RELAZIONE ATTIVITA' ANNUALE DEI DOTTORANDI – PRIMO ANNO
REPORT ON THE PH.D. ACTIVITY – FIRST YEAR

Nome e cognome ***Name and surname***	MUHAMMAD UMAR ZESHAN

Corsi frequentati con sostenimento di esame finale ***Attended courses (with final exam)***	***Votazione riportata*** ***Mark***	***Numero di ore*** ***Hours***

Corsi frequentati senza sostenimento di esame finale ***Attendance courses (attendance only)***	***Numero di ore*** ***Hours***

Altre attività formative (seminari, workshop, scuole estive, ecc.) - Descrizione ***Other Ph.D. oriented activities (seminars, workshops, summer schools, etc.) - Description***	***Numero di ore*** ***Hours***
AI for Society summer school (La Maddalena)	20

Attività di ricerca eventualmente svolta (max. 3000 caratteri) ***Research activity (max. 3000 characters)***

Research activity during the first year:

Understanding the topic: First of all, when I started my research on the topic of Adversarial Attacks in Recommender Systems in Software Engineering, the first challenge was to build a strong background on the topic before contributing to more advanced topics.

Literature Background: I focused on building a strong base on the research topic by studying the available literature. I found the topic of adversarial attacks quite trending, as most of the papers available related to this topic have been published in the last five years. For this purpose, I decided with my supervisor's suggestion, to write a review paper first which can be helpful in the remaining period of PhD and can excel in my research.

Gathering the Literature: Firstly, to understand the Recommender systems, I found about 33 papers from the database of SE venues to have a better understanding and can help me define the problem and find the solution. Later, I filtered out about 84 research papers, with the specific query focused on the topic of Adversarial Attacks in SE. And finally, refined that query even further to find 48 more papers that defined the different kinds of adversarial attacks.

After gaining an understanding of more than 100 research papers, I started writing the research paper which is addressing the two key RQs:

RQ1: How well does the currently available literature address the problem of AML in Software Engineering? I conduct a literature review to see if there has already been any work done to understand and address threats to Software Engineering stemming from malicious data.

RQ2: What are the different kinds of threats that can impact software engineering systems? This question aims to identify the different types of attacks (i.e. Backdoor, Evasion, Random Forest Attack, Anomalies, etc.) and the way they can cause damage.

The paper is in the final stages of the writing process and will be submitted to the suitable SE venue next month. After that, The focus will be to study and publish papers in the field of building a malware detection and defense system that can contribute largely to the field of Software Engineering.

My time in the first year of the Ph.D. was cut short because of visa legalities, that's why I was late to attend the courses on time, however, I am planning to take 2 courses to cover the Credit hours this semester alongside my research activities.

I also attended summer school in La Maddalena on the topic of AI for Society. I gained a lot of insights and knowledge about the latest research trends especially the multi-disciplinary approaches to contribute to society. I also presented my poster there to gather some very interesting questions to make my topic even better.

I was in the "Group Farinella" for the final presentations, and we got the FIRST prize for the best topic and presentation for the topic "Intelligent University Systems (IUS)". My contribution to this task was to add the role of recommender systems for the successful replies by the proposed University Chatbot System.

Eventuali pubblicazioni ***Publications (if available)***

Data ***Date***	20-09-2023	***Firma*** ***Signature***