Yash More yash.more@alumni.ashoka.edu.in

The widespread usage of machine learning algorithms in social media, video games, and search engines influences each of us, guiding our interactions directly or indirectly. As we increasingly rely on ML systems, I want to understand them better and make them safer and more explainable for their users. As a first step to understanding the foundations of ML, I entered Ashoka University as a first-generation college student majoring in Computer Science. Although I was financing my tuition and family expenses through part-time jobs, I managed to dedicate the time required to learn the core concepts of Computer Science and Mathematics. I also gained research and industry experience in machine learning (ML) during my undergraduate years.

In being exposed to the field, I understood its possibilities and limitations - like how ML models are widely adopted yet need to be more trustworthy. Since their inception, interpreting neural networks has been difficult, and one often sees them as black boxes. Moreover, ML systems are unsustainable due to the high amounts of computing and data required to train ML models. I wish to address these challenges and work on problems of **safety, security, and sustainability** in ML as a Master's student at KTH Royal Institute of Technology. Solving these problems would equip me with the essential tools to build a trustworthy ML system. The Master's program shall be a cornerstone for my academic journey, helping me seek a Ph.D. and eventually lead a research lab in Trustworthy Machine Learning.

After taking machine learning courses in my first year, I was eager to apply the concepts I had learned. Research projects provided me with the space to implement and understand the concepts, with the bonus of discovering the current limitations surrounding ML concepts. Despite the research's unstructured nature, research projects allowed me to use my creativity and ideas to develop a unique roadmap for the solution.

In my first research project, I created a one-of-its-kind short-range object detection system using low-frequency radio waves and computer vision models. The prototype resulted from our goal of building an inexpensive object detection system that could replace resource-intensive radars without compromising quality. I co-authored three papers while actively contributing to developing the prototype. I acquired the hands-on skills required to build machine learning models and developed an intuition to identify and articulate problems in ML research.

Shortly after, I formed a research group to explore problems within Federated Learning(FL). Existing secure-federated learning approaches offer a distributed way to train models but are limited in privacy and use a large number of algorithmic operations, thus making them infeasible to scale. To solve this problem, I built an FL framework based on trusted execution environments that can train models efficiently without compromising privacy. Our work got accepted at the Euro S&P Conference. In my next project, I built an FL framework for decentralized gradient aggregation using secure outsourced computation and secret sharing. The framework helps users overcome the reliance on central aggregators and adds another layer of protection from adversaries. As the primary author, I presented our work at the Privacy Preserving Artificial Intelligence Workshop at AAAI. These projects helped deepen my understanding of safety and security in ML and broadened my interest in federated learning.

At KTH, I would love to work with Dr. Stefan Bauer in artificial intelligence and focus on causality and generalizability problems, especially in robotics. Having worked on privacy-preserving machine learning and trustworthy systems, I would like to continue working on similar areas under the guidance of Dr. Tobias Oechtering. As an MLOps developer handling cloud infrastructure, ETL pipelines, and model orchestration, I am also interested in working alongside Dr. Paris Carbone on the intersection of data science and distributed computing. I also found Dr. Ragnar Thobaben's work in information theory+ ML and graph-based information processing quite intriguing, and I am interested in working in such areas. With my research and development skills and a passion for collaborating, I am confident that I will be able to excel as a graduate student at KTH Royal Institute of Technology.