Prodipta Sen Amartya

(+880) 1517-006253 • prodiptasen-2018325324@cs.du.ac.bd
prodipta-sen-amartya • Prodipta0109 • prodipta0109.github.io • Google Scholar

Education

University of Dhaka • Dhaka, Bangladesh January 2019 – December 2023
Bachelor of Science • *Computer Science and Engineering* • CGPA: 3.49/4.0
• *Academic Transcripts*

Test of English as a Foreign Language (TOEFL iBT) • November 2024
Overall: 95 • Reading: 25 • Listening: 22 • Speaking: 24 • Writing: 24

Research Interests

- AI for Security; Trustworthy and Interpretable AI; Computer Security; Software Security; Decision-making under Uncertainty

Publications

- **Prodipta Sen Amartya**, Shaily Kabir, Sagar Chandra Karmaker Babu, and Mosarrat Jahan. "An Interval Creation Approach to Construct Interval Type-2 Fuzzy Sets." *2024 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE)*, IEEE World Congress on Computational Intelligence (WCCI), 2024. (Paper | Slides)

Preprints and Technical Reports

- Tahmid Imtiaz Imu, Emama Nahid, **Prodipta Sen Amartya**, et al. "Cancerous Backdoor Attack: Gradual Activation via Invisible Tokens and A Stage Controller." *arXiv preprint arXiv:2610.12644*, 2026. (Paper)

Research Experience

Backdoor Attacks in Large Language Model Reasoning
Supervisor: Dr. Honghui Xu,
Kennesaw State University, Georgia, USA July 2026 – Present

- Investigating vulnerabilities in large language models' chain-of-thought reasoning under adversarial backdoor triggers
- Designing and evaluating a novel backdoor attack strategy targeting multi-step reasoning; manuscript currently in preparation
- **Technical Skills:** Python, PyTorch, Hugging Face Transformers

Security Analysis of Federated Learning and Split Learning
Supervisor: Dr. Md Tariqul Islam,
University of Maryland - Baltimore County, USA January 2026 – Present

- Systematizing attack patterns and defense mechanisms across federated learning and split learning paradigms
- Evaluating the generalizability of existing defenses when applied across federated and split learning settings
- Establishing theoretical grounds and evaluation metrics for the transferability of attack and defense methods between the two paradigms

- Co-authoring a Systematization of Knowledge (SoK) paper targeting ***IEEE S&P (Oakland) 2027***
- **Technical Skills:** CNN, GAN, adversarial attacks & defense mechanisms

Improving Security of Systems Integrated in Ultrasound Devices
Samsung R&D Institute Bangladesh, Dhaka, Bangladesh August 2026 – Present

- Investigating how module updates can silently invalidate assumptions neighboring ultrasound modules rely on
- Developing a contract-based method to scope re-verification to only the affected modules, avoiding full-stack retesting
- **Technical Skills:** CodeQL, Semgrep, pydicom

Evaluation of the Behavior and Performance of Interval Type-2 Fuzzy Sets
Supervisor: Dr. Shaily Kabir
University of Dhaka, Dhaka, Bangladesh March 2023 – January 2024

- Designed the Interval Creation Approach (ICA), constructing interval type-2 fuzzy sets from type-1 sets of arbitrary shape — triangular, trapezoidal, Gaussian, generalized bell-shaped, symmetric, and asymmetric
- Benchmarked ICA on synthetic and real-world datasets against state-of-the-art methods, reducing pre-processing overhead and overall computational cost
- Evaluated the improved performance of ICA-constructed interval type-2 fuzzy sets in decision-making under uncertainty
- First author of "An Interval Creation Approach to Construct Interval Type-2 Fuzzy Sets", published from this research
- Conducted under supervision of Dr. Shaily Kabir of the *LUCID Lab (Lab for Uncertainty in Data and Decision Making), University of Nottingham*
- **Technical Skills:** R, Python, MATLAB, PYIT2FLS, Juzzy

Industry Experience

Senior Software Engineer
Samsung R&D Institute Bangladesh, Dhaka, Bangladesh March 2026 – Present

■ ***Project: Cardiac TEE Rendering – 5D Viewer, Samsung Medison***
A rendering platform for interactive visualization of 3D/4D cardiac ultrasound data.

- Resolved clinical UI sync failures by redesigning cross-process polling, eliminating viewer-engine RPC race conditions
- Designed the volume interaction layer — rotation, slicing, repositioning — and its .NET-to-C++ binding to the rendering engine
- Refactored the UI for lower latency and full Unicode label support
- **Technical Skills:** C++, C#, .NET, HLSL, DirectX

Software Engineer
Samsung R&D Institute Bangladesh, Dhaka, Bangladesh March 2024 – February 2026

■ ***Project: Cardiovascular Workstation – HelloMom, Samsung Medison***
Cloud and on-premises DICOM server for Samsung ultrasound machines, accessed through paired Windows and web clients.

- Built authentication end-to-end — login, sign-up, Google OAuth 2.0, SSO across Samsung Medison apps — and role-based access control governing file permissions
- Developed the DICOM tag parser organizing studies into a server-side hierarchy, and the REST APIs serving both clients

- Implemented the WPF and React UI with behavioral parity
- Deployed the on-premises IIS/Windows Server environment
- **Technical Skills:** C#, .NET, WPF, React, Next.js, Redux Toolkit, OAuth 2.0, DICOM, IIS Windows Server

■ ***Project: Cloud Solutions – SonoSync, Samsung Medison***
Real-time streaming and remote operation of ultrasound machines over the web.

- Owned real-time publication of the ultrasound stream to web clients, and contributed to the transport layer between machine and remote clients
- Replaced the project's ffmpeg dependency with a custom stream reader, implementing double buffering over DirectShow and Media Foundation
- Built the cloud integration enabling remote control of machine components
- **Technical Skills:** C++, .NET, DirectShow, Media Foundation, WebRTC

Academic Service

Reviewer
Workshop on Trustworthy AI for Good (AI4GOOD), ICML 2026

- Reviewed submissions for the AI4GOOD workshop at the *International Conference on Machine Learning* (Workshop | Certificate)

Judge and Question Setter
Bangladesh Artificial Intelligence Olympiad 2026

- Set problems and evaluated submissions for the regional stage, contributing to candidate selection for the national round

Academic Projects

Gardening Tukitaki
University of Dhaka, Dhaka, Bangladesh 2023

- Full-stack agricultural blog and marketplace platform (Project Code)
- Designed the relational schema and backend APIs serving both, including a fertilizer calculator deriving input quantities for a crop from published agricultural studies
- **Technical Skills:** Python, Django, SQLite3, JavaScript, HTML/CSS

Find Your Doctor
University of Dhaka, Dhaka, Bangladesh 2022

- Native Android app for finding doctors and booking appointments, with separate patient and practitioner roles (Project Code | Documentation)
- **Technical Skills:** Java, Firebase, Android SDK, automated testing

Book Your Ride
University of Dhaka, Dhaka, Bangladesh 2021

- Engineered an Android bus ticketing system with schedule lookup by route and date, replacing physical tickets with digital ones (Project Code)
- Designed the backend and seat inventory, preventing double-booking via Firebase transactions
- **Technical Skills:** Java, Firebase, Android SDK

Library Management System
University of Dhaka, Dhaka, Bangladesh 2020

- Designed a normalized relational database for an institutional library, enforcing referential integrity across circulation records through foreign key constraints (Project Report)

- **Technical Skills:** SQL, Oracle Database

Awards & Honors

- 1st position out of 400 participants, Basic AI/ML Exam, 2025, SRBD
- Talent Pool Scholarship in HSC, 2019-2023, Dhaka, Bangladesh
- Agriculturist (Krishibid) Institute Scholarship, 2019-2023, Dhaka, Bangladesh

Co-curricular Activities

Online & Offline courses -

- Generative AI & Deep Learning training | BUET × SRBD | Certificate
- Machine Learning & Data Science: The Complete Visual Guide | Udemy | Certificate
- Microservices: Designing Highly Scalable Systems | Udemy | Certificate
- Introduction to Cloud Computing on AWS for Beginners [2025] | Udemy | Certificate
- Website Hacking / Penetration Testing | Udemy | Certificate

Extra-curricular Activities

- Co-organizer, Study Group on Self-Adapting LLM Vulnerabilities, 2026 – Present, East West University, Dhaka, Bangladesh
- Volunteer, Code Samurai by BJIT, 2022, University of Dhaka, Dhaka, Bangladesh
- Member, DU YESS, 2019-2023, University of Dhaka, Dhaka, Bangladesh

Skills

- **Programming Languages:** C, C++, C#, Java, Python, JavaScript/TypeScript, SQL
- **Databases:** SQLite3, Firebase Real-time Database & Cloud Firestore
- **Framework & SDK:** .NET, Django, Android SDK, Bootstrap, React, Next.js, Node.js
- **Operating System:** Windows, Linux (Debian)
- **Machine Learning Tools:** NumPy, Pandas, scikit-learn
- **Web Languages:** HTML, CSS
- **Security & ML Research:** PyTorch, Hugging Face Transformers, CodeQL, Semgrep, FuzzyR
- **Other Tools:** Docker, Azure, WebRTC, CI/CD (GitHub Actions), REST APIs

References

- **Dr. Shaily Kabir**
  Assistant Professor
  School of Computer Science
  University of Nottingham
  Nottingham, United Kingdom
  Email: Shaily.Kabir5@nottingham.ac.uk

- **Dr. Md Tariqul Islam**
  Assistant Professor
  Department of Information Systems
  University of Maryland Baltimore County
  Baltimore, MD, USA
  Email: mtislam@umbc.edu

- **Dr. Honghui Xu**
  Assistant Professor
  Department of Information Technology
  Kennesaw State University
  Marietta, GA, USA
  Email: hxu10@kennesaw.edu