

Sahiti Bommareddy

AI Agent Platform & Distributed Systems Engineer

b.sahiti@gmail.com · 404-786-1767 · linkedin.com/in/bsahiti · github.com/b-sahiti · b-sahiti.github.io · Mountain View, CA

SUMMARY

AI agent-platform architect with deep distributed-systems expertise, translating customer needs into reusable foundations for building, orchestrating, evaluating, and safely operating AI agents in production. At Ema, owns major platform areas that let agents connect to and act across enterprise systems and enable no-code creation of validated agent capabilities. Ph.D. in real-time Byzantine-resilient distributed systems.

EXPERIENCE

Ema — Software Engineer

Feb 2025–Present

Core agent platform: automated capability creation, integrations, agent runtime, workflows, governed execution, and reliability

- Own Ema's integrations and external-actions platform end to end and designed the agent that automatically turns API specifications, documentation, MCP servers, and other system descriptions into validated, test-run, publishable tools—moving integration delivery from weeks of engineering toward minutes without hand-written integration code.
- Designed Ema's multi-tool planning and execution agent and drove shared agent-harness capabilities for connecting to and acting across external systems, including planning and replanning, caller-scoped tools, dependency resolution, validation, model selection, multi-model evaluation, safeguards, and configurable human approval.
- Designed major parts of the governed action and tool-execution platform, including isolated script execution using Go services, containerized V8 isolates, sandboxing, network restrictions, identity boundaries, credential isolation, recovery, and per-call auditability.
- Owned event-driven and long-running agent execution across schedules, webhooks, polling, static and dynamically planned workflows, delegation, human-in-the-loop pause/resume, durable state, deduplication, re-drive, and partial-failure recovery.
- Designed MCP support for agents and Ema's no-code agent builder; drove migration of the connector catalog to Ema-native capabilities and established CI/CD, lifecycle, publication, authentication, permission, and quality controls that maintain and distribute it.
- Set technical direction through architecture reviews, closely mentored three engineers, and coordinated delivery across more than 15 geographically distributed engineers.
- Developed production observability and structured failure attribution across agent execution, reducing detection and resolution time by more than 70%.

Johns Hopkins University — Doctoral Researcher, Distributed Systems and Networks Lab

2019–2025

- Designed and built real-time distributed systems for critical-infrastructure protection, including power-grid substations, combining Byzantine fault-tolerant replication, resilient networking, and proactive recovery to preserve correct operation under compromised components and network attacks.
- Developed cybersecurity and machine-learning capabilities for critical infrastructure, including network intrusion detection and situational awareness integrated with resilient control systems.
- Developed methods for analyzing and tolerating compound cyber and physical threats to critical infrastructure; research received the IEEE SRDS 2024 Best Paper Award.
- Shipped open-source resilient systems including Spire, Prime, and Spines, with work delivered for deployment at Pacific Northwest National Laboratory (PNNL) and major power-grid vendors including GE, Siemens, and Hitachi Energy.

Aktrix Technologies — Software Engineer

2013–2016

- Led and expanded a team of nine performance engineers, owning test strategy, resource coordination, delivery risk, and training across client engagements.
- Pioneered an automated monitoring and analysis platform for multi-cloud environments, combining operational data pipelines with machine-learning-based load and resource prediction to reduce root-cause analysis effort and improve latency by approximately 2–5× across projects.

Deloitte — Performance Engineering Analyst

2011–2012

- Led performance testing across seven projects and developed approximately 40 performance test plans, partnering with application, database, and infrastructure teams to diagnose bottlenecks in geo-distributed systems.
- Optimized transaction latency to meet service-level objectives through traffic, CPU, memory, and utilization analysis; received an Applause Award for performance optimization and root-cause analysis.

TECHNICAL SKILLS

Agent architecture	Agent building, agent harness, multi-tool planning and execution, orchestration and delegation, dynamic replanning, skills and context, human-in-the-loop
Tools & evaluation	Automated no-code integration generation, MCP, controlled tool execution, model selection, multi-model and agent evaluation, dependency validation, load testing
Distributed execution	Workflow runtimes, durable state, event-driven systems, scheduling, webhooks, polling, idempotency, re-drive, partial-failure recovery, Byzantine resilience
Security & governance	Containerized V8 isolation, sandboxing, network restrictions, enterprise authentication, OAuth2, API keys, mTLS, credential lifecycle, permission scoping, approval gates, audit
Production systems	Python, Go, TypeScript, C, Java, PostgreSQL, REST/OpenAPI, Prometheus, Grafana, ClickHouse, CI/CD, incident response
Applied ML	PyTorch, TensorFlow, Hugging Face, intrusion detection, time-series and regression models, evaluation and regression analysis

EDUCATION

- Ph.D., Computer Science**, Johns Hopkins University, 2025 · Advisor: Yair Amir
- M.S., Computer Science**, Duke University, 2019
- B.Tech., Electronics & Communication Engineering**, Jawaharlal Nehru Technological University, 2011

SELECTED RESEARCH & OPEN SOURCE

- Real-time Byzantine resilience.** Built intrusion-tolerant infrastructure for protecting critical systems, including power-grid substations, combining proactive recovery, diverse replicas, and resilient networking with strict sub-cycle latency.
- Compound-threat resilience.** Developed methods for analyzing and tolerating combined cyberattacks and severe physical disruption in critical-infrastructure control systems.
- Selected publications.** [IEEE SRDS 2024](#); [IEEE PESGM 2024 \(ByzSec\)](#); [IEEE SRDS 2022](#); [ERSA at IEEE RTSS 2022](#); [DCDS at IEEE/IFIP DSN](#).
- Open-source systems.** [Spire](#)—intrusion-tolerant SCADA; [Prime](#)—Byzantine fault-tolerant replication with performance guarantees; [Spines](#)—resilient overlay messaging.

Full publications, open-source systems, and technical case studies: b-sahiti.github.io