Chapter 2
Energy Optimization in Cryptographic Protocols for the Cloud

Swapnoneel Roy
University of North Florida, USA

Sanjay P. Ahuja
University of North Florida, USA

Priyanka D. Harish
University of North Florida, USA

S. Raghu Talluri
University of North Florida, USA

ABSTRACT

In this chapter, we study the energy consumption by various modern cryptographic protocols for the cloud from the algorithmic perspective. The two categories of protocols we consider are (1) hash functions and (2) symmetric key encryption protocols. We identify various parameters that moderate energy consumption of these hashes and protocols. Our work is directed towards redesigning or modifying these algorithms to make them consume lesser energy. As a first step, we try to determine the applicability of the asymptotic energy complexity model by Roy on these hashes and protocols. Specifically, we try to observe whether parallelizing the access of blocks of data in these algorithms reduces their energy consumption based on the energy model. Our results confirm the applicability of the energy model on these hashes and protocols. Our work is motivated by the importance of cryptographic hashes and symmetric key protocols for the cloud. Hence the design of more energy efficient hashes and protocols will contribute in reducing the cloud energy consumption that is continuously increasing.

DOI: 10.4018/978-1-5225-4044-1.ch002

INTRODUCTION

Motivation to consider energy efficiency in delivering information technology solutions for the Cloud comes from: 1) the usage of data centers in the Cloud with strong focus on energy management for server class systems; 2) the usage of personal computing devices in the Cloud such as smartphones, handhelds, and notebooks, which run on batteries and perform a significant amount of computation and data transfer; and, 3) Cloud providers expecting to invest in equipment that will form an integral part of the global network infrastructure. On the other hand, information security has become a natural component of all kinds of technology solutions for the Cloud. Security protocols consuming additional energy are often incorporated in these solutions. Thus, the impact of security protocols on energy consumption needs to be studied. Ongoing research in this context has been mainly focused on energy efficiency/consumption on specific hardware and/or different systems/platforms. Very little is known or has been explored regarding energy consumption or efficiency from an "applications" perspective, although apps for smartphones and handhelds abound.

Cryptography has evolved from the earliest forms of secret writing to current era of computationally secure protocols, addressing range of security issues. In modern age, cryptography is not only about encryption, but it has larger objective of ensuring data protection from adversary's activities. Scope of modern cryptography also includes techniques and protocols to achieve authentication, nonrepudiation, and integrity objectives. Complexity of cryptology methods and its applications have continuously increased and evolution of computers has given a completely new dimension to this. Now cryptography problems/algorithms are measured in terms of computational hardness. In this journey, cryptography has always received a threat of getting obsolete because of rapidly increasing computational capabilities.

However, cryptography techniques still have great relevance and importance for the cloud, and the cloud enabled industry to keep them protected from dynamically changing threat scenarios (Jasim et al., 2013; Li et al., 2013; Somani et al., 2010; Li et al., 2010; Muñoz et al., 2016).

Energy has become a first-class parameter now days. This has been triggered with the ever-increasing energy generation by the data centers, and with the advent of the hand-held battery-driven devices like laptops, PDAs, etc. Cryptographic protocols have become an integral part of these devices to make them secured. Also, the cryptographic protocols are generally very expensive in terms of their energy consumption. Therefore, especially for hand held devices, the protocols drain out a lot of battery power while operating. A network flooding attack with the intention of causing a simple denial of service by depleting the battery life of the device has been illustrated in (Salerno et. al 2011). They show that these flooding attacks can be carried out utilizing a smartphone as the aggressor in order to attack other mobile devices and that the procedure for such attacks is not difficult. A simple tool has been developed in order to carry out these attacks and to show that even though these attacks are relatively simple, they can have profound effects.

Therefore, the necessity of reducing the energy consumption of cryptographic protocols comes into picture. As mentioned, we have considered two classes of cryptographic protocols to implement a parallelism technique based on the energy model of (Roy et al., 2013) that leads to reduction in their energy consumption.