THARINDU RANATHUNGA

Cork, Ireland tharindu.prf@gmail.com | +353851805078 | linkedin.com/in/tharind/ | GitHub | Scholar | Web

Agentic AI | Distributed Systems | Zero Trust | Cyber Physical Systems

Innovative Research Engineer with 10+ years of experience in designing, implementing, and deploying advanced software solutions, with a strong focus on **AI, distributed systems, decentralization, trust and security**. Led the technical direction and hands-on implementation of research initiatives across agentic AI, federated learning, data spaces, and distributed ledger technologies and IoT. Experienced in applying AI/ML techniques across diverse domains including manufacturing, energy management, supply chain, and FinTech. Specialized in end-to-end R&D workflows, from experimentation to scientific publications and **project delivery**. A collaborative team player, skilled in mentoring junior developers on AI best practices, software architecture, and agile methodologies. An open-source enthusiast passionate about building a future shaped by intelligent, decentralized systems.

- Agentic AI
- Machine Learning (ML)
- Federated Learning (FL)
- MCP and A2A
- LLM Inference & Optimising
- Edge AI & IoT
- Model Training & Fine Tuning
- Data Space Design
- Data Veracity and Trust
- Data Engineering
- Semantic Modelling
- Blockchain & DLT
- Smart Contracts
- Observability & Traceability
- ROS 2 / Robot Operating System
- Smart Manufacturing
- Microservices Architecture
- Agile/Scrum/Lean Methodologies
- Team Leadership & Mentorship
- Process Improvement
- Product Development

Related Research & Engineering Projects

- **Cobot Claw (2026 Feb – Present):** A multi-agent AI system enabling natural language control of UR collaborative robot arms and end-effectors no programming required. Designed for Smart Factory and industrial automation contexts.
  - **Architected a multi agent LLM-powered system** coordinated via MCP servers, with hardware-agnostic tool discovery supporting grippers, vacuum pumps, and custom end-effectors. (PyDantic AI, Llama Index, ROS 2, FastMCP, Ollama, OpenAI SDK, Anthropic SDK)
  - **Designed a safety-first autonomy layer** with a dedicated monitoring agent that continuously watches robot state and intervenes in real time, supporting both local inference (DGX Spark) and cloud APIs with a one-line config switch.
- **Agentic Cognitive Firewall (ACF SDK) (2026 March – Present):** An open-source Zero Trust security SDK implementing a policy-driven control layer for LLM-based agentic systems, developed under the C2SI open-source organisation. [Link]
  - **Designed the reasoning control plane architecture** to intercept and validate all inputs before they enter model context, blocking prompt injection, memory poisoning, context manipulation, and unsafe tool-output re-injection. (Python, GoLang)
  - **Defined the policy enforcement model** for production agentic deployments, establishing validation gates across the full agent input pipeline (Open Policy Agent, Rego)
- **CORDS: Collaborative Data Space for Manufacturing (Jan 2023 – Jan 2026)**: A decentralised **federated learning** platform built on top of the **International Data Space Protocol** aimed at self-sovereign cross party federated learning model training orchestration for manufacturing domain. [Link]
  - **Led the design & implementation of a Data Space** infrastructure (Python, JavaEE, SPARQL, Apache Camel, OPCUA, Docker, Kubernetes) and **semantic library** for machine learning workflows. (Python, RDF, Protege).
  - **Designed & Implemented** a **Decentralized & Federated Machine Learning** Service on top of the **Data Space Protocol** (SARIMA, Python, Kafka, Pytorch, Flower.AI, ML Flow).
- **Context Guard (Apr 2025 – Dec 2025)**: A PoC for policy enforcement & incentivising data providers on Model Context Protocol for Generative AIs using Smart Contracts.
  - **Designed a middleware for connecting MCP servers** that act as a policy enforcement and incentive layer (Python MCP SDK, MCP Use, OpenAI SDK, LangChain).
  - **Implementing the EVM & AVM compatible Smart Contract generator** for on chain policy enforcement (Solidity, OpenZapplin, ChainLink Data Feeds).

Career History & Achievements

Nimbus Research Centre | *MTU, Cork, Ireland*
Senior Researcher ***Jan 2023 – Present***

Scope of Duties: Software Development | Architecture Design Engineering & Deployment | AI Strategy | Federated Learning | Project Management | Technical Research & Documentation | Data Engineering | Scientific Publications | Funding Acquisitions

Key Contributions:

- **Led development of European and National Funded Projects** that advances cyber physical systems, IoT and decentralized ecosystems and AI driven innovations to address industry and societal challenges.
- **Spearheaded technical design and delivery of** Data Space Architectures, Distributed Ledger Integrations, Trust Management Services and Edge AI.
- **Defined AI/ML/FL/GenAI technical direction** aligning with the EU's vision for a human-centric AI-driven Smart Society, focusing on ethical, secure, and responsible AI adoption.

- **Collaborated with industry leaders** such as IBM, DELL, Gilead, and Analog Devices, as well as EU data space stakeholders like IDSA and GaiaX to pilot use cases, discuss architectural designs, and align project deliverables with EU standards.
- **Led Nimbus Research Centre's strategic** technical initiatives across three pillars: standardising development best practices and engineering workflows, building and growing an open-source community, and defining the Centre's **AI strategy and roadmap**.
- **Contributed to Horizon Europe funding acquisition** by developing technical work packages, defining research scope, and engaging industry and academic partners across consortium bids targeting cyber-physical systems, AI, and data space initiatives.

Researcher ***Apr 2019 – Dec 2023***

Scope of Duties: DLT Integrations | Machine Learning (ML) | Decentralised Ecosystems | Technical Project Management | Research & Development (R&D)

Key Contributions:

- **Drove R&D activities on DLT** to improve quality, overall efficiency, records management, and risk mitigation across supply chain, energy and facility management domains.
- **Accelerated the blockchain adoption** by developing a decision support toolkit to evaluate the necessity of blockchain integration and guide optimal design and technical decisions.
- **Conducted research on the convergence of DLT and AI** by leveraging trusted off-chain execution workflows to enhance trust and security in off-chain processes.
- **Supported creation of feasibility analyses, project requirement specifications, and white papers** in support of Research & Development activities.

Ceylon Computer Science Institute (C2SI)| Colombo, Sri Lanka | Remote

Open-Source Developer ***Dec 2017 – Present***

Scope of Duties: Open-Source Development | Project Management | Student Mentorship | Program Administration

Key Contributions:

- **Managed multiple open-source software projects,** such as ASSET and Bassa that provide low cost sustainable solutions to problems in developing countries.
- **Excelled in overseeing administration of Google Open-Source programs** (GSoC and GCI) and mentoring students on software development skills and techniques.
- **Steered adoption of open source and C2SI solutions** by organising outreach programs and promoting the technologies.

London Stock Exchange Technology | Colombo, Sri Lanka

Software Engineer ***Mar 2017 – Aug 2018***

Scope of Duties: Software Development | Code Writing & Review | Application Testing | Continuous Integration | Technical Reports

Key Contributions:

- **Implemented feature requests** and **addressing issues** in front running stock exchange product as per the clients requests.
- **Introduced rigorous automated testing practices** in controlled environments before going live, hence reducing software bugs and accelerating the software release cycle.
- **Led the implementation** of a code quality (dynamic & static) assessment tool for all the projects in the company.

OTHER CAREER HISTORY

Community Organiser | Google Developer Group – Cork, Ireland | Dec 2018 – Mar 2020

Manager | RSVP.NOW – Colombo, Sri Lanka | Jul 2015 – Mar 2019

Software Engineering Intern | 99X Technology – Colombo, Sri Lanka | Aug 2015 – Feb 2016

EDUCATION & CERTIFICATION

PhD in Electronic & Electrical Engineering |A DLT Based Trust Framework for IoT Ecosystems| Munster Technological University, Ireland | 2023

BSc (Hons) in Computer Science | University of Colombo School of Computing, Sri Lanka | 2017

Advanced Level, Information Technology | Anuradhapura Central College | 2011

TECHNICAL SKILLS

Languages: Python, Java, C, C++, Go, JavaScript

Agentic AI & LLMs: Multi-Agent Systems, LLMs, Fast MCP, LangChain, vLLM, Ollama, Pydantic AI, RAG, Prompt Engineering, Evals

ML & Data: PyTorch, Scikit-Learn, Flower.ai, MLFlow, Kafka, OPCUA, MQTT, Data Space Protocol

Robotics: ROS 2, Universal Robots (UR3e), OpenCV, Vision Language Models, NVIDIA Jetson

Blockchains: Hyperledger Fabric, Ethereum, Algokit, Chainlink, Caliper, Chaincodes, BigChainDB, Smart Contracts

Cloud & DevOps: Azure, GCP, AWS, Docker, Kubernetes, Swarm, CI/CD, Git

Frameworks/Tools: Flask, Node.js, Vue.js, D3.js, Elasticsearch, MEAN, Protégé, Grafana