March 2022
Volume 2
Issue 3

pixels

Department of Computer Science and Engineering

ANNUAL SPORTS & GAMES MEET 2022

On 11 March 2022, the Department of Physical Education organized Annual Sports and Games Meet 2022 in the college ground. The National Skating Champion and Trainer, Mr. Siyad K. S. was the chief guest. The whole playground was adorned with flags. All students and faculty of CSE department participated in the Meet. Ms. Sherin K. A. and Ms. Anagha Pradeep, Assistant Professors of CSE Dept. were awarded 2nd and 3rd prizes respectively in the walking competition held for faculty. The prizes were distributed by Dr. M. Sivanandan (Chairman), Prof. K. S. Pradeep (Manager), Mr. V. P. Asprasad (Treasurer) and Dr. Sagini Thomas Mathai (Principal).

Ms. Anakha Krishna C. R.(2018 - 2022 batch) got first prize in both 4x100 m relay and Long jump. Ms. Sanjana Sajeevan (2018-2022 batch) got first prize in 4x100 m relay. Ms. Merin Benny (2018 - 2022 batch) got third prize in Shotput. The prizes were distributed by Dr. Sagini Thomas Mathai (Principal).

SNGIST
GROUP OF INSTITUTIONS
E-mail: sngistcse18@gmail.com
www.sngist.org
04842887000
9947281122

HOLI CELEBRATION @ 2022

Holi is a popular ancient Hindu festival, of Spring, the festival of colors or the festival of Love. The festival celebrates the eternal and divine love of Radha & Krishna. It also signifies the triumph of good over evil. The SNGIST campus was decorated for the Holi Celebration. The celebration held on 18 March 2022 was coordinated by final year students of B. Tech. All the students and faculty participated in a jovial mood befitting the occasion.

PLACEMENT

Ms. Rakendhu Ravi (2018-2022 batch) got placed as Associate, Sutherland, Kochi.

Ms. Sneha K. J. (2018 - 2022 batch) got placed as Associate, Sutherland, Kochi.

Ms. Delna K. J. (2018-2022 batch) got placed as System Engineer, Infosys.

Hearty Congratulations to Rakendhu Ravi, Sneha K. J. and Delna K. J.

ELITE APTITUDE

On 17 March 2022, the Department of CSE started Placement Training for S8 (2018 - 2022 Batch) students. Mrs. Sherin K. A., Assistant Professor, CSE was the resource person. She covered the topic - Age, Profit & Loss and Time. The training provided the right platform to develop and sharpen the pre - placement skills for students. The students were trained to develop aptitude which, in turn, equip them for the recruitment process.

WORKSHOPS

Agamya Pramod E. P, Asst. Prof., CSE attended a FDP on *Advances in Natural Language Processing using AI*, organized by Vimal Jyothi Engineering College, Kannur during 14-18 March 2022.

TECH SAVVY

Ms. Sanjana Sajeevan (S8 CSE)

DECENTRALIZED DEEP LEARNING FOR MULTI-ACCESS EDGE COMPUTING: A SURVEY ON COMMUNICATION EFFICIENCY AND TRUSTWORTHINESS

Deep learning (DL) was first proposed to solve problems where a set of training data was collected for centralized data processing. In recent years, with the rapid advancement in this field, its applications have extended to various industries, benefiting people's lives. However, collecting and transmitting such enormous data into centralized storage facilities is usually time - consuming, inefficient, and with privacy concerns. Limitations in network bandwidths and so on could bring in high latency. Moreover, the risk of personal data breaches co related with data transmission to a centralized computing resource causes data privacy concerns. Especially with the increase of data privacy awareness in society, legal restrictions such as the General DataProtection Regulation (GDPR) have been promoted making such a centralized framework even impractical.

Decentralized deep learning (DDL) such as federated learning and swarm learning as a promising solution to privacy-preserving data processing for millions of smart edge devices, leverages distributed computing of multi-layer neural networks within the networking of local clients, whereas, without disclosing the original local training data. Notably, in industries such as finance and healthcare where sensitive data of transactions and personal medical records is cautiously maintained, DDL can facilitate the collaboration among these institutes to improve the performance of trained models while protecting the data privacy of participating clients. In this survey paper, we demonstrate the technical fundamentals of DDL that benefit many walks of society through decentralized learning. Decentralized deep learning (DDL) as a key enabler of the Multi-access Edge Computing benefits society through distributed model training and globally shared training knowledge. However, crucial fundamental challenges have to be overcome in the first place to make DDL feasible and scalable, which are decentralization techniques, communication efficincy, and trustworthiness.

The concept of decentralized deep learning (DDL) was first proposed to facilitate the training of a deep network with billions of parameters using tens of thousands of CPU cores. A few years later, the famous federated learning (FL) was proposed by Google, allowing privacy-preserving collaborative learning among edge devices by leveraging on-device model training and trained model sharing. For one thing, local model training greatly reduces the latency in a centralized framework. Another important point is that a large system consisting of thousands of clients improves its perfo-rmance by aggregating the results from local model training, without disc-losing raw training data.

Despite the success of FL, in real life, a participating local device typically necessitates certain qualifications for efficient local model training. Limitations in device memory and computation capability can greatly increase the local training time of a client, and network bandwidth limitations can result in the increase of clients' waiting time for transferring models thus causing a delay in an FL training cycle. Even in a decentralized frame-work like FL, an attacker still can compromise systems by injecting a trojan into either a client's local training data or its local model,and such an attack can further expand its influence to other clients through model sharing. In other cases, an attacker could even steal information from clients by observing the transmitted model gradients. To overcome these threats, defense strategies aiming to improve systems robustness and detect malicious behaviors are applied in FL. To this end, there are three pillars for the development of scalable decentralized deep learning covering FL technical fundamentals, communication efficiency, and security and privacy (trustworthiness).

In multi - access edge computing, decentralized deep learning (DDL) is considered to facilitate privacy - preserving knowledge acquisition from enormous various types of edge data. This survey provides an overview of DDL from two novel perspectives of communication efficiency and trustworthiness, offering state-of-the-art technologies to tackle challenges in leveraging DDL for social practices.

Federated learning as a classical solution to data privacy in centralized learning, aims to leverage local model training for collective machine learning among multiple clients. Whereas, real-life challenges such as edge heterogeneity and adversarial attacks have greatly limited the capability and scalability of this technology. Given the capability limitation of an edge device the convergence of a complicated model is costly and time consuming. A more compatible architecture appears to be split learning, which brings the gap between a centralized computing resource and decentralized data sources. Besides, data heterogeneity is a common problem when applying real world data, to this end, a more adaptive client selcction policy could benefit the fast convergence of FL. Moreover, the topic of trustworthiness in DDL has also been attracting an explosive growth of interest in recent years. We summarized the latest threat models in DDL based on various criteria and provided our novel taxonomy. Finally, we discussed some of the most promising defense strategies against such threats on FL. In addition, there are still other important topics not covered in this survey, including mitigating algorithmic bias in DDL and incentive mechanism for mobile device participation.

The current rapid advancement and broad application of deep learning in today's society necessitates building trust in such emerging technology. The privacy - preserving DDL offers practical solutions to future large-scale multi-access edge computing. The breadth of papers surveyed suggests that DDL is being intensively studied, especially in terms of privacy protection, edge heterogeneity, and adversarial attacks and defenses. Furthermore, the future trends of DDL put weight on topics such as efficient resource allocation, asynchronous communication, and fully decentralized frameworks.