Faishal Uddin Himel

Basundhara R/A, Block-2C
01987779101
himelfaishal@gmail.com
linkedin.com/in/faishal-uddin-himel-b7b29a236/
https://my-portfolio-cyan-nu-69.vercel.app/
GitHub

CAREER OBJECTIVE

I am passionate about contributing to the advancement of computing technologies through multidisciplinary collaboration and innovative problem-solving. With a strong foundation in AI, cybersecurity, and backend development, I aim to apply my diverse technical skills to address complex challenges in emerging technology domains. I am committed to continuous learning, proactive research, and making a meaningful impact by developing intelligent, secure, and future-ready solutions.

PROFILE SUMMARY

- Highly motivated and research-driven AI & Cybersecurity Engineering student with a solid foundation in backend systems, intelligent automation, and advanced computing technologies. Demonstrates strong academic performance with a consistent record of excellence.
- Experienced in multidisciplinary research across cybersecurity, IoT, artificial intelligence, and machine learning, with practical involvement in academic publications, system development, and real-world problem-solving.
- Proficient in diverse programming languages including Python, C++, C#, Java, PHP, HTML, CSS, JavaScript, SQL, and R. Experienced in developing AI/ML models, building secure RESTful APIs, and implementing agent-based intelligent systems using tools and frameworks such as Git, Overleaf, TensorFlow, PyTorch, Scikit-learn, and FastAPI for research and production-level development.
- Passionate about leveraging technical expertise and collaborative teamwork to address complex technological challenges. Recognized for leadership, communication skills, and a commitment to continuous learning and impactful innovation.

WORK EXPERIENCE

AI Developer & Automation Engineer
Betopia Group, Bangladesh [On-site/Remote] January 2026 – Present

- Developing and deploying AI-powered features for internal products and client projects.
- Designing automation workflows to streamline business processes and reduce manual operations.
- Building backend services and integrations (APIs, databases, third-party tools) to support AI/automation pipelines.
- Implementing data processing, model evaluation, and performance improvements for production readiness.
- Collaborating with cross-functional teams to deliver end-to-end solutions and maintain documentation.

Research Intern
Applied Intelligence and Informatics Lab (AIIL), Nottingham, UK [Remote] October 2025 – December 2025

- Conducted research aligned with AIIL's core focus areas in applied artificial intelligence and informatics.
- Performed in-depth literature reviews to support model development and experimental design.
- Designed, implemented, and evaluated machine learning and AI research models.
- Collaborated with international researchers through virtual meetings and technical discussions.
- Contributed to research documentation and journal publication preparation targeting Q1/Q2 indexed journals.

Leader
Team Tech Wing, American International University-Bangladesh (AIUB) October 2023 – Present

- Supervised all laboratory activities to ensure seamless operations and effective utilization of technical resources.
- Provided mentorship and guidance to junior members, assisting in their technical and professional skill development.
- Organized and led knowledge-sharing sessions and technical workshops to promote collaborative learning within the team.

EDGE Project
AIUB Institute (EDGE Project – Enhancing Digital Government and Economy) June 2024 – January 2025

- Worked on a project-based assignment using Python, contributing to research and development under the national EDGE initiative.
- Collaborated with academic supervisors to implement digital solutions aligned with project goals.
- Supervisor: Dr. Mohammad Saef Ullah Miah (saef@aiub.edu)

Intern App Developer
RIC-Series August 25, 2025 – November 10, 2025

- Assisting in the development of gaming applications and contributing to codebase enhancements.
- Collaborating with development teams to improve application performance and user experience.

RESEARCH / WORK INTERESTS

- AI Agent
- AI Automation
- Cyber Security
- Data Science
- APIs
- AI

RESEARCH PROJECTS

AI-Powered Endpoint Detection and Response (EDR) System with API Integration

- Supervisor: Dr. Mohammad Saef Ullah Miah
- Developed an intelligent endpoint protection system using machine learning for real-time malware and anomaly detection.

- Designed and implemented secure RESTful APIs to enable communication between endpoints and the central detection engine.
- Integrated automated threat response mechanisms, including process isolation and alert generation.
- Applied feature extraction and model optimisation techniques to improve detection accuracy and reduce false positives.
- Evaluated system performance using real-world malware and benign datasets.

Self-Healing Federated AI CyberShield for Adaptive Threat Detection and Recovery in Smart IoT Environments

- Supervisor: Dr. Mohammad Saef Ullah Miah
- Research focused on building a federated AI-based cybersecurity framework for threat detection and autonomous system recovery in smart IoT networks.

Multi-Agent AI CyberShield with Three Cooperative Detection Agents

- Supervisor: Dr. Mohammad Saef Ullah Miah
- Designed a distributed CyberShield architecture using three cooperative AI-based detector agents for network, host, and application-level threat detection.
- Implemented independent machine learning models within each agent to detect malware, intrusion, and anomalous behavior in real time.
- Developed an agent coordination and decision-fusion mechanism to improve detection accuracy and reduce false alarms.
- Integrated the system with a central response unit for automated alerting and threat mitigation.
- Validated the multi-agent framework using mixed benign and attack datasets in a simulated enterprise–IoT environment.

PhishDoc-ML: An Explainable Ensemble Learning Framework for Phishing Email Detection

- Supervisor: Mir Md. Kawsur
- Developed an interpretable ensemble machine learning framework aimed at identifying and mitigating phishing attacks through email analysis.

A Comparative Study of IDS Dataset Limitations and Adaptive Learning Solutions

- Supervisor: Dr. Rajarshi Roy Chowdhury
- Analyzed popular intrusion detection system (IDS) datasets, identifying their shortcomings and proposing adaptive learning techniques for enhanced detection accuracy.

PROJECTS

LLM-Driven Reflective Multi-Agent Economic Simulation System 2024 – 2025
Microsoft Imagine Cup *American International University-Bangladesh*

- Built a multi-agent economic simulation modeling heterogeneous individuals under real-world constraints such as wages, education, consumption, and savings.
- Designed a hybrid decision architecture where rule-based economics enforces feasibility and LLMs act as a reflective policy layer for adaptive labor decisions.
- Implemented LLM-based reflection memory enabling agents to reason over past outcomes while preserving mathematical and budget constraints.

- Integrated rate-limited LLM invocation and simulated economic shock scenarios to evaluate resilience and behavioral adaptation.
- Produced interpretable analytics and visualizations (labor trends, savings by education, mood dynamics) to validate emergent behaviour.
- **Technologies:** Python, OpenAI GPT-4o / GPT-4o-mini, Multi-Agent Systems, Prompt Engineering, NumPy, Pandas, Matplotlib

CyberShield: Reflective Multi-Agent Zero-Day Cyber Defense System 2025
Independent Research / Academic Project *American International University-Bangladesh*

visualisations

- Designed an end-to-end autonomous cyber defense system for zero-day attack detection using unsupervised GAN-based anomaly detection.
- Implemented a WGAN-GP critic trained exclusively on normal network traffic to identify previously unseen attacks without labeled data.
- Developed a Coordinator Agent to perform temporal correlation of anomalies, enabling escalation from isolated events to confirmed attack campaigns.
- Built a Responder Agent capable of automated defense actions, including monitoring, host isolation, and IP blocking based on attack severity.
- Integrated reflective incident memory and feedback loops to reduce false positives and enable campaign-level reasoning.
- Produced comprehensive visual analytics, including anomaly score distributions, temporal escalation timelines, attack lifecycle diagrams, and explainability overlays.
- **Technologies:** Python, TensorFlow, WGAN-GP, GAN-Based Anomaly Detection, Multi-Agent Systems, Cybersecurity Analytics, NumPy, Pandas, Matplotlib

AI-Based Phishing Email Detection System
American International University-Bangladesh

- Role: Machine Learning Engineer, Model Development and Integration.
- Developed an AI-driven phishing detection system using NLP and machine learning classifiers to identify malicious emails in real time.
- Implemented feature extraction using TF-IDF and word embeddings, and evaluated models such as SVM, Random Forest, and Neural Networks.

AI-Enhanced Endpoint Malware Protection with Adversarial Robustness 2025
Research Internship Project *Applied Intelligence and Informatics Lab (AIIL), UK*

- Designed and implemented an end-to-end AI-based endpoint malware detection pipeline using static feature analysis of executable files.
- Developed transformer-based deep learning models alongside classical machine learning baselines for robust malware classification.
- Integrated adversarial robustness mechanisms, including GAN-based malware augmentation and PGD adversarial attacks, to evaluate model resilience against evasion.
- Performed extensive experimental evaluation using ROC-AUC, PR-AUC, precision-recall, calibration analysis, and adversarial distance metrics.
- Analyzed the impact of synthetic data augmentation under different filtering thresholds to balance generalization and overfitting.

- Visualized malware and synthetic sample distributions using t-SNE and feature-space analysis to validate distributional fidelity.
- Exported trained models to ONNX format and verified consistency between PyTorch and deployment-ready inference.
- **Technologies:** Python, PyTorch, Transformer Models, GANs, PGD Attacks, ONNX, Scikit-learn, NumPy, Pandas, Matplotlib

Web Tech – Home Service Web Application
American International University-Bangladesh

- Role: Backend and Database Management, Coding (PHP, JavaScript, JSON, HTML, CSS).
- Developed a platform to connect users with home service providers, focusing on secure backend architecture and efficient data management.

Web Tech – Event Management System
American International University-Bangladesh December 2024 – Present

- Role: Backend and Database Management, Coding (PHP, JavaScript, JSON, HTML, CSS).
- Designed and implemented backend logic and data storage for a system that manages university events and participants.

Python/Django Personal Website December 2024 – Present

- Role: Full-Stack Development – Backend, Frontend, and Database Integration.
- Built a personal portfolio site using Django, featuring dynamic content, contact forms, and project showcases.

EDGE Project – Enhancing Digital Government and Economy June 2024 – January 2025

- Contributed to national-level digital transformation efforts through Python-based system development.
- Supervisor: Dr. Mohammad Saef Ullah Miah (saef@aiub.edu)

Intelligent DDoS Attack Detection using Machine Learning 2024
Academic / Research Project *American International University-Bangladesh*

- Designed a machine learning-based DDoS detection framework for identifying volumetric and protocol-based network attacks.
- Performed network traffic preprocessing, feature extraction, and normalization from flow-level datasets.
- Trained and evaluated multiple supervised learning models to distinguish between normal and attack traffic patterns.
- Conducted performance evaluation using accuracy, precision, recall, F1-score, and ROC-AUC metrics.
- Analyzed traffic behavior under different attack intensities to assess model robustness and detection latency.
- Developed visual analytics including traffic rate distributions, confusion matrices, and attack detection timelines.
- **Technologies:** Python, Scikit-learn, Network Traffic Analysis, Machine Learning, NumPy, Pandas, Matplotlib

PERSONAL QUALIFICATIONS

- Effective in maintaining good communication with others

- Capable of learning new tools and technology very quickly
- Able to work under pressure to meet tight deadlines
- Hardworking, punctual, and a good team player
- Strong leadership ability with experience in guiding team members and coordinating technical tasks
- Proven capability to take initiative, manage responsibilities, and deliver results in team-based projects

CERTIFICATES & TRAINING

LLM Pentesting: Mastering Security Testing for AI Models
Udemy – Certificate of Completion *June 2024*

Artificial Intelligence & Machine Learning Fundamentals
Certificate of Completion *May 2024*

Generative AI: Prompt Engineering Basics
IBM – Certificate of Completion *April 2024*

Professional Web, Android & iOS Penetration Testing
Cyber-Bangla – Certificate of Completion *October 2024*

Python for Data Science and Machine Learning
IBM – Certificate of Completion *September 2024*

Python Django Development Course
IIT, Jahangirnagar University *December 2024*

Advanced Cybersecurity Course
Team Matrix – Elite Hackers *March 2025*

Cisco Certified Network Associate (CCNA)
AIUB Institute of Continuing Education
Cisco *August 2025*

EDUCATION

Bachelor of Science in Computer Science and Engineering
American International University-Bangladesh (AIUB) 2022 – 2025 (Completed)

Higher Secondary Certificate (HSC)
Pakundia Govt. College 2018 – 2020

· Major: Science

REFERENCES

Prof. Dr. Dip Nandi
Associate Dean
Faculty of Science and Technology
American International University-Bangladesh
Email: dip.nandi@aiub.edu

Dr. Md. Saef Ullah Miah
Associate Professor, Additional Director (IQAC)
Department of Computer Science
American International University-Bangladesh
Email: saef@aiub.edu