RADemics

Cyber Deception Strategies Using AI-Powered Honeypots and Generative Models for Attacker Behavior Profiling

R. Shobana, V. Pavithra, R. Baghia Laxmi

ANNAI MIRA COLLEGE OF ENGINEERING AND TECHNOLOGY, SRM INSTITUTE OF SCIENCE AND TECHNOLOGY, ST. JOSEPH'S COLLEGE OF ENGINEERING

Cyber Deception Strategies Using AI-Powered Honeypots and Generative Models for Attacker Behavior Profiling

[1]R. Shobana, Assistant Professor, Department of Computer Science and Engineering, Annai Mira College of Engineering and Technology,(Affiliated to Anna University) , Arappakkam, Ranipet- 632517 , shobanavasu.mca@gmail.com

[2]V. Pavithra, Assistant Proffesor, Computer Science and Applications, SRM Institute of science and technology, Chennai, Ramapuram, vpavithra.1989@gmail.com

[3]R. Baghia Laxmi, Assistant Professor, artificial intelligence and data science, St. Joseph's College of Engineering, (An autonomous institution), OMR, Chennai - 119, Tamilnadu. laxmiram1995@gmail.com

Abstract

Cyber deception strategies, powered by artificial intelligence (AI), have emerged as a critical tool in defending against increasingly sophisticated cyber threats. This chapter explores the integration of AI-driven honeypots and generative models for enhancing cybersecurity defenses, with a particular focus on mitigating cloud supply chain attacks. Cloud environments, characterized by their complexity and interconnected nature, have become prime targets for cybercriminals seeking to exploit vulnerabilities in trusted vendor relationships. AI-powered honeypots simulate realistic decoy systems within cloud infrastructures, luring attackers into engaging with fake environments, thus providing valuable intelligence on attacker tactics, techniques, and procedures (TTPs). The use of generative models, such as Generative Adversarial Networks (GANs), further strengthens deception by generating dynamic and convincing cloud service interactions, complicating attackers' efforts to identify legitimate systems. By continuously adapting to attacker behavior, AI-driven deception frameworks can offer real-time detection, analysis, and mitigation of supply chain compromises. The chapter also highlights the role of AI in enhancing the capabilities of traditional cybersecurity tools, such as intrusion detection systems (IDS) and Security Information and Event Management (SIEM) platforms, by providing more accurate and timely threat intelligence. As cloud-based services continue to grow, the application of AI-driven honeypots and generative models is poised to become a fundamental aspect of proactive, scalable, and adaptive defense mechanisms against cloud supply chain attacks.

Keywords: Cyber Deception, AI-Powered Honeypots, Cloud Supply Chain Attacks, Generative Models, Attack Detection, Threat Intelligence.

Introduction

The rapid adoption of cloud computing has transformed the way businesses operate, providing enhanced flexibility, scalability, and cost-efficiency. Cloud environments, however, are inherently complex, comprising interconnected systems, third-party vendors, and distributed resources. While this interconnectedness provides significant operational benefits, it also presents a substantial attack surface for cybercriminals. Cloud supply chain attacks, in particular, have emerged as a critical concern for organizations, as they exploit vulnerabilities in the relationships between service providers, software vendors, and cloud-based infrastructure. These attacks often bypass traditional security defenses by targeting trusted partners and leveraging indirect paths to infiltrate systems. Detecting and mitigating such attacks is a complex task, as they often go unnoticed for extended periods due to the nature of the cloud's shared infrastructure. As organizations continue to integrate cloud technologies into their operations, the need for advanced, proactive security measures becomes more pressing.

AI-driven deception strategies, which employ advanced techniques such as honeypots and generative models, offer a promising solution to this growing threat landscape. Honeypots, as decoy systems, lure attackers into interacting with fake environments, providing an opportunity to monitor and analyze their behavior. AI-powered honeypots take this concept a step further by leveraging machine learning and adaptive algorithms to create dynamic, intelligent decoys that evolve in real-time based on attacker interactions. By simulating a wide range of cloud service environments, these honeypots can mimic legitimate systems, making it more difficult for attackers to distinguish between real and fake assets. This approach not only helps identify potential vulnerabilities but also aids in understanding the tactics, techniques, and procedures (TTPs) employed by attackers during supply chain attacks.

Generative models, such as Generative Adversarial Networks (GANs), play a crucial role in enhancing AI-driven deception frameworks. These models generate realistic, synthetic cloud service interactions, including data exchanges, software updates, and API calls, which are often targeted during supply chain attacks. By simulating these processes, generative models make it challenging for attackers to differentiate between legitimate and deceptive systems. Moreover, these models can continuously evolve based on the latest attack data, ensuring that the deception framework remains relevant and effective against emerging threats. The ability to simulate various aspects of cloud service interactions, such as complex vendor relationships and third-party integrations, enhances the realism of the decoy systems, making them more likely to attract and engage attackers.

AI-driven deception not only helps in detecting supply chain attacks but also provides valuable insights into the attacker's methods and movements within the cloud environment. Traditional cybersecurity measures, such as intrusion detection systems (IDS) and Security Information and Event Management (SIEM) platforms, typically rely on signature-based detection and anomaly detection. While these tools can identify known threats and patterns, they often struggle to detect novel attack strategies that do not conform to previously observed behaviors. By integrating AI-powered honeypots with these traditional tools, organizations can enhance their ability to detect and respond to emerging threats. The combination of real-time attacker behavior analysis and enriched threat intelligence allows security teams to implement more accurate and adaptive defense strategies, which are critical for mitigating the risks posed by cloud supply chain attacks.