## *ABSTRACT*

*Software-Defined Networking (SDN) is a new approach to network management that separates the control plane from the data plane. With this architecture, network configuration can be done more flexibly through software such as the Ryu controller. However, SDN also has serious challenges in terms of security, one of which is the HTTP Flood-based Distributed Denial of Service (DDoS) attack that can cause service disruption. This study aims to implement and analyze rate limiting techniques on the Ryu controller as a mitigation effort against HTTP Flood attacks. Tests were conducted in three scenarios: normal traffic, attacks without mitigation, and attacks with mitigation. Traffic data was analyzed using the Support Vector Machine (SVM) algorithm to classify between normal and attack traffic. The evaluation focused on the Round Trip Time (RTT) and confusion matrix parameters. The test results showed that the implementation of mitigation was able to reduce the maximum RTT value significantly. In the scenario of two attacking hosts, the maximum RTT value decreased from 707,569 ms to 100,681 ms after the implementation of Rate Limiting. Furthermore, based on the confusion matrix evaluation, the developed classification system achieved an accuracy of 94%-96%, demonstrating quite good performance. This study concludes that the integration of rate limiting and SVM can be an efficient approach in detecting and mitigating DDoS attacks on SDN. Suggestions for future research include expanding the scope of attack types and developing a more adaptive and real-time approach.*

**Keywords*:* Software Defined Networking, HTTP Flood, Rate Limiting, Ryu Controller, Support Vector Machine, Attack Mitigation, RTT**