Intelligent Cobots & Data Privacy: Leveraging Aggregated Learning

Building Smarter Cobots Through Collaborative Learning Without Data Sharing

Image: Universal Robots

The Challenge: Cobot Intelligence vs. Data Privacy

The Balancing Act: Intelligence and Confidentiality

- Cobots benefit greatly from reinforcement learning (RL) and AI, requiring extensive data.
- Customer data is highly sensitive and cannot be shared directly.
- How do we build intelligent cobots while respecting data privacy?

Solution 1: Federated Learning (FL)

Federated Learning: Distributed Intelligence

- Model training occurs on local customer devices.
- Only model updates (gradients) are shared, not raw data.
- Enables collaborative learning without data transfer.

Solution 2: Privacy-Enhancing Techniques

Fortifying Privacy: Differential Privacy & More

- Differential Privacy: Adds noise to data to prevent identification.
- Homomorphic Encryption: Allows computation on encrypted data.
- Secure Multi-Party Computation (SMPC): Enables joint computation without revealing inputs.
- Edge Computing: Local data processing to decrease data transfer.

Implementation & Benefits

Robust security measures and clear data governance are essential.

- Enhanced cobot intelligence and adaptability.
- Preserved customer data privacy.
- Accelerated development of advanced cobot capabilities.
- Data aggregation without individual data sharing.

Conclusion & Future Outlook

The Balancing Act: Intelligence and Confidentiality

- Combining FL, privacy techniques, and edge computing unlocks new possibilities.
- Continuous research is crucial for advancing privacy-preserving AI.
- Call to action: working together to create a secure and smart automated future.

Thank you

Dhiraj Patra

I'm a dedicated professional and the holder of patented AI applications with a strong foundation in Data Science and Data Analytics, and a passion for designing and implementing Cloud Architectures for AI applications. My expertise lies in harnessing the power of Industry 4.0.

https://dhirajpatra.github.io/