POLITECNICO DI MILANO

PhD in INGEGNERIA DELL'INFORMAZIONE / INFORMATION TECHNOLOGY - 38th cycle

Research Area n. 1 - Computer Science and Engineering

PNRR_352 Research Field: GREEN-IS-ALL-YOU-NEED IN PRIVACY-PRESERVING MACHINE AND DEEP LEARNING

Monthly net income of PhDscholarship (max 36 months)
€ 1250.0 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	Privacy-preserving machine and deep learning is a new and promising research area aiming at designing machine and deep learning models able to operate on encrypted data, hence guaranteeing the privacy of user data. This is a crucial ability in a technological and regulation scenario aiming at enforcing the privacy of users when sensitive data (e.g., health or biometric data, data revealing political opinions or personal info) are processed through Cloud-based on-line services or mobile applications. The ability to design machine and deep learning services operating on encrypted data comes at the expense of an extremely-high energy consumption due do the high computational complexity of the privacy-preserving operations (80x overhead in computational time and 40x in memory demand), making this solution not scalable from the energetic point of view and far from being a "green" technology. This is a challenging issue requiring a highly interdisciplinary research activity to be addressed (integrating machine and deep learning, privacy-preserving computation, and hardware aspects) with very few solutions present in the literature. The aim of the research is the definition of a "green direction" in privacy preserving machine and deep learning by introducing from the methodological point of view (i.e., hardware, machine/deep learning, algorithms)

	the design of "energy-efficient" privacy-preserving machine and deep learning solutions.
Methods and techniques that will be developed and used to carry out the research	The objectives of the research will be achieved by advancing the state-of-the-art in the field of privacy-preserving computation (e.g., based on Homomorphic Encryption, Federated Learning and Differential Privacy) as well as in the field of green machine and deep learning operating in a "as-a-service" manner.
Educational objectives	The Ph.D. will gain high-quality and integrated competences in the field of machine and deep learning as-a-service as well as privacy-preserving and green computation.
Job opportunities	The novel and heterogeneous background (strong competences on both theory and application) of the Ph.D. candidate will pave the way to positions in the academia, in research centers and in all the companies designing and developing machine and deep learning solutions for Cloud Computing.
Composition of the research group	0 Full Professors 1 Associated Professors 0 Assistant Professors 2 PhD Students
Name of the research directors	Prof. Manuel Roveri / Davide Chiggiato

Contacts
email: manuel.roveri@polimi.it, tel: 0223993590, web-page: http://roveri.faculty.polimi.it/

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	625.0 €
By number of months	6

National Operational Program for Research and Innovation	
Company where the candidate will attend the stage (name and brief description)	DHIRIA S.r.l.
By number of months at the company	6
Institution or company where the candidate will spend the period abroad (name and brief description)	IBM Research, Zurich Research Laboratory, Zurich, Switzerland https://research.ibm.com
By number of months abroad	6

Additional information: educational activity, teaching assistantship, computer availability, desk availability, any other information

Attinenza alla tematiche, alle missioni/componenti prescelte del bando PNRR v. D.M. 352, art.6

The research activities addressed by this research proposal are perfectly in line with the "vision" of the National Recovery and Resilience Plan (PNRR) as part of Mission 2 "Green Revolution and Ecological Transition", in particular in the priority "M2C2.5 Developing international, industrial and research and development leadership in the main transition chains". More generally, the research activities aspires at introducing "green and smart" transversal solutions at the basis of the digital transition (M1C1), innovation, competitiveness of the production system (M1C3), innovation, research and digitalization of the NHS (M6C2)

Impresa, presso cui si svolgerà l'attività esterna

Dhiria s.r.l. è uno Spin-off del Politecnico di Milano fondato ad Ottobre 2021. La mission di Dhiria è lo sviluppo di soluzioni innovative di intelligenza artificiale in modalità platform-as-a-service e software-as-a-service capaci di operare sia su dati in chiaro che su dati criptati da per garantire la privacy degli utenti. Più in dettaglio, la capacità di fornire soluzioni avanzate di machine e deep learning in modalità "as-a-service" e la capacità di elaborare i dati degli utenti in maniera crittografata sono le due caratteristiche distintive e altamente innovative delle soluzioni offerte da DHIRIA. Il dottorando svolgerà presso Dhiria Srl un periodo di 6 mesi.

Ente, università, azienda, centro di ricerca presso cui si svolgerà il periodo di studio e ricerca all'estero.

IBM Research, Zurich Research Laboratory, Zurich, Switzerland
https://research.ibm.com
Il dottorando svolgerà presto IBM Research un periodo di 6 mesi. L'attività di ricerca svolta presso IBM Research riguarderà tematiche di federated learning applicate a privacy-preserving computation.
Collaborazioni pregresse:

- tesisti di master co-supervisionati POLIMI-IBM Zurich
- articolo scientifici (uno in pubblicazione e due in preparazione)
- scientific talk presso IBM Research

All information regarding educational activities, personal funding, regulations and obligations of Ph.D. candidates are available on the web site https://dottoratoit.deib.polimi.it/