International Journal of Natural Computing Research
Volume 10 • Issue 2 • April-June 2021

Symmetric and Asymmetric Encryption Algorithm Modeling on CPU Execution Time as Employed Over a Mobile Environment

Ambili Thomas, Botho University, Botswana
V. Lakshmi Narasimhan, University of Botswana, Botswana

ABSTRACT

This paper presents results on modelling of AES and RSA encryption algorithms in terms of CPU execution time, considering different modelling techniques such as linear, quadratic, cubic, and exponential mathematical models, each with the application of piecewise approximations. C#.net framework is used to implement this study. The authors consider the symmetric encryption algorithm named AES and the asymmetric encryption algorithm named RSA to carry out this study. This study recommends quadratic piecewise approximation modelling as the most optimized model for modelling the CPU execution time of AES and RSA towards encryption of data files. The model proposed in this study can be extended to other symmetric and asymmetric encryption algorithms, besides taking them over a mobile cloud environment.

KEYWORDS

AES Algorithm, Asymmetric Encryption, CPU Execution Time, Mathematical Modelling, Mobile Computing, Optimization, Piecewise Approximation, RSA Algorithm, Symmetric Encryption

INTRODUCTION

Mobile environment facilitates data sharing between devices, which supports mobility across mobile networks. Developed and developing countries experience a tremendous growth in mobile devices' penetration and mobile technologies' usage (Kaliisa et al., 2017). Several studies show that the count of mobile phone subscriptions has surpassed the global population by 2018 and, nearly the entire world population lives within the mobile network range (Telecommunication Union, 2018). Countries in Africa and Asia-Pacific continents have made an incredible growth in this arena within the last five years (Albertini et al., 2019). Increased mobile device penetration results in significant increase in the development of mobile applications in various domains. Mobile users download and use numerous mobile applications in their mobile devices. Therefore, mobile devices consume substantial amount of energy to run the augmented number of mobile applications. But the mobile devices depend on the constrained energy sources to operate (Callou et al., 2010), (Toldinas et al, 2014). Thus, it is important to ponder about the optimized energy consumption of mobile devices. Ubiquity of mobile phones implies that secured data transmission over the mobile environment, along with its performance are major areas of concern. Now-a-days, organizations operate their business effectively through the

DOI: 10.4018/IJNCR.2021040102

implementation of various mobile computing techniques. This situation demands for high security of organizations' sensitive data and optimized energy consumption of mobile devices.

A tradeoff exists between the security and the energy consumption of mobile devices. Higher security is achieved with the cryptographic algorithm having a bigger number of rounds and long encryption key sizes. Due to the higher computation complexity involved, cryptographic algorithms consume substantial amount of energy and execution time. Higher security demands higher energy consumption (Toldinas et al., 2014). The execution of cryptographic algorithms to encrypt the data results in reduction of battery lifetime in mobile devices (Toldinas et al., 2014). Since cryptographic algorithms are widely used to ensure security of data at rest and data in transit and, it is important to examine the performance of cryptographic algorithms running within the context of energy used. Central Processing Unit (CPU) execution time which consumes majority of the energy during execution, is used as one of the metrics to analyze cryptographic algorithms' energy consumption. The estimation of CPU execution time and energy consumption are essential [11] to be carried out in the mobile environment. Thus, an optimized energy model which supports the most possible secured data processing is essential in the mobile environment.

Symmetric and asymmetric encryption algorithms are chosen for this study in order to utilize the advantages of both categories of cryptographic encryption algorithms. The same key is used for encryption and decryption processes of symmetric encryption, while separate keys are used in case of asymmetric encryption (Singh and Supriya, 2013). Advanced Encryption Standard (AES) is chosen as the symmetric encryption algorithm and Rivest, Shamir, and Adelman (RSA) is chosen as the asymmetric encryption algorithm for this study. As symmetric cryptography involves private key maintenance, it is less secure and more prone to network attacks (Jamgekar and Joshi, 2013). Compared to asymmetric cryptography, symmetric cryptography is faster and is a better fit for applications which supports heavy data transfer.

Considering the wide popularity, AES algorithm has been chosen. Montoya et al. (2013) conclude AES as an optimum algorithm for mobile environment, where the battery consumption is a critical factor. Considering the wide use in encrypted connections and digital signatures (Karakra and Alsadeh, 2016), RSA algorithm has been chosen. Optimized models based on CPU execution time of AES and RSA algorithms have been proposed. The metric chosen for this study is the CPU execution time taken by the AES and RSA algorithm for encrypting a data file.

The objective of this study is to examine and find out the actual CPU execution time taken by the AES and RSA algorithms. This result can be used to analyze and optimize the energy consumption of the AES and RSA algorithms. The rest of the paper is organized as follows: section 2 provides an overview of the related literature, while section 3 describes the proposed model. Section 4 provides experimental analysis of data and, section 5 compares the mathematical models. The conclusion summarizes the paper and provides pointers for further work in this arena.

BACKGROUND

AES algorithm is chosen for this study as this is one of the most widely used security algorithm and is suitable for the resource constraint mobile devices. Lu and Tseng (2002) have proposed an AES algorithm architecture which is suitable for the mobile devices. Toldinas et al. (2014) propose an energy security tradeoff model based on cryptography which describes how the cryptographic algorithms' security and energy consumption relate. This study concludes AES as one of the most energy efficient asymmetric algorithms among other analyzed algorithms such as RC4 and Serpent. They discuss that a higher dependency exists between the key size and the energy consumption of asymmetric algorithms. The AES algorithm is selected because it is most widely used for encryption and energy efficiency. Ramesh and Suruliandi (2013) have done a comparative study on the performance of cryptographic algorithms, such as AES, Data Encryption Standard (DES), and BLOWFISH using performance metrics - execution time, memory usage and throughput. A study has been conducted by Elminaam