

## ALLEGATO B

UNIVERSITÀ DEGLI STUDI DI MILANO

selezione pubblica per n. 1 posto di Ricercatore a tempo determinato in tenure track (RTT)

per il settore concorsuale 01/B1 - Informatica,

settore scientifico-disciplinare INF/01 - Informatica,

presso il Dipartimento di INFORMATICA "GIOVANNI DEGLI ANTONI",

(avviso bando pubblicato sulla G.U. n. 41 del 21/05/2024) Codice concorso 5551

### CURRICULUM VITAE

**LARA MAURI**

#### INFORMAZIONI PERSONALI

COGNOME	MAURI
NOME	LARA
DATA DI NASCITA	██████████

#### ISTRUZIONE E FORMAZIONE

- 2018 – 2022      **Dottorato di Ricerca in Informatica**  
Dipartimento di Informatica, Università degli Studi di Milano  
Tesi: “*Data Partitioning and Compensation Techniques for Secure Training of Machine Learning Models*”  
Supervisor: Prof. Ernesto Damiani
- 2015 – 2017      **Laurea Magistrale in Sicurezza Informatica**  
Dipartimento di Informatica, Università degli Studi di Milano  
Voto di laurea: 110/110 con lode
- 2012 – 2015      **Laurea Triennale in Informatica**  
Dipartimento di Informatica, Università degli Studi di Milano  
Voto di laurea: 110/110 con lode

#### CONTRATTI DI RICERCA

- Nov. 2022 – presente      **Assegno di Ricerca di tipo B**  
Dipartimento di Informatica, Università degli Studi di Milano  
Titolo assegno: “*SOV-EDGE-HUB: Machine Learning Security*”  
Docente responsabile: Prof. Ernesto Damiani
- Giu. 2018 – Set. 2018      **Assegno di Ricerca di tipo B**  
Dipartimento di Informatica, Università degli Studi di Milano  
Titolo assegno: “*Studio di politiche di sicurezza e privacy per gli Enti di formazione e ricerca universitaria conformi alle misure di sicurezza AgID e al regolamento europeo GDPR*”  
Docente responsabile: Prof. Ernesto Damiani

## **ATTIVITÀ PROGETTUALI**

---

Partecipazione ai seguenti progetti di ricerca:

- ◆ Piano Nazionale di Ripresa e Resilienza (PNRR): *Multilayered Urban Sustainability Action (MUSA)* - Spoke 2 Big Data-Open Data in Life Sciences, 2022–2025
- ◆ Technology Innovation Institute di Abu Dhabi: *Prevention of Adversarial Attacks on Machine Learning Models (PALM)*, unità operativa: Università degli Studi di Milano, 2020–2023
- ◆ SEED 2019 (Bando Straordinario per Progetti Interdipartimentali 2019 – Piano di Sostegno alla Ricerca [Linea 3], Università degli Studi di Milano): *Cripto-valute: sfida alla sovranità dello Stato? Un'indagine storico-economica, giuridica e tecnica (CRIPTO S.O.S.)*, 2020–2021
- ◆ Programma EU Horizon 2020 (SU-ICT - Boosting the effectiveness of the Security Union): *Cyber security cOmpeteNce fOr Research anD Innovation (CONCORDIA)*, 2019–2023
- ◆ Programma EU Horizon 2020 (EU.3.7.4 – Improve cyber security): *Cyber Security Threats and Threat Actors Training - Assurance Driven Multi-Layer, end-to-end Simulation and Training (THREAT-ARREST)*, 2019–2022

## **GRUPPI DI RICERCA**

---

Appartenenza ai seguenti gruppi di ricerca:

- ◆ HH4AI, gruppo di ricerca interdisciplinare dell'hub scientifico Human Hall Università degli Studi di Milano – Direttrice: Prof.ssa Marilisa D'Amico
- ◆ SEcure Service-oriented Architectures Research (SESAR) Lab Dipartimento di Informatica, Università degli Studi di Milano – Direttore: Prof. Ernesto Damiani

## **ATTIVITÀ DIDATTICHE**

---

- ◆ Docente tutor per i seguenti corsi delle Lauree Magistrali in Sicurezza Informatica ed Informatica, Dipartimento di Informatica, Università degli Studi di Milano:  
A.A. 2023/2024 *Sicurezza delle architetture orientate ai servizi*  
A.A. 2022/2023 *Sicurezza delle architetture orientate ai servizi*
- ◆ Tutor didattico per i seguenti corsi della Laurea Triennale in Sicurezza Informatica dei Sistemi e delle Reti Informatiche (edizione online) [ex Art. 45 del Regolamento Generale d'Ateneo], Dipartimento di Informatica, Università degli Studi di Milano:  
A.A. 2023/2024 *Progettazione di software sicuro*  
A.A. 2022/2023 *Progettazione di software sicuro*  
A.A. 2021/2022 *Progettazione di software sicuro*  
A.A. 2020/2021 *Progettazione di software sicuro*  
A.A. 2019/2020 *Progettazione di software sicuro*  
A.A. 2018/2019 *Progettazione di software sicuro*  
A.A. 2017/2018 *Progettazione di software sicuro*

- ◆ Tutor per *CyberChallenge.IT* – programma di addestramento introduttivo alla cybersecurity organizzato dal Laboratorio Nazionale Cybersecurity del CINI in collaborazione con il Centro di Ricerca di Cyber Intelligence e Information Security della Sapienza di Roma, Dipartimento di Informatica, Università degli Studi di Milano, Mar. 2018 – Giu. 2018
- ◆ Tutor per i seguenti corsi della Laurea Triennale in Informatica ed in Sicurezza Informatica dei Sistemi e delle Reti Informatiche [Art. 19 del Regolamento della collaborazione degli studenti ai servizi dell'Università], Dipartimento di Informatica, Università degli Studi di Milano:  
Ott. 2017 – Dic. 2017 *Progettazione del software / Progettazione di software sicuro*
- ◆ Attività di docenza per la promozione della cultura digitale presso sedi di biblioteche della provincia di Cremona, Associazione Cremasca Studi Universitari, Mar. 2017 – Apr. 2017
- ◆ Attività di docenza per la promozione della cultura digitale presso sedi di biblioteche della provincia di Cremona, Associazione Cremasca Studi Universitari, Nov. 2016 – Dic. 2016

## **ORGANIZZAZIONE DI CONFERENZE E WORKSHOP**

---

### **Membro del Program Committee**

- ◆ COMPSAC 2024 Symposium on Security, Privacy & Trust in Computing (SEPT), Osaka, Japan, July 2–4, 2024
- ◆ COMPSAC 2023 Symposium on Security, Privacy & Trust in Computing (SEPT), Torino, Italy, June 26–30, 2023
- ◆ 2021 IEEE International Conference on Smart Data Services (IEEE SMDS 2021), Virtual conference, September 5–10, 2021
- ◆ COMPSAC 2021 Symposium on Security, Privacy & Trust in Computing (SEPT), Virtual conference, July 12–16, 2021
- ◆ 7th International Conference on Information Systems Security and Privacy (ICISSP 2021), Virtual conference, February 11–13, 2021
- ◆ 6th International Conference on Information Systems Security and Privacy (ICISSP 2020), Valletta, Malta, February 25–27, 2020

### **Membro dell'Organizing Committee**

- ◆ “Blockchain technology: una prospettiva accademica ed aziendale”, SEED 2019, Dipartimento di Informatica, Università degli Studi di Milano, 16 Novembre 2021
- ◆ “Criptovalute e diritto: problemi attuali e sfide future”, SEED 2019, Webinar, 26 Marzo 2021
- ◆ “Criptovalute: sfida alla sovranità dello stato? Un'indagine storico-economica, giuridica e tecnica”, SEED 2019, Webinar, 20 e 27 Ottobre 2020

## **SEMINARI**

---

Relatrice dei seguenti seminari:

- ◆ “Robust ML Model Ensembles Via Risk-driven Anti-clustering of Training Data”, Corso di *Sicurezza delle architetture orientate ai servizi*, Dipartimento di Informatica, Università degli Studi di Milano, 9 Maggio 2024
- ◆ “Robust ML Model Ensembles Via Risk-driven Anti-clustering of Training Data”, Corso di *Sicurezza delle architetture orientate ai servizi*, Dipartimento di Informatica, Università degli Studi di Milano, 25 Maggio 2023

## **PARTECIPAZIONE A CONFERENZE, WORKSHOP, SUMMER SCHOOL, ETC.**

---

- ◆ IEEE International Conference on Cyber Security and Resilience (CSR 2021), virtual conference (due to COVID-19), July 26-28, 2021
- ◆ 13th IEEE International Conference on Cloud Computing (CLOUD 2020), virtual conference (due to COVID-19), October 20, 2020
- ◆ 3rd Distributed Ledger Technology Workshop (DLT 2020), Ancona, Italy, February 4, 2020
- ◆ 6th Summer School on Network and Information Security (NIS19), Heraklion, Greece, September 16–20, 2019
- ◆ 2nd Summer School on Industry Digital Evolution (IDE19), Carovigno, Italy, June 5–7, 2019
- ◆ 2nd Distributed Ledger Technology Workshop (DLT 2019), Pisa, Italy, February 12, 2019

## **ATTIVITÀ DI CORRELATORE**

---

Correlatrice delle seguenti tesi di laurea:

- ◆ Adriano Giaquinta  
Titolo: “EOS: Analisi e caratteristiche di una piattaforma blockchain”  
Università degli Studi di Milano
- ◆ Alessia Pilato  
Titolo: “Analisi e confronto di sistemi e-voting con blockchain”  
Università degli Studi di Milano

## **ATTIVITÀ DI REFERAGGIO**

---

### **Referaggio per Riviste Internazionali**

- ◆ IEEE Transactions on Services Computing
- ◆ IEEE Transactions on Fuzzy Systems
- ◆ IEEE Transactions on Network and Service Management

- ◆ Computers & Security
- ◆ International Journal of Knowledge and Learning
- ◆ IET Information Security
- ◆ Electronic Commerce Research and Applications
- ◆ Electronics
- ◆ Future Internet
- ◆ Human-centric Computing and Information Sciences
- ◆ Mathematics
- ◆ Multimedia Tools and Applications
- ◆ Security and Communication Networks

#### **Referaggio per Conferenze Internazionali**

- ◆ ICISSP 2021 - 7th International Conference on Information Systems Security and Privacy, Virtual conference, February 11–13, 2021
- ◆ ICISSP 2020 - 6th International Conference on Information Systems Security and Privacy, Valletta, Malta, February 25–27, 2020
- ◆ WCNC-SFCS 2019 - IEEE Wireless Communications and Networking Conference, Marrakech, Morocco, April 15–18, 2019
- ◆ ICME 2018 - IEEE International Conference on Multimedia and Expo, San Diego, USA, July 23-27, 2018
- ◆ SEKE 2018 - 30th International Conference on Software Engineering and Knowledge Engineering, San Francisco Bay, USA, July 1–3, 2018

---

#### **ATTIVITÀ DI TRADUZIONE**

- |      |   |
|------|---|
| 2021 | Collaborazione alla realizzazione dell'edizione italiana dell'opera " <i>Sicurezza dei computer e delle reti</i> " di W. Stallings, edito da Pearson Education, in qualità di traduttrice |
|------|---|

---

#### **PUBBLICAZIONI SCIENTIFICHE**

##### **Indicatori bibliometrici [21/06/2024]**

*Google Scholar*: h-index = 8; citazioni = 161

*Scopus*: h-index = 7; citazioni = 111

## Articoli su Rivista

- ◆ M. M. Alani, L. Mauri, and E. Damiani, “A two-stage cyber attack detection and classification system for smart grids,” *Internet of Things*, 24: 100926, 2023
- ◆ L. Mauri, B. Apolloni, and E. Damiani, “Robust ML model ensembles via risk-driven anti-clustering of training data,” *Information Sciences*, 633, 122-140, 2023
- ◆ L. Mauri and E. Damiani, “Modeling Threats to AI-ML Systems Using STRIDE,” *Sensors* 22, no. 17: 6662, 2022
- ◆ L. Mauri and E. Damiani, “Estimating Degradation of Machine Learning Data Assets,” *ACM Journal of Data and Information Quality* 14, 2, Article 9, 2022

## Capitoli di Libri

- ◆ L. Mauri and E. Damiani, “Securing Machine Learning Models: Notions and Open Issues,” In book: *Engineering Mathematics and Artificial Intelligence*, 485-508, 2023

## Atti di Convegno

- ◆ L. Mauri and E. Damiani, “STRIDE-AI: An Approach to Identifying Vulnerabilities of Machine Learning Assets,” In IEEE International Conference on Cyber Security and Resilience (CSR) 2021, Rhodes, Greece, July 26-28, 2021  
**Selezionato tra i migliori paper della conferenza** per la pubblicazione di una versione estesa nello Special Issue di *Sensors* “Selected Papers from the IEEE CSR 2021”
- ◆ L. Mauri, S. Cimato, E. Damiani, “Untangling the XRP Ledger: Insights and Analysis,” In: Furnell, S., Mori, P., Weippl, E., Camp, O. (eds) *Information Systems Security and Privacy. ICISSP 2020. Communications in Computer and Information Science*, vol 1545. Springer, Cham.
- ◆ L. Mauri, E. Damiani, S. Cimato, “Be Your Neighbor’s Miner: Building Trust in Ledger Content via Reciprocally Useful Work,” In 13th IEEE International Conference on Cloud Computing, CLOUD 2020, Beijing, China, October 18-24, 2020
- ◆ L. Mauri, S. Cimato, E. Damiani, “A Formal Approach for the Analysis of the XRP Ledger Consensus Protocol,” In Proceedings of the 6th International Conference on Information Systems Security and Privacy, ICISSP 2020, Valletta, Malta, February 25-27, 2020  
**Selezionato tra i migliori paper della conferenza** per la pubblicazione di una versione estesa in *Communications in Computer and Information Science* (CCIS, vol 1545)
- ◆ C. Braghin, S. Cimato, E. Damiani, F. Frati, L. Mauri, E. Riccobene, “A Model Driven Approach for Cyber Security Scenarios Deployment,” In *Computer Security – ESORICS 2019 International Workshops, IOSec, MSTEC, and FINSEC*, Luxembourg City, Luxembourg, September 26-27, 2019 - *Lecture Notes in Computer Science*, vol 11981, Springer, 2019
- ◆ C. Braghin, S. Cimato, S. Raimondi Cominesi, E. Damiani, L. Mauri, “Towards Blockchain-Based E-Voting Systems,” In *Business Information Systems Workshops – BIS 2019 International Workshops*, Seville, Spain, June 26-28, 2019 - *Lecture Notes in Business Information Processing*, vol 373, Springer, 2019
- ◆ L. Mauri, S. Cimato, E. Damiani, “A Comparative Analysis of Current Cryptocurrencies”, In Proceedings of the 4th International Conference on Information Systems Security and Privacy, ICISSP 2018, Funchal, Madeira, Portugal, January 22-24, 2018

## Poster

- ◆ L. Mauri and E. Damiani, “Improving Machine Learning Model Robustness via Risk-Driven Ensemble Modeling,” 3<sup>rd</sup> General Meeting MUSA, May 15, 2024

## Tesi di Dottorato

- ◆ L. Mauri, “Data Partitioning and Compensation Techniques for Secure Training of Machine Learning Models” *Scuola di Dottorato in Informatica*, XXXIV ciclo. Università degli Studi di Milano. Settore Scientifico-Disciplinare: INF/01 Informatica. Tutor: Prof. Ernesto Damiani. Co-tutor: Prof. Bruno Apolloni. Direttore della Scuola di Dottorato: Prof. Paolo Boldi, 2022

---

Data

21/06/2024

Luogo

Milano