# CHAPTER I
# INTRODUCTION

## 1.1. Background

The Internet of Things (IoT) has transformed how we interact with technology and brought significant changes to the technological landscape. According to a report by Statista, the number of IoT devices is projected to reach 29.4 billion units by 2030, nearly tripling from 9.7 billion units in 2020 [1]. This surge is driven by the increasing adoption of smart home, smart city, smart agriculture, industrial IoT (IIoT), and digital health monitoring systems [2] The presence of IoT provides substantial benefits such as automation, process efficiency, and ease of data-driven decision-making. However, behind these remarkable benefits and massive growth, there are increasing potential points for cyber threats and opportunities for exploitation in IoT security.

Most IoT devices are designed with priorities on cost efficiency, low power consumption, and ease of deployment, often sacrificing security aspects [3]. The simple internal design of IoT devices and their reliance on low-power hardware result in various limitations in both hardware and software, making them incompatible with advanced security mechanisms [4]. These limitations make IoT devices unable to implement self-protection techniques or systems that require high computing capacity. In addition, IoT devices have many vulnerable entry points, ranging from memory, firmware, physical interfaces, and web interfaces to network resources, which can be exploited through weak components [4]. This situation is further aggravated by the very large number of IoT devices, making it difficult to regularly monitor and patch vulnerabilities.

Distributed Denial of Service (DDoS) attacks are now becoming a serious threat to digital infrastructure, including IoT networks. Cloudflare's Q3 2024 report recorded the largest DDoS attack in history with a volume reaching 4.2 Tbps, which utilized thousands of IoT devices already infected with malware [5]. In Indonesia, the situation is also concerning. Data reported by AwanPintar.id recorded more than 133 million cyberattacks in just the first six months of 2025, or around 740 thousand attacks every day [6]. If it occurs in an IoT environment, a DDoS attack not only causes service disruption, but can also endanger safety, for example in medical devices, infrastructure monitoring systems, or industrial control systems [7].

In facing DDoS threats, two main approaches that are widely used are rule-based detection and machine learning. The rule-based approach is one of the methods most often used because it is simple, fast, and can work directly without a model training process. This system evaluates traffic characteristics based on rules or thresholds, such as the number of packets per second, connection frequency, or TCP flag patterns[8]. Its main advantage is very low latency [9]. However, there are several important weaknesses: this method depends heavily on the accuracy of threshold determination. If the threshold is too strict, the system tends to produce a high number of false positives, while a threshold that is too loose can lead to false negatives, allowing attacks to go undetected [10].

Machine learning (ML)-based approaches are increasingly being used because they are able to recognize complex attack patterns. Models such as Random Forest, Support Vector Machine (SVM), and Deep Neural Networks (DNN) have proven to provide high accuracy in detecting DDoS attacks [2]. For example, research by Shakya and Abbas (2024) showed that XGBoost was able to achieve an accuracy of up to 99.82% on the CICIoT2023 dataset [11]. However, ML has its own challenges. Models with high accuracy require large computation, longer inference time (5–50 ms), and higher memory consumption, making them unsuitable for IoT devices, which are generally resource-constrained [9]. A study by Tekin et al. (2023) showed that deep learning models consume 3–8 times more energy than lightweight models [12] Therefore, the direct application of machine learning on IoT devices is often not feasible, and intermediary solutions such as edge computing or gateway-based detection are needed [13].

From various studies, it is evident that there is still no solution that can truly balance the speed of rule-based methods with the high accuracy of machine learning in a single system that remains efficient for resource-limited devices such as IoT. Research by Hussain et al. (2024) proposed a hybrid IDS architecture for Cyber-Physical Production Systems (CPPS) that combines rule-based methods and machine learning [14]. However, the design they proposed places the ML model as the first-layer classifier, so all traffic must go through the inference process before being validated by rules. Several hybrid studies have been conducted, but their architectures still impose a heavy computational burden on edge devices because ML as the first layer makes the system less optimal [15][16]. This condition creates the need for a hybrid detection system with a smarter cascade architecture, where the rule-based

method acts as a fast filter, while machine learning is only used for ambiguous traffic. Such an approach can improve efficiency without sacrificing accuracy.

To address this gap, this study proposes the development of a hybrid DDoS detection system that integrates rule-based methods with machine learning through a cascade mechanism, in which the rule-based method provides instant decisions for very clear traffic and only suspicious traffic is sent to the machine learning model. Raspberry Pi was chosen as the edge gateway platform because of its adequate performance, energy efficiency, and relatively low cost; this combination makes Raspberry Pi widely used as a prototyping platform for IoT systems and network security [17]. With this approach, it is expected that detection accuracy can remain high while ensuring that the detection process remains fast and efficient, so that it can run well on IoT devices with limited resources.

## 1.2. Problem Formulation

Based on the background above, the problem statements are formulated as follows:

1. How can a DDoS detection system based on hybrid detection (rule-based and machine learning) with a cascade mechanism be designed for IoT networks?
2. How can the implementation of a cascade-based hybrid detection system on Raspberry Pi as a security gateway with limited resources be optimized?
3. To what extent is the effectiveness of a cascade-based hybrid detection system in detecting DDoS attacks on IoT network traffic in real time?

## 1.3. Research Objectives

The objective of the study is the target to be achieved in the research process. The objective of this study is to develop and evaluate a DDoS attack detection system based on hybrid detection with a cascade mechanism on IoT networks using Raspberry Pi as a security gateway.

## 1.4. Research Benefits

The benefits of this study are as follows:

1. Provide a cascade-based hybrid detection system design that is able to combine the speed of rule-based methods with the accuracy of machine learning for DDoS detection in IoT.

2. Provide a lightweight and efficient Raspberry Pi-based security gateway implementation model that can be used in small- to medium-scale IoT networks.
3. Provide technical and academic references regarding the development and evaluation of a hybrid detection-based DDoS detection system on devices with limited resources.

### 1.5. Research Limitations

In order for this research to run in a focused and directed manner, several problem boundaries are established as follows:

1. Dataset: This research uses the CICIoT2023 dataset for the development of rule-based methods, training, and evaluation of the machine learning model. Other datasets are not used in this research.
2. Types of DDoS Attacks: Testing in the dataset evaluation stage covers various types of attacks contained in the CICIoT2023 dataset. However, live testing and pentester validation are focused on the three main DDoS categories, namely volumetric attack, protocol attack, and application layer attack. Attack types outside these categories are not included in the scope of this research.
3. Machine Learning Algorithm: The machine learning model used is limited to the Random Forest algorithm. Comparison with other algorithms is not included in the scope of this research.
4. System Architecture: This research only explores a cascade-based hybrid detection architecture. Other hybrid architectures such as parallel, feedback-loop, or full ensemble are not discussed.
5. Detection Mechanism: The system combines rule-based and machine learning approaches in a hybrid detection scheme. The development of other detection methods outside this approach is not the focus of this research.
6. Packet Capture: The system uses Scapy based on Python userspace as the packet capture and flow aggregation mechanism. Kernel-based solutions such as libpcap, eBPF, or NetFlow are not used in this research.
7. Mitigation Mechanism: The system uses iptables-based blocking as the mitigation mechanism. Advanced mitigation techniques such as traffic shaping or rate limiting are not included in the scope of this research.

8. Network Scope: The system is designed for small- to medium-scale IoT networks. Implementation on enterprise-scale networks is not the focus of this research.
9. Number of IoT Devices: Testing is conducted using one IoT device (MQTT-based ESP32) as a representation. Testing with a large number of IoT devices simultaneously is not carried out in this research.
10. Testing: Testing is conducted using traffic and attack simulations in a controlled environment, including internal testing by the researcher and external validation by a penetration tester. Testing in a production environment is not conducted.
11. Monitoring Interface: The system does not develop a web-based dashboard or monitoring visualization. The system output consists of log files, audit trails, and real-time notifications through the Telegram Bot API.