

Chapter 81

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

Norah Alassaf

Umm Al-Qura University, Makkah, Saudi Arabia

Adnan Gutub

 <https://orcid.org/0000-0003-0923-202X>

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.

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 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;

14 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/simulating-light-weight-cryptography-implementation-for-iot-healthcare-data-security-applications/268671

Related Content

Blockchain and Clinical Data Economics: The Tokenization of Clinical Research in the EU

Ana Pêgo, Inês Graça Raposo and Mitchell Loureiro (2021). *Political and Economic Implications of Blockchain Technology in Business and Healthcare* (pp. 269-291).

www.irma-international.org/chapter/blockchain-and-clinical-data-economics/282345

Will Blockchain Bring an End to Corruption?: Areas of Applications and Potential Challenges

Kibum Kim and Taewon Kang (2021). *Research Anthology on Blockchain Technology in Business, Healthcare, Education, and Government* (pp. 1846-1856).

www.irma-international.org/chapter/will-blockchain-bring-an-end-to-corruption/268693

Building, Sustaining, and Growing Multidisciplinary, Multi-Departmental Partnerships to Teach Open Science Tools

Cody Hennesy, Caitlin Bakker, Nicholas J. H. Dunn, David Naughton, Franklin Sayre and Stacie Traill (2022). *Handbook of Research on Academic Libraries as Partners in Data Science Ecosystems* (pp. 169-188).

www.irma-international.org/chapter/building-sustaining-and-growing-multidisciplinary-multi-departmental-partnerships-to-teach-open-science-tools/302753

A Survey of Authentication Schemes in the Internet of Things

Yasmine Labiod, Abdelaziz Amara Korba and Nacira Ghoulmi-Zine (2021). *Research Anthology on Blockchain Technology in Business, Healthcare, Education, and Government* (pp. 1715-1732).

www.irma-international.org/chapter/a-survey-of-authentication-schemes-in-the-internet-of-things/268684

Challenges for Convergence of Cloud and IoT in Applications and Edge Computing

Rashmi S., Roopashree S. and Sathiyamoorthi V. (2022). *Research Anthology on Edge Computing Protocols, Applications, and Integration* (pp. 644-662).

www.irma-international.org/chapter/challenges-for-convergence-of-cloud-and-iot-in-applications-and-edge-computing/304328