CHAPTER 1
INTRODUCTION

1.1 Background

In today‘s virtual technology, many gadgets are made to assist facilitate human work. This is because of the growing want for matters which might be sensible and fast. Security is one of the issues of concern. First, what do we mean by the word ”security”? Security refers to the level of protection from harm, risk, loss, and misconduct. It is a kind of development and wellness skill. Welfare systems provide a kind of guarantee that ensures the safety and security of assets when their owners are at home or away. A security system is a process that improves the quality of life at home or at work by creating a flexible, comfortable and safe environment [1][2].

Most existing security systems are expensive, complex, bulky, and require wiring. Therefore, a simple, fully portable and simple welfare system needs to be innovated to fill these loopholes [1]. This research presents a web server that will be the dashboard and its implementation using Raspberry pi that provides a cost-effective solution to the above problems [1][3]. Web servers are now a common interface for all smart devices. The proposed solution can be applied to the industry where the condition of machines can be monitored and operated through this system. It can also be used in residential areas [3]. The role of the web server is to receive and respond to client requests on the Internet, the web server must be protected from the vulnerability. From a network security perspective, there are three important aspects of network security, also known as confidentiality, integrity, availability, or (CIA). Web server availability is one aspect of network security that is often exploited by attackers. A form of attack on the availability aspect of a web server that attackers often use includes Denial of Service (DoS).

Research on smart security systems has been carried out before. As in research on ”Implementation and Analysis of Virtual Network Security Against DoS and DDoS Attacks with HIPS Snort”. The analysis describe HIPS Snort’s defense capabilities SYN Flood and UDP Flood Attack Web Server creates a virtual network that simulates DoS and DDoS attacks against web servers over TCP and UDP protocols to investigate the behavior of Investigate IDS against DoS and DDoS cyber attacks An investigation will be conducted by The DoS and DDoS attack tool used is hping3. Deployed on the router side, Snort provides data digest evidence when an attack occurs. As a result of this research, HIPS Snort is able to drop 96.65% of DoS SYN flood attack packets, 97.92% of DDoS SYN flood attack packets, 95.54% of DoS UDP flood attack packets, and 95.07% of DDoS UDP flood attack packets when activated. Thus, snort can prevent DoS and DDoS attacks. [4]

Subsequent research on smart security systems that use Raspi has been carried out by Kadek Susila Satwika with the title "INTRUSION DETECTION SYSTEM (IDS) USING RASPBERRY PI 3 BASED ON SNORT CASE STUDY: STMIK STIKOM INDONESIA". In this study, the IDS system was used with a Raspberry Pi 3 Model B based Snort and tested in three variants attacks, i.e. PING attacks, port scans, DOS/DDoS attacks. The CPU utilization, memory (RAM), and network utilization of the Raspberry Pi 3 Model B are monitored each time an attack is executed. In the event of an attack or unusual activity on your computer network, you will be notified via the BASE website and sent via SMS (Short Message Service) to network administrator mobile real time. [5]

However, the two studies have differences where the above research only detects using snort-based raspi. Meanwhile, in this study not only detection but also prevention which will later appear on the web server dashboard and only experiment with DoS attacks. DoS attacks are a major problem for today's computer networks and information security. Early DoS attacks were technical games played among underground attackers. In India, do-make has caused more than 6 million web attacks. Through this attack, an attacker steals sensitive data. Recently, Russia launched a DoS attack on a U.S system. This only attacks users who are using or connected to the Internet [6]. DoS attacks can be prevented by implementing a server-side security system. An intrusion prevention system approach is a defense system that can be used to block DoS attacks. An Intrusion Preventing System (IPS) is an Intrusion Detection System (IDS) designed to detect suspicious activity and prevent or stop such activity [7].

The study in this research is done by creating a web server using Raspberry Pi which will provide a database rule for snort that will be the dashboard and its implementation to simulate a DoS attack and investigating the behavior of IPS against a DoS cyber attack. This research uses a Host-based Intrusion Prevention System (HIPS) Snort as a web server defense system to prevent DoS attacks. Snort is located on the router side and provides evidence of a summary of the data in the event of an attack [6][7]. This research is important to do because a smart security system based on raspberry pi can prevent Dos attacks. This research is also an update from previous research where this research can bring up warnings from DoS attacks. Based on those issues research about "DESIGN MAIN SERVER CONTROLLER

IMPLEMENTATION AS A DASHBOARD USING RASPBERRY PI" is feasible to do.

1.2 Problem Formulation

The primary objective of this research is to create and implement a Main Server Controller dashboard on Raspberry Pi, incorporating Snort for network security. The Main Server Controller must be able to efficiently manage and monitor connected devices and systems while integrating Snort.

1.3 Objectives

The goal of this research is to create a Main Server Controller dashboard utilizing the Raspberry Pi as the base with Snort integration. The Main Server Controller will oversee and keep an eye on various connected devices and systems. The dashboard must have an intuitive interface for immediate monitoring and control of these connected devices.

1.4 Scope of Work

The problem limitation in this research are as follows:

1. Personal Computer (PC) uses to make a web server using Raspberry Pi.
2. Design and implementation of Main Server Controller dashboard with Snort integration on Raspberry Pi platform.
3. Raspberry Pi must be able to handle processing demands of Main Server Controller and Snort.
4. The final product should be scalable and flexible.
5. User-friendly interface for real-time monitoring, control, and network security through Snort integration.

1.5 Research Method

The method of this research is as follows:

1. Identification of research problems
   At this stage, the collection materials used for reference are taken from a variety of sources, including magazines, articles selected from the Internet, and books useful for dissertations related to the design and implementation of the Main Server Controller dashboard on Raspberry Pi with Snort integration and other tools such as Mysql, Barnyard2, Pulledpork, BASE, and Apache2.

2. Model development and problem description
   In this stage, a model for the Main Server Controller dashboard will be developed and described in detail. This will include the design of the user interface, the integration of Snort and other tools, and the requirements for real-time monitoring and control of connected devices.

3. Develop problem-solving models and quantify complexity
   This step will involve developing problem-solving models and quantifying the complexity of the Main Server Controller dashboard implementation.

4. Problem-solving model testing and research validation
   This step will involve testing the developed problem-solving models to validate the research and determine the effectiveness of the solution.

5. Data collection and data analysis
   This step will involve collecting data related to the Main Server Controller dashboard implementation and analyzing the data to identify patterns and relationships.

1.6 Research Organization

The rest of this thesis is organized as follows:

- Chapter 2 BASIC CONCEPT
  This chapter contains an explanation of the theory.

- Chapter 3 PROPOSED TECHNIQUE
  This chapter contains workflow and system planning flow.

- Chapter 4 PERFORMANCE EVALUATION
  This chapter contains the simulation and testing steps, the test results.

- Chapter 5 CONCLUSIONS
  This chapter contains the conclusion and suggestion.