

MD SADIK HOSSAIN SHANTO

+8801767901647 shantosadikrglhs@gmail.com
Dhaka, Bangladesh [Site: frost101.github.io](https://frost101.github.io)
[Google Scholar](#) [ResearchGate](#)

EDUCATION

June 2025 - Present	Bangladesh University of Engineering and Technology (BUET) - CGPA: 4.00/4.00 (9 credits completed)	MSc in Computer Science and Engineering
February 2020 - March 2025	Bangladesh University of Engineering and Technology (BUET) - CGPA: 3.90/4.00 - Three-time Dean's List Award & Two-time University Merit recipient	BSc in Computer Science and Engineering

WORK EXPERIENCE

April 2025 - May 2026	Ministry of Defense – Healthcare Services • Lead: Dr. Ehsan Hoque (Prof., University of Rochester; MIT PhD) · w/ Sabri Boughorbel (QCRI), Abdulrhman Aljouie (KSAU-HS) - Research, build, and deploy clinical-grade AI for healthcare, autism (ASD) speech & language therapy; 2 papers (Interspeech 2026 + preprint) from this work. - Architected Digital Harf , a multimodal AI therapy platform (3 therapy modules + AI Caregiver Assistant) powered by an Agentic Synthetic Data Engine that auto-generates culturally grounded content. - Built Harf-Speech , fine-tuning Whisper , Omni-ASR , wav2vec2 for Arabic phoneme-level assessment with advantages over proprietary Azure Cognitive Services . - Integrated into Sehhatek , Saudi Arabia's national healthcare app serving millions of users (in staging; clinical trial beginning), with partners King Fahad Armed Forces Hospital, Mohammed Bin Salman Autism Program & Madinah Autism Society. - Contributed to cross-team efforts: Wae (autism screening, Univ. of Cambridge collaboration) and AIDA (autism screening, MIT Media Lab collaboration).	Remote AI Research Engineer – Kingdom of Saudi Arabia
-----------------------	--	--

TEACHING EXPERIENCE

June 2022 - January 2025	ROOTS Edu - Taught ICT, introductory programming and CS basics to 7,000+ students over three years at Roots Edu, one of Bangladesh's leading online EdTech platforms, covering languages, data structures, algorithms, and OOP fundamentals - Developed structured lesson plans and assessments from scratch, translating abstract CS concepts into accessible, beginner-friendly modules	Online ICT & Programming Instructor
--------------------------	--	--

RESEARCH EXPERIENCE & PUBLICATIONS

AI Safety & Security	SequentialBreak: Large Language Models Can be Fooled by Embedding Jailbreak Prompts into Sequential Prompt Chains • ACL 2025 (Student Research Workshop) · 22 Citations • w/ Md. Rafi Ur Rashid, PhD Student, Pennsylvania State University, USA - As large language models move into real products, their safety guardrails stay surprisingly brittle. SequentialBreak exposes a striking blind spot – burying a harmful request inside a chain of ordinary ones slips it past these defenses in a single query, revealing how fragile the alignment really is.	[Link:Paper]
VLM Uncertainty	The Art of Saying "Maybe": A Conformal Lens for Uncertainty Benchmarking in VLMs • EACL 2026 • w/ Dr. Mohammad Saifur Rahman, Prof., BUET and Md. Rizwan Parvez, Research Scientist, QCRI - Today's vision-language models stay confident even when they are wrong. This work tackles a neglected question – do they know what they don't know? – delivering the first broad benchmark of their uncertainty and a way to measure it even for closed, commercial models.	[Link:Paper]
Healthcare AI HCI HAI	Harf-Speech: A Clinically Aligned Framework for Arabic Phoneme-Level Speech Assessment • Interspeech 2026 · Remote AI Research Engineer, Ministry of Defense, Healthcare Services, Saudi Arabia • w/ Dr. Ehsan Hoque (Prof., University of Rochester; MIT PhD), Sabri Boughorbel (QCRI), Abdulrhman Aljouie (KSAU-HS) - What if speech assessment were available anytime, anywhere, without losing clinical quality? With Arabic-trained speech pathologists scarce, Harf-Speech automatically evaluates Arabic(MSA) at the same fine-grained level clinicians use, with results validated against certified specialists.	[Link:Paper]
Healthcare AI Agentic Systems Multimodality HCI HAI	Digital Harf: A Clinically Integrated Multimodal AI System for Pervasive Arabic Speech and Language Therapy • Under Review · Remote AI Research Engineer, Ministry of Defense, Healthcare Services, Saudi Arabia • w/ Dr. Ehsan Hoque (Prof., University of Rochester; MIT PhD), Sabri Boughorbel (QCRI), Abdulrhman Aljouie (KSAU-HS) - Children with autism in Arabic-speaking regions face a shortage of specialists and almost no culturally relevant therapy material. Digital Harf carries clinician-led speech therapy into the home through an AI engine that generates culturally grounded content – treating cultural fit as core infrastructure rather than an afterthought.	[Link:Preprint]

AI Safety
& Security

Robustness of Vision Language Models Against Split-Image Harmful Input Attacks [\[Link:Preprint\]](#)
• **Under Review:** ACM CCS 2026
• **w/ Dr. Shagufta Mehnaz (Asst. Prof.), Md. Rafi Ur Rashid, Vishnu Dasu (PhD Students), Pennsylvania State University, PA, USA**
- Vision-language models have learned to refuse harmful images – but only when the harm arrives in one piece. This work reveals that splitting a harmful image across fragments quietly defeats their safety training, introduces attacks that expose this overlooked gap, and proposes a defense to close it.

Computer Vision
Deepfakes

DFCon: Attention-Driven Supervised Contrastive Learning for Robust Deepfake Detection [\[Link:Competition\]](#) · [\[Link:Report\]](#)
• **1st Runner-Up, IEEE Signal Processing Cup at ICASSP 2025** · **Team Lead** · **2 Citations**
• **w/ Dr. Mohammad Saifur Rahman, Prof., BUET**
- As AI-generated faces grow indistinguishable from real ones, catching them in the wild remains an open problem. **I have lead this BUET team** at IEEE ICASSP 2025, we built a deepfake detector that blends complementary vision models to generalize across unseen generation methods and source datasets.

Remote Sensing
Computer Vision

AttMetNet: Attention-Enhanced Deep Neural Network for Methane Plume Detection in Sentinel-2 Satellite Imagery [\[Link:Award\]](#) · [\[Link:Preprint\]](#)
• **Highly Commended, Global Undergraduate Awards (Computer Science)** · **Under Review:** Expert Systems with Applications Journal
• **w/ Dr. Tanzima Hashem, Prof., BUET and w/ Sultanul Arifin, Lecturer, BRAC University, Dhaka**
- Methane is a potent driver of climate change, yet spotting its plumes from satellites is buried under false alarms that demand expert review. AttMetNet is a lightweight, attention-driven model that hones in on a methane-sensitive spectral signature to flag true plumes, making reliable global-scale monitoring practical.

SKILLS

Languages:	Python, C++, Java, JavaScript, C, SQL, Bash
AI/ML:	PyTorch, HuggingFace, LangChain, OpenCV, scikit-learn, Transformers, LLMs, VLMs, RAG
Frameworks:	FastAPI, Node.js, Express.js, React, Next.js, PostgreSQL, MySQL, Oracle, Prisma ORM
Tools:	Git, GitHub, Linux, Docker, $\LaTeX$, Postman, Wireshark, NS3
Cloud:	Google Cloud, Alibaba Cloud, DigitalOcean

HONORS & AWARDS

2025	IEEE Signal Processing Cup at ICASSP 2025 1st Runner-Up · Team Lead · [Link:Award] Secured 1st Runner-Up in the <i>Deepfake Face Detection in the Wild</i> challenge at IEEE ICASSP 2025, leading the BUET team
2025	The Global Undergraduate Awards Highly Commended – Computer Science · [Link:Award] Undergraduate Thesis recognized among top undergraduate research worldwide in Computer Science category
2020-2025	Dean's List Award and University Merit Dean's List Award (3×) · University Merit (2×) Awarded Dean's List for outstanding academic performance in three academic years; awarded University Merit for two semesters at BUET
2023	Intra BUET Capture The Flag (CTF) Competition 1st Runner-Up Achieved 2nd place among 35 teams in cybersecurity competition organized by BUET Cyber Security Club
2022	BD-Flag Hunt CTF Competition 9th Position Ranked 9th among 100+ teams in national cybersecurity challenge
2024	Microcontroller, Microprocessor and Embedded System Sessional Project Honorable Mention 6-DOF Robotic Arm mounted on a bot awarded Honorable Mention in CSE Department, BUET

LEADERSHIP & CONTRIBUTIONS

2025	Deep Learning Sprint, BUET CSE FEST 2025 Organizer · [Link: Part1] · [Link:Part2] Problem formulation, dataset curation & management for a 120+ team open deep learning contest at BUET's flagship technical festival
2024	Capture The Flag (CTF), BUET CSE FEST 2024 Organizer · [Link] Organized and maintained full competition infrastructure for a 60+ team cybersecurity challenge
2024-2025	BUET Cybersecurity Club Director of Technology Led technical operations; organized inter-university cybersecurity competitions and workshops