Title: Performance Evaluation of Privacy-Preserving Machine Learning for IoT

Abstract: The Internet of Things (IoT) has revolutionized data collection and analysis, but it also poses significant privacy challenges. This master's project focuses on the evaluation (and possible development) of privacy-preserving machine learning techniques tailored for IoT environments, addressing challenges unique to IoT data and exploring their applications in smart and connected systems.

Objectives:

1. **IoT Data Privacy Analysis:** Investigate the privacy challenges associated with IoT data, including data localization, data aggregation, and privacy risks in edge computing environments.
2. **Privacy-Preserving Machine Learning Techniques:** Research, implement, and evaluate privacy-preserving machine learning techniques suitable for IoT data, such as federated learning, edge-based privacy-preserving analytics, and secure multi-party computation.
3. **IoT Applications:** Identify specific IoT applications where privacy-preserving machine learning is essential, such as predictive maintenance, health monitoring, smart cities, or industrial automation.
4. **Prototype Development:** Develop prototypes or proof-of-concept systems that demonstrate the application of privacy-preserving machine learning in IoT scenarios.
5. **Performance Evaluation:** Evaluate the performance, accuracy, and privacy guarantees of the implemented techniques in real or simulated IoT environments. Consider factors like communication overhead, data locality, and energy efficiency.

Methodology:

- **Literature Review:** Conduct an extensive review of IoT data privacy challenges and state-of-the-art privacy-preserving machine learning techniques.
- **Data Collection:** Gather IoT datasets or simulate IoT data generation to represent specific application scenarios.
- **Prototype Development:** Implement privacy-preserving machine learning techniques in IoT environments. Design and develop prototype IoT systems that incorporate these techniques.
- **Performance Evaluation:** Conduct experiments to assess the performance and privacy preservation capabilities of the implemented solutions in IoT contexts. Measure factors like data accuracy, communication overhead, and data privacy.
- **Application Case Studies:** Apply privacy-preserving machine learning techniques to real or simulated IoT applications. Analyze the impact on data privacy, model accuracy, and the feasibility of real-time analytics.

Deliverables:

- A research paper detailing the investigation, implementation, and evaluation of privacy-preserving machine learning techniques in IoT.
- Open-source code and prototypes demonstrating the practical application of privacy-preserving techniques in IoT scenarios.
- Case studies illustrating the effectiveness and relevance of privacy-preserving machine learning in IoT applications.