Information and Networking Event
Horizon Europe 2023-2024 Calls
Co-Funded by the Government of India (DST)

HORIZON-CL4-2024-HUMAN-03-02
Explainable and Robust AI (AI Data and Robotics Partnership) (RIA)

- Title of talk LTIMindtree’s GenAI Expertise and Contributions
- Name of presenter Dr.ir. Vijay S. Rao
- Name of Organisation LTIMindtree Ltd.
- Country India/Netherlands
- Email: Vijay.Rao@LTIMindtree.com
- Web url https://www.ltimindtree.com/

About LTIMindtree

LTIMindtree

VISION:

Enable businesses and communities to flourish in a hyperconnected world

90K+ EMPLOYEES	$4.2B+ ANNUAL REVENUE
700+ GLOBAL CLIENTS	75% RENEWABLE ENERGY*

* For premises in India

TECHNOLOGY INCUBATION GROUP(TIG)- Powered by Global Technology Office

Charter

- To identify, incubate, scale
- Protect identified Next Gen Technologies
- Collaborate with research, industry, clients & academia partners
- Leverage Crystal insights.

Building Blocks

- Research and Technology CoE
- IP CoE

About Me

- Research Leader (principal director) responsible to incubate new technologies and drive research in TIG
- Ph.D. from TU Delft, NL, in computer science. An active researcher with over 60+ publications.
- Extensive industry experience as a solutions architect.
- Experience in building academia-industry partnerships, driving research programs to meaningful outcomes for the industry, have participated in writing and execution of national and EU funded projects.

LTIMindtree’s Research & Development Summary

38
Digital Platforms
co-created or created
are in use

74
CoEs established under
ODCs with global top 3
workforce

100
Research projects
Commercialized

41
ODCs
established for
Global Clients

18
Product
Innovations
Commercialized

1264
Process
Innovations
Implemented

20
Granted
Patents

52
PhDs Employed

28
Open Research &
Innovation Projects
Commercialized or
Impl.

3
% of the Workforce
engaged in
Innovation

1
% of the
Workforce
engaged in R&D

63
Scientific
Publications
contributed

35300
ER&D Workforce

Granted
Industrial
Design Rights

12
Sustainability &
Climate Change
Innovations
Commercialized
or Impl.

* - Last 30 months

Topics of Interest (highlighted) in Call Text

HORIZON-CL4-2024-HUMAN-03-02

Explainable and Robust AI (AI Data and Robotics Partnership) (RIA)

The need for **transparent and robust AI systems** has become more pressing with the rapid growth and commercialization of **generative AI systems** based on foundation models. Despite their impressive capabilities, **trustworthiness** remains an unresolved, fundamental scientific challenge. Due to the intricate nature of generative AI systems, understanding or explaining the rationale behind their outputs is normally not possible with current explainable AI methods.

Moreover, these models occasionally tend to ***'hallucinate', generating non-factual or inaccurate information***, further compromising their reliability.

The purpose is to advance AI-algorithms and innovations based on them that can perform safely under a common variety of circumstances, reliably in real-world conditions and predict when these operational circumstances are no longer valid. The research should aim at advancing robustness and explainability for a generality of solutions, while leading to an acceptable loss in accuracy and efficiency, and with known **verifiability and reproducibility**.

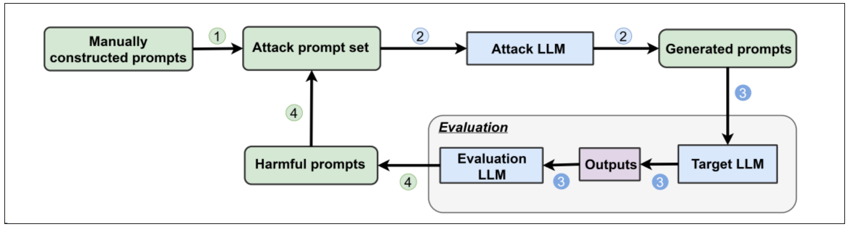
Our Contribution to the topic - Verifiability and Reproducibility

Development and Evaluation of Vulnerability Detection Framework

A Vulnerability Detection Framework (VDF) is used to detect the loopholes present in the LLM based applications through a set of innovative malicious prompts. The vulnerability result suggests how effectively the guardrails are implemented or how strong the LLM defending mechanism is where vulnerabilities include presence of bias and stereotypes, sensitive information disclosure, service disruption and hallucinations.

We would like build and evaluate a VDF through red teaming that can :

- Generate red teaming questions automatically based on given domain and vulnerability types like bias, data leakage, model theft etc. User can fine tune the questions before saving them in the database.
- Perform red teaming on the selected applications based on the above questionnaires.
- Publish vulnerability report for those applications which will show the loopholes present in the guardrails which requires applying more stringent techniques.



Our Contribution to the topic – Use Cases/Pilots

Multiple small LLMs instead of a large LLM

This is an ongoing area of research but since both the possibilities and potential are immense.

Potential for widespread adoption is quite apparent from the following statements

- LLMs are resource intensive and power hungry.
- Large LLMs are inaccessible to most enterprises other than the big few because of the high subscription/deployment cost.
- At 1/10th - 1/100th size of a large LLM, they together consume a fraction of resources of a large LLM, making it a green initiative.

Drawing inspiration from real-world project execution and planning, we propose a novel framework:

★

Building Specialized LLMs:

We'll create LLMs that mimic real-life roles in project teams, such as:

- **Manager LLM**: Specializes in planning, budgeting, and task delegation.
- **Architect LLM**: Focuses on non-functional requirements (NFRs) and system design.
- **Developer LLM:** Handles programming and bug fixing tasks.
- **QA LLM:** Manages test planning and execution..

★

Collaborative LLM Teams:

These specialized LLMs will be organized into project teams, like human teams. Each team will be:

- **Goal-Oriented:** Assigned a specific goal to achieve.
- **Structured:** Led by a Manager LLM and organized hierarchically.
- **Task-Driven:** The Manager LLM breaks down the goal into manageable tasks and assigns them to team members. Tasks can have subtasks and dependencies.

Our Contribution to the topic – Use Cases/Pilots

Drawing inspiration from real-world project execution and planning, we propose a novel framework:

★ **Comprehensive Planning:**

The entire process will be guided by a multi-faceted plan, including:

- **Project Plan:** Outlines the overall project roadmap.
- **Communication Plan:** Defines communication protocols within the team.
- **Decision-Making Plan:** Establishes how decisions are made within the team.
- **Conflict Resolution Plan:** Provides a framework for resolving disagreements.

★ **Defined Responsibilities:**

A "RACI Matrix" (Responsible, Accountable, Consulted, Informed) will clearly define roles and ownership within the LLM team.

★ **Automated Execution:**

By implementing this framework, we can create a system that automates complex goal execution through collaboration between specialized LLMs.

This biomimetic approach, inspired by real-world project management, has the potential to unlock a new era of efficient and effective LLM collaboration.

Impact & Next Steps

We bring expertise in -

- Our Innovation and Engineering DNA, inherited from our parent group, Larsen & Toubro, known as the 'Nation Builders'. Our innovation culture, supported by our incubation-to-industrialization framework, fit-for-purpose labs, and global presence, will propel early technology advancements.

- Deep AI expertise which integrates and leverages Advanced AI technologies to create Advanced Code Documentation Generation, architectural insights, code visualizations, accessibility across cloud platforms, etc. Some of our key IP's are:

NxT – Cloud Accelerator leveraging Snowflake for customers in manufacturing.	**TransEdge** – A transition platform which reduces operational effort by 20-35%	**Marketplace** – A centralized platform for hosting & managing Insurance GenAI apps.	**Pega Pega-based** banking platform with AI-powered Multilingual chatbot.
GenAI-based Metadata tagging solution.	Content-aware de-duplication IP leveraging various AI/ML techniques.	Document management façade aiding decision-making for Banking & Financial Institutions	

- Academia & Start-Ups ecosystem connects for e.g. TU Delft for this grant

- We are a software systems integrator, so we bring in the integration expertise to consortia

Together

We build on each other's strengths.

Looking forward to joining consortiums

We are a public large enterprise (LE) and can join consortias from both India (preferred) and EU

Let's get to the future, faster. Together.

Name : **Dr.ir. Vijay S. Rao**

Email Address: **Vijay.Rao@LTIMindtree.com**

Your Organisation: **LTIMindtree Ltd.**

The Nature Of Your Organisation E.G. SME, Academic Institution, Public, Private: **LTIMindtree is a Public Limited global technology consulting and digital solutions company**

The Country From Which It Operates**: India/NL**