



Dr. Prasad N. Golla

Founder, Aggi Technologies LLC • Plano, Texas

AI SECURITY • TRUSTWORTHY AI • SECURITY BY DESIGN • AI FOR REGULATED INDUSTRIES

Dr. Golla brings 20+ years in secure systems and cybersecurity to a simple question: can people trust the AI they are about to depend on? He conceived and architected Aggi ARIA (Aggi Responsible Intelligence Assessor), a platform that continuously tests how AI models and agents behave and produces the evidence that security reviews and audits ask for. A former research scientist and university instructor, he is known for making deep technical topics clear to business and general audiences.

Background

- Security and compliance engineering at Citi, Bank of America, Amazon Kuiper and Nokia
- Senior Research Scientist III, Alcatel-Lucent Corporate Research Labs
- 10+ granted U.S. and European patents across software, hardware and networking
- Ph.D. in Computer Engineering (dissertation: Kernel-User Multithreaded Architecture, sharing system resources efficiently while protecting the memory and execution integrity of the kernel, each process and each thread); M.S. in Electrical Engineering; M.S. in Computer Science; MBA in Technology Management and Entrepreneurship
- Taught networks, distributed computing and security at SMU's Lyle School of Engineering
- Winner, Richardson US Ignite Smart Cities Gigabit Reverse Pitch (2017), with Narender Ramireddy

Formats

- Keynotes and conference talks • panels • podcasts
- Workshops, including a live AI incident tabletop exercise
- Guest lectures and executive briefings

Audiences

- Founders and product teams building AI products
- CTOs, CISOs and compliance leaders
- Healthcare, financial services and public-sector leaders
- University students and faculty

Talk topics

Your AI passed the demo. Can it pass the hospital's security review?

Why promising AI products stall when they reach a regulated buyer, what reviewers actually ask, and how a small team gets ready before the deal is on the line.

Drift or noise? When your AI changes and nobody decided it

The same question can return different answers even with randomness turned off. How to tell engineering noise from genuine change in an AI's behavior, and why it matters wherever AI is trusted with real decisions.

When the agent goes wrong: an AI incident tabletop

A live walk-through of an AI incident, from the first strange complaint to the restart decision. Who decides, how fast, and with what evidence.

Security first, not bolted on

Building AI products with security as the first design principle, and moving fast with AI coding tools without skipping the engineering basics.

The \$20,000 prototype

AI tools have cut the cost of a working product from hundreds of thousands of dollars to tens of thousands. What founders still need to know about engineering, hosting and security to make that real.

Treat AI agents like user accounts

Every agent that can act on your systems deserves the same controls as an employee: an identity, limited access, a record of what it did, and a way to switch it off.

Invite Dr. Golla: prasad@aggicorp.com • pngolla@yahoo.com • (972) 351-3342 • [linkedin.com/in/drgolla](https://www.linkedin.com/in/drgolla) • aggicorp.com • Based in Dallas-Fort Worth; available in person or remote