




Md Shafayatul Haque

☎ +8801640667059 | @ mdshafayatulhaque@gmail.com |  LinkedIn |  GitHub |  Portfolio |

EDUCATION

Bangladesh University of Engineering and Technology

B.Sc. in Computer Science and Engineering; CGPA: 3.76/4.00

Dhaka, Bangladesh

Feb 2020 – Feb 2025

Notre Dame College

Higher Secondary Certificate; GPA: 5.00/5.00

Dhaka, Bangladesh

June 2017 – May 2019

Mymensingh Zila School

Secondary School Certificate; GPA: 5.00/5.00

Mymensingh, Bangladesh

2015 – 2017

SKILLS

Languages: Python, C/C++, C#, Java, JavaScript, Assembly, Bash, HTML, CSS

Technologies: PyTorch, Pandas, Numpy, Matplotlib, SeaBorn, scikit-learn, React.js, Express.js, Next.js, , MongoDB, Prisma, PostgreSQL

Tools: Git, Github, Postman

Cloud: AWS EC2

Misc. \LaTeX typesetting

RESEARCH INTEREST

Machine Learning, Deep Learning, Computer Vision, Federated Learning, Adversarial Attacks, Distributed Systems

PROFESSIONAL EXPERIENCE

UAP - University of Asia Pacific

Lecturer

Dhaka, Bangladesh

July 2025 – Present

IUBAT - International University of Business Agriculture and Technology

Lecturer

Dhaka, Bangladesh

RESEARCH EXPERIENCES

PCA-Based Backdoor Attack Detection and Trigger Mitigation in Federated Learning | [GitHub](#)

- **Supervisor:** Dr. Muhammad Abdullah Adnan (BUET)
- Proposed a PCA-based defense mechanism to detect and mitigate backdoor poisoning attacks in federated learning settings. Achieved a 100% attack detection rate and significantly reduced the impact of triggers in the global model.
- Injected trigger patches into MNIST, FMNIST, and CIFAR-10 datasets to simulate adversarial behavior in client data.
- Used PCA on client model updates to identify anomalous clients with poisoned datasets based on dimensional variance patterns.
- Applied PCA on CNN activation maps to isolate and reduce the influence of backdoored images at the client level.
- **Technologies Used:** PyTorch, Torchvision, Scikit-Learn, Flower
- **Publication Status:** Under phase 2 review at **AAAI**

GuardFL: Detection and Removal of Malicious Clients Through Majority Consensus | [GitHub](#)

- **Supervisor:** Dr. Muhammad Abdullah Adnan (BUET)
- **Published:** COMPSAC 2024, Osaka, Japan
- Designed and implemented **GuardFL**, a defense framework for identifying and isolating malicious clients in federated learning environments through majority consensus and client feedback.
- Demonstrated that even a single malicious client can introduce severe backdoors, and that GuardFL effectively neutralizes such threats.

- Validated GuardFL on benchmark datasets (CIFAR-10, MNIST, FMNIST), achieving high accuracy in attacker identification and model recovery.
- **Technologies Used:** PyTorch, Torchvision, Flower

AWARDS & ACHIEVEMENTS

Dean's List: Dean's List recognition twice (2021 & 2022) at BUET

Others: Board scholarships in talentpool category in HSC, SSC, PSC, JSC etc.

PROJECTS

Email Subject Line Generation Using T5 on Enron Dataset | [GitHub](#)

- Curated and preprocessed the Enron email corpus, cleaning HTML, stripping quoted text and signatures, and producing 20 000 high-quality (body, subject) pairs.
- Engineered a text2text pipeline with Hugging Face's datasets, pandas and BeautifulSoup, normalizing and tokenizing inputs for Seq2Seq training.
- Fine-tuned the t5-base model via Seq2SeqTrainer, employing beam search and early stopping;
- **Technologies Used:** Python, PyTorch, Hugging Face Transformers, Datasets, pandas, BeautifulSoup, evaluate (ROUGE).

Poultry Disease Detection | [GitHub](#)

- A website that predicts the health of poultry based on an image of their feces. The model is fine-tuned using an EfficientNet architecture on a custom poultry fecal dataset. Achieved 99% accuracy on the test dataset.
- Built a front-end interface with Next.js where users can upload poultry fecal images and receive predictions.
- **Technologies Used:** Pytorch, TorchVision, Scikit-Learn, Pandas, Next.js, Flask.

Pancreatic Disease Detection | [GitHub](#)

- Developed a CNN-based deep learning model to classify pancreatic CT scan images into normal and tumor-affected categories using a publicly available Kaggle dataset. Applied preprocessing techniques such as resizing, normalization, and augmentation (horizontal flip, rotation) to enhance model generalization. Evaluated model performance using confusion matrices and accuracy metrics, achieving high classification accuracy.
- **Technologies Used:** Python, PyTorch, torchvision, KaggleHub, NumPy, OpenCV, Matplotlib

Spam Email Detection | [GitHub](#)

- Built a spam detection model using Natural Language Processing (NLP) techniques. Preprocessed text data with tokenization, stopword removal, and TF-IDF vectorization. Trained and evaluated multiple models including Naïve Bayes and SVM to classify spam vs. non-spam emails..
- **Technologies Used:** Scikit-Learn, Pandas, NumPy, NLTK, Seaborn.

Machine Learning Algorithms | [GitHub \(FNN\)](#) [GitHub \(EM/PCA\)](#) [GitHub \(LR\)](#)

- Implemented core machine learning algorithms including Feedforward Neural Networks, Linear Regression, Ensemble Techniques, Principal Component Analysis, and the Expectation-Maximization algorithm from scratch.
- **Language:** Python **Libraries:** PyTorch

Cryptosystem Implementation | [GitHub](#)

- Independently developed AES encryption with Cipher Block Chaining (CBC) mode for secure data transmission.
- Implemented Elliptic Curve Diffie-Hellman (ECDH) key exchange for secure symmetric key generation.
- Integrated encryption and key exchange into a real-time communication system using socket programming.
- Applied cryptographic best practices to ensure data confidentiality and integrity across networks.
- **Language:** Python

Ray Tracing with OpenGL | [GitHub](#)

- Rendered bitmap images using ray tracing and the Phong Illumination Model to simulate realistic lighting and shading effects.
- Supported 3D geometric shapes such as plane, sphere, triangle, pyramid, and cube with customizable viewpoint and lighting.
- **Language:** C++ **Library:** OpenGL

AI Mini Projects | [GitHub](#)

- **N-Puzzle:** Implemented heuristic search strategies such as Hamming distance and Manhattan distance for solving tile-based puzzles.
- **Car Evaluation:** Developed a decision tree classifier to evaluate cars based on various attributes.
- **Mancala Game:** Built an AI agent using adversarial search and game-tree strategies.

File Server System | [GitHub](#)

- Built a multi-client file server allowing file upload, download, and real-time requests.
- Implemented authentication to ensure unique usernames and prevent duplicate logins.
- Used a directory-based system for organizing user-specific files and managing access control (private/public).
- Enabled real-time messaging between users via server-side broadcasting and tracked online/offline status.
- **Language:** Java **Technologies:** Sockets, Multi-threading

Network Simulator-3 | [GitHub](#)

- Implemented a congestion control algorithm, TCP Adaptive Reno, in NS-3 to simulate efficient network traffic handling.
- **Language:** C

Error Detection and Correction | [GitHub](#)

- Implemented CRC checksum for error detection and Hamming distance-based correction, simulating data link layer operations.
- **Language:** C++

Design Patterns Implementation | [GitHub](#)

- Implemented a suite of design patterns including Creational (Factory, Singleton), Structural (Adapter, Decorator), and Behavioral (Observer, Strategy) patterns.
- **Language:** Java

C Compiler Implementation | [GitHub](#)

- Implemented a compiler for a subset of the C programming language, including lexical analysis, parsing, and basic semantic checks.
- **Language:** C++ **Libraries:** Flex, Bison

Football Club Management System | [GitHub](#)

- Built a management application to maintain a football club's player database, supporting operations such as search, add, transfer, and delete.
- Implemented a user-friendly graphical interface using JavaFX for administrators to manage player and club data efficiently.
- **Language:** Java **Library:** JavaFX

DX Ball Game | [GitHub](#)

- Recreated the classic DX Ball arcade game featuring paddle control, brick breaking mechanics, and score tracking.
- **Language:** C **Framework:** iGraphics

ByteBooks | [GitHub](#) • [Live Demo](#)

- A full-stack audiobook library platform featuring distinct interfaces for admins, readers, and creators. Admin tools include user, book, and creator management, report handling, and access to insightful analytics through interactive visual charts. Creators can use an integrated editor to manage and publish audiobooks.
- Readers benefit from personalized recommendations based on preferences, real-time progress tracking, notifications for new releases, a customizable bookshelf, highlight management, and personal analytics for habit tracking and progress insights.
- **Technologies Used:** Next.js, MongoDB, Prisma, and Framer Motion.

Portfolio Website | [GitHub](#) • [Live Demo](#)

- A personal portfolio website built using React and TailwindCSS to showcase projects, skills, and contact information in a responsive and modern UI.
- Integrated EmailJS for seamless contact form functionality without requiring a backend server.
- **Technologies Used:** ReactJS, TailwindCSS, EmailJS.

REFERENCES

- **Dr. Muhammad Abdullah Adnan**
Department of CSE, BUET
Email: abdullah.adnan@gmail.com Phone: +880 1552-336926
Thesis Supervisor
- **Dr. Md. Mostofa Akbar**
Department of CSE, BUET
Email: mostofa@cse.buet.ac.bd Phone: +880 1715-006345
University Advisor