ABSTRACT

In the increasingly complex digital era, Distributed Denial of Service (DDoS) cyberattacks have become a serious threat to network security, as they can cripple systems and services by overwhelming the target with excessive data traffic. This study proposes an innovative DDoS detection system that combines the strengths of Software-Defined Networks (SDN) with the Random Forest machine learning algorithm. Traffic data is analyzed to extract features such as packet count, inter-packet time, and average packet size. These features are utilized due to their high discriminatory capability in detecting anomalous patterns. The trained model is subsequently integrated into an SDN controller, such as the Ryu Controller, enabling it to detect suspicious traffic patterns swiftly and accurately. The system demonstrated its effectiveness with a detection accuracy rate of 88%. These results highlight that the combination of SDN technology and Random Forest provides a reliable solution for protecting digital infrastructure against DDoS attacks, thus preventing significant damage to network systems.

Keywords— ***Software Defined Network (SDN), Distributed Denial of Service (DDoS), Random Forest***