POLITECNICO DI MILANO

PhD in INGEGNERIA DELL'INFORMAZIONE / INFORMATION TECHNOLOGY - 39th cycle

Research Area n. 1 - Computer Science and Engineering

THEMATIC Research Field: SECURITY OF MACHINE AND FEDERATED LEARNING SYSTEMS

Monthly net income of PhDscholarship (max 36 months)
€ 1400.0 In case of a change of the welfare rates during the three-year period, the amount could be modified.

Context of the research activity	
Motivation and objectives of the research in this field	The increasing adoption of machine learning (ML) and federated learning (FL) systems in critical sectors such as healthcare and the Internet of Things (IoT) requires robust security measures to safeguard sensitive data and ensure the integrity of predictive models. This PhD research aims to systematically investigate, identify, and mitigate potential vulnerabilities and threats in ML and FL systems, with a specific focus on adversarial attacks, data poisoning, and model inversion attacks. The goal is to enhance the resilience of these systems against malicious actors, ensuring their reliability and trustworthiness in critical applications.
Methods and techniques that will be developed and used to carry out the research	The research will study the threat model of machine and federated learning systems. Both offensive and defensive security techniques will be used to scrutinize machine learning algorithms for vulnerabilities and subsequently craft defense mechanisms. The research will utilize simulation environments and real-world datasets, evaluating the resilience of ML and FL systems under various adversarial conditions.
Educational objectives	The PhD program aims to equip the candidate with in-depth knowledge and practical skills in cybersecurity, machine learning, and federated learning. The candidate

	will gain expertise in identifying and mitigating security threats specific to ML and FL systems in critical sectors.
Job opportunities	Graduates of this program will be well-positioned for roles in academia, research institutions, and industries focused on cybersecurity, machine learning, and federated learning. The demand for professionals with advanced knowledge in this area is expected to continue to grow, especially for those with domain-specific knowledge.
Composition of the research group	1 Full Professors 0 Associated Professors 3 Assistant Professors 6 PhD Students
Name of the research directors	Prof. Michele Carminati

Contacts
michele.carminati@polimi.it https://www.deib.polimi.it/eng/people/details/642676

Additional support - Financial aid per PhD student per year (gross amount)	
Housing - Foreign Students	--
Housing - Out-of-town residents (more than 80Km out of Milano)	--

Scholarship Increase for a period abroad	
Amount monthly	700.0 €
By number of months	6

Additional information: educational activity, teaching assistantship, computer availability, desk availability, any other information
List of Universities, Companies, Agencies and/or National or International Institutions that are cooperating in the research: 1. Politecnico di Milano 2. CERN 3. CNR 4. Università Milano Bicocca EDUCATIONAL ACTIVITIES (purchase of study books and material, including computers, funding for participation in courses, summer schools, workshops and conferences): financial aid per PhD student.

TEACHING ASSISTANTSHIP: (availability of funding in recognition of supporting teaching activities by the PhD student) There are various forms of financial aid for activities of support to the teaching practice. The PhD student is encouraged to take part in these activities, within the limits allowed by the regulations.

COMPUTER AVAILABILITY: individual use

DESK AVAILABILITY: individual use