Vanderbilt University

Tools and Techniques for Privacy-aware, Edge-centric Distributed Deep Learning

Ziran Min, Robert E. Canady

Uttam Ghosh, Aniruddha S. Gokhale

ziran.min,robert.e.canady,uttam.ghosh,
a.gokhale@vanderbilt.edu

Vanderbilt University
Nashville, TN

Akram Hakiri

akram.hakiri@issatm.rnu.tn

University of Carthage, ISSAT Mateur
Mateur, Tunisia

Unresolved problems in Edge-based Deep Learning

- Real-time needs of some edge-based applications
- The variable and long latencies between the edge and the cloud.
- The need to dynamically discover sensors and edge-based compute resources

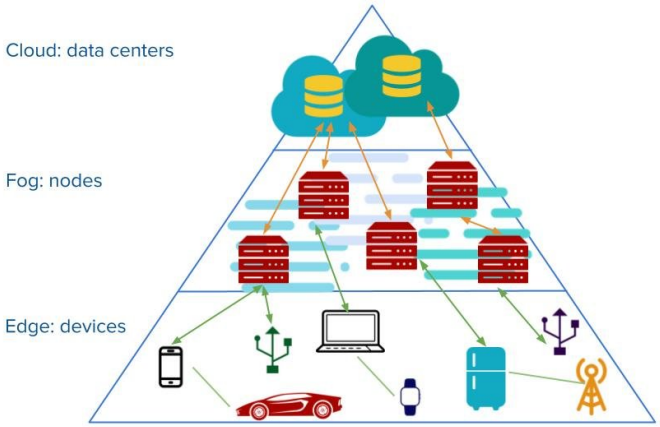

Figure 1: At the edge of navigating the cloud [1]

Figure 2: Autonomous cars [2]

Figure 3: Disaster response[3]

[1] Blog post: https://info.varnish-software.com/blog/edge-cloud-fog-computing
[2] Blog post: https://www.ansys.com/blog/challenges-level-5-autonomous-vehicles
[3] Abrahamsen, H.B. A remotely piloted aircraft system in major incident management: concept and pilot, feasibility study. BMC Emerg Med 15, 12 (2015). https://doi.org/10.1186/s12873-015-0036-3

Outline

- TECHNICAL CHALLENGES
  - Privacy-aware, edge resource discovery
  - Cohabiting model update and inferencing with other tasks on heterogeneous edge devices
  - Addressing the CAP dilemma and achieving consensus in federated machine learning
- PROPOSED SOLUTIONS
  - Privacy-aware Edge Resource Discovery and Deployment
  - Cohabiting and Distributing Model Update and Inferencing
  - CAP-driven Trade-offs and Blockchain-based Consensus
- Conclusion

TECHNICAL CHALLENGES

Challenge 1: Privacy-aware, edge resource discovery

- Highly distributed and uncontrolled edge resources
- Not all the resources can be discovered.
- Continuously training, updating, and inferencing learning parameters can lead to the leakage of users' private and sensitive data.

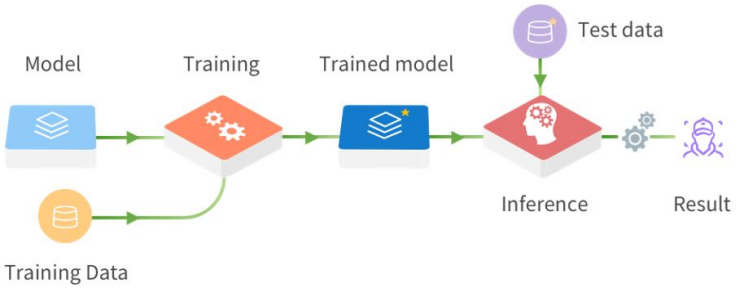

Figure 4: A Typical Deep learning process [4]

Novel approaches are needed to discover and deploy trusted edge resources.

[4] Blog post: https://blog.mellanox.com/2018/12/an-efficient-scale-out-deep-learning-cloud-your-way/

Challenge 2: Cohabiting model update and inferencing with other tasks on heterogeneous edge devices

- The discovered edge resources may not be all the same.
- Active devices may influence the size of the network
- Different edge resources may illustrate different execution times and energy consumption for the same task.

Novel approaches are needed to partition model update and inferencing tasks across the different resources

Challenge 3: Addressing the CAP dilemma and achieving consensus in federated machine learning

- Substantial uncertainty in resource availability.
- *Consistency Availability Partition Tolerance (CAP)* dilemma
- Model updates throughout the training process can reveal sensitive information.
  - A huge amount of aggregated data coming from multiple parties
  - Multiple parties increase the risk of the data breach

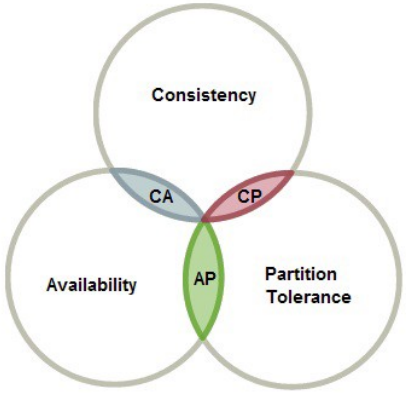

Figure 5: CAP dilemma [5]

A new collaborative scheme between untrusted federated edge parties is needed to enhance privacy-preservation

[5] Blog post: https://towardsdatascience.com/cap-theorem-and-distributed-database-management-systems-5c2be977950e

PROPOSED SOLUTIONS

Resolving Challenge 1: Privacy-aware Edge Resource Discovery and Deployment

- Three layers architecture
  - The top is the cloud computing layer
  - The middle is the edge computing layer
  - The bottom is the domain controller layer

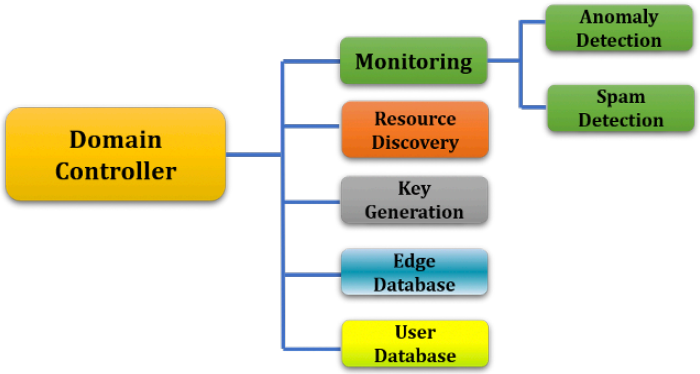

Figure 7: Functionalities of the Domain Controller.

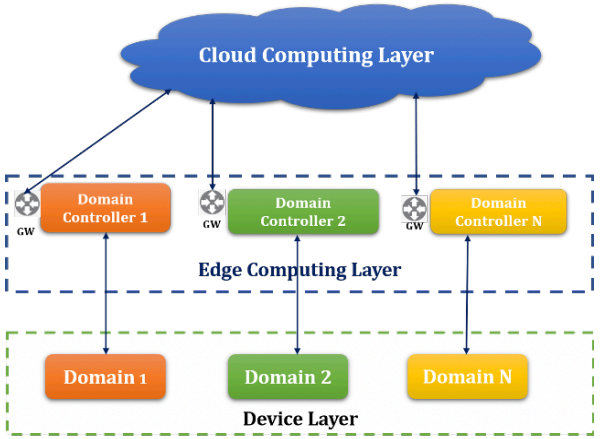

Figure 6: Proposed Resource Discovery Architecture.

- We introduce a domain controller (server) for each domain in the bottom layer.

Resolving Challenge 2: Cohabiting and Distributing Model Update and Inferencing

- Using an asynchronous training loop
- A data sharding policy is required by considering the actual states of the workers.
- Novel approaches are needed to partition model update and inferencing tasks across the different resource
  - Anticipate a low amount of participation
  - Tolerate heterogeneous hardware
  - Be robust to dropped devices in the network

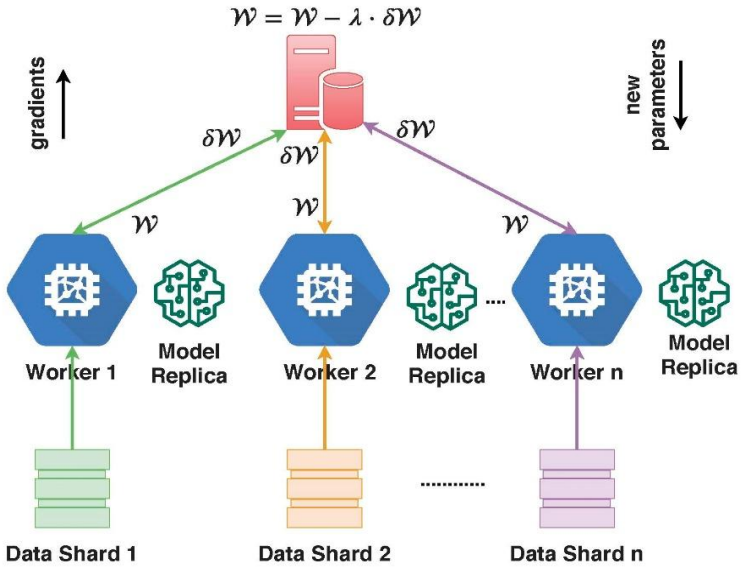

Figure 8: Parameter Server Architecture

Resolving Challenge 3: CAP-driven Trade-offs and Blockchain-based Consensus

- Hybrid consensus algorithm
  - Computation efficiency
  - Shared data reliability
  - Scalability
- Privacy-preserving homomorphic encryption scheme for the blockchain
- Blockchain-based data distribution and training platform

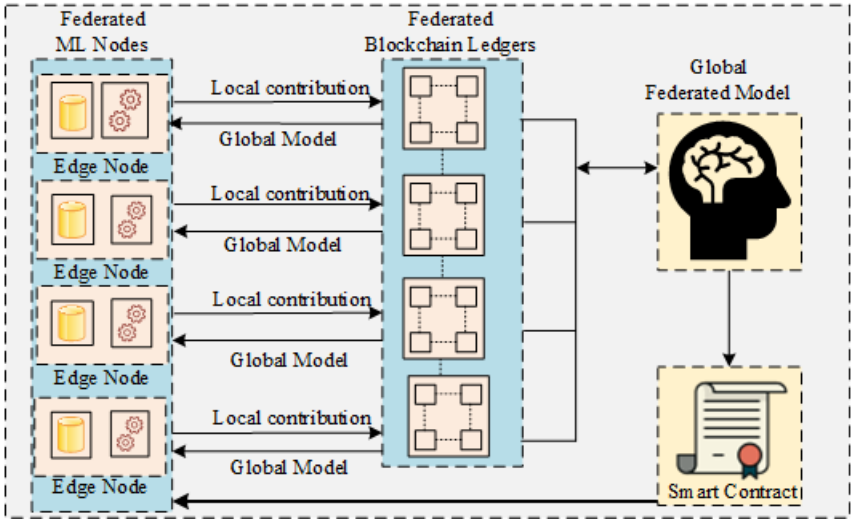

Figure 9: FedML Architecture

Conclusion

- We illustrated several unresolved problems in Edge-based DL.
- We analyzed the potential challenges in exploring Edge-based DL.
  - The need to discover the right resources
  - Heterogeneity in resource types
  - Increased incidences of failures and network dysconnectivity
  - Preserving privacy of data used in ML tasks
- In the future, we will demonstrate a systematic approach to real-time, privacy- aware distributed machine learning on heterogeneous edge devices.
- Discussion points:
  - Blockchain and distributed consensus in Deep Learning

Thank you for listening!

Any Questions?