



Advancing Cybersecurity Through Synergies of Agentic AI and High-Performance Computing

Satyadhar Joshi^{1*}

¹Alumus, International MBA, Bar Ilan University, Israel

ORCID ID: 0009-0002-6011-5080, satyadhar.joshi@gmail.com

*Corresponding author

DOI: <https://doi.org/10.63680/ijstate0625022.13>

Abstract

This paper explores the transformative role of Agentic AI in cybersecurity and its synergy with high-performance computing (HPC). We review recent advancements, challenges, and opportunities in deploying autonomous AI systems for threat detection, incident response, and risk management. The discussion is supported by a comprehensive analysis of recent key publications from industry and academia, highlighting trends and future directions in this rapidly evolving field. We review frameworks, adoption trends, and practical deployments, citing all relevant recent literature. We examine the core components, architectures, and applications of autonomous AI systems in threat detection, incident response, and risk management. The study highlights key technical terms, mathematical foundations, and algorithms essential for implementing these systems, supported by recent advancements from industry and academia. The paper also presents a layered reference architecture integrating HPC, cloud infrastructure, and edge computing to enable scalable and real-time cybersecurity solutions. Challenges, adoption trends, and future directions are discussed, emphasizing the need for secure and ethical deployment of agentic AI in critical systems.

Keywords: Agentic AI, Cybersecurity, High-Performance Computing, Autonomous Agents, Edge Computing, Cloud Security; Threat Modeling

1. Introduction

The convergence of Agentic AI and high-performance computing (HPC) is revolutionizing cybersecurity through autonomous threat detection, adaptive defense mechanisms, and real-time risk mitigation. The emergence of agentic AI systems marks a paradigm shift in cybersecurity [1], [2], [3], [4], [5]. These systems exhibit autonomy, adaptability, and proactive decision-making, surpassing traditional automation [5], [6]. The integration of AI agents into enterprise, defense, and cloud environments is accelerating [7], [8], [9], [10]. The integration of Agentic AI into cybersecurity represents a paradigm shift from reactive to proactive threat management [1]. These autonomous systems leverage large language models (LLMs) to plan, reason, and act independently across complex security tasks [5]. Concurrently, the convergence of AI and high-performance computing (HPC) is enabling unprecedented scalability for these solutions [11].