Group A :

1. Aritra Mazumdar

2. Soumodeep Karmakar

3. Debottam Kar

1. Proposed Domain: Security, Cloud Computing/Edge Computing, Artificial Intelligence/Machine Learning.

2. Broad Objective

To investigate, develop, and evaluate Explainable AI (XAI) models tailored for enhancing security across the cloud-edge continuum. The primary goal is to bridge the gap between the detection capabilities of complex AI systems and the need for human-interpretable, trustworthy, and actionable security insights.

3. Short Description

The proliferation of devices across the cloud-edge continuum has created a distributed and complex network environment, expanding the attack surface for security threats. While artificial intelligence offers a powerful solution for automated threat and anomaly detection across this landscape, the increasing complexity of AI models often renders their decision-making processes opaque. Our motivation is to investigate the role of explainable AI (XAI) in securing the cloud-edge continuum, bridging the gap between sophisticated, automated security systems and the need for human comprehension and trust.

In the context of the cloud-edge continuum, where security decisions must be made rapidly at various points—from resource-constrained edge gateways to powerful cloud servers—explainability is paramount. It ensures that security professionals can confidently interpret, validate, and act upon AI-driven insights, regardless of where a threat is detected. Understanding why a specific data flow from an IoT device is flagged as malicious is as critical as the detection itself. This interpretability not only enhances decision accuracy but also fosters trust in the automated security mechanisms governing the entire ecosystem.

Our research aims to develop XAI models tailored for the cloud-edge environment. These models will be designed to deliver high-performance threat detection while providing transparent reasoning for their security alerts, ensuring that security operations are both intelligent and fully scrutable from the network edge to the cloud core.

References

[1] J. Ables *et al.*, “Eclectic Rule Extraction for Explainability of Deep Neural Network based Intrusion Detection Systems,” *arXiv preprint arXiv:2401.10207*, 2024.
[2] M. A. Yagiz and P. Goktas, “LENS-XAI: Redefining Lightweight and Explainable Network Security through Knowledge Distillation and Variational Autoencoders,” *arXiv preprint arXiv:2501.00790*, 2025.