International Journal of E-Health and Medical Communications
Volume 10 • Issue 4 • October-December 2019

Simulating Light-Weight-Cryptography Implementation for IoT Healthcare Data Security Applications

Norah Alassaf, Umm Al-Qura University, Makkah, Saudi Arabia
Adnan Gutub, Umm Al-Qura University, Makkah, Saudi Arabia

ABSTRACT

Short period monitoring and emergency notification of healthcare signals is becoming affordable with existence of internet of things (IoT) support. However, IoT does not prevent challenges that may hinder the appropriate safe spread of medical solutions. Confidentiality of data is vital, making a real fear requesting cryptography. The limitations in memory, computations processing, power consumptions, and small-size devices contradict the robust encryption process asking for help of low-weight-cryptography to handle practically. This article presents a comparative analysis of performance evaluation of three trusted candidate encryption algorithms, namely AES, SPECK and SIMON, which are simulated and compared in details to distinguish who has the best behaviour to be nominated for a medical application. These encryption algorithms are implemented and evaluated in regard to the execution time, power consumption, memory occupation and speed. The implementation is carried out using the Cooja simulator running on Contiki operating system showing interesting attractive results.

KEYWORDS

AES, Contiki Operating System, Cooja Simulation, Encryption, Healthcare Data System, Internet of Medical Things - IoMT, Internet of Things - IoT, Light-Weight-Cryptography - LWC, SIMON, SPECK

INTRODUCTION

Internet of Things (IoT) play affective role in supporting the ubiquitous computing, allowing all devices to communicate and interact facilities of exchange of data. Network Architecture of the IoT is known having three basic layers: perception layer, network layer, and application layer (Wu et al., 2010). The perception layer can be defined as the source of information collection. The network layer is used to connect the perception layer to the user application layer. Finally, the application layer is used to involve users into the scenario. IoT play increasing role impacting different fields such as smart transport, energy, cities, and healthcare applications (Gutub, 2015).

This work is focusing on improving IoT healthcare services. The presence of remote healthcare monitoring systems has led reducing the cost of treatment while enhancing the quality of services. In fact, the number of elderly people is increasing by the day, while the number of young people

DOI: 10.4018/IJEHMC.2019100101

under 25 is becoming reduced to the least demanding more and more healthcare services (Zhang, Thurow, & Stoll, 2014). Thus, the need for hospitals increased as well as the treatment costs. However, successful deployment of healthcare systems depends on having the adequate security and privacy of the patient's data (Gutub, 2011). A common solution is to secure data via trusted cryptography, i.e. symmetric-key or public-key cryptography (Gutub & Khan, 2012), where many research works have been presented earlier to secure data via RSA or more advanced elliptic curve cryptography (Gutub, Tabakh, Al-Qahtani, & Amin, 2013). However, when it comes to the highly constrained devices, these traditional cryptographic algorithms need significantly high resources in order to execute (Gutub, 2003). Some research proposed constrained solution via hardware special arithmetic implementation involving efficient extraordinary adders (Gutub, & Tahhan, 2008) or redesigning SRAM sub-threshold crypto hardware for low-power utilizations (Gutub & Khan, 2011). Others even further presented investigation slightly modifying the crypto algorithm by merging its arithmetic on pipelined VLSI cryptographic ASIC architecture (Gutub,2006), which is found currently unpractical for healthcare mobile devices demanding more innovative research. With this in mind, light-weight-cryptography (LWC) has been involved, i.e. LWC algorithms are found more suitable to help secure the healthcare systems (AlAssaf et al., 2017). In fact, LWC uses fewer resources and saves time conserving the necessary security measures. Also, from a practical point of view, reducing the encryption time is essential to maintain the patient's life knowing his/her condition in a measurable time. On the other hand, increasing the crypto-computation time may lead to disastrous opposite result such as complications of the health status maybe leading to death of the patient.

In this paper, we propose an extension of securing internet of things (IoT) data for healthcare system via lightweight cryptography (LWC) using block-ciphers as elaboration investigation study to the work previously presented in (AlAssaf et al., 2017). This extension study focused on the preceding results considering implementing the best three candidate LWC algorithms, assuming the same healthcare scenario. With this in mind, many lightweight encryption algorithms have been designed and modelled targeting the IoT hardware applications. This work focuses on AES, SPECK, and SIMON, which have been proven modelled flexible to operate on different platforms (Beaulieu et al., 2015). Other lightweight encryption algorithms have been designed dedicated for specific platform making them out of this investigation. The main contributions of this work are:

1. Select remote healthcare monitoring system, suitable to collect data and transmit it to hospitals to keep track of the patient situation;
2. Protect patient's medical data via encryption security before transmitting into internet, i.e. starting from sensors;
3. Study main hardware and software constraints of the IoT devices asking for LWC;
4. Implement the three encryption algorithms namely: SPECK, SIMON and AES using Cooja simulator and Contiki OS;
5. Evaluate the LWC used regarding execution time, memory consumption and speed.

The flow of this paper is as follows. Next section, Section 2, presents the adopted studied architecture of the healthcare IoT used. Section 3 discusses the security and constraints involved in the medical sensors. Then, Section 4 details the three focused LWC algorithms, i.e. the candidates block ciphers building the scope of this work, to protect the medical data in the IoT utilization. Next, the simulation platform is briefed in Section 5. Then, Section 6 describes the implementation details evaluating the performance and comparing the three encryption algorithms expressing the results in terms of execution power consumption, memory occupation, and speed performance. Finally, Section 7 concludes the work summarizing the results and its attractive applicability.

Lived Experiences in ‘Active’ Small Group Learning

P. Ravi Shankar (2012). *International Journal of User-Driven Healthcare (pp. 14-17).*
www.igi-global.com/article/lived-experiences-active-small-group/64325?camid=4v1a

Adoption of ICT in an Australian Rural Division of General Practice

Patricia Deering and Arthur Tatnall (2008). *Encyclopedia of Healthcare Information Systems (pp. 23-29).*
www.igi-global.com/chapter/adoption-ict-australian-rural-division/12918?camid=4v1a