# Chapter 61
# An Efficient Privacy-Preserving Approach for Secure Verifiable Outsourced Computing on Untrusted Platforms

**Oladayo Olufemi Olakanmi**
*University of Ibadan, Ibadan, Nigeria*

**Adedamola Dada**
*University of Ibadan, Ibadan, Nigeria*

## ABSTRACT

*In outsourcing computation models, weak devices (clients) increasingly rely on remote servers (workers) for data storage and computations. However, most of these servers are hackable or untrustworthy, which makes their computation questionable. Therefore, there is need for clients to validate the correctness of the results of their outsourced computations and ensure that servers learn nothing about their clients other than the outputs of their computation. In this work, an efficient privacy preservation validation approach is developed which allows clients to store and outsource their computations to servers in a semi-honest model such that servers' computational results could be validated by clients without re-computing the computation. This article employs a morphism approach for the client to efficiently perform the proof of correctness of its outsourced computation without re-computing the whole computation. A traceable pseudonym is employed by clients to enforce anonymity.*

## 1. INTRODUCTION

Exponential increase in demand by weaker devices to perform high computation has increased research efforts on how weaker devices can effectively outsource their computation to more powerful devices such as cloud servers or any other devices with more computational power. In commensalism and parasitism network paradigm, workers are not trustworthy or otherwise can be easily compromised by the activities

DOI: 10.4018/978-1-7998-8954-0.ch061

of adversaries by modifying the client's computation and return reasonable but invalid results. This may be as a result of attack on the server or non-cooperation of the server by not performing the outsourced computations. Apart from this, privacy of the client also needs to be protected either in outsourcing computing or Internet of Things (IoT) networks (Gupta et al., 2016; Negil et al., 2013; Li et al., 2018; Gupta et al., 2018).

Several works had been done on how clients can validate the result of the outsourced computation without re-computation. Some of them involve an interactive approach to validate results at a considerable overhead. One of the approaches involves the client sending the same task to multiple workers and compares their results. If there is considerable similarity in the results of the targeted worker and other workers, the client ascertains correctness of the computation as done by the targeted worker otherwise invalidate the results. This approach shows that verifiable outsourced computation is possible, however it is cost ineffective in practice. A verifiable computation scheme becomes efficient and adoptable if it is efficient and has a low computation overhead. As a result of this, another approach with minimum overhead is required by the client for outsourcing computation with an effective proof of correctness feature. Elusiveness of efficient verifiable outsourcing computation schemes has made it to be a serious research interest in cloud computing, IoT and parasitic computing, even for a certain class of functions.

In this paper, a novel approach which allows clients to store and outsource their computation to a more powerful service such that the correctness of the computation could not only be validated but the privacy of the clients is preserved at a minimum overhead.

## 2. RELATED WORKS

The wide variety of small computationally weak devices and the growing number of computationally intensive tasks makes the delegation of computation to large data centers a desirable solution. Much research had been done on outsourcing computation, few of them delve into how computation can be outsourced to honest workers while other proposed different ways to verify outsourced computation results from semi-honest workers. However, in some of these outsourcing and verification schemes, users lose direct access to the computational tasks, and may experience possible threats like data privacy and invalidity of results.

For example, Anmin et al. (2018) proposed two efficient algorithms for outsourcing multiple and single composite modular exponentiations. Their proposed scheme remarkably improved checkability by allowing user to discover any misbehavior and inconsistency. The scheme has a subroutine to realize identity-based signatures and identity-based multi-signatures schemes. However, their scheme only checks the integrity of the result not the correctness of the result. Xing and Chunming (2014) proposed a protocol for outsourcing characterization of polynomials and computation of Eigen values of a matrix. The protocol engaged disguise approach for the construction of efficient, verifiable outsource computation scheme without much cryptography assumption. Their scheme is application centric. Also, Kai et al. (2017) proposed a scalable verifiable outsourcing computation protocol for marine cloud computing to combat the problem of low storage and computation associated with the ocean-going vessels. Their protocol allows users who have verification tokens to verify the correctness of the computational results returned by the cloud. They engaged a non-interactive method for the proof of correctness using an oracle random model.