DOI: doi.org/10.47363/JAICC/TechFusion2025/2025(4)10

TechFusion 2025 - AI, Cybersecurity, and Emerging Trends in Computer Sciences

Conference Proceedings November 27-28, 2025 (Virtual)

Building Intelligent Workflows with the Model Context Protocol (MCP): Servers, Clients, and Extensible Tools

Saravanan Prabhagaran

Virginia, USA

Abstract:

The Model Context Protocol (MCP) is transforming how AI systems interact with enterprise data, tools, and applications by establishing a standards-based, secure, and extensible communication layer between LLMs and external resources. This presentation introduces the core architecture of MCP, explains how servers expose structured capabilities, how clients (including Claude Desktop, custom apps, or headless agents) consume these capabilities, and how developers can build or integrate extensions-such as file systems, databases, APIs, automation frameworks, or custom logic.

Attendees will gain a practical understanding of message formats, transport layers, capability registration, authentication models, session state, and best practices for designing robust MCP servers. Real-world use cases-including workflow automation, data orchestration, RAG pipelines, and developer productivity tooling-demonstrate how MCP enables LLMs to execute actions reliably and safely. The talk concludes with hands-on patterns and design guidelines for creating scalable, secure, and production-ready MCP ecosystems.