UNIVERSITI TEKNOLOGI MARA

DATA MODIFICATION ATTACKS PROTECTION USING BLOCKCHAIN SIGNING AND VERIFICATION PROCESS IN BLUETOOTH LOW ENERGY NETWORK

AIMAN NURRASYID BIN SHAHRUL KAMIL

Master of Science in Computer Networking

JANUARY 2020

ABSTRACT

Data integrity is a major concern in IoT technologies, and this issue has started to increase in recent years due to the use of Bluetooth Low Energy (BLE) devices. The unauthorized modification of confidential data is one the main threats and is commonly addressed by cryptographic mechanisms, through encryption. However, in BLE 4.2 environment, encryption algorithms are only applied between BLE devices and gateway thus leaving the network to be vulnerable on the public side of the BLE network which is between the gateway and the server. The vulnerabilities in BLE 4.2 and 5.x add an attractive perspective to the security of IoT technology. The issue of providing end-to-end data protection should has been given highest priority by IoT application developer because the data in both private and public networks can be modified and disrupted by attacker. This research proposes some of the blockchain function which is signing and verification process on the BLE (Bluetooth Low Energy) network environment due the security issue on the BLE itself using three different hash algorithm MD5, SHA1 and SHA256. There are four experiment conducted such as processing time, power usage, memory usage and data modification attack. Based on the results, even though the proposed solution requires double hashing process it is still acceptable to be implemented due to it only require lower processing time and power/memory usage.

ACKNOWLEDGEMENT

Alhamdulillah, praises and thanks to Allah because of His Almighty and His utmost blessings, I was able to finish this research within the time duration given. Firstly, it is a pleasure to express my deep sense of thanks and gratitude to my supervisor, Dr. Mohd Faisal Ibrahim, who has been so inspiring, so demanding yet so caring, especially for his timely-guidance, encouragement and give me a lot of suggestions that have pushed me farther than I thought I could go to a great extent to finally finish my project. My heartiest gratitude goes to my respected class lecturer, Dr. Siti Arpah Ahmad for her sincere guidance and helped for completing this project.

Special appreciation also goes to my beloved parents, En. Shahrul Kamil Bin Yunus and , who stood by me like a pillar in times of need, for their endless support over the years was the greatest gift anyone has ever given me.

Lastly, I also place on record, my sense of gratitude to friends from class of CS708 program, directly and indirectly, that have helped during discussion, sharing knowledge and moral support in completing this project.

TABLE OF CONTENTS

CHAPTER ONE
INTRODUCTION

1.1 Research Background

Recently, Bluetooth Low Energy (BLE) sensor has become increasingly popular to be used in IoT devices. This device is becoming more regularly used in mobile applications and is likely to be the predominant connected devices to the Internet (Ericsson, 2016). According to Ericsson, by 2022, there will be more than 5.2 billion connected short-range IoT devices (Ericsson, 2016). Therefore, most IoT devices manufacturers have started to integrate BLE device into their IoT-based applications.

Security is still the leading issue with BLE devices even in the most recent version of BLE. There are currently many security risks associated with BLE in particular the Man-in-the-Middle (MITM) attack (Yaseen et. al., 2019). Secure connections are introduced in BLE 4.2 which the Elliptic-curve Diffie–Hellman algorithm has been implemented in order to introduce a more complex process of key authentication (Pallavi, 2019). This provides default protection from passive eavesdropping and allows the device to be secured. However, this solution does not provide end-to-end data encryption, thus allowing an attacker to modify the data between the gateway and the server.

The work presented in this dissertation focuses on improving the data integrity aspect of BLE network by developing a modified blockchain signing and verification process based on secret key. For this purpose, a protection mechanism was added to the hashing process, using a Caesar Cipher Shift operation. The experimental results obtained show that the proposed solution proved to be secured and recommended hashing technique such as MD5, SHA1 and SHA256 can be applied due to its low processing time, memory usage and power consumption.