COMPLEXITY AWARE INTELLIGENT INTRUSION DETECTION FOR DDOS ATTACKS

Thesis submitted to the partial fulfilment of the requirements for the

Degree of Doctor of Philosophy in Computer Science

By

KALAIVANI M.

(18PHCSP005)

Supervisor

Dr. G. PADMAVATHI

Department of Computer Science

Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore - 641 043

JANUARY 2025

80_Recommendations

- Based on the progress of the research made in this thesis, future studies should focus on two significant aspects to contribute to the improved versatility of the given IDS in real environments. First of all, the effectiveness of the developed model has to be confirmed on real-time datasets. Benchmark datasets provide insights, experiments on current, real datasets are needed to mimic real-world problems and capture facets missed in a controlled environment. By doing this validation, we will get a better estimative of the system's flexibility and effectiveness in facing new cyber threats.

- Secondly, it is vital to determine not only the capability of the model in identifying and mitigating AI enhanced and Deep DDoS threats, attack types. These attacks will employ artificial intelligence to change its attack patterns in response to the target making it even more complex and difficult to identify. Testing the system is possible using both AI-Enhanced DDoS prototype attacks and real AI-Enhanced DDoS attacks will help to determine its performance in real-life scenarios and estimate the system's ability to cope with contemporary threats. It will ensure the system is robust and reliable enough to counter modern and ever-changing cyber threat practices.