INTRODUCTION

Distributed Denial-of-Service (DDoS) is an attack carried out over a computer network that results in the server being unable to provide services to users. DoS attacks are most common because they are easy to perform, however, detecting and dealing with these attacks is very difficult because DoS attacks come in many forms. DDoS has three types, namely application layer attacks, protocol-based attacks, and volume attacks [2]–[4].

DDoS is also effectively used to stop services on Internet of Things systems based on the Message Queuing Telemetry Transport (MQTT) protocol. In the system, the seller usually sells a broker that is used to manage data traffic between the issuer and the customer. Several research projects have been undertaken to detect DDoS in the Internet of Things (IoT) using machine learning [5], [6]. For example, smart House Networks are more vulnerable to security threats because they are heterogeneous and nodes in smart house networks usually occur in heterogeneous and hosted environments [3], [7], [8]. An IoT Malware named Mirai was reported in 2016, which infected about 2.5 million IoT devices and launched DDoS attacks [9].

The solution to the problem was given by Roopak [10]. Roopak [10] proposes the development of DDoS detection based on Naive Bayes and Random Forest. The results of experiments conducted in the research have detection accuracy is Naive Bayes 94.19% and Random Forest 93.64%. In addition, Mubarakali [11] has also developed an SVM-based DDoS detection system. But the results obtained are not very significant. That's about 96.23%. From some existing research, it is proven that generally still have low detection accuracy in predicting DDoS.

The research is structured as follows: Part II describes the theoretical basis, Part III provides an overview of the proposed methods, Part IV includes experiments and results, and Part V describe the conclusion, and in Part VI explains about future works.

A. Objective

Build a DDoS detection system based on machine learning. Then perform testing using data sets generated through DDOS simulation in the IoT environment and perform analysis and compare the results of ANN and KNN predictions.

B. Scope of Problem

Problem boundaries are used to determine research boundaries so as not to get out of the research topic.

1. The algorithms used in the research are Neural Network (NN) and K-Nearest Neighbor (KNN).
2. The datasets used in the study were obtained from research [1] and simulation datasets conducted independently.