UNIVERSITI TEKNOLOGI MARA

DDOS ATTACK DETECTION SYSTEM USING ARTIFICIAL NEURAL NETWORK (ANN)

MUHAMMAD SYAMIL BIN YUSRI

BACHELOR OF COMPUTER SCIENCE (Hons.)

JANUARY 2024

ACKNOWLEDGEMENT

I completed this study in the allocated time, and I give Allah honour and appreciation for His grandeur and the various treasures He has bestowed upon me. First and foremost, I would like to thank my adviser; this work would not have been possible without the assistance and counsel of Sir Mohd Hanapi bin Abdul Latif, who not only assisted me in completing this study but also committed his time and effort to it. In addition, I'd like to thank Madam Ummu Fatihah Binti Mohd Bahrin, who acted as my lecturer for CSP 600/CSP650 and shared her expertise with me, offered support, and motivated me throughout the semester.

My family members have been more crucial to me in the pursuit of this goal than anybody else. My deeply loved parents deserve a particular thank you for their constant physical and emotional support, as well as encouragement and even financial aid when I needed it the most. I am grateful to everyone I had the pleasure of working with on this project. I'd want to thank my favourite classmates for giving me a helping hand and offering emotional support in order for me to successfully complete the final year project.

ABSTRACT

DDoS attacks represent a substantial danger to network availability and security. Because of their sophistication, traditional DDoS detection technologies sometimes struggle to effectively identify and neutralise such attacks. In this project, offer a novel method for detecting DDoS attacks using Artificial Neural Networks (ANNs). To detect aberrant network traffic associated with DDoS attacks, the system uses the capability of ANNs, which are capable of learning complicated patterns and generating accurate predictions. The suggested system is divided into two stages: training and detection. A systematic strategy is used in the study framework, which includes problem identification, data gathering, preprocessing, ANN implementation, and performance assessment. The project's goal is to improve network security by identifying and categorising DDoS attacks properly. The implementation of ANNs using the Sequential model was tested using different training/testing splits (80/20, 70/30, 60/40) and epochs. The 70/30 split regularly outperformed others, with an accuracy rate of 92.29%. Detailed parameter tweaking was carried out for the 80/20, 70/30, and 60/40 splits, finding that a three-hidden-layer architecture with 256, 128, and 8 neurons produced the highest accuracy of 92.54%. Multiple ANN models were evaluated, and the best-performing model achieved 92.54% accuracy, 93.01% precision, 91.05% recall, and a 92.10% F1-score. However, the research recognises several limits, such as the time-consuming nature of ANN model training, possible scaling concerns due to hardware restrictions, and fluctuation in dataset appropriateness. To overcome these constraints, the project propose future recommendations like as using advanced techniques like parallel processing, automated methods for dynamic dataset selection, and hybrid approaches that combine ANN with other methods to increase accuracy.

TABLE OF CONTENTS

CONTENT **PAGE**