Monirul I. Mahmud

529 E 54th ST Brooklyn, New York 11203, USA
Email: monirul.mahmud9@gmail.com
Website: https://monirules.github.io

Education

M.Sc. in Computer & Information Science, Fordham University, *New York, USA* *Aug. 2024 – May 2026*

- As a Full time Graduate Student, 90% of my Tuition Fee is funded by **GSAS Centennial Scholarship**.
- Relevant Coursework: Data Mining, Blockchain, Cloud Computing, NoSQL Databases and Data Visualization **(CGPA: 3.89 / 4.00)** **[Transcript]**

B.Sc. in Computer Science, North South University, *Dhaka, Bangladesh* *Feb. 2020 – Dec. 2023*

- Engaged in a comprehensive curriculum covering key areas such as Applied Statistics, Artificial Intelligence, Software Engineering, Theory of Computation and Machine Learning.
- Thesis on "*Multi-Head Temporal Attention with Positional Encoding for Sensor-based Human Activity Tracking"*. **[Transcript] [Certificate]**

Current Research Interests

- **Applied Cryptography & Blockchain** (zero-knowledge proofs, intrusion detection, homomorphic encryption, consensus, smart contracts, DeFi security)
- **Cyber Physical System** (IoT/IoMT, digital health systems, SCADA systems, human activity, autonomous vehicles, WBAN)
- **AI & VLM Security** (adversarial ML, data/model poisoning, explainable AI, Federated Learning, Computer Vision, Vision Language Model-VLM, Multimodal AI).

Technical Skills

- **Blockchain & Decentralized Systems:**
  Smart Contracts, Ethereum, Solidity, Hyperledger Fabric, Web3.js, Merkle Trees, Consensus Algorithms, Ganache, Polygon, Distributed Ledger Technology (DLT).
- **Machine learning:**
  TensorFlow, Google Cloud Platform, R, Deeplearning4j, Matplotlib, Seaborn, Scikit- learn, GAN, Transformer, Federated Learning, A/B testing, t-test.
- **Programming Languages**:
  Language: Python, C/C++/C#, Java, Assembly, Perl, Ruby, JavaScript, PHP.
  Framework: JQuery, Ajax, D3.js, Flask, FastAPI, Docker, AWS (Sagemaker), Django, Stream lit.
- **Database Administration**:
  Redis, MySQL, SQL, SQLite, MongoDB, Cassandra.
- **Simulation and Analysis:** MATLAB, SAS, SPSS, Sketchup, Roboflow, AutoCAD, Tableau.

Research Experience

Research Assistant, *Fordham University* *Jul. 2025 - Present*

- Collaborated with **Dr. Mohamed Rahouti** on research projects – *'FairRate for Ride Sharing Platform'*, '*Merkle Trees and Zero-Knowledge Proof enhanced Secure Credit Risk Modeling'* and *'FL-Proof of Reputation based WBAN/IoMT'*.
- Contributed to the development of privacy-preserving *Smart Contracts*, focusing on cryptographic techniques with *Federated Learning* for data security and transparency.

Graduate Research Assistant, *Design Inclusion & Access Lab (DIAL)* *Jan. 2024 - Feb 2025*

- **Team Lead** of *Data Science* group - mentoring 5 members to ensure successful project execution under the supervision of **Dr. Nova Ahmed**.

- Worked on 2 projects - *'Attention and Residual Mechanism-based Deepfake Recognition*' and *'Reliable and Trustworthy Diabetic Foot Ulcer Detection'* projects.

Student Researcher, *Design Inclusion & Access Lab (DIAL)* *Jul. 2023 – Jan. 2024*

- Collaborated on the '*Feasibility of Alternative Credit Scoring for the Credit Invincibles*' project funded by **NSU-CTRG (CTRG-23-SEPS-02)**, increasing loan approval by 20%.
- Implementing feature selection techniques - information gain, gain ratio, and fisher score to enhance model interpretability in the *Credit Scoring* project, aiming to optimize loan risk for South Asian banks. **[Experience Letter]**

Work Experience

Machine Learning Engineer, *EMPERIO IT, New York, USA* *Jan. 2025 – Jun. 2025*

- Developed **AI-Agent** for customer support with retrieval-augmented generation (RAG), enabling automated answers to customer queries from company knowledge bases and FAQs.
- Integrated the **Agent** with **Jira** and **ServiceNow**, reducing manual ticket escalations by ~40% and improving response time for support requests.

Junior Data Scientist, *COSMIC IT LTD, Dhaka, Bangladesh* *Sep. 2022 – Dec. 2023*

- Worked on a Government project for the **Road Transport Authority**, developing an Automated Toll Collection system using *Live Vehicle License Plate Scanning*.
- Designed and deployed interactive data visualization dashboards for client reporting and system monitoring, using Tableau, Google Looker Studio, and D3.js.

Trainee Engineer (Data Science), *SYSTECH DATASOFT, Dhaka, Bangladesh* *Apr. 2022 – Jul. 2022*

- Developed and customized an **Automated Resume Screening System** for Systech Datasoft, achieving **97.92% accuracy** in predicting candidate suitability by using **advanced PDF parsing** and data analysis. **[Experience Letter]**
- Designed a data-driven solution that fasten the **hiring process** at Systech Datasoft, significantly improving the efficiency and accuracy of candidate shortlisting. **[Certificate]**

Ongoing Projects

1. **FairRate: Fairness-Calibrated Reputation with Agentic AI for Ride-Hailing Platforms**

   Developed an end-to-end **Agentic AI**-powered reputation update framework that separates contextual factors (traffic, weather, surge) from actual driver performance when computing star-rating scores in **Uber/Lyft**. Integrated rater reliability modelling, **adversarial attack** detection, and **cryptographic audit** commitments to resist rating manipulation and ensure every reputation decision remains transparent and contestable. **[Documentation]**

2. **Multimodal Jailbreaking and Adversarial Attacks on Vision-Language Models: A Survey**

   Conducted a comprehensive security survey of Vision-Language Models (VLMs), proposing the systematic taxonomy of **multimodal jailbreaking** and **adversarial attacks** across visual, textual, and cross-modal threat surfaces. Analyzed **100+** attack methods (2023–2026), developed architecture-to-vulnerability mappings, and evaluated defense mechanisms highlighting fundamental safety gaps in VLM. **[Documentation]**

3. **ReMerkle: Proof of Reputation-driven Federated Learning with Merkle Verification for Consumer-centric IoMT** **(M.S. Thesis)**

   Storing every model update onto the chain produces large "gas" charges and long delays. So, this study introduces ReMerkle, a **lightweight** security design for consumer-centric IoMT. Instead of storing whole updates, the system keeps only a 32-byte Merkle Root on the chain through Compact **Merkle Tree** Verification while free up storage by 99.96%. **[Preprint]** **[Thesis Slides]**

Journal Publications

[1] M. I. Mahmud, J. Bieniek, M. Rahouti, A. Chehri, and G. Jeon, "Towards Trustworthy Consumer-Centric IoMT: Reputation-Driven Federated Learning for Secure Medical Data Sharing," *IEEE Transactions on Consumer Electronics*, 2026. (Accepted) DOI: 10.1109/TCE.2026.3685994 **[Paper]**

[2] M. I. Mahmud, M. S. Reza, M. O. A. Akash, F. Elias, and N. Ahmed, "DFU_DIALNet: Towards Reliable and Trustworthy Diabetic Foot Ulcer Detection with Synergistic Confluence of Grad-CAM and LIME," *PLoS ONE.* 2025. DOI: 10.1371/journal.pone.0330669 **[Code]**

[3] M. S. Reza, F. Elias, **M. I. Mahmud**, and N. Ahmed, "Attention and Residual Mechanism-based CNN Architecture (ARC-Net) with Enhanced Fairness Generalization for Deepfake Facial Image Detection," *PLoS ONE.* 2025. DOI: 10.1371/journal.pone.0340099. **[Code]**

[4] M. I. Mahmud, M. S. Reza, F. Elias, K. A. Ahmed, M. Ahammad, I. A. Abeer, and N. Ahmed, "Multi-Domain Validation of Bayesian Optimized Stacking Ensembles for Next-Generation Credit Risk Modeling with Granular Explainability and Robust Statistical Inference," *Annals of Data Science.* 2025 (**Q1**, under revision). DOI: 10.20944/preprints202510.0484.v1 **[Code]**

[5] M. I. Mahmud, S. Patel, M. Rahouti, and A. Chehri, "Trustworthy and Secure Credit Scoring: A Merkle Tree and Zero-Knowledge Proof-Enhanced Approach with Proactive Security Strategies," *IEEE Transactions on Information Forensics & Security.* 2025 (**Q1**, under review). **[Code]**

Conference Publications

[1] M. I. Mahmud, "Towards Trustworthy Keylogger detection: A Comprehensive Analysis of Ensemble Techniques and Feature Selections through Explainable AI," *arXiv.org*, May 22, 2025. https://arxiv.org/abs/2505.16103 **[Code]**

[2] M. S. Reza, **M. I. Mahmud**, I. A. Abeer and N. Ahmed, "Linear Discriminant Analysis in Credit Scoring: A Transparent Hybrid Model Approach," *2024 27th International Conference on Computer and Information Technology (**ICCIT**)*, Cox's Bazar, Bangladesh, 2024, pp. 56-61, DOI: 10.1109/ICCIT64611.2024.11022149.

[3] M. I. Mahmud, M. S. Reza, and S. S. Khan, "Optimizing Stroke Detection: An Analysis of Different Feature Selection Approaches," in *Companion of the 2024 on ACM International Joint Conference on Pervasive and Ubiquitous Computing (**UbiComp '24**)*. New York, NY, USA: Association for Computing Machinery, 2024, pp. 142–146. DOI: 10.1145/3675094.3677602.

[4] M. I. Mahmud, "ZeroML: A Next Generation AutoML Language," *arXiv.org*, May 23, 2025. https://arxiv.org/abs/2505.18243

[5] M. I. Mahmud, M. S. Reza, and H. Akter, "Human Activity Recognition Using Multiple Learning & XAI Techniques with Wearable Sensor Data," *North South University*, Dhaka, Bangladesh. 2023. https://repository.northsouth.edu/handle/123456789/1093 **[Poster]**

Benchmark Datasets

[1] Multimodal Human Activity Tracking Dataset

A comprehensive dataset of 72,000 time-series readings from 6 participants using thermal and infrared imaging camera and 3D accelerometer data collected via Raspberry Pi. Includes a mobile app prototype for data collection and prediction.

[2] Diabetic Foot Ulcer (DFU) Dataset

A curated set of 500 labeled foot images (250 normal, 250 ulcers), collected under IRB approval (*NSU IRB 2024/OR-NSU/IRB/1110*) for DFU detection research. **[Dataset Access]**

[3] Bangladeshi DeepFake and Real Face Image Dataset

500 facial images (real + deepfake), sourced with written consent from diverse individuals. Approved by IRB (*NSU IRB 2024/OR-NSU/IRB/1109*). **[Dataset Access]**

[4] Ground-Based Cloud Segmentation Dataset

110 annotated ground-based sky/cloud images for training U-Net-based segmentation models. Annotated using Roboflow.

Awards & Extra-Curricular Activities

- Fordham University **GSAS Centennial** Scholarship, 2024 - Present
- Served as a **Reviewer** for Peer-reviewed journal **IEEE Pervasive Computing**.
- ACM ICPC Regional Contest (Dhaka) 2022 - Placed **6th** among 90 teams.
- Banglalink Ennovators-6.0 (Bangladesh) 2023 – Placed **7th** among 86 teams.
- Primary School Talent-pool Scholarship by UNICEF and the Government of Bangladesh.
- IEEE NSU Student Branch (INSB) – worked on ***Team Content Writing and Publication.***
- NSU ACM Student Chapter – worked on ***Team Operation***.

Mentoring

- **Zawad Mahmud**, M.Sc student, Fordham University, New York, USA.
- **Shahran Rahman Alve**, Ph.D. Candidate, The University of Texas at Dallas, USA.

References

1) **Dr. Nova Ahmed**
   Professor, Department of Electrical & Computer Engineering (ECE)
   North South University, Dhaka, Bangladesh
   Email: *nova.ahmed@northsouth.edu*

2) **Dr. Ruhul Amin**
   Assistant Professor, Department of Computer and Information Science
   Fordham University, New York, USA
   Email: *mamin17@fordham.edu*

3) **Dr. Mohamed Rahouti**
   Assistant Professor, Department of Computer and Information Science
   Fordham University, New York, USA
   Email: *mrahouti@fordham.edu*