Data Privacy Concerns of Using AI

Mohammad Asad
Fakultät für Informatik
Otto von Guericke University
Magdeburg, Sachsen Anhalt
mohammad@st.ovgu.de

ABSTRACT

Artificial Intelligence (AI) is reshaping the world, but it may also be silently redefining the boundaries of our privacy. As the use of AI grows, concerns around user privacy are also increasing. AI systems such as machine learning, natural language processing, and computer vision depend on large datasets often collected without the user’s consent. These systems can use a variety of methods, including model inversion attacks and attribute inference, to infer sensitive information.

In this paper, I aim to survey at least five academic papers to study the privacy concerns and threats associated with AI, along with possible resolutions. I will also examine the approaches recommended in these studies, such as federated learning, differential privacy, noise injection, data perturbation, and Human-in-the-Loop (HITL) approaches. These techniques aim to make AI systems more privacy-aware and secure.

The objective of this literature survey is to spread awareness and motivate the responsible and ethical use of AI technologies in the future.