

Keynote speech

Adaptive AI-Driven Cybersecurity: From Reactive Detection to Predictive and Continuously Learning Defense

Kalyana Krishna Kondapalli,
CEO - Mytecz, CTO - AiGlo
USA
kalyanakondapalli@gmail.com

ABSTRACT

Modern cyber threats evolve faster than static, signature-driven defenses can respond, creating a need for security architectures that can continuously observe, interpret, predict, and adapt to changing attack behavior. This talk presents an adaptive AI-driven cybersecurity approach that combines real-time security telemetry, machine-learning-based threat classification, behavioral anomaly detection, external threat intelligence, predictive risk assessment, and automated defensive response. The presentation explains how these capabilities can be organized into a continuous Observe–Detect–Analyze–Predict–Respond–Learn lifecycle for dynamic enterprise, cloud, and interconnected environments. Drawing on Kalyana Krishna Kondapalli’s published patent application, “Artificial Intelligence-Driven Cybersecurity System and Its Method Thereof,” and related IEEE research in adaptive threat intelligence and Internet of Medical Things (IoMT) cybersecurity, the talk examines architectural principles for moving cyber defense from reactive detection toward adaptive, continuously improving protection. It also discusses how supervised learning, unsupervised anomaly detection, predictive intelligence, automated response, and continuous learning can be coordinated within a unified security architecture while maintaining scalability across distributed and cloud-based systems.

Index terms— *Adaptive Cybersecurity; Threat Intelligence; Behavioral Anomaly Detection; Predictive Risk Assessment; Automated Response; Continuous Learning; Cloud Security; IoMT Security.*

Speaker’s short biography:



Kalyana Krishna Kondapalli is an IEEE Senior Member, 2026 Chair of the Lance Stafford Larson Student Award of the IEEE Computer Society, CEO of Mytecz, and CTO of AiGlo. He is an enterprise technology architect, AI and cybersecurity researcher, inventor, and engineering leader with more than 18 years of experience designing and modernizing large-scale systems across government, healthcare, financial services, e-commerce, automotive, SaaS, and technology environments. His expertise includes enterprise systems architecture, artificial intelligence, cybersecurity, cloud-native and distributed computing, intelligent automation, adaptive threat intelligence, and secure intelligent systems. He is the inventor of the published patent application “Artificial Intelligence-Driven Cybersecurity System and Its Method Thereof.” His recent IEEE-published research includes work on adaptive AI-driven threat intelligence and IoMT-centric cyber-attack-surface modeling. He also contributes to the professional community through IEEE leadership, technical reviewing, scholarly evaluation, conference activities, and mentoring.