TNANO) *2018*

16. Journal of Multiple-Valued Logic & Soft Computing *2017*
17. IEEE Computer Society Annual Symposium on VLSI (ISVLSI) *2017*
18. Springer Quantum Information Processing Journal *2016*
19. IEEE Region 10 Conference (TENCON) *2016*
20. IEEE International Symposium on Circuits & Systems (ISCAS) Conference *2016*

Professional Development and membership

- CRA Career Mentoring Workshop *2026*
- UA Grant Writing Workshop *2026*
- IEEE Member *2025*
- CRA Widening Participation Workshop *2025*
- USENIX Association Member *2025*
- ACM SIGSAC Member *2025*
- CITI Human Study Certification Program *2024*
- Asian CHI Symposium 2020, Honolulu, Hawaii *2020*
- Cornell, Maryland, Max Planck Research School, Germany *2019*
- Apprentice Teaching *Pedagogical* development program, UC Riverside *2018*
- PhD Pivot Workshop, UC Riverside *2018*
- UC Ethical Values and Conducts Training, UC Riverside *2018*
- UC Cyber Security Awareness Training, UC Riverside *2018*

Skills

Programming Skills

- C/C++, Python, Scikit-learn, TensorFlow, Pytorch, R, Java, SQL, Spark, Tableau, Weka
- Android Programming, Assembly Language, Shell Programming

Software Skills

- MS Word, Excel, Powerpoint, Photoshop, Graphic Design, JIRA
- Oracle, SQL Server, DB2, MongoDB, MySQL, Matlab, SWI-Prolog, Arduino, Android Studio, OpenGL, OpenCV