POLITECNICO DI MILANO

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

Research Area n. 1 - Computer Science and Engineering

THEMATIC Research Field: ARTIFICIAL INTELLIGENCE FOR CYBERSECURITY

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 digital transformation of small and medium-sized enterprises (SMEs) has significantly enhanced productivity through improved monitoring of machinery and equipment. However, this increased connectivity also exposes these enterprises to heightened cyber risks. Cybersecurity represents a systemic challenge that necessitates specialized and often costly expertise. This Ph.D. research aims to systematically investigate and identify AI-based applications to support cybersecurity operations and the security of such solutions.
Methods and techniques that will be developed and used to carry out the research	The research will study the application of AI methods to the cybersecurity field. These systems will collect and disseminate cyber threat intelligence from various sources. They will identify and inform about cyber threats and vulnerabilities and provide tailored, actionable recommendations based on current and historical data, enabling entities involved to build in-house expertise and enhance long-term cybersecurity resilience. In addition, it will analyze the security of AI systems. Offensive and defensive security techniques will be used to scrutinize learning algorithms for vulnerabilities and design defense measures.
Educational objectives	The Ph.D. program aims to equip the candidate with in-

	depth knowledge and practical skills in applying Artificial Intelligence (AI) to cybersecurity. The candidate will gain expertise in identifying and mitigating security threats specific to ML and AI 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 and artificial intelligence. 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. Stefano Zanero, Prof. Michele Carminati

Contacts

stefano.zanero@polimi.it
https://www.deib.polimi.it/ita/personale/dettagli/407782
+39 02 2399 4017
---
michele.carminati@polimi.it
https://www.deib.polimi.it/eng/people/details/642676
+39 02 2399 4041

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

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