Enhancing E-health Data Security with Dynamic User Revocation and Key Exchange

By**: Mohammed Ali Kmoona**
Supervisor**: Dr. Ahmad Mousa Altamimi**

Abstract

E-health is a relatively recent healthcare practice supported by electronic processes and communication. It provides an easy sharing way of personal healthcare data between multiple organizations and offered real-time monitoring for the patient’s health status. However, having the data in such a distributed setting rises the need for having secured data sharing with only legitimate users, as the data could be critical and stored in a third-party service provider. Therefore, several approaches have been proposed to secure the data in such a distributed environment. Two main security approaches have been considered, the Cryptographic and Non-Cryptographic methods. While Cryptographic is associated with the process of converting ordinary data into unreadable data for unauthorized users to protect it from theft or alteration, the Non-Cryptographic does not alter the data but provide a simple mechanism to deliver user authentication.

This work enhances the E-health data security in terms of performance, and it is threefold: in the first part, an in-depth review has been conducted to identify the E-health system’s security challenges and solutions. To this ends, the security requirements and methods needed to secure the health data have been outlined. Moreover, a comparison between a set of proposed security mechanisms has been conducted to point out their benefits, features, issues, and open problems. Ultimately, a set of open problems have been listed, such as user revocation and cryptographic key exchanging problems.

Therefore, in the second part of this research, we proposed an access control model to provide efficient user revocation in Cipher-text Attribute-Based Encryption (CP-ABE). Here, a unique identifier is generated using the Pseudo-Random Number Generator (RC4) and associated with each user. This identifier is added to the policy CP-ABE logic gates and removed dynamically when revoking the user. This offers an effective user revocation process disinclining any complex operations such as key re-distribution and data re-encryption with the least possible overhead. To support the evaluation of the proposed model, a prototype implementation is developed and compared with other notable work. Results showed that it outperforms the other work and has the least possible computational overhead.

Finally, the last part of this research focusses on the problem of key exchange where two users must exchange the crypto key before any encryption process. One of the most used methods is the Diffie-Hellman protocol, which is an Asymmetric key mechanism designed

specifically to exchange crypto keys safely over the untrusted network. However, the Diffie-Hellman suffers from the Man in the Middle Attack (MITM). To overcome this particular problem, we proposed an authenticated Diffie-Hellman protocol model using a digital signature, where the RSA algorithm is utilized as a suitable digital signature mechanism to authenticate users during communication. To ground our conceptual idea, we have implemented our model and compared it with other remarkable work. Results showed that our system has better computational time for key exchanging.