A distributed deep learning approach with mobile edge computing for next generation IoT networks security

Shailendra Rathore
Pradip Kumar Sharma
Heena Rathore

Rathore, S., Sharma, P.K. & Rathore, H. (2023) 'A distributed deep learning approach with mobile edge computing for next generation IoT networks security'. In: *2023 World Conference on Communication & Computing (WCONF): proceedings*. IEEE , 2023 World Conference on Communication & Computing, Raipur, India, 14-16 July 2023.
DOI: https://doi.org/10.1109/WCONF58270.2023.10235095

A Distributed Deep Learning Approach with Mobile Edge Computing for Next Generation IoT Networks Security

Shailendra Rathore
Division of Cybersecurity, School of Design and Informatics
Abertay University
Dundee, Scotland, UK
s.rathore@abertay.ac.uk

Pradip Kumar Sharma
Department of Computing Science
University of Aberdeen
Aberdeen, UK
pradip.sharma@abdn.ac.uk

Heena Rathore
Department of Computing Science
Texas State University
Texas, USA
heena.rathore@txstate.edu

***Abstract*— Along with recent development in Next Generation IoT, the Deep Learning (DL) has become a promising paradigm to perform various tasks such as computation and analysis. Many security researchers have proposed distributed DL supporting DL task at the IoT device level to deliver low latency and high accuracy. However, due to limited computing capabilities of IoT devices, distributed DL is failed to maintain Quality-of-service demand in practical IoT applications. To this end, BlockDeepEdge, a Blockchain-based Distributed DL with Mobile Edge Computing (MEC) is proposed where MEC supports the lightweight IoT devices by delivering computing operations to them at the edge of the network. The blockchain provide a secure, decentralized and P2P interaction among IoT devices and MEC server to carryout distributed DL operation.**

Keywords—IoT, 5G, Distributed Deep Learning, Mobile Edge Computing, Blockchain

I. INTRODUCTION

Next Generation IoT supports computation and analysis of data produced by sensors and devices connected over the next generation wireless network (5G) [1]. It relies on various machine learning methods to deliver an automates analytical model that consists of pre-programmed or algorithms to iteratively learn the hidden insight of data for data analysis. Along with the rapid development of IoT, Deep Learning (DL) has become an emerging machine learning method that provide a reliable mining (i.e., extraction and representation of hidden patterns) of real-time sensing data to support efficient data analysis in IoT including tasks such as object detection, speech recognition and many more [2]. Many IoT applications, object detection, speech recognition has employed the DL approach for data classification, data labeling, and prediction of future trends. However, DL approach requires huge amount of data and incurred high computational overhead to obtain higher accuracy for underlying DL task in IoT. Moreover, the boom of DL in IoT also meets significant challenges, such as requirement of huge amount of data to obtain higher accuracy for underlying DL task in IoT. Due to the heterogeneous devices and dynamic network conditions, the huge amount of data is stored on the central servers, which bring huge costs of data storages and bandwidth, incurred high computational overhead, and fail to obtain low latency requirement. In addition, privacy leakage is an issue as third party, i.e., cloud or edge server can leak the private data of IoT devices or perform data falsification [3]. Recently, Blockchain-based Distributed DL (Blockchain-DDL) has been proposed as a promising decentralized solution and has been applied in various distributed scenarios [4], [5]. The Distributed DL distributes the computation load of the overall DL task among several parties (i.e., multiple parties upload their local model updates to the parameter sever and download a global model update from the server) participating in the data analysis process. The Blockchain provides security and privacy with the help of a distributed public ledger, which records transactions among multiple parties in a public or private peer-to-peer network. Leveraging Blockchain -DDL concept, Weng et al. [4] proposed a privacy-preserving DL with Blockchain to prevent against malicious server or mistrustful participants who may damage or fraudulent the overall DL model i.e., collection of incorrect model update or parameter updating. The proposed approach relies on a value-driven incentive mechanism based on Blockchain where incentives are given to mistrustful parties participating in the DDL task, sharing model updates to accomplish the DL task in a secure manner. Similarly, our recent research [5] proposed a Blockchain - based secure DL, where distributed DL operations are carried out at the IoT device level and Blockchain is leveraged to perform transaction among IoT devices ensuring the confidentiality and integrity. However, due to the limited computing capabilities of parties and IoT devices, the blockchain-based DDL is failed to maintain Quality-of-service demand in practical IoT applications, where lightweight IoT devices such as wearables devices, tablets, and mobile phones are employed.

To support lightweight IoT devices, a Mobile Edge Computing (MEC) has become very prominent these days that delivers the computing capabilities at the edges of the network and provides computing operations to the users or IoT devices [6]. The Small Base Stations (SBSs) deployed with MEC servers lower the storage costs and the bandwidth requirement and offers low-latency services to end devices (users). Li et al. [7] proposed a DL paradigm at the edge network on IoT platform that improves network performance by reducing network traffic from IoT devices to centralized cloud and maximizing the count of operations at the MEC servers. Similarly, authors in [8] combined DL and edge computing to design a robust mobile crowd sensing framework, where DL supports the data validation operation and edge computing signifies local processing. Recently, the

MEC is integrated with the blockchain to provide full play of its benefits and mitigate the significant issues. Xiong et al. [9] employed MEC concept in mobile blockchain applications, where an IoT blockchain mining operation is offloaded to MEC server by using an efficient edge resource management strategy. Pan et al. [10] applied a permissioned blockchain technique with the MEC to associate the edge cloud resources with each IoT device's account in an IoT framework. The authors demonstrated that the integration of blockchain with MEC can be achieved with an acceptable usage and reasonable cost to gain the security advantages of blockchain.

Given that the Blockchain-based Distributed DL overcomes challenges in conventional DL paradigm by integrating DL and Blockchain, and MEC can support the lightweight IoT devices by delivering computing operations to them at the edge of the network. In this paper, we propose BlockDeepEdge, a Blockchain-based Distributed DL with MEC to deliver a secure and decentralized DL operation considering the low computing capability of an IoT device and requirement of a low latency on IoT platform.

II. BlockDeepEdge Architecture

As shown in Fig. 1, a Blockchain-based Distributed DL approach is works upon a layered architecture consisting of four layers: Device, Small Base Station (SBS), MEC, and Cloud layer. The cloud layer leverages several Virtual Machines (VMs) and supports scalable computing resources to host the DL models. The MEC layer are equipped with MEC servers and functions like the cloud at the edge of the network by configuring VMs with DL models. The MEC server obtains a set of local updates (i.e., gradients of local DL models) generated by its surrounding devices via associated SBSs and carry out pre-processing and computation task on the local updates to generate a global update (i.e., average of local updates). Here, a MEC server processes the local updates from its associated SBSs. The SBSs act as local agents that support their associated devices in preparing local DL model (i.e., offloading the DL task) and transferring the generated local updates to their associated MEC sever. The IoT devices, such as smart phones, tablets, and wearables devices are geographically distributed and can connect to their nearby SBS through Internet (5G network) to offload DL tasks. The key modules of the proposed architecture can be described as follows:

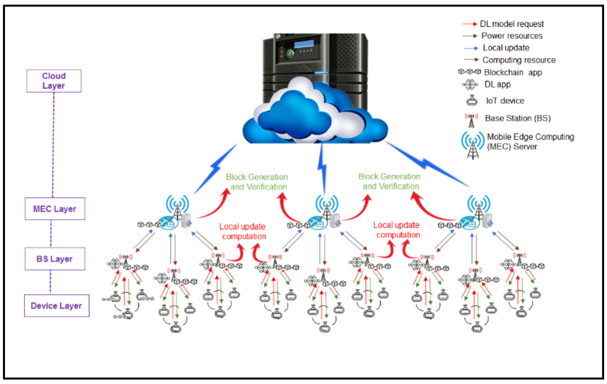

Fig. 1. Architectural design overview of the BlockDeepEdge

a) End devices: The end devices consist of different kinds of devices, such as tablets, smartphones, and so on. In order to obtain DL model for performing the various big data analysis tasks, such as object detection, prediction, the devices can send requests of DL model and required power resources (i.e., to execute the blockchain and DL operation) to the associated SBSs via internet. The requests are satisfied by SBSs connected through blockchain and paid incentives to the blockchain network.

b) SBSs: An SBSs are associated with a group of devices in their premises and responsible to provide network services to the connected devices. However, due to the scarcity of resources such as computational power, training data, the SBSs face a challenge of generating an accurate DL model (i.e., Global update). To mitigate this challenge, the SBSs can request computing tasks from MEC servers that have reasonable number of resources after paying incentive to them in the blockchain network.

c) MEC Servers: They are equipped with resource rich computing capabilities and work as service providers to provide their resources and computing capabilities in service of preparing an accurate DL model (i.e., Global update). Additionally, they obtain incentive from the SBSs in the blockchain in response of providing an accurate DL model to them.

d) Blockchain Network: The blockchain network provides an immutable distributed ledger to record and transfer transactions (i.e., local and global update) in a decentralized, secure manner among all entities end devices, SBSs, and MEC servers in the layered architecture. A private blockchain is employed in the proposed architecture that delivers low latency with higher throughput (i.e., significantly required for DL task in IoT) by providing control of application owners over the blockchain and avoid pure peer-to-peer control unlike the public blockchain.

III. CONCLUSION

In this paper, we studied the problem and challenges of Distributed deep learning in Next Generation IoT. To mitigate the challenges, we proposed BlockDeepEdge, a Blockchain-based Distributed DL with Mobile Edge Computing wherein MEC servers are employed to provide their communication and computing resources for supporting DL operation at the lightweight IoT devices and blockchain delivers a secure, decentralized and P2P interaction among IoT devices and MEC servers to carryout distributed DL operation.

Acknowledgment

References

[1] S. Rathore, J. H. Park, and H. Chang. "Deep learning and blockchain-empowered security framework for intelligent 5G-enabled IoT," IEEE Access, vol. 9, pp. 90075-90083, 2021.

[2] M. Q. Tran, et al. "Reliable Deep Learning and IoT-Based Monitoring System for Secure Computer Numerical Control Machines Against Cyber-Attacks With Experimental Verification," IEEE Access, vol. 10, pp. 23186-23197, 2022.

[3] K. Xie. et . al. "An efficient privacy-preserving compressive data gathering scheme in WSNs," Information Sciences, vol. 390, pp. 82-94, 2018.

[4] J. S. Weng, J. Weng, M. Li, Y. Zhang, and W. Luo, "DeepChain: Auditable and Privacy-Preserving Deep Learning with Blockchain-based Incentive," IACR Cryptology ePrint Archive, vol. 2018, pp. 670-679, 2018.

[5] S. Rathore, J. H. Park. "A blockchain-based deep learning approach for cyber security in next generation industrial cyber-physical systems." IEEE Transactions on Industrial Informatics vol. 17, no. 8, pp. 5522-5532, 2020

[6] Y. Chen, W. Gu, and K. Li. "Dynamic task offloading for internet of things in mobile edge computing via deep reinforcement learning." International Journal of Communication Systems, 2022.

[7] H. Li, K. Ota, and M. Dong. "Learning IoT in edge: Deep learning for the Internet of Things with edge computing." IEEE network, vol. 32, no. 1, pp. 96-101, 2018.

[8] Z. Zhou, et. al., "Robust mobile crowd sensing: When deep learning meets edge computing, " IEEE Network, vol. 32, no. 4, pp. 54-60, 2018

[9] Z. Xiong, Y. Zhang, D. Niyato, P. Wang., & Z. Han, "When mobile blockchain meets edge computing," IEEE Communications Magazine, vol. 56, pp. 33-39, 2018

[10] J. Pan, J. Wang, A. Hester, I. Alqerm, Y. Liu, and Y. Zhao, "Edgechain: An edge-iot framework and prototype based on blockchain and smart contracts, " IEEE Internet of Things Journal, vol. 6, no. 3, 2018.