Asif Shahriar

☎ +8801742471521 ✉ asif.asr11@gmail.com 🌐 asif-shahriar11.github.io/ github

Research Interests

- Computer security, AI for security, Security for AI
- Adversarial ML, Trustworthy Generative AI, Secured Agentic Frameworks
- Natural Language Processing, Large Language Models, Retrieval Augmented Generation

Education

Bangladesh University of Engineering & Technology (BUET) **2019 - 2024**

B.Sc in Computer Science & Engineering

- CGPA: **3.85/4.0**
- CSE major-only CGPA: **3.91/4.0**
- **Dean's List** award for academic excellence

Publications

5GPT: 5G Vulnerability Detection by Combining Zero-Shot Capabilities of GPT-4 With Domain Aware Strategies Through Prompt Engineering

A. Shahriar, S. J. Hisham, K. M. A. Rahman, R. Islam, M. S. Hossain, R. H. Hwang, and Y. D. Lin

IEEE Transactions on Information Forensics and Security (IEEE TIFS), 2025

- Demonstrated that out-of-the-box GPT-4 is capable of identifying high-level logical inconsistencies, and ambiguous protocol rules; but suffers from hallucinations and struggles to capture deep protocol-level issues
- Introduced a novel domain-aware strategy to teach GPT-4 about security properties and hazard indicators from related works. Showed that domain-aware GPT-4 successfully identifies sophisticated multi-state and cross-procedure attacks, cryptographic and integrity violations, message spoofing, injection, privacy and identity exposure, and resource management exploits, while reducing false-positives

Inceptive Transformers: Enhancing Contextual Representations through Multi-Scale Feature Learning Across Domains and Languages

Asif Shahriar, Rifat Shahriyar, M Saifur Rahman

Accepted for presentation in **EMNLP 2025**

- Developed an inception-style multi-scale feature extraction framework for enhancing the contextual representations of encoder transformer models
- Experiments show that Inceptive Transformer improves both general-purpose (RoBERTa, DeBERTa, ModernBERT, XLM-RoBERTa) and domain-pretrained (BERTweet, BioBERT, CT-BERT, BanglaBERT) baselines by up to **14%** in FIVE different tasks

Ongoing Research Works

5G Vulnerability Detection using Retrieval-Augmented Generation **2024 - Ongoing**

- Supervisors: **Dr. Md. Shohrab Hossain** and **Dr. Syed Rafiul Hussain (Penn State)**
- We propose a novel, fully automated end-to-end framework that utilizes a Retrieval-Augmented Generation (RAG) pipeline to ground LLM outputs in verified, domain-specific data to minimize hallucinations
- We also introduce a robust context retrieval mechanism to overcome the cross-section dependency challenges

Cross-modal Deception: There is More than what Meets the Eyes **2025 - Ongoing**

- Supervisors: **Dr. Md. Shohrab Hossain** and **Dr. Rizwan Parvez (QCRI)**
- In traditional jailbreak attacks, user is the adversary while LLM is the victim. We aim to introduce a novel class of attacks that deceive both the user and the LLM
- The model is compromised by a hidden instruction, while the human user, who may be interacting with the model through a completely benign-looking image, is an unwitting participant in the attack

Secured Multi-agent Systems **2025 - Ongoing**

- Supervisors: **Dr. Rizwan Parvez (QCRI)**
- LLM-based agentic frameworks are on the rise, performing tasks like browsing the web, grocery shopping from amazon, running OS commands, and more
- In this work we focus on security in addition to utility: what if the cheapest deal is being offered at a phishing website? That's what we aim to find out

Teaching Experience

Department of CSE, BRAC University **2024 – Current**

Full-time Lecturer faculty-webpage

- Artificial Intelligence (Theory and Sessional)
- Data Communications (Theory)
- Data Structures (Sessional)
- Algorithms (Sessional)

Work Experience

North-West Power Generation Company Limited **May 2023 – June 2023**

Machine Learning Internship github-link

- Some of the ultrasonic flow-meters used by the company had engineering problems. I developed a machine learning algorithm that can predict the health status of a flow-meter given various readings, which achieved **83%** accuracy.

Technical Skills

Languages: Python • Java • Javascript • C • C++ • LaTeX • Assembly
Development: Next.js • nest.js • Node.js • React • GraphQL • Docker • HTML • CSS • Bootstrap
Database: OracleDB • PostgreSQL
Machine-Learning: NumPy • Pandas • Scikit-learn • SciPy • Matplotlib • Seaborn
Deep-Learning: PyTorch • TensorFlow • Convolutional Neural Networks (ResNet, InceptionNet, ViT) • Recurrent Neural Networks (RNN, LSTM, GRU) • Generative Models (GAN, VAE)
NLP: Word2Vec • Transformers • LangChain • Language models • LLMs • RAG
Networking & Security: 5G • LTE • Cryptography • EDR • NS2 • Open5GS • UERANSIM • 5GReplay • Scapy • CPPCheck • WireShark
Hardware: ATMega32 • Arduino-Uno • Fingerprint sensor • LCD Display

Top Projects

WhiskerDocs: A health-care solution for your pets **June 2023 - September 2023**

Software development project back-end | front-end

- Analyze symptoms | Book a vet based on location, experience and rating | Dashboard | History recorded | Blogs | Subscription | Payment module | Appointment scheduling | Prescription template | Auto-completion
- **Tools:** GraphQL | Next.js | nest.js | openstreetmap | PostgreSQL | Docker | ElasticSearch | Stripe
- **project-presentation** | **partial-demo**

Machine Learning from Scratch **December 2023 - February 2024**

Supervised learning, unsupervised learning, deep learning github-link

- **Classification using Ensemble Learning.** Accuracy: **80%-91%** on three different datasets.
- **Handwritten Letters Identification** using **Feed-forward Neural Network**. Accuracy: **91%**.
- **Unsupervised clustering** using EM algorithm. PCA for dimensionality reduction.

Rasterization and Ray-tracing **July 2023 - September 2023**

Computer graphics project github-link

- Designed a fully controllable magic cube that can smoothly transition between a sphere and an octahedron (a fair bit of geometry was involved)

- Developed the raster-based graphics pipeline used in OpenGL through modeling transformation, view transformation, projection transformation, and clipping & scan conversion using Z-buffer algorithm
- Implemented a ray-casting and recursive ray-tracing application using OpenGL and Phong lighting model for rendering a photorealistic 3D world preview with various geometric objects under appropriate illumination

DC-Vegas: A Congestion Control Algorithm for Datacenters — March 2023

Networking project with NS2 simulation — github-link

- Aims to achieve the excellent performances of DC-TCP congestion control algorithms in datacenters at the low deployment cost of TCP-Vegas algorithm
- NS2 simulation shows that DC-Vegas can produce better throughput and packet delivery ratios than TCP-Vegas

Subset C Compiler — June 2022 - August 2022

Compiler project — github-link

- Given a .c input file, this compiler scans the .c file for specific tokens, performs a syntax and semantics analysis, and finally, if the source code does not contain any error, generates assembly code for Intel 8086 assembly language
- **Tools:** C++ | Lex | Yacc | Emu8086

Fingerprint-based Automated Attendance System — August 2022

Microcontroller project

- Fingerprint based attendance system with a real-time clock module for cut-off entry time. Stores attendance in a text file.
- **Hardware:** Arduino Uno | R305 Fingerprint sensor | RTC Module DS3231 | SD card Module | LCD Display

Honours and Awards

- **Best paper award** in 11th International Conference on Networking, Systems, and Security (NSysS 2024)
- **Dean's List award** for academic excellence in undergrad
- **Talent-pool scholarship** in Higher Secondary (**10th** in Dhaka Board)
- **Talent-pool scholarship** in Secondary (**26th** in Dhaka Board)

References

- **Dr. Md. Shohrab Hossain**, *thesis supervisor, co-author*
  Professor, CSE, BUET
  Email: mshohrabhossain@cse.buet.ac.bd, contact: +8801819250196
- **Dr. M Saifur Rahman**, *research supervisor, co-author*
  Professor, CSE, BUET
  Email: mrahman@cse.buet.ac.bd, contact: +8801715010010