UNIVERSITI TEKNOLOGI MARA

PASSWORDLESS AUTHENTICATION PROTOCOL FOR MOBILE E-HEALTH NETWORK ARCHITECTURE USING UNIQUE IDENTITY BASED TECHNIQUE

NAZHATUL HAFIZAH BINTI KAMARUDIN

Thesis submitted in fulfillment
of the requirements for the degree of
PhD
(Electrical Engineering)

Faculty of Engineering

December 2018

ABSTRACT

Mobile e-health provides potential benefits to the health technology system by encouraging a secure growth to the implementation of the Internet of Things. This research also supports the use of Internet of Things and healthcare tools to improve the medical performance system and to facilitate their secure access. Since authentication is a door to every network security, it is very important to enhance the authentication scheme and develop a security protocol during the authentication phase. Traditional health system is heavily dominated by large medical centers where security and privacy in e-health system can be seriously threatened by security attacks. It is noted that the use of username and password as an authentication scheme in mobile e-health has been exposed to various security attacks such as replay attack and sensor node cloning attack where the adversary can listen to e-health network traffic to get the personal information and also the unauthorized access to the e-health data file. Thus, a secure and strong non-regenerated unique identity-based authentication protocol is designed for a wireless embedded e-health sensor node and mobile e-health in order to propose a secure and seamless authentication. The implementation of the mobile e-health application as well as the mobile e-health test bed is also extensively explored in this research. Passwordless authentication can achieve practical and efficient communication and suggests a great assistance in patient-doctor seamless interaction. Since most of the mobile e-health systems are using the third-party service provider server in their network architecture, a framework of a two-tier mobile e-health system is presented in this research to eliminate the involvement of a third party server. It is highly important to protect the confidentiality of the network since mobile e-health transmits highly sensitive and private data. A non-regenerated unique identity of the e-health sensor node is generated as well as the mobile e-health authentication protocol is developed to improve the security of the mobile e-health network architecture. The newly proposed lightweight authentication protocol has successfully reduced the memory utilization up to 65 percent reduction thus making it practicable to be implemented in the mobile e-health system. A thorough security analysis is also conducted through formal analysis method AVISPA to analyze the security of the designed mobile e-health protocol and finally the designed authentication protocol has been proved to be secured from replay attack and sensor node cloning attack.

ACKNOWLEDGEMENT

In the name of Allah SWT, the Most Merciful, the Most Benevolent, I would like to express my highest level of gratitude to Him as without His blessings, none of this would have even been remotely possible. Peace be upon our beloved Prophet Muhammad, his family and all his companions.

A special thanks to my dear parents, Kamarudin Abd Karim and Che Rahana Ab Rahaman who have always been there since the first step of this journey. The physical and emotional support that you have invested throughout the process has made this academic voyage plausible. I can never thank you enough. To my dearest husband, Khairul Mizan Mohd Fauzi, I would like to personally thank you for always being there for me through thick and thin. The fact that you have selflessly chose to embark on this journey with me, I could not have been more grateful. To my dear parents-in-law, Mohd Fauzi Ghazali and Kelesum Awang, I will always be grateful for the continuous moral supports that you have endowed me with throughout this journey. Not to forget to my four sisters, Saidatul Izyanie, Ainatul Aqilah, Izzatul Izwanie, and Zahratul Shahira whom I truly cherish, all the laughter, the smiles and those little sibling fights we all share have definitely made this journey more bearable and memorable indeed.

To my academic supervisors, Ir Dr Yusnani Mohd Yussoff and Prof Ir Dr Habibah Hashim, I extend my sincere thanks to both of you for your virtuous guidance and endless assistance along the process. It has been quite an academic journey for me and I cannot thank both of you enough for always being by my side, academically and emotionally. I thank you for your support.

To my extended family members and friends whom have brought meaning to my personal life and has made me the person that I am today, I would like to express my most sincere gratitude to each and every one of you.

Last but not least, to my son, Muhammad Al Ayyash, whatever I do, whatever I have done, and whatever I will do, I do it for you. I dedicate this to you.

TABLE OF CONTENT

CHAPTER ONE
INTRODUCTION

1.1 Background

E-health network can support integrated healthcare services and data interoperability to communicate in the form of electronic health records accessible through Wireless Sensor Networks (WSN) [1]. Even if the users are far from the healthcare centre, e-health monitoring devices can be applied to obtain the user data and to get access to the healthcare services [2]. Since the last decades, WSN are continuously being utilized within the healthcare system in order to improve the efficiency and reliability of the healthcare operation system. Healthcare services costs are getting higher nowadays and therefore, it is essential for the healthcare organizations to consider adopting e-health system. It will allow the healthcare centre to modernize their health application processes and provide more efficient and reliable services in a cost-effective manner. With a fast growing development of the Internet of Things (IOT), e-health system provides a strong infrastructure and offer viable healthcare services over the network. Utilizing the latest technologies in the healthcare services is an important approach for the healthcare organizations to enhance the healthcare services and reduce operational costs [3][4]. High demand in healthcare services and shortages of qualified healthcare professionals show the need for e-health implementation by the healthcare organizations. New research advancements in WSN and Internet technology have assisted the development of e-health services.

The healthcare professionals also benefit from the development of the e-health system where they can save more time to attend patients and have the opportunity to attend more severe cases [5]. Besides, they are able to have a faster access to their patient health condition by integrating the e-health technology in the healthcare system [6]. The application of the IOT in healthcare system provides several advantages such as a secure patient identification and systematic data collection. Recent technology offers the ability to monitor patient condition autonomously through remote monitoring system. By taking advantage from the IOT emerging paradigm, it is now achievable to monitor patient activity outside the healthcare