I. INTRODUCTION

The usage of the Internet of Things (IoT) [1] has been increasing exponentially due to the Covid-19 pandemic, such as smart body temperature detection (Medical IoT), smart hydroponic (Agriculture IoT), smart industrial control system, and many more. This rapid growth will require standardized security protocols [2] and the development of appropriate architectures [3] to provide services for secured IoT devices. IoT transforms critical data over public networks. There are around 10.7 billion devices that are connected worldwide in 2021 and the data must be protected with high-level security. However, security engineers and developers should consider that IoT Devices have small resources and limited computation before developing their secure end-to-end communication (e.g., reconnaissance attacks, eavesdropping, denial-of-service, trojan/botnets, etc.). Cybercriminals can compromise IoT devices connected to the Internet and use them in bulk to carry out attacks. By This research was collaborated between School of Computing and School of Applied Science, Telkom University. This research was also funded by PPM, Telkom University. Attackers Scanner/ Target Loader Infect Command Infected IoT Devices scan Infect Bot Figure. 1: IoT Botnet attack showcase knowing the attacks from Shodan (with filter MQTT)), cybercriminals [4]–[6] can seize those IoT devices and employ their collective computing power to take on larger targets in DDoS attacks, sending spam, stealing information, or even spying with sound recording or camera capabilities. Enormous botnet constructed from thousands or even billions of IoT devices has been used to accomplish attacks as can be seen in Figure 1. An IoT botnet is a network of devices connected to the Internet, typically routers / Rasberry Pi / Arduino Uno / Camera CCTV, that have been infected by malware (specifically IoT botnet malware) and taken over by the command and control (C&C). Many scrutiny and methods to prevent botnet attacks on IoT networks have been proposed i.e hardening and prevention script from malware infection on the IoT device [7], blockchain-based architecture from Mirai botnet attacks [8], and deep autoencoders [6]. This challenge is further compounded by the lack of a convenient user interface on many consumer IoT devices. Based on the N-BaIoT dataset [6], this research designed and proposed a one-dimensional convolutional neural network (1DCNN) to detect botnet attacks on IoT devices. The contributions of this research are as follows: 1) Proposing the Deep residual CNN Model to detect Botnet in IoT Device traffics. 2) Processing and presenting the occurring Botnet attacks on IoT devices by using the proposed model. 3) Comparing the proposed model with other hybrid algorithms and different optimizers. The II reviews the existing works on the use of deep learning algorithms for detecting attacks on IoT devices while III explains the proposed approach to extending accuracy. Then, the specific aspects of the algorithm and optimizer experiments are described in IV. Finally, V gives the conclusions and future recommendations of this research.