Md Mazharul Islam

mazharul.islam1@northsouth.edu | +880 1834 311240 | mazharulmd.github.io

LinkedIn | Google Scholar | ORCID | Scopus | GitHub | Medium

Dhaka, Bangladesh

Research Interests

Cybersecurity and trustworthy-AI researcher pursuing a PhD in secure, privacy-preserving, and resilient computing for intelligent and critical infrastructure. My work spans privacy-preserving cryptography (searchable and homomorphic encryption), trustworthy and adversarially robust AI, including federated learning and LLM security, and the security and resilience of cyber-physical systems and AI-enabled cloud infrastructure. I am motivated by deployable, theoretically grounded solutions that strengthen the security and privacy of the systems on which critical infrastructure depends.

Education

- North South University — *Graduated: Summer 2020*
  Master of Science in Computer Science and Engineering (MSc) — Dhaka, Bangladesh
  - **CGPA:** 3.97 / 4.00 (approx. 99 / 100; first-class standing)
  - **Thesis:** *"A Practical Framework for Storing and Searching Encrypted Data on Cloud Storage"* — cloud security, privacy-preserving storage, and efficient search over encrypted data.
- North South University — *Graduated: Summer 2018*
  Bachelor of Science in Computer Science and Engineering (BSc) — Dhaka, Bangladesh
  - **CGPA:** 3.24 / 4.00 (approx. 81 / 100)

Publications

J=Journal, C=Conference, T=Thesis, R=Under Review

Peer-Reviewed Journal Articles

[J.1] **Md Mazharul Islam**, Mubasshir Ahmed, Rajesh Palit, Mohammad Shahriar Rahman, Salekul Islam. Fraud Detection in Privacy Preserving Health Insurance System Using Blockchain Technology. *Engineering Reports* 7, no. 8 (2025): e70315, DOI: 10.1002/eng2.70315.

Peer-Reviewed Conference Proceedings

[C.10] **Md Mazharul Islam**, Mubasshir Ahmed, Niaz Ashraf Khan. CPS-Guard: Defensive Architectures for Securing Large Language Models in Cyber-Physical Systems. *28th International Conference on Computer and Information Technology (ICCIT)*, Bangladesh, 2025, pp. 2802–2807, DOI: 10.1109/ICCIT68739.2025.11491276.

[C.9] Niaz Ashraf Khan, Md. Ferdous Bin Hafiz, **Md Mazharul Islam**, Md. Aktaruzzaman Pramanik. Harnessing Explainable AI to Detect Threats in DNS over HTTPS Traffic. *16th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, Indore, India, 2025. (Accepted & Presented)

[C.8] Niaz Ashraf Khan, Md. Ferdous Bin Hafiz, **Md Mazharul Islam**, Md. Aktaruzzaman Pramanik. Enhancing Software Quality with Feature-Aware Defect Prediction Models. *16th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, Indore, India, 2025. (Accepted & Presented)

[C.7] **Md Mazharul Islam**, Mubasshir Ahmed, Md Redowan Zaman Anik, Mamunur Rashid Alex, Niaz Ashraf Khan. Federated Fine-Tuning of Large Language Models for Cybersecurity: Towards Privacy-Preserving and Secure AI. *16th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, Indore, India, 2025. (Accepted & Presented)

[C.6] **Md Mazharul Islam**, Mubasshir Ahmed, Niaz Ashraf Khan. A Blockchain-Based Medical Record Storage System for Healthcare Data Management. *4th International Conference on Advances in Communication Technology and Computer Engineering (ICACTCE'24)*, Lecture Notes in Networks and Systems, vol. 1312, Springer. DOI: 10.1007/978-3-031-94620-2_24

[C.5] **Md Mazharul Islam**, Tahmid Ashraf Khan, Sunjare Zulfiker, A S M Jahid Hasan, Hafiz Abdur Rahman. Remotely Accessible Cyber-Physical System Testbed for Power Grid's Security and Reliability. *8th International Conference on Smart Grid and Smart Cities (ICSGSC)*, Shanghai, China, 2024, pp. 436–441, DOI: 10.1109/ICSGSC62639.2024.10813893.

[C.4] **Md Mazharul Islam**, Mubasshir Ahmed, Rajesh Palit. Fault Detection and Diagnostics of Air Handling Unit in Hospital Building Using Machine Learning. *15th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, India, 2024, pp. 1–6, DOI: 10.1109/ICCCNT61001.2024.10724490.

[C.3] **Md Mazharul Islam**, Mubasshir Ahmed, Rajesh Palit. Storage and Maintenance of Sensitive Data using Homomorphic Encryption. *16th International Conference on Security of Information and Networks (SIN)*, Jaipur, India, 2023, pp. 1–6, DOI: 10.1109/SIN60469.2023.10474775.

[C.2] **Md Mazharul Islam**, Rajesh Palit. A Keyword Based Searching and Sharing Scheme on the Encrypted Cloud Data. *14th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, Delhi, India, 2023, pp. 1–6, DOI: 10.1109/ICCCNT56998.2023.10308309.

[C.1] **Md Mazharul Islam**, Rajib Imran, Shazzad Hosain. The Evaluation of Enterprise Resource Planning using ISO 25010 Based Quality Model. *2nd International Informatics and Software Engineering Conference (IISEC)*, Ankara, Turkey, 2021, pp. 1–6, DOI: 10.1109/IISEC54230.2021.9672349.

Thesis

[T.1] **Md Mazharul Islam**, Rajesh Palit. A Practical Framework for Storing and Searching Encrypted Data on Cloud Storage. Master's thesis, North South University, 2023; available as arXiv:2306.03547. DOI: 10.48550/arXiv.2306.03547

Manuscripts Under Review

[R.5] **Md Mazharul Islam**, Abrar Mohammed Tanzim Alam, and Mubasshir Ahmed. CR-SHE: Collusion-Resilient Searchable Homomorphic Encryption for Multi-Cloud IoT Data Sharing. *IEEE Internet of Things Journal*, 2026. (Under Review)

[R.4] **Md Mazharul Islam**, Mohammad Kaosain Akbar, Niaz Ashraf Khan. SyPrFL: Sybil-Resilient Privacy-Preserving Federated Learning via Differentially-Private Projection Clustering. *Journal of Information Security and Applications* (Elsevier), 2026. (Under Review)

[R.3] **Md Mazharul Islam**, Abrar Mohammed Tanzim Alam, Md. Sadikur Rahman Rony, Susmay Das. Data-Centric, Robust, and Explainable Multimodal Deep Learning for Clinical Decision Support: A Systematic Review. *International Journal of Medical Informatics* (Elsevier), 2026. (Under Review)

[R.2] Mubasshir Ahmed, **Md Mazharul Islam**, Rajesh Palit, Shahriar Rahman, Salekul Islam. SHIELD: Secure Hybrid Insurance Ledgers & Ensemble Detection for Health Insurance Fraud Prevention. *IET Blockchain*, 2025. (Under Review)

[R.1] **Md Mazharul Islam**, Md. Shahadul Alam Patwary, Salekul Islam, Rajesh Palit. CryptoCloud: A Usable Framework for Storing, Searching and Sharing Encrypted Data on Cloud Storage. *Security and Privacy* (Wiley), 2025. (Under Review)

Research Experience

- Institute for Advanced Research (IAR) Lab — *January 2024 – Present*
  Research Assistant — United International University & North South University
  - Developing a privacy-preserving fraud-detection framework for healthcare data using cryptographic techniques and machine-learning anomaly detection, resulting in a peer-reviewed journal publication.
  - Leading research on machine learning–based fault detection and anomaly identification using real-world data, with a focus on reliable and secure operation of critical infrastructure.

- Cyber-Physical System (CPS-PMU) Research Lab — *February 2022 – April 2024*
  Graduate Research Assistant — North South University
  - Developed and tested a cyber-physical system (CPS) testbed using Node-RED for simulating smart-grid environments with integrated data and power-network flows to study security and reliability.
  - Utilized GridPACK, NS-3, and HELICS to model and synchronize communication and control layers on Linux-based simulations, enabling experiments on power-grid resilience and cybersecurity.

Honors and Awards

- **Vice-Chancellor's Gold Medal, 25th Convocation** — *December 2024*
  North South University, Bangladesh
- **Huawei ICT Competition 2023–2024 (Network Track)** — *Jan–May 2024*
  Huawei ICT Academy — Bangladesh, Indonesia, China
  Secured 2nd place as part of a 3-member team in the Global Final (Shenzhen, China).
  Placed 3rd in the National Round (Bangladesh); attended the Asia-Pacific ceremony in Jakarta, Indonesia.

- **Reviewer, Int. Conf. on Data, Computation, and Communication (ICDCC-2024)** — *November 2024*
  VIT Bhopal University, India
- **Reviewer, Int. Conf. on Innovations in Data Science (ICIDS-2024)** — *November 2024*
  Manipal University Jaipur, India

Teaching Experience

- Department of Electrical & Computer Engineering (ECE) *July 2023 – June 2024*

Graduate Teaching Assistant North South University

- Conducted supplemental instruction and review sessions for CSE411, CSE422, and CSE482, strengthening students' understanding of advanced database systems, simulation, and web technologies.
- Supported faculty with grading, course logistics, and student consultations to ensure effective delivery of course content.

Technical Skills

- **Cryptography & Privacy:** AES, RSA, PKI; homomorphic and searchable encryption; identity-based encryption; differential privacy; privacy-preserving storage and search; blockchain-based protocols.
- **Machine Learning & AI:** Anomaly and threat detection, fault diagnostics, defect prediction, and security analytics; federated learning, adversarial robustness, and LLM security; model design, feature engineering, and evaluation in Python (scikit-learn, PyTorch/TensorFlow).
- **Security & Threat Analysis:** Vulnerability assessment, penetration testing, intrusion detection (IDS), SIEM, network-traffic analysis, DNS-over-HTTPS (DoH) threat detection.
- **Programming & Research Tools:** Python, Bash, Git, LaTeX; Linux-based experimentation and simulation pipelines.
- **Cloud & Infrastructure:** Oracle Cloud Infrastructure (OCI), AWS, Azure; infrastructure automation with Terraform, Docker, and Kubernetes.
- **CPS & Simulation Tools:** NS-3, GridPACK, HELICS, Node-RED for cyber-physical and power-grid studies; Wireshark, Metasploit, Burp Suite, Nmap.
- **Operating Systems & Virtualization:** Linux (Ubuntu, CentOS, Red Hat), KVM, Hyper-V.

Professional Experience

- Bangladesh Data Center Company Limited (BDCCL) [🌐] *April 2024 – Present*

Assistant Manager (Cloud) Dhaka, Bangladesh

- Provision and manage Oracle Cloud Infrastructure (OCI) resources – compute, storage, and databases – tailored to client requirements under an Infrastructure-as-Code (IaC) model.
- Automate infrastructure delivery with Terraform for consistent, repeatable, and auditable deployments.

- Ethics Advanced Technology Limited (EATL) [🌐] *September 2023 – November 2023*

Cyber Security Lab Instructor Dhaka, Bangladesh

- Conducted hands-on cybersecurity training for 50+ IT professionals from leading banks using EC-Council's ICBT: Cybersecurity Essentials iLabs.
- Designed and managed interactive lab exercises in network security, ethical hacking, and incident response.

- One World Infotech Limited [🌐] *December 2020 – May 2021*

Solution Engineer Gulshan-1, Dhaka, Bangladesh

- Deployed enterprise multi-factor authentication (OneSpan) and conducted threat and vulnerability assessments to strengthen client cybersecurity posture.
- Collaborated on incident-response readiness and SOC transformation, aligning solutions with organizational security frameworks and compliance needs.

Certifications

- **AWS Certified Cloud Practitioner (CLF-C02)** [AWS] *June 2025*
- **AWS Certified AI Practitioner (AIF-C01)** [AWS] *June 2025*
- **Certified Ethical Hacker (Master)** [EC-Council] *January 2025*
- **Certified Ethical Hacker (ANSI)** [EC-Council] *January 2025*
- **Certified Ethical Hacker (Practical)** [EC-Council] *December 2024*
- **OCI 2024 Generative AI Certified Professional** [Oracle Cloud] *July 2024*
- **OCI 2024 Certified AI Foundations Associate** [Oracle Cloud] *August 2024*
- **Microsoft Certified: Azure Data Fundamentals** [Microsoft Azure] *July 2023*
- **Ultimate AWS Certified Solutions Architect Associate (SAA-C03)** [Udemy] *December 2022*

REFERENCES

Dr. Rajesh Palit
Professor
Department of Electrical & Computer Engineering
North South University
Email: rajesh.palit@northsouth.edu
Phone: +88 02 55668200 | Ext – 6741
Mobile: +880 1719-557447
Relationship: Master's Thesis Supervisor

Dr. Hafiz Abdur Rahman
Professor
Department of Electrical & Computer Engineering
North South University
Email: hafiz.rahman@northsouth.edu
Phone: +88 02 55668200 Ext – 1535
Mobile: +880 1766-243111
Relationship: PI of CPS-PMU Research Lab