

18th March 2025					
Session	Time	Room	#Papers	Title	Authors
oral S5-A	14:00-15:00	Cosmos 3c	4	A Class Incremental Learning Framework for DDoS Detection	Borrini, Eugenio*; De Santis, Enrico; Rizzi, Antonello
long S5-A	15:30-16:30	Cosmos 1&2	4	Building Paths to Reduce Latency and Increase Resilience to Cyberattacks	Olenic, Kevin; Dubé, Michael; Houghten, Sheridan*
Session Chair: Suresh Sundaram				Anonymization of Documents for Law Enforcement with Machine Learning	Eberhardinger, Manuel*; Takenaka, Patrick; Griefhaber, Daniel; Maucher, Johannes
				Enhancing Intrusion Detection Systems with representation methods: A comparative study	Meyer, Bruno*; Nogueira, Michele; Zola, Wagner; Pozo, Aurora
LBP S5	15:30-16:30	Cosmos 1&2	1	Evaluating Familial Membership Inference Attack under Differentially Private Synthetic Genomic Data Generated by Large Language Model	Al-Saidi, Reem*; Kobti, Ziad; strufe, thorsten
19th March 2025					
Session	Time	Room	#Papers	Title	Authors
oral S5-B	9:00-10:00	Cosmos 3c	4	A Decentralized Greedy Assignment-Learning Spiking Neural Network-based Solution for A Perimeter Defense Problem	P, Thousi*; Velhal, Shridhar; Sundaram, Suresh; Sundararajan, Narasimhan
long S5-B	10:00-11:00	Cosmos 1&2	4	Investigating the computation of smoothed deceptive routes in topographic terrains for agent-based simulation systems	Souza, Luigi*; Rodrigues Silva Leão, Thiago; Lenhard, Christopher; PIGNATON DE FREITAS, EDISON; de Lima Silva, Luis Alvaro
Session Chair: Suresh Sundaram				Exploring the Effect of Dimensionality Reduction Techniques on Filtration Attacks	Durdabak, Keremalp*; Zincir-Heywood, Nur; Heywood, Malcolm; Jou, Stephan; Pospelova, Maria; Koduvely, Hari M.; Narayanan, Asad
				A Curriculum Learning Framework to Boost Object Detection on Unmanned Aerial Vehicles	ASLAN, EMRE*; Polikar, Robi; Ditzler, Gregory; Naddeo, Kyle; Bouhsine, Taha
short S5-A	10:00-11:00	Cosmos 1&2	6	Leveraging Deep Learning for Unobtrusive User Authentication: A Hybrid Approach	Prakash, Ravi; Prabhakar, Anjana*
				Hyperparameter Tuning of Convolution Neural Network for Intrusion Detection Systems using Particle Swarm Optimization	Grossi, Gina*; de Carvalho, Glaucio; Ombuki-Berman, Beatrice
				RSA Cryptanalysis: An Elitist Genetic Algorithm for Integer Factorization	Kumari, Aarti; Garain, Utpal; Bandyopadhyay, S; Mishra, Girish; K. Pal, Saibal; Bhattacharyya, Malay*
				Imbalanced malware classification: an approach based on dynamic classifier selection	Souza, José Vinicius*; Barbosa Vieira, Camila; Cavalcanti, George; Menelau Oliveira e Cruz, Rafael
				Digital Twin Knowledge Distillation for Federated Semi-Supervised Industrial IoT DDoS Detection	Belay, Mohammed Ayalew*; Rasheed, Adil; Salvo Rossi, Pierluigi
				Evolving Deep-Learners as Classifiers for Co-evolving Malware	Nitschke, Geof*