# *ABSTRACT*

*The rapid growth of internet usage has significantly increased the risk of cyber threats, including Distributed Denial of Service (DDoS) attacks based on DNS Amplification. This type of attack exploits open DNS resolvers to send large-sized DNS responses to a target by spoofing the source IP address, thereby overwhelming the target's network infrastructure and degrading service performance or rendering it completely inaccessible. This study aims to design and implement a real-time detection and mitigation system for DNS Amplification attacks in a Software-Defined Network (SDN) environment using Access Control List (ACL) techniques through the Ryu Controller. The detection mechanism is based on a Support Vector Machine (SVM) classification model trained on traffic features extracted from UDP packets on port 53. The dataset was generated through simulations of normal and attack traffic using Mininet and Scapy, and evaluated using a confusion matrix and standard classification metrics. Experimental results demonstrate that the system achieves a detection accuracy of 94.69%, successfully blocking 6,584 out of 7,367 attack packets through automatic ACL rule injection. Although a false negative rate of 5.31% was observed, indicating room for improvement in model sensitivity, the overall mitigation success rate reached 78.97%. These findings confirm the effectiveness of the proposed SDN-based machine learning and dynamic mitigation approach in addressing DDoS threats while maintaining legitimate traffic continuity.*



***Keywords—Access Control List, DDoS, DNS Amplification, SDN, SVM, Ryu Controller***