

Chapter 24

A Secure Robust and Privacy Enhanced Mobile Healthcare Framework

Hisham M. Alsaghier

Majmaah University, Kingdom of Saudi Arabia

Shaik Shakeel Ahamad

Majmaah University, Kingdom of Saudi Arabia

ABSTRACT

This article describes how the exponential growth of mobile applications has changed the way health-care services function, and mobile healthcare using the Cloud is the most promising technology for healthcare industry. The mobile healthcare industry is in a continuous transition phase that requires continual innovation. There has been identified some of the challenges in the area of security protocols for mobile health systems which still need to be addressed in the future to enable cost-effective, secure and robust mobile health systems. This article addresses these challenges by proposing a secure robust and privacy-enhanced mobile healthcare framework (SRPF) by adopting a Community Cloud (CC), WPKI cryptosystems, Universal Integrated Circuit Cards (UICCs) and a Trusted Platform Module (TPM). All the security properties are provided within this framework. SRPF overcomes replay attacks, Man in the Middle (MITM) Attacks, Impersonation attacks and Multi-Protocol attacks as SRPF was successfully verified using a scyther tool and by BAN logic.

1. INTRODUCTION

Mobile cloud computing (MCC) is a new technology based on mobile web services. MCC is likely to play a vital role in mobile healthcare. Mobile cloud computing (MCC) is an integration of cloud computing (CC) into the mobile healthcare applications of mobile devices. In the cloud healthcare data can be stored and transmitted to hospitals and doctors, but security and privacy of this information is the major drawback and bottleneck of healthcare systems so in order to overcome these flaws US govern-

DOI: 10.4018/978-1-7998-1204-3.ch024

ment introduced Health Insurance Portability and Accountability Act (HIPAA) to regulate US healthcare industry. Following are the motivations for adopting MCC in healthcare. MCC can improve healthcare services by providing Centralization, Performance, Modernization, Scalability, Portability, Collaboration and Virtualization. The main advantage of Mobile healthcare is it provides users easy and quick access to the healthcare infrastructures which includes PHR (patient health records) and doctors.

1.1. Motivations for the Research

1. According to ABI Research all the healthcare infrastructures are susceptible to attacks, in spite of this healthcare industry is spending very less amount for cybersecurity (Steven C. Morgan, 2015);
2. By 2020, 80 percent of healthcare data will be at cloud at some point of time (Julie Bird, 2016).

1.2. Related Work

(Mohammad Wazid, Sherali Zeadally, Ashok Kumar Das & Vanga Odelu, 2016)

Paper identifies some challenges in the realm of security protocols for mobile health systems which needs to be addressed in the future in order to ensure cost-effective, secure and robust mobile health systems. Following are the challenges outlined in this research work.

Challenge 1: Confidentiality, data integrity, accountability, availability, and access control are the most important security requirements for mobile health systems. For ensuring these security requirements, developing efficient key distribution protocols becomes challenging task in the mobile health system.

Challenge 2: Recent studies in the literature have shown that the public key operations (for example, elliptic curve cryptography) are practical in mobile devices. However, the Digital signature generation is very costly because of their computational complexity. Thus, efficiency of these credentials needs to be addressed. Since mobile healthcare applications deal with sensitive patient data, authenticity of the public keys should be efficient and cost effective to protect the data from unauthorized access.

Challenge 3: In contrast to public-key cryptography, symmetric key cryptography is superior and is easier to implement in term of its computational efficiency. However, symmetric key cryptography is not suitable because it relies on distributing the key in the mobile health system to provide different security services which include privacy of credentials, mutual authentication, and secrecy of session keys. Hence, designing efficient and flexible key distribution protocols for mobile healthcare applications needs to be addressed in the future.

Challenge 4: Obtaining passwords from unconscious patients is not possible so biometric mechanisms should be used for authentication. However, the biometric methods that work with unique biometric features from unconscious patients for identification purposes still needs further research attention in order to correctly authenticate an unconscious patient.

Challenge 5: The privacy of the information stored in the mobile healthcare application must be guaranteed. In this case, designing lightweight, efficient, and robust privacy enhancing techniques for the wearable sensors remains an area of future research.

17 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/a-secure-robust-and-privacy-enhanced-mobile-healthcare-framework/243125

Related Content

Fuzzy Bayesian Context-Aware System to Reduce Electricity Consumption

Kavita Pankaj Shirsat and Girish P. Bhole (2021). *International Journal of Data Analytics* (pp. 86-98).

www.irma-international.org/article/fuzzy-bayesian-context-aware-system-to-reduce-electricity-consumption/272110

Learning Analytics in the Monitoring of Learning Processes: 3D Educational Collaborative Virtual Environments

Rosa Reis and Bertil P. Marques (2021). *Advancing the Power of Learning Analytics and Big Data in Education* (pp. 142-169).

www.irma-international.org/chapter/learning-analytics-in-the-monitoring-of-learning-processes/272952

Using Smartphones to Capture Personal Travel Behavior

Sheila Ferrer and Tomás Ruiz (2014). *Mobile Technologies for Activity-Travel Data Collection and Analysis* (pp. 171-186).

www.irma-international.org/chapter/using-smartphones-to-capture-personal-travel-behavior/113210

Analysis of Heart Disease Using Parallel and Sequential Ensemble Methods With Feature Selection Techniques: Heart Disease Prediction

Dhyan Chandra Yadav and Saurabh Pal (2021). *International Journal of Big Data and Analytics in Healthcare* (pp. 40-56).

www.irma-international.org/article/analysis-of-heart-disease-using-parallel-and-sequential-ensemble-methods-with-feature-selection-techniques/268417

Data Analysis and Visualization in Python for Polar Meteorological Data

V. Sakthivel Samy, Koyel Pramanick, Veena Thenkanidiyoor and Jeni Victor (2021). *International Journal of Data Analytics* (pp. 32-60).

www.irma-international.org/article/data-analysis-and-visualization-in-python-for-polar-meteorological-data/272108