





# Shoumik Saha

 shoumiksaha.github.io  
 (+1)240-9279795

smksaha@umd.edu  
 in/shoumik-saha

 /ShoumikSaha

## RESEARCH INTEREST

---

- **Machine Learning** - Adversarial Machine Learning, Security for Machine Learning
- **Security** - Computer security, Malware, Adversarial Attack

## EXPERIENCE

---

### Graduate Research Assistant

Department of Computer Science  
University of Maryland

Supervisor - Dr. Soheil Feizi

**Full Time**

Jan 2024 – Present

### Graduate Research Assistant

Maryland Cybersecurity Center

Supervisor - Dr. Tudor Dumitras

**Full Time**

Aug 2022 – Dec 2023

### Lecturer

Department of Computer Science and Engineering  
United International University

**Full Time**

Jul 2021 – Jul 2022

### Research Assistant

Data Science and Engineering Research Lab

Bangladesh University of Engineering and Technology (BUET)

**Part Time**

Mar 2021 – Jul 2022

## EDUCATION

---

### University of Maryland

Ph.D. in Computer Science and Engineering (Ongoing)

Aug 2022 – Present

○ CGPA – 3.74/4.0

○ Advisor – Dr. Soheil Feizi

### Bangladesh University of Engineering and Technology (BUET)

BSc. in Computer Science and Engineering

Mar 2016 – Feb 2021

○ CGPA – 3.66/4.0

○ Advanced GPA – 3.79/4.0

○ Thesis supervisor – Dr. Atif Hasan Rahman

### Notre Dame College

Higher Secondary Certificate

Jul 2013 – Jun 2015

○ GPA – 5.00/5.00

## RESEARCH

---

- **DRSM: De-Randomized Smoothing on Malware Classifier Providing Certified Robustness**

Shoumik Saha, Wenxiao Wang, Yigitcan Kaya, Soheil Feizi, Tudor Dumitras

*ICLR 2024 (International Conference on Learning Representations)* ([arxiv](#)) ([OpenReview](#))

We are the first to propose certified robustness in the domain of static malware detection from executables. We demonstrated both theoretical and empirical robustness of our proposed DRSM framework. Besides, we published a new benign dataset, named PACE.

- **MAlign: Explainable Static Raw-byte Based Malware Family Classification using Sequence Alignment**

Shoumik Saha, Sadia Afroz, Atif Rahman

*Computers & Security Journal* ([url](#))

We proposed a novel approach, namely MAlign, incorporating concepts from Bioinformatics into Malware Security. We developed a static raw-byte-based malware family classifier with better accuracy and robustness. MAlign also provides explainability by relocating the code blocks responsible for malicious attacks.

- **Is Machine Learning Sufficient for Malware Detection in the Wild?**

Yigitcan Kaya, Yizheng Chen, **Shoumik Saha**, Fabio Pierazzi, Lorenzo Cavallaro, David Wagner, Tudor Dumitras  
*Under Review* ([url](#))

We presented a quantitative study of how sandbox traces differ from real-world ones, and how it impacts machine learning models. We identified this distribution shift and proposed a solution for ML models that boosted the TPR from 14% to 20%@1%FPR.

- **Contrastive Self-Supervised Learning Based Approach for Patient Similarity: A Case Study on Atrial Fibrillation Detection from PPG Signal**

**Shoumik Saha**, Subangkar Shanto, Atif Rahman, Mohammad Masud, Mohammed Eunus Ali  
*Under Review* ([arxiv](#))

We proposed Contrastive Learning based Deep Learning solution to find the patient similarity using physiological signal. We demonstrated the efficacy of our method by applying it to detect Atrial Fibrillation using PPG signals collected from smartwatches.

## SCHOLARSHIPS AND ACHIEVEMENTS

---

- Awarded 'Dean's Fellowship' from the University of Maryland
- Awarded 'Innovation Fund' for research from the ICT division of Bangladesh government
- Achieved 'Merit Stipends' from BUET in five out of seven terms
- Got 'Dean's Award' in Junior year for extra-ordinary result
- Achieved 'Talent-Pool Scholarship' in High School

## TEACHING

---

### Teaching Assistant

University of Maryland

Fall 2023

Data 200: Knowledge in Society: Science, Data and Ethics

### Lecturer

United International University

Fall 2021 - Summer 2022

Discrete Mathematics, Data Structure and Algorithm, Operating Systems

## SELECTED ACADEMIC PROJECTS

---

- **Website Development for Flight and Hotel Room Reservation System** ([Github link](#))  
*Tools:* Django, SQLite
- **Software Development for Football Club Management** ([Github link](#))  
*Tools:* Java, JavaFX, Oracle Database
- **Micro-controller Project for Real-time Detection of Car Theft** ([Youtube video link](#))  
*Tools:* Arduino, GPS, GSM module, Sonar, LDR sensor
- **Multi-player Shooting Game** ([Github link](#))  
under the same network. *Tools:* Java, JavaFX, Java Networking
- **Tic-Tac-Toe** ([Github link](#))  
*Tools:* C, iGraphics

## ACTIVITIES

---

- General Secretary, BUET Photographic Society
- Participant, ICPC Dhaka Regional
- President, Notre Dame Nature Study Society
- Vice President, Gregorian Science Club