Background:

Recently is privacy-preserving AI a hot issue.

(https://towardsdatascience.com/perfectly-privacy-preserving-ai-c14698f322f5)

Google made TensorFlow Quantum. They apply the machine leaning to quantum computer. (https://www.zdnet.com/article/googles-tensorflow-is-ready-for-quantum-but-is-ai-ready-for-quantum/)

Papers:

Privacy preserving for AI applications:

- Privacy Preserving in Blockchain based on Partial Homomorphic Encryption System for AI Applications

  https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8634280

- A Survey on Collaborative Deep Learning and Privacy-Preserving

  https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8411925

  - Membership inference attacks against machine learning models

  https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7958568

- Privacy-Preserving Deep Learning

  http://www.cs.cornell.edu/~shmat/shmat_ccs15.pdf

  - Deep Models Under the GAN: Information Leakage from Collaborative Deep Learning

  https://dl.acm.org/doi/pdf/10.1145/3133956.3134012

  - SecureML: A System for Scalable Privacy-Preserving Machine Learning

  https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7958569

- Privacy-Preserving Scoring of Tree Ensembles: A Novel Framework for AI in Healthcare

  https://ieeexplore.ieee.org/abstract/document/8622627

Privacy-preserving approach using machine learning:

- A hybrid deep learning architecture for privacy-preserving mobile analytics

  https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8962332

- A machine-learning based approach to privacy-aware information-sharing in mobile social networks

  https://hal.archives-ouvertes.fr/hal-01108962/file/Bilogrevic2015PMC.pdf

- The feasibility of dynamically granted permissions: Aligning mobile privacy with user preferences

  https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7958626

- Turtle Guard: Helping Android Users Apply Contextual Privacy Preferences

  https://www.usenix.org/system/files/conference/soups2017/soups2017-tsai.pdf

- SmarPer: Context-Aware and Automatic Runtime-Permissions for Mobile Devices

  https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7958625

- ConXsense – Automated Context Classification for Context-Aware Access Control

  https://dl.acm.org/doi/pdf/10.1145/2590296.2590337

- FlowIntent: Detecting Privacy Leakage from User Intention to Network Traffic Mapping

  https://arxiv.org/pdf/1605.04025.pdf

- AutoPer: Automatic Recommender for Runtime-Permission in Android Applications

  https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8754004

- Contextualizing Privacy Decisionsfor Better Prediction (and Protection)

  https://dl.acm.org/doi/pdf/10.1145/3173574.3173842

- Keeping Context In Mind: Automating Mobile App Access Control with User Interface Inspection

https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8737510

- iprivacy: Image privacy protection by identifying sensitive objects via deep multi-task learning
  https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7775034

Others:

- Crowd-ml: A privacy-preserving learning framework for a crowd of smart devices
  https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7164888

- Blind Data Classification Using Hyper-Dimensional Convex Polytopes
  https://www.aaai.org/Papers/FLAIRS/2004/Flairs04-090.pdf

- Deep learning with differential privacy
  https://arxiv.org/pdf/1607.00133.pdf%20