Chapter 3

Data Confidentiality and Integrity Preserving Outsourcing Algorithm for System of Linear Equation to a Malicious Cloud Server

Malay Kumar
National Institute of Technology Raipur, India

Manu Vardhan
National Institute of Technology Raipur, India

ABSTRACT

Cloud computing has become a revolution in the field of computing, which enables flexible, on-demand, usage of computing resources in pay-as-per-use model. However, data and computation go to some third-party cloud server beyond the physical control of client escalates various privacy and security concern. This paper proposes an improved outsourcing algorithm for system of linear equation (SLE). The improvements are first, the existing work uses expensive cryptographic computation such as Paillier encryption for security arrangement, the proposed solution does not use such cryptographic primitives rather uses efficient linear transformation method. Secondly, the previous work uses an iterative process, which required L rounds of communication between the client and cloud server, at the same time each iteration causes burden of a decryption followed by a matrix vector multiplication. However, the proposed solution required an optimal one round of communication and one-time transformation and retransformation service. Third, the previous work gives result verification method with (1/2l$^{)}$ *error probability, the value of l is a trade-off between security and efficiency. However, the proposed solution gives an error checking with an optimal probability of one. Moreover, a security analysis has been performed on the previous method, which proves marginal security arrangement due to inappropriate use of the Paillier encryption scheme. The proposal has been verified through theoretical and experimental analysis, which demonstrate the superiority of the proposed algorithm as compared to the existing algorithm.*

DOI: 10.4018/978-1-5225-5222-2.ch003

INTRODUCTION

Cloud computing has become increasingly important in both business and academia due to strong financial viability. It reduces both the capital and operational investment spend on the procurement and maintenance of IT infrastructure. Cloud computing enables ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction (NIST, Mell, & Grance, 2011). A resource-constrained client usually has relatively limited CPU, storage and battery. If a client connected to cloud server over internet is no longer restricted to limited CPU, storage, and bandwidth else it leverages the abundance of computing resources due to seamless access to the data centers (Shiraz, Gani, Khokhar, & Buyya, 2013). The cloud computing paradigm empowers them to execute massive computations by outsourcing their computation load to the cloud server. Despite the tremendous benefits, this promising paradigm brings many security and privacy concerns, which makes a client reluctant to outsource their sensitive and classified data to the cloud server. The first security concern is the privacy of confidential data. The input data have been often sensitive, it may be personal identifiable information, financial records, and trends of stock prices, scientific research data and many more. Therefore, the input data needs to be encrypted to maintain the confidentiality and integrity of data before transferring to the cloud server. One method to address such security concern is to apply some encryption scheme, but the tradition encryption scheme would not work out here, because it changes the input into the cipher and performing computation on cipher is very difficult. The second concern is the correctness of the result. The client has no information about how the cloud server performs the computation inside their data centers. The cloud server may return invalid result due to a flaw, bug in the logic or may be intentionally deviated from the algorithm instruction (behave maliciously), means there is no guaranty on the integrity of the result. Therefore, an outsourcing algorithm must be capable of providing privacy to the confidential data (input and output) and proficiently in verification of the result. The other challenges are efficiency and correctness of algorithm. To outsource the computation on the cloud server, it is required to do some preprocessing such as input transformation for privacy, result verification, computation of the problem and ultimately the re-transformation. Therefore, the computation perform on the client system (viz., transformation, verification, and retransformation) must be substantially lesser than executing the SLE else the outsourcing has no mean (F. Chen, Xiang, & Yang, 2014; Lin & Chen, 2010; Mohassel, 2011).

In summary an outsourcing algorithm must satisfy the following four design goals: correctness, security, verifiability, and efficiency (Xiaofeng Chen et al., 2015).

1. **Correctness:** The client and the cloud server should follow the outsourcing algorithm instructions then only the outsourcing algorithm will produce correct result.
2. **Security:** There are two goals of the transformation operation. The first is to provide security to the confidential data and the second is to allow the cloud server to carry out meaningful operation on the transformed data (Lei, Liao, Huang, & Heriniaina, 2014; Wang, Ren, & Wang, 2011; Wang, Ren, Wang, & Urs, 2011; Zhang & Blanton, 2014).
3. **Verification:** The verification algorithm of the outsourced computation should be design in such a way that the client will able to detect cheating and server misbehavior. However, the verification algorithm should be efficient and not involved in expensive computation. Moreover the cost of verification should strictly be less than executing the problem itself.