AVVISO RISERVATO AL PERSONALE INTERNO PER IL CONFERIMENTO DI N. 1 INCARICO/ATTIVITÀ, SENZA RETRIBUZIONE AGGIUNTIVA, PRESSO IL DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE E SCIENZE MATEMATICHE

Dipartimento di Ingegneria dell'Informazione Scienze Matematiche

progetto o attività	**Analysis of the vulnerability of AI-based classifiers against adversarial attacks**
descrizione attività progettuale/progetto	The goal of the research is to analyze the data distribution of widely used image datasets in AI - like MNIST, CIFAR-10, Food101 and possibly others - to understand structural and statistical properties that may influence model robustness. The focus will be on assessing how data geometry and high dimensional structure contribute to the emergence of adversarial examples. In a second phase the findings of the analysis will be evaluated by the light of existing theoretical work on the concentration of measure phenomenon, which suggests why, in high dimensions, small perturbations can significantly alter model predictions. Understanding how these theoretical insights manifest in real-world datasets can help identify intrinsic vulnerabilities in current AI models and guide the design of more robust learning

	systems. Eventually, the validity of the results of the theoretical analysis will be assessed experimentally, on a pool of classifiers trained on the datasets used for the analysis.
responsabile del progetto /responsabile gestionale e scientifico	Prof. Mauro Barni
durata dell'incarico	12 mesi
requisiti/competenze	PhD on themes related to the objective of the contract. Research experience in AI. Knowledge of Python programming language
sede di svolgimento delle attività e motivazione	DIISM
valutazione delle domande	esame curriculum e colloquio da parte di: Mauro Barni, Benedetta Tondi, Pietro Bongini; supplente: Alberto Toccafondi
indirizzo e-mail per l'invio delle domande	amministrazione@diism.unisi.it
giorni previsti per la presentazione delle domande	7 giorni

Siena, data della firma digitale

Il Responsabile della struttura
Prof. Valerio Vignoli