LITERATURE SURVEY

|  |  |
| --- | --- |
| Paper Title | Findings |
| Distributed Intelligent Model for Privacy and Secrecy in Preschool Education | Application for preschoolers data - stochastic gradient descent to update the model parameters ( weight of neural network) - each agent estimates model parameters of self and neighbour nodes - uses Consensus algorithm which has two steps: communication step and adapt step - communication: shares weights and parameters of neighbour nodes - adapt: gradient descent based updation of model parameters - use of RSA encryption and decryption system on the weight values of the neural network shared between two neighbouring nodes in the network. No clear explanation on the what was the application |
| Privacy-preserving federated learning for scalable  and high data quality  computational-intelligence-as-a-service in Society 5.0 | Decentralized federated learning framework, DCIaaS (Decentralized Computational Intelligence as a Service), blockchain for secure data and model sharing, improving model accuracy for tasks like biomedical image classification and hazardous litter management. DCIaaS framework is applied to medical and smart city applications within the context of Society 5.0 - artificial intelligence and the Internet of Things, are integrated to improve the quality of life for individuals and society as a whole. Gives a comparison of performance between Federated Learning, Homomorphic encryption and Differential Privacy. One Global Iteration (GI) and One Local Iteration (LI) are terms used in the context of federated learning, specifically in the training process of machine learning models. These terms refer to the iterations performed during the training phase where global weights are updated based on the aggregation of local model updates. Uses Smart Contract to provide security for the weights generated from each iteration of learning. DCIaaS to include agent-based modeling on a decentralized blockchain network in future for autonomous vehicles. |
| A Survey on Federated Learning and its Applications for Accelerating Industrial Internet of Things | Explains about Federated Learning and its various applications in the Industry 4.0. The paper outlines the steps involved in FL, using industrial equipment health monitoring as an example of Horizontal Federated Learning (HFL), from model initialization to training and aggregation of local models, enabling collaborative learning without sharing raw data.  Describes the ideas and motivations described by various research papers that implements federated Learning for various industrial activities like Product Life cycle management, supply chain management, Target detection model to face challenges in AR technology. |
| Federated Transfer Reinforcement Learning for Autonomous Driving | Proposes an online federated RL transfer process for  real-time knowledge extraction where all the participant agents make corresponding actions with the knowledge learned by others, even when they are acting in very different environments. FTRL uses the Deep Deterministic Policy Gradient (DDPG) algorithm, where an RL agent interacts with a stochastic environment, making observations, taking actions, and receiving rewards. The training process within the FTRL framework consists of three main steps. Firstly, there is an online transfer process where knowledge is shared among RL agents as they interact with their respective environments. Secondly, each RL agent undergoes standard training and inference processes independently. Lastly, the FedAvg process aggregates the knowledge learned by all RL agents to improve the overall model performance. The framework's effectiveness is demonstrated through real-life collision avoidance systems on JetsonTX2 Remote Controlled cars and Airsim simulators, showcasing superior performance compared to non-federated local training processes. Doesn’t discuss much about privacy. Can induce the privacy concept by implementing this training collaboratively between multiple companies and the companies not compromising on their own agent’s data |

**Techniques:** Federated Learning and Block chain-based privacy techniques.

**Applications:**

* Supply chain data management for demand prediction based on warehouse and logistics data
* Object detection using in store cameras detect customer behavior, such as product interactions, to optimize store layouts