## *ABSTRACT*

### *SECURITY SYSTEM ANALYSIS ON SOFTWARE-DEFINED NETWORK WITH HYBRID HONEYPOT USING QUALITY OF SERVICE*

By

Revanza Hafiz Erianto

20102142

*Indonesia has 185.3 million internet users (66.5% of the population) by early 2024, Indonesia faces a significant surge in cyber threats. In 2023, 603,276,807 cyberattacks were recorded, including Distributed Denial of Service (DDoS) attacks that caused disruption to the 2024 Election domain, as well as 11,081,392 SSH Brute Force attempts against government sites. To address these challenges, this research designed a Software-Defined Network (SDN) based security system using a Hybrid Honeypot equipped with an Intrusion Detection System (IDS) to detect and deflect attacks. The results showed that the DDoS ICMP Flood, SYN Flood, HTTP Flood, and SSH Brute Force attacks were successfully diverted to the Honeypot using Flow Rules on the Floodlight Controller, so that the server remained safe. Quality of Service measurements showed that the SYN Flood attack increased throughput from 172.5 bit/s in the 5th minute to 182.6 bit/s in the 20th minute, with delay decreasing from 13,219 ms to 10,244 ms . The HTTP Flood attack caused the throughput to decrease from 545.5 bit/s in the 5th minute to 490.3 bit/s in the 20th minute, while the delay increased from 153,945 ms to 296,158 ms . ICMP Flood showed stable throughput at around 8,000 bit/s, but packet loss increased to 3.05% in the 20th minute, with delay changing from 60.06 ms in the 5th minute to 62.11 ms in the 20th minute. Meanwhile, the SSH Brute Force attack increased the throughput from 3.24 bit/s in the 5th minute to 3.81 bit/s in the 20th minute, while the delay decreased from 367 ms to 272 ms .*



***Keywords : Distributed Denial of Service, Hybrid Honeypot, Intrusion Detection Systems, Quality of Service, Software-Defined Network, SSH Brute Force***