CERTIFICATE NO : ICLTSEMH /2025/C0125211

A Study of Distributed Denial of Service Attacks (DDoS) in Cloud Computing

Moram Sunil Kumar Reddy

Research Scholar, Ph. D. in Computer Science and Engineering
Dr. A.P.J. Abdul Kalam University, Indore, M.P., India.

ABSTRACT

Distributed Denial of Service (DDoS) attacks pose a significant threat to cloud computing environments, disrupting services by overwhelming network resources with malicious traffic. As cloud platforms continue to grow in scalability and accessibility, they have become prime targets for attackers seeking to exploit vulnerabilities. This paper explores the nature of DDoS attacks in cloud computing, examining their impact on service availability, data integrity, and overall system performance. It discusses various attack vectors, including volumetric, protocol-based, and application-layer attacks, and highlights the challenges in detecting and mitigating such threats in dynamic cloud environments. Advanced security measures, such as anomaly detection using artificial intelligence (AI), machine learning (ML)-based traffic analysis, and software-defined networking (SDN), are essential to strengthening cloud resilience against DDoS attacks. Additionally, the integration of cloud-based security frameworks, including rate limiting, traffic filtering, and automated incident response mechanisms, enhances protection. The study also emphasizes the importance of proactive defense strategies, such as zero-trust architectures and blockchain-based authentication, in mitigating future DDoS risks. Findings suggest that a multi-layered security approach combining real-time monitoring, adaptive traffic control, and collaborative threat intelligence sharing is crucial for safeguarding cloud infrastructures against evolving DDoS threats.