CHAPTER I

INTRODUCTION

1.1 Background

The Internet of Things (IoT) represents a novel conceptual framework wherein objects are interconnected via the Internet, enabling them to engage in intelligent interactions, comprehend their surroundings, and exchange data in a sophisticated manner. The development of the Internet of Things (IoT) commenced with the convergence of wireless networks and the internet. Alongside the exponential growth in the development of the Internet of Things, which is evident in the emergence of IoT platforms for smart homes, smart health, and even smart cars, the issue of data communication responsiveness and security is becoming increasingly prominent.

In overcoming the high response time based on previous research using fog computing, Hindreen in his journal , Migration from cloud computing towards fog computing [1]. It is showed that using fog computing makes IoT processing faster because data communication requests are first sent to the nearest fog node rather than directly to the cloud, which can minimise response time and errors in authenticating and sending data.

As well as in terms of the security of IoT communications, where NFT blockchain technology has recently been used with the IoT, they provide a distributed and cryptographically secure blockchain that allows data traces to be irreversible and guarantees data ownership and user privacy. This is reinforced by the research of [2] in his journal titled 'Making smart contract references that occur on the NFT blockchain', where the journal identifies the most popular application domains for NFT smart contracts today and has compiled a list of features and extensions that are commonly used in smart contracts. These features and extensions have been compiled into a comprehensive smart contract suite that supports the ERC721 standard.

Therefore, the focus of this research is the use of fog computing schemes in the integration of IoT microcontrollers with NFT blockchain smart contract technology for authentication, so that connectivity can be established more quickly between IoT microcontrollers and fog nodes (fog computing) that are placed locally on the user side using Raspberry Pi. In the process, the smart contract using the NFT blockchain creates an ID token containing the key management and identity of the contract, which is then stored in the EEPROM (Electrically Erasable Programmable Read-Only Memory) of the IoT microcontroller using the esp8266. This allows the IoT device to authenticate based on the token ID created using the NFT blockchain smart contract with blockchain decentralisation on the fog node device, where the fog node is installed with a decentralised service (DApp) that communicates wirelessly.

1.2 Problem Identification

The rise in the number of IoT devices in use across a range of sectors has given rise to several challenges in terms of the speed and efficiency of the authentication process for these devices. The following research problem has been formulated:

1. How to authenticate IoT microcontroller with fog node in fog computing scheme using NFT blockchain smart contract?

2. How can fog nodes in a fog computing scheme support scalability and efficiency in managing authentication of a growing number of IoT devices?

3. How does the addition of microcontrollers connected to the fog node (DApp) affect the scalability performance of NFT blockchain smart contract-based authentication in fog computing schemes?

1.3 Objectives

The objective of this research is to integrate and test the responsiveness of Internet of Things (IoT) microcontroller authentication using the ESP8266 with a Token ID from the NFT blockchain Smarcontract with a Fog Node (DApp) in a Fog Computing scheme. Additionally, the research aims to assess the scalability and performance of authentication with Fog Nodes (DApp) in Fog Computing schemes by incorporating IoT devices.

1.4 Problem Limitations

The problem limitations in this study are as follows:

1. This research only focuses on testing authentication responsiveness using response time parameters between the IoT microcontroller and the fog node (DApp).
2. The tests in this study focus on the effect on scalability performance of adding 3 microcontrollers that are constantly connected to the fog node (DApp).
3. The testing in this research is limited to the edge device of the fog node user in the fog computing scheme which is used as a decentralised system (DApp) in managing the authentication of IoT devices not up to the cloud.

1.5 Hypothesis

Based on research by Geethu Mary George and L.S.Jayasharee with the title Ethereum Blockchain-Based Authentication Approach for Data Sharing in Cloud Storage Model (3rd) in research conducted in the journal where the test system uses Ethereum blockchain authentication and access control to verify between the system and the cloud [3]. Where the method achieved results with a true user detection rate of 95%, a maximum search accuracy of 95%, and a response time in authentication between the system and the cloud of 2.25 seconds.

Based on the results of previous research, which is the main reference of this research, where the level of responsiveness in authentication between the system and the cloud of 2.25 seconds is a fairly high value in an IoT computation that requires fast and real-time authentication speed. Therefore, in this research, a scheme for IoT computing is created using the ESP8266 microcontroller device, the smart-contract blockchain and raspberry pi as a distributed service in the fog computing scheme. So, in practice, the smartcontract blockchain creates a new contract and minting to create a unique token ID that is recorded on the blockchain, and then the unique token ID is stored in the EEPROM of the esp8266 microcontroller as a key for authentication. This allows the microcontroller to use the token ID to authenticate with a distributed service in the form of a Raspberry Pi, which is placed on a fog node in the fog computing scheme.

1.6 Research Methodology

Figure 1.1 shows the research methods used in this study.

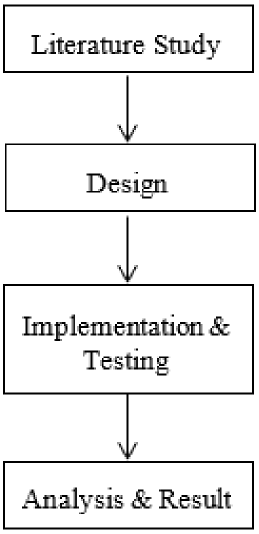

Figure 1.1. Research Methodology

1. Literature Study

   The first stage of the research is a literature review to obtain references from various previous studies related to the research to be conducted and to obtain the latest references for related research, such as research on smart contracts, NFT blockchain, fog computing, decentralised services (DApp) and all things related to and supporting this research.

2. Design

   The design stage determines the needs of working tools, such as the type of microcontrollers used for authentication, NFT blockchain smart contract services, and the decentralised devices used. In addition to the need of work tools, the design stage also requires an analysis of the scheme used, where in this research scheme fog computing is used as the scheme and fog nodes are used as the decentralised service centre to manage the authentication of microcontrollers.

3. Implementation & Testing

   System implementation and testing is a phase to implement the design that has been made and conduct trials to measure responsiveness performance with response time parameters when authenticating IoT microcontrollers with decentralised services (DApp), and to test the effect of scalability performance when adding 3 IoT microcontroller devices connected to decentralised services (DApp).

4. Analysis & Result

   Analyse the responsiveness of the authentication response time between microcontroller and decentralised service (DApp). As well as calculating ART (Average Response Time) to obtain the average response time value of each microcontroller and analyse the effect of testing the scalability performance of IoT microcontrollers with decentralised services (DApp) in the fog computing scheme. Then, it can be concluded that the results obtained by comparing the results with the main reference journal used as a comparison and the effect of scalability between an IoT microcontroller and other IoT microcontrollers simultaneously authenticated with decentralised services (DApp) in the fog computing scheme.