ABSTRACT

The increasing reliance on cloud computing has made it a critical target for Distributed Denial of Service (DDoS) attacks, which threaten the availability, performance, and reliability of cloud-hosted applications. This paper introduces the DDoS Protection System for Cloud using AWS and Machine Learning, a comprehensive and adaptive solution for real-time detection and mitigation of DDoS attacks. The proposed framework exploits both the scalability of AWS cloud services and the intelligence of machine-learning algorithms to perform advanced traffic analysis in order to differentiate legitimate users from malicious entities. The system integrates anomaly-based detection techniques, dynamic resource allocation, and automated mitigation workflows to handle high-volume, complex attack patterns while minimizing latency in operational activities. Key features are real-time alerting, seamless scalability, and efficient use of cloud resources, making the solution practical for dynamic cloud environments. The experimental evaluations clearly indicate effectiveness in neutralizing various vectors of DDoS attacks and maintaining high availability and optimising resource consumption. With a combination of cloud-native tools and intelligent analytics, the research work here has a positive impact on advancing cloud security and provides the groundwork for further development in hybrid and multi-cloud architectures. Such findings therefore present insight for organizations that seek to fortify defences against evolvement of cyber threats.