Sifat Muhammad Abdullah

✉ sifat@vt.edu 🌐 https://sifatmd.github.io ☎ 540-449-2710

EDUCATION

Virginia Tech, Blacksburg, VA Jan 2021 - Present (Expected 2025)
Ph.D. in Computer Science
Advised by Dr. Bimal Viswanath

BUET, Dhaka, Bangladesh 2015 - 2019
B.S. in Computer Science and Engineering
(GPA: 3.91/4.0)

RESEARCH INTERESTS

Security of Multimodal LLMs, Adversarial Robustness of Generative AI Defenses, Improving Defenses with better Content Semantics understanding using Multimodal Foundation models, toxicity mitigation in Large Language Models.

PUBLICATIONS

- **An Analysis of Recent Advances in Deepfake Image Detection in an Evolving Threat Landscape**
  Sifat Muhammad Abdullah, Aravind Cheruvu, Shravya Kanchi, Taejoong Chung, Peng Gao, Murtuza Jadliwala, and Bimal Viswanath.
  IEEE S&P, San Francisco, CA, May 2024.
- **A First Look at Toxicity Injection Attacks on Open-domain Chatbots**
  Aravind Cheruvu(co-lead), Connor Weeks(co-lead), **Sifat Muhammad Abdullah**, Shravya Kanchi, Danfeng Yao, and Bimal Viswanath.
  ACSAC, Austin, TX, Dec 2023.
- **Deepfake Text Detection: Limitations and Opportunities**
  Jiameng Pu(co-lead), Zain Sarwar(co-lead), **Sifat Muhammad Abdullah**, Abdullah Rehman, Yoonjin Kim, Parantapa Bhattacharya, Mobin Javed, and Bimal Viswanath.
  IEEE S&P, San Francisco, CA, May 2023.
- **CHAPAO: Likelihood and hierarchical reference-based representation of biomolecular sequences and applications to compressing multiple sequence alignments**
  Md Ashiqur Rahman (co-lead), Abdullah Aman Tutul(co-lead), **Sifat Muhammad Abdullah**(co-lead), Md Shamsuzzoha Bayzid.
  PLOS ONE Journal, 2022.
- **A Web-Based System for Efficient Contact Tracing Query in a Large Spatio-Temporal Database**
  Shadman Saqib Eusuf, Kazi Ashik Islam, Mohammed Eunus Ali, **Sifat Muhammad Abdullah**, Abdus Salam Azad.
  ACM SIGSPATIAL, Seattle, WA, Nov 2020.

EXPERIENCE

Virginia Tech SecML Lab Jan 2022 - Present

Graduate Research Assistant Blacksburg, VA

- Conducted large-scale study on the robustness of state-of-the-art deepfake image detectors by developing low-cost adversarial strategies using Stable Diffusion and GAN-based text-to-image generators.
- Studied various toxicity injection attacks in dialog-based learning setup on open-domain language models, e.g. BART & BlenderBot.
- Evaluated state-of-the-art deepfake text detectors against real-world large language model based services e.g. T5 and GPT-3 powered bots', and developed fully black-box adversarial attack without any surrogate model.

Virginia Tech Jan 2021 - Dec 2021

Graduate Teaching Assistant Blacksburg, VA

- Conducted office hours and programming labs in java and python.

BUET DataLab — Jan 2020 - Dec 2020

Graduate Research Assistant — Dhaka, Bangladesh

- Developed efficient query techniques for large spatio-temporal database to aid contact tracing of COVID patients
- Built road network detection systems with graph convolution and differentiable pooling

REVE Systems — May 2019 - Dec 2019

Software Engineer — Dhaka, Bangladesh

- Built a chatbot system to enhance overall user experience

ACHIEVEMENTS

Invited Talks

- VT Skillshop Series: Leveraging Creative Technologies - Integrating Generative AI to your benefit (Oct 2023)

Awards and Scholarships

- CCI SWVA Cyber Innovation Scholarship: 2024-2025
- BUET Dean's List Award: 2015-2019

Features

- CCI Research Showcase: 2024
- *The Dark Side of AI* - VPM News Focal Point: 2023
- CCI Student Spotlight: 2023
- *The Rise of the Chatbots* - Communications of the ACM: 2023
- *The strengths and limitations of approaches to detect deepfake text* - TechXplore: 2022

TECHNICAL

• **Languages**:	Python, C/C++, Bash, Java, Javascript, Assembly
• **Frameworks**:	PyTorch, Tensorflow, Keras, Django
• **Libraries**:	Scikit-learn, NumPy, pandas, Matplotlib
• **Developer Tools**:	Git, Vim, Jupyter Notebook, VS Code, Markdown, LaTeX, Linux, Docker