Proposing Secure and Lightweight Authentication Scheme for IoT Based E-Health Applications

Maria Almulhim*, Noor Zaman*
*College of Computer Sciences and IT, King Faisal University, Saudi Arabia
maria.almulhim1@gmail.com, nzaman@kfu.edu.sa

***Abstract*— The Internet of Things (IoT) is the collection of connected smart devices\objects through internet network. The rapid development of IoT and vast expansion of wireless technologies unfold the new chances of growth in several domains such as, Education, Transportation, Agriculture, and especially in the Healthcare sector. Introducing the IoT through healthcare applications fetch several benefits, including cost savings through lowered hospital visiting costs, health care provider costs, transportation costs, human resource costs and the insurance costs. It leads to an added advantage of improved quality care in health care. However, increasing use of the IoT services in E-health applications has led to increase the concerns of security and privacy, especially in healthcare domain. In fact, healthcare applications are prone to data breaches and widening issues in security aspects owing to increasing number of access points to sensitive data through electronic medical records, as well as the rising popularity of wearable technology. For example, of these issues, authentication of the different connected entities, energy efficiency and exchanged data confidentiality form the major concerns for users. Therefore, the successful deployment of IoT-based E-health application rely on overcome the major security concerns for the users which needs to be addressed in energy efficient way. Though a number of researches have conducted for lightweight secure authentication, there is still a great room for further research to address security challenges as well as its energy efficiency for those security authentication schemes in IoT. There is a great need to design and develop a lightweight secure authentication model, which offers significant security level against multiple attacks such as mainly: Impersonation attacks, man in the middle attack and unknown key sharing attacks for IoT base E-health domain. This research proposed a secure group-based lightweight authentication scheme for IoT based E-health applications, the proposed model will provide mutual authentication and energy efficient, and computation for healthcare IoT based applications. Which will use elliptic curve cryptography (ECC) principles that provide mentioned featured of suggested model.**

***Keywords*— Secure, Authentication, Light weight, ECC, IoT**

I. Introduction

During last few years, IoT (IoT) is rapidly gaining ground in the field of networking wireless and communications. The basic idea is the connection between heterogeneous objects such as Mobile phones, Sensors, Radio-Frequency Identification (RFID) tags, etc. Therefore, everything becomes virtual, which means that everything is readable, addressable, and locatable on the Internet. The IoT is growing in several domains such as, Education, Transportation, Agriculture, and especially in the healthcare sector [1].

Healthcare application is reflecting one of the most IoT technologies and it is named as IoT-based healthcare applications. It provides multiple of features like continuous remote monitoring of data, so patients can be monitored daily by using sensors in mobile devices such as cell phones or wearable devices. Thus, it is expected that IoT-based healthcare applications to offer multiple of benefits that include such as cost savings through lowered hospital costs, health care provider costs, transportation costs and insurance costs. Therefore, this will have led to improved quality of care and time saving for patients and hospital staff. Therefore, facilitate flexible and secure interactions between patient and healthcare providers is the main goal [2].

So, with rapid deployment of IoT this has brought a lot of challenges, issues and security and privacy concerns. Security is substantial part at lifecycle of medical information of IoT-based healthcare applications and aim to provide the secrecy of those medical data [3].

There are multiple of security issues that need to be handled are: authentication (which is the aim of our research), availability, data integrity, Confidentiality, and non-repudiation to save the data and maintain the efficiency and quality of healthcare provider services. Authentication is an important part at IoT, it enables each object at network to authenticate each other so it will let to forwarding the data to the receiver without any alternation in information [3].

In fact, healthcare applications are prone to data breaches and widening issues in security aspects owing to increasing number of access points to sensitive data through electronic medical records, as well as the rising popularity of wearable technology [1].

Though a number of researchers have discussed open issues in IoT security, there is a need for further research to address security challenges in IoT [4]. The main goal is to make security a fundamental part in design of IoT based healthcare technology for protected data transfer, use and exchange [5].

So, based on that our paper aim to propose a secure group-based lightweight authentication scheme for IoT based E-health applications, which offers high security level against multiple attacks and mutual authentication with less costs in healthcare IoT based applications.

At beginning paper, we discuss briefly about security issues of IoT based E-health applications. The reminder of this paper organized in four different sections. In section II, we present Literature review. In section III, we proposed our scheme and