TU WIEN Informatics

Adversariale Beispiele Überdenken

DIPLOMARBEIT

zur Erlangung des akademischen Grades

Diplom-Ingenieur

im Rahmen des Studiums

Data Science

eingereicht von

B.Sc. Yahya Jabary
Matrikelnummer 11912007

an der Fakultät für Informatik

der Technischen Universität Wien

Betreuung: Univ. Prof. Dr. Schahram Dustdar
Mitwirkung: Univ. Prof. Dr. Roger Wattenhofer
Dipl. Ing. Alireza Furutanpey
M.Sc. Andreas Plesner

Wien, 1. Jänner 2025

Yahya Jabary	Schahram Dustdar

TU WIEN Informatics

Rethinking Adversarial Examples

DIPLOMA THESIS

submitted in partial fulfillment of the requirements for the degree of

Diplom-Ingenieur

in

Data Science

by

B.Sc. Yahya Jabary
Registration Number 11912007

to the Faculty of Informatics

at the TU Wien

Advisor: Univ. Prof. Dr. Schahram Dustdar
Assistance: Univ. Prof. Dr. Roger Wattenhofer
Dipl. Ing. Alireza Furutanpey
M.Sc. Andreas Plesner

Vienna, January 1, 2025

Yahya Jabary | Schahram Dustdar

Erklärung zur Verfassung der Arbeit

B.Sc. Yahya Jabary

Hiermit erkläre ich, dass ich diese Arbeit selbständig verfasst habe, dass ich die verwendeten Quellen und Hilfsmittel vollständig angegeben habe und dass ich die Stellen der Arbeit – einschließlich Tabellen, Karten und Abbildungen –, die anderen Werken oder dem Internet im Wortlaut oder dem Sinn nach entnommen sind, auf jeden Fall unter Angabe der Quelle als Entlehnung kenntlich gemacht habe.
Ich erkläre weiters, dass ich mich generativer KI-Tools lediglich als Hilfsmittel bedient habe und in der vorliegenden Arbeit mein gestalterischer Einfluss überwiegt. Im Anhang „Übersicht verwendeter Hilfsmittel“ habe ich alle generativen KI-Tools gelistet, die verwendet wurden, und angegeben, wo und wie sie verwendet wurden. Für Textpassagen, die ohne substantielle Änderungen übernommen wurden, haben ich jeweils die von mir formulierten Eingaben (Prompts) und die verwendete IT- Anwendung mit ihrem Produktnamen und Versionsnummer/Datum angegeben.

Wien, 1. Jänner 2025

Yahya Jabary