Published in Towards Data Science

Dr. Santanu Bhattacharya
Jan 27, 2019 · 5 min read · Listen

The New Dawn of AI: Federated Learning

Democratized and Personalized AI, with Privacy by Design

We predict growth and adoption of Federated Learning, a new framework for Artificial Intelligence (AI) model development that is distributed over millions of mobile devices, provides highly personalized models and does not compromise the user privacy. The model development, training, and evaluation with no direct access to or labeling of raw user data. In markets such as India where hyper-personalisation and contextual recommendation will be key in driving app adoption or e-commerce purchases, the bet is that federated learning will play a key role in 2019. A new dawn for the AI world and a new hope!

Disclaimer: the author is an investor and advisor in the Federated Learning startup S20.ai. In case you are wondering, S20 stands for “Software 2.0”.

. . .

The emerging AI market model is dominated by tech giants such as Google, Amazon and Microsoft, who offer cloud-based AI solutions and APIs. This model offers users little control over the usage of AI products and their own data that is collected from their devices, locations etc. In the long run, such a centralized model is not good for the society or the market, as it could lead to monopolization of only a few strong players. Eventually, it would limit the participation of smaller companies or even larger enterprises in AI innovation, as well as lack of interoperability and interpretability of decisions driven by AI systems. Luckily, as the spring of AI emerges in 2019, we are seeing the beginning of a decentralized AI market, born at the intersection of on-device AI, blockchain, and edge computing/IoT.

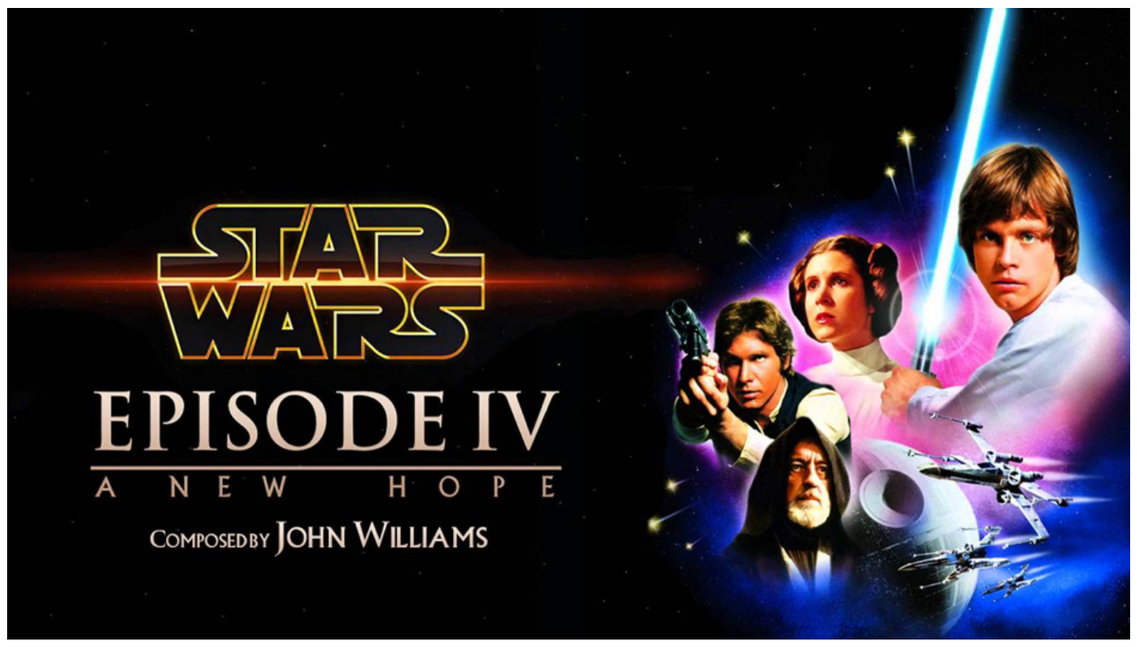

Figure 1: The new dawn of AI: a new hope. Photo Credit: Lucasfilm/ Disney

Standard Machine Learning Models require centralizing of the training data on one machine or in a datacenter. For example, when an ecommerce start-up wants to develop a model to understand its consumer’s propensity to purchase a products, it runs the models on the data collected from its website or app. Such data may include the time spent on a particular product page, products bought together, products browsed but purchased etc. Typically anywhere between 50 to even up to 1000’s of data points are collected on every user, over a period of time. Such data are passed and sent over to a centralized data center or machines for computation.

Recently, a new approach has been considered for models trained from user interaction with mobile devices: it is called *Federated Learning*. Federated learning distributes the machine learning process over to the edge. It enables mobile phones to collaboratively learn a shared model using the training data on the device and keeping the data on device. It decouples the need for doing machine learning with the need to store the data in the cloud.

What is Federated Learning?

While the comparisons may be somewhat simplistic, the history of computing may be a decent proxy to what Federated learning is all about. In the early days of information technology, we had large mainframes doing the heavy lifting of most of the computing. Eventually, we moved to a client server framework where the computes were distributed between central server(s) and multiple client computers.

The Federated Learning architecture deploys a similar model. Machine learning models, instead of being computed on large, centralized machines, are distributed over mobile devices for computation. This model of computing, while being theoretically possible, would not have been practical in the past, since computational abilities of mobile phone were very limited for running any ML model.

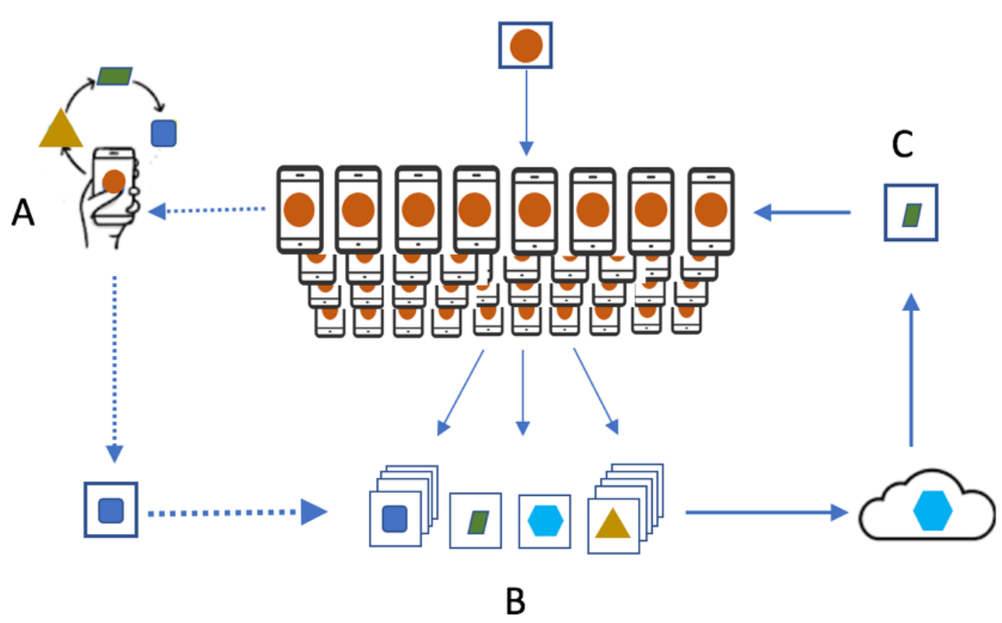

Figure 2: A user's phone personalizes the model locally, based on her usage (A). Many users' updates are then aggregated (B) to form a consensus change © to the shared model. This process is then repeated

However, something changed in the mid-to-late 2018s. As a billion plus smartphones, equipped with AI chips and significant computing power, starting with Samsung S9, or Apple X series, get shipped in the next 3–5 years, many of the ML models will be able to run locally on these mobile devices.

Functionally, a mobile device that is a part of a FL computing architecture, downloads a model that is meant for running on mobile devices. It then runs the model locally on the phone and improves it by learning from data stored there. Subsequently, it summarizes the changes as a small update, typically containing the model parameters and corresponding weights.

The update to the model is then sent to the cloud or central server using encrypted communication, for example, homomorphic encryption (HE). This update is then averaged with other user updates to improve the shared model. Most importantly, all the training data remains on user's device, and no individual updates are identifiably stored in the cloud.

Federated Learning allows for faster deployment and testing of smarter models, lower latency, and less power consumption, all while ensuring privacy. Also, in addition to providing an update to the shared model, the improved (local) model on your phone can also be used immediately, powering experiences personalized by the way you use your phone.

What will Enable the Growth of Federated Learning?

In the next few years, model building and computation on the edge, based on Federated Learning and secured with Homomorphic Encryption will make a significant progress. As one billion plus smartphones, equipped with AI chips and possessing significant computing power get into the market in the next 3–5 years, many of the ML models will be able to run locally on these mobile devices. Distributing the heavy duty analytics and computations over smartphones "on the edge", as opposed to central computing facilities, will drastically reduce time to develop data products such as hyper-personalized recommendation engines, e-commerce pricing engines etc. Enterprises will embrace a distributed machine learning model building framework for taking advantage of faster model

deployment and to provide quicker response to fast-changing consumer behaviour, besides a vastly reduced cost.

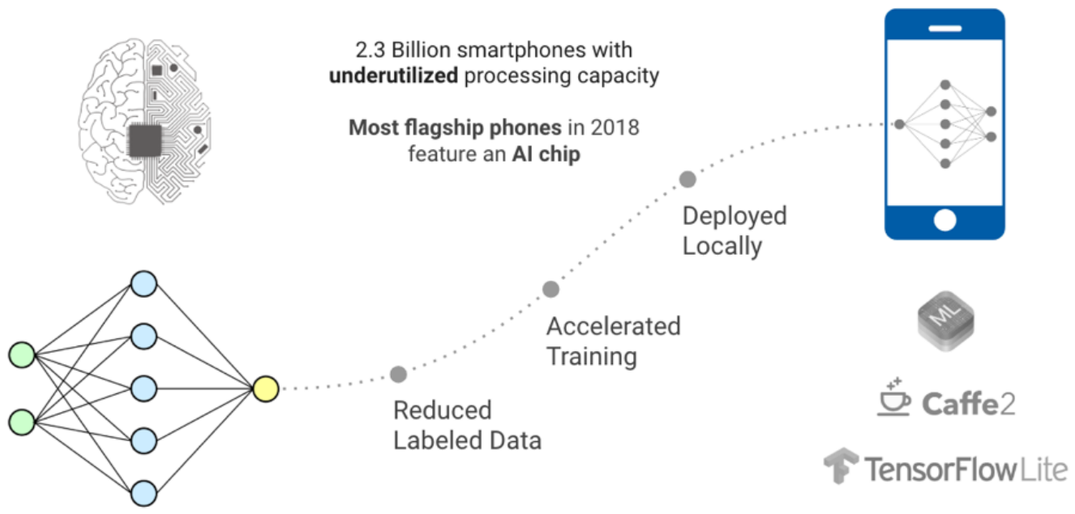

Figure 3: As a billion plus smartphones being equipped with AI chips and significant computing power get shipped in the next 3–5 years, Federated learning applications will grow

For the machine learning practitioners and enthusiasts, this paradigm shift provides an exciting opportunity to democratize AI. It also opens up new avenues for adopting new tools, and most importantly, a new way of thinking about solving large-scale ML problems.

Model development, training, and evaluation with no direct access to or labeling of raw data, will be challenging at first. However, in emerging markets such as India, where hyper-personalization and highly contextual recommendation engine will be key for driving say, app adoption, or e-commerce purchase, our bet is Federated Learning will play a key role in the future. We believe the user benefits of Federated Learning make tackling the technical challenges worthwhile.