ACQUISITION INNOVATION RESEARCH CENTER

Collective Intelligence Decision Making via Dynamic Knowledge Graph with Trusted Cross-Organizational and Privacy Preserving Integration

INCUBATOR EXECUTIVE SUMMARY

JULY 2024

PRINCIPAL INVESTIGATOR
Feng Liu, *Stevens Institute of Technology*

CO-PRINCIPAL INVESTIGATOR
Xinyue Ye, *Texas A&M University*

STEVENS INSTITUTE OF TECHNOLOGY

TEXAS A&M UNIVERSITY

SPONSOR
Office of the Under Secretary of Defense for Acquisition and Sustainment

EXECUTIVE SUMMARY

Our objective is to develop a comprehensive decision-making framework that harnesses collective intelligence to effectively determine the optimal integration and collaboration mechanism for responsible agencies within the Department of Defense (DoD) when tackling complex tasks that entail cross-domain and cross-organizational operations. The framework will be based on privacy preserving and cross organizational federated learning to achieve the strategic goal of improved enterprise-wise interoperability. We aim to establish DoD domain specific knowledge graph (KG) aggregating data from multiple agencies of DoD without exchanging or sharing the data at each agency. To facilitate the interpretation of federated learning-based KG (Fed-KG), large language models (LLMs) under the federated learning paradigm are used and fine-tuned to understand the collaborative connections among all agencies within DoD.

Our team finished all the tasks for developing the DoD Fed-KG and further investigated the feasibility of fine-tuning LLMs under federated learning paradigm considering the data privacy constraint among different agencies within DoD. The data analysis, information retrieval, and visualization system design framework highlight the feasibility and effectiveness of federated learning approach on constructing enterprise level KG without sharing data among DoD agencies. The federated fine-tuning to enhance the domain specific understanding of LLMs while maintaining data privacy showcases the feasibility of building a domain specific privacy preserving LLM for DoD. The federated approach not only leverages diverse instructional data from multiple sources but also achieves competitive performance compared to established models like ChatGPT 4 and 3.5. The results underscore the potential of federated learning in overcoming the limitations of centralized data collection and paving the way for more secure and efficient training methodologies in the realm of natural language processing (NLP).

DISCLAIMER

The Acquisition Innovation Research Center (AIRC) is a multi-university partnership led and managed by the Stevens Institute of Technology and sponsored by the U.S. Department of Defense (DoD) through the Systems Engineering Research Center (SERC)—a DoD University-Affiliated Research Center (UARC).

This material is based upon work supported, in whole or in part, by the U.S. Department of Defense through the Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S)) and the Office of the Under Secretary of Defense for Research and Engineering (OUSD(R&E)) under Contract HQ0034-19-D-0003, TO#0285.

The views, findings, conclusions, and recommendations expressed in this material are solely those of the authors and do not necessarily reflect the views or positions of the United States Government (including the Department of Defense (DoD) and any government personnel), the Stevens Institute of Technology, or Texas A&M University.

No Warranty.

This Material is furnished on an "as-is" basis. The Stevens Institute of Technology and Texas A&M University make no warranties of any kind—either expressed or implied—as to any matter, including (but not limited to) warranty of fitness for purpose or merchantability, exclusivity, or results obtained from use of the material.

The Stevens Institute of Technology and Texas A&M University do not make any warranty of any kind with respect to freedom from patent, trademark, or copyright infringement.

SYSTEMS ENGINEERING RESEARCH CENTER

AIRC ACQUISITION INNOVATION RESEARCH CENTER

STEVENS INSTITUTE OF TECHNOLOGY 1870