Allegato alla domanda di partecipazione

Curriculum formativo, didattico, scientifico e professionale del candidato

Dichiarazione sostitutiva di certificazioni

(Art. 46, D.P.R. 28 dicembre 2000 n. 445)

Dichiarazione sostitutiva dell'atto di notorietà

(da sottoscrivere davanti all'impiegato addetto o da presentare o spedire con la fotocopia di un documento di identità)
(Art. 47, D.P.R. 28 dicembre 2000 n. 445)

Estremi del bando di selezione	Selezione pubblica per il conferimento di Assegni di Ricerca, ai sensi dell'art. 22 della L. 30/12/2010, n. 240 - Tipo B - Assegni su altri fondi (D.R. n. 110 del 05.11.2020). Titolo del Progetto: "Apprendimento robusto contro la contaminazione dei dati di addestramento" - Area: 09 - Ingegneria industriale e dell'informazione - Settore Concorsuale: 09/H1-Sistemi di elaborazione delle informazioni – SSD: ING-INF/05- Responsabile Scientifico: Dott. Battista Biggio
Informazioni aggiornate al	05.02.2021
Nome e Cognome	Kathrin Grosse
Data di nascita	24.11.1990

Si raccomanda di indicare con precisione tutti gli elementi valutabili ai sensi del bando di selezione (aggiungere o togliere righe secondo necessità).

Esperienza professionale

Periodo	Ente	Principali attività e responsabilità
12.10.20-29.01.21	**Disney Research Zurich**	**Research in audience understanding**
15.05.19-15.08.19	**IBM**	**Research in ML security**

Istruzione, formazione (es. titoli di studio, certificazioni professionali/linguistiche/informatiche)

Data	Titolo / Principali tematiche	Ente
15.04.2016	**Master of Science in Computer Science**	**Saarland University**
09.09.2013	**Bachelor of Science in Cognitive Science**	**Osnabrueck University**

Pubblicazioni / Convegni

Nico Döttling, Kathrin Grosse, Michael Backes and Ian Molloy. Adversarial examples and metrics. Under submission.
Kathrin Grosse and Michael Backes. Do winning tickets exist before DNN training?. To appear in: SIAM DM (2021).
Kathrin Grosse, Michael Thomas Smith, and Michael Backes. Killing four birds with one Gaussian process: The relation between different test-time attacks. To appear in: ICPR (2020).
Kathrin Grosse, Thomas A. Trost, Marius Mosbach, Michael Backes and Dietrich Klakow, On the security relevanve of initial weights in deep neural networks, ICANN (1) 2020: 3-14.
Kathrin Grosse, Taesung Lee, Youngja Park, Michael Backes and Ian Molloy. A new measure for overfitting and its implications for backdooring of deep learning. arXiv preprint arXiv: 2006.06721 (2020).

Michael Thomas Smith, Kathrin Grosse, Michael Backes and Mauricio A. Alvarez, Adversarial vulnerability bounds for Gaussian process classification, in Workshop on ML with Guarantees at NeurIPS (2019).
Kathrin Grosse, Nicolas Papernot, Praveen Manoharan, Michael Backes and Patrick D. McDaniel, Adversarial examples for malware detection, ESORICS (2) 2017: 62-79.
Kathrin Grosse, Praveen Manoharan, Nicolas Papernot, Michael Backes, and Patrick McDaniel. On the (statistical) detection of adversarial examples. arXiv preprint arXiv:1702.06280 (2017).
Kathrin Grosse and Jilles Vreeken, Summarizing event sequences using serial episodes and an ontology, 4th workshop on interactions between data mining and natural language processing, (2017).
Carlos Iván Chesñevar, María Paula González, Kathrin Grosse and Ana Gabriela Maguitman, A first approach to mining opinions as multisets through argumentation. AT 2013: 195-209.
Kathrin Grosse, Carlos Iván Chesñevar, Ana Maguitman and Elsa Estevez, Empoweringan e-government platform through twitter-based arguments. Inteligencia Artificial. Revista Iberoamericana de Inteligencia Artificial 15.50 (2012): 46-56.
Kathrin Grosse, Carlos Iván Chesñevar and Ana Gabriela Maguitman, An argument-based approach to mining opinions from Twitter. AT 2012: 408-422.

Altre attività scientifiche

Talk at Robust Artificial Intelligence Workshop of the Lorentz Center, NL, 19.01.2021 Reviewer at IJCAI-PRICAI '20, TTML '20 at ICLR, SPML'19 at ICML, ...

Ulteriori informazioni pertinenti

Nominated as #KI50 Newcomer* in 2019

Cagliari, 5.02.21