Task 2 Concept Paper

Student ID:20301393
Student Name: Fahim Ahamed Romit
Course Code:CSE449
Section: 1

Review: Sharing, Licensing, Buying, Selling, and Operationalizing ML Models: A Deep Learning-based Co-operative and Co-ordinated Security Use Case

URL: https://ieeexplore.ieee.org/document/10368564

1. Summary of the paper

1.1 Motivation/purpose/aims/hypothesis (1 pt)

The paper is about how we all want to share ML models among the different organizations in a cooperative way, but also adherence with GDPR and possibly CCPA. Its objective is to deliver a framework in Acumos with plug-and-play components for sharing, licensing and monetizing ML models across different verticals including cybersecurity. The idea is that by sharing the model instead of data it makes collaboration and respect easier in addition to getting a utility towards using models.

1.2 Contribution (1 pt)

The paper is about the Acumos Federation and Licensing, which would allow easier selling, purchasing or sharing of machine learning models. The system provides defense coordination against threats such as DDoS, allows for lucrative trades of ML models and privacy issues are tackled too. It speaks to how the platform is useful across a range of data privacy and collaborative intelligence applications.

1.3 Methodology (2 pts)

The methodology includes:
Setting up Acumos Federation: Authors of the paper have shown how the various instances of Acumos, being clients or vendors, federate amongst them for models exchange, peer connection as well as to establish SSL communication.

Monetization and Licensing: Describes the Acumos License Usage Manager (LUM), the mechanism by which model sales and usage rights may be monitored and licensed.

Use Case: DDoS Attack Classification Using the CICDDOS2019 dataset, train a random forest model to classify DDoS attacks.It employs a single model, shared between the three federated sites, in order to model interorganizational collaboration-Acumos instances-for better defense against DDoS attacks.

Model Deployment: The article concludes with the explanation of the deployment of models as microservices on platforms such as AWS or Kubernetes so that model consumers are capable of retraining and serving their own needs.

1.4 Conclusion (1 pt)

This paper is about how Acumos Federation and Licensing provide the methodical, scalable, and legally compatible way of sharing and operationalizing ML models amongst enterprises. Based on collaborative intelligence, this paradigm facilitates cooperation in solving mutual issues like cybersecurity and leads to improved solutions.

2. Critiques or Limitations

2.1 1st Critique/Limitation (1 pt)

It is difficult to understand the advantages of the Acumos platform over the existing ones because the paper does not compare performance, scalability, or security with other existing federated learning frameworks.

2.2 2nd Critique/Limitation (1 pt)

The exposition concerning the versatility of the framework is done too narrowly-it was focused on the problem of DDoS attack classification and partially considered its applications in other domains.

2.3 Third Remark/Restrictions (1 point)

The paper does not discuss the problems that may arise during the process of maintaining long-term federated links among different companies, important for real-world implementation, including technological compatibility, trust, and privacy problems.

3 Synthesis (2 pts): Potential applications/future possibilities/scopes/implications/complexities/applicability to the same/different domains.

3.1 1st potential/idea of a new/follow-up/extension paper

Secondary work can demonstrate how Acumos may be applied in other industries including banking and health care where data security has to be maximized. Comparing with other federated learning frameworks will be helpful to find what works well, when different cases are considered.

3.2 2nd potential/idea of a new/follow-up/extension paper

An even more detailed one might elaborate some of the solutions that parties engaged in long-term federated learning might employ to address some of the emerging trust and tech-related challenges. It may address how Acumos deals with security, compliance and the integrity of data over large timelines across many industries.