Light-weight Accountable Privacy Preserving (LAPP) Protocol Allowing to Audit the Third-Party Auditor in the Cloud Environment

Mohamed Ben Haj Frej, Julius Dichter, Navarun Gupta
Department of Computer Science and Engineering
University of Bridgeport, Bridgeport, CT

Abstract

Cloud computing is situating its position in the market as the next disruptive utility paradigm based on the pay as you use model. It is changing the way information technology (IT) operates from individuals and companies' perspectives. Cloud computing comes with different offerings to accommodate diverse applications. Security concerns are what's making many companies reluctant from fully embracing the cloud realm. To enhance trust and entice adoption between cloud clients (CC) and cloud service providers (CSP), cloud computing based on a third-party auditor (TPA) has been introduced.

Hence introducing a solution with a TPA, comes with its toll in terms of trust and processing overhead. A light-weight security protocol to give the CC an extra control with tools to audit the TPA and the CSP is paramount to the solution.

In this paper, we are introducing a novel protocol: Light-weight Accountable Privacy Preserving (LAPP) Protocol. Our proposed protocol is based on a novel mathematical model along with three algorithms. We have conducted simulation experiments to measure the impact of our method, compared to the most eminent privacy preserving methods, using the GreenCloud simulator. Our results showed superiority in performance for LAPP concerning time complexity, accuracy, and computation time on auditing.

Introduction

- Cloud computing is based on pay as you use computing rather than having local servers or personal devices to handle applications.
- Computing services, such as database transactions, storage, software, computing, and applications, are delivered to local devices through Internet.
- There are four delivery models in cloud computing, namely:
  - Public cloud,
  - Private cloud,
  - Community cloud,
  - Hybrid cloud.
- Based on the services, the cloud is divided into three models:
  - Infrastructure as a Service (IaaS).
  - Platform as a Service (PaaS).
  - Software as a Service (SaaS).
- The third party auditor systematically examines evidence for compliance to established criteria.
- As security is the main concern, TPA is becoming more and more important with constraints:
  - accomplish efficient auditing,
  - avoid involving new security vulnerabilities.
- TPA could intentionally or unintendedly become a source of vulnerabilities to the overall solution.
  - We need a protocol to determine the dishonest role of TPA when auditing the records.
  - The design requires low communication and computation overhead.

Algorithm 1

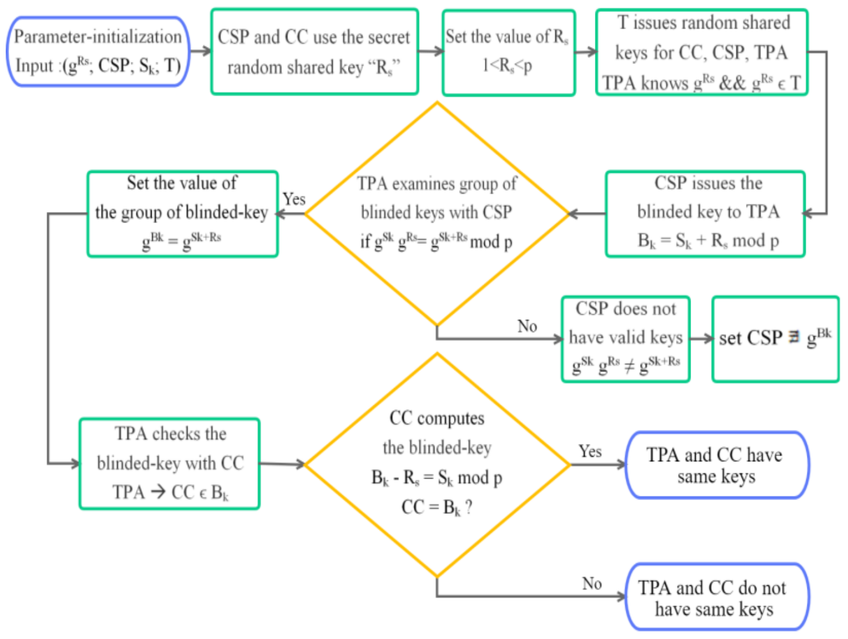

Figure 1: The key-extraction process of three stakeholders

Algorithm 2

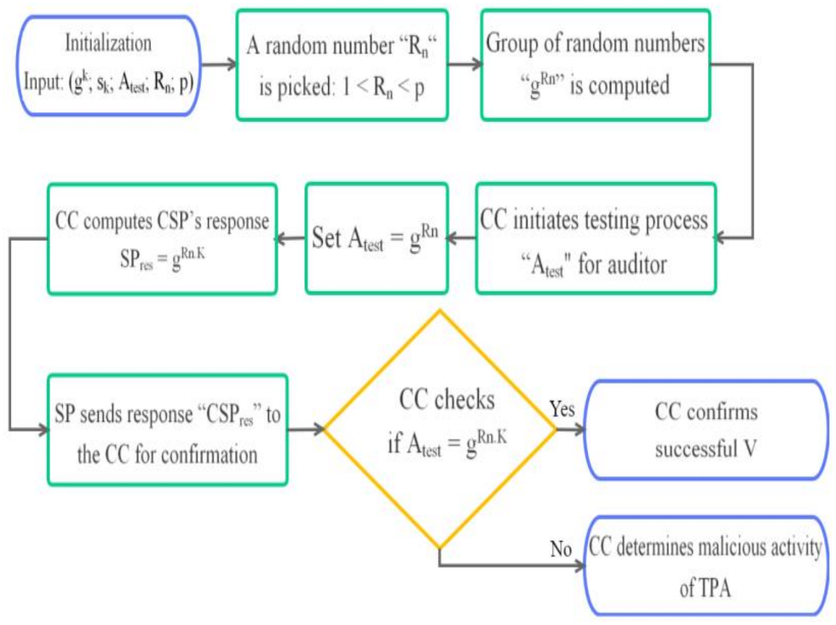

Figure 2: The Key Validation process to avoid the malicious role of TPA

Algorithm 3

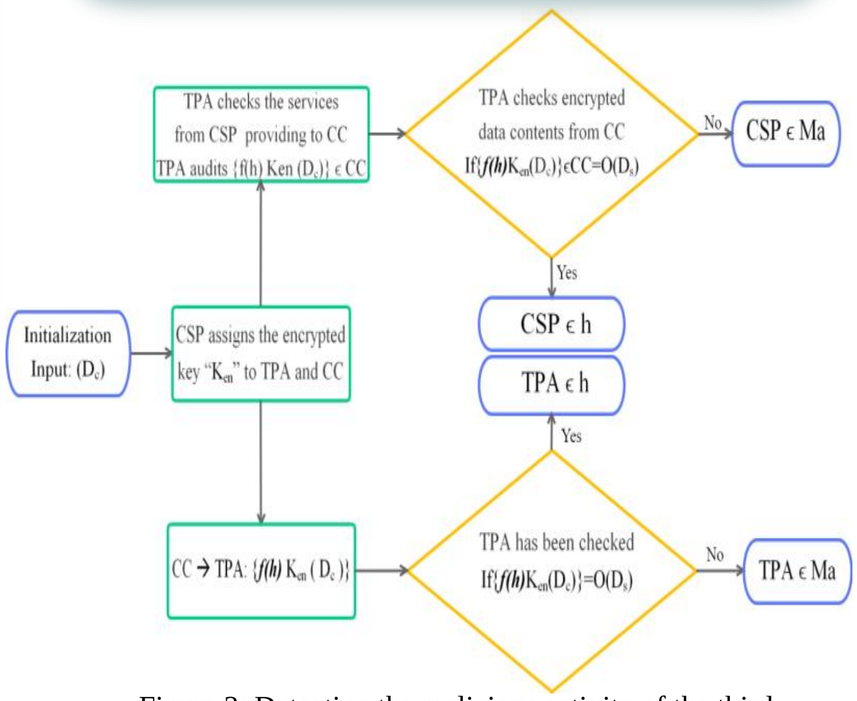

Figure 3: Detecting the malicious activity of the third-party auditor and the cloud service provider

LAPP's Mathematical Model

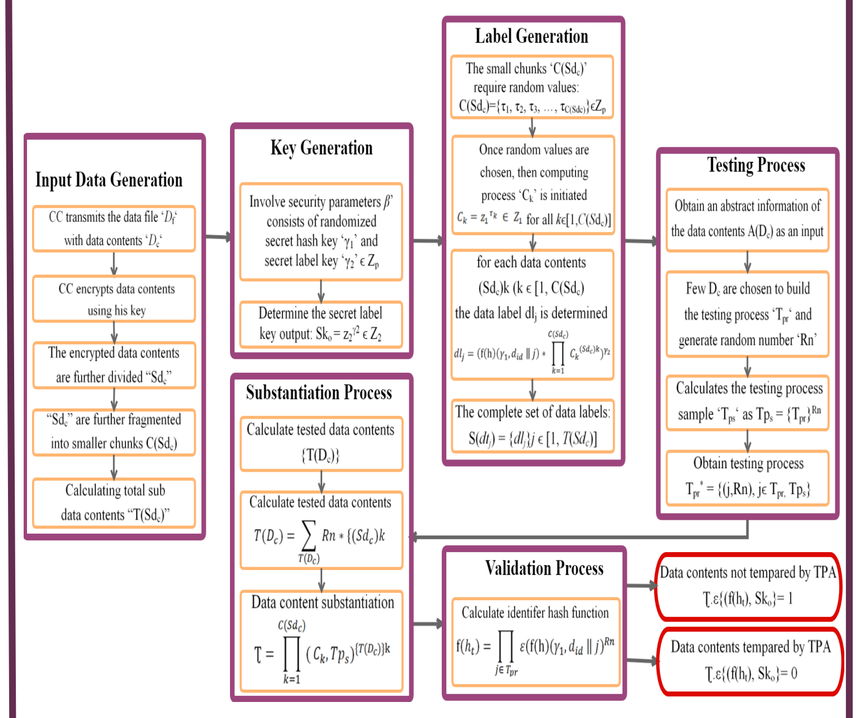

Figure 4: Mathematical Model

Simulations

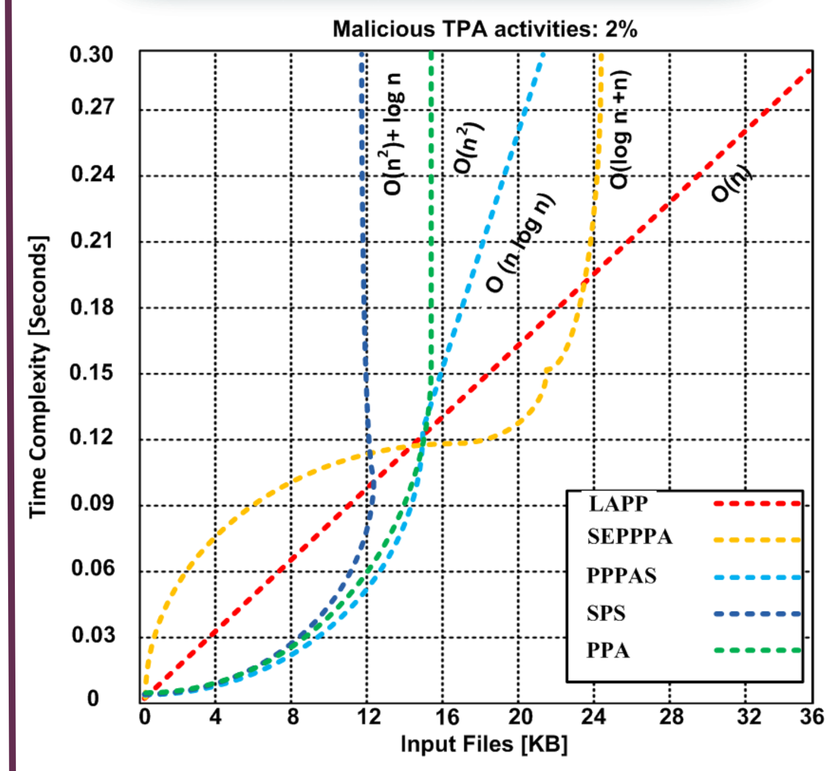

Figure 5: Time complexity versus input files

Conclusion

- A TPA comes with its issues, mainly trust and an extra cost regarding processing and communication
- To verify LAPP's performance, we have conducted simulations measurements with the introduction of TPA's malicious attempts at the rates of 0%, 1%, 2% and 5% as follows:
  - Computation time on Auditing (Number of Challenged Data Blocks).
  - Accuracy (Number of Malicious Attempts).
  - Time complexity (Input Files).
- All simulation results have shown noticeable superiority of our introduced method (LAPP)
- In our future work, we are planning to simulate our protocol along with the other methods on different size networks.

References:

1. Mell, P. and T. Grance, *The NIST definition of cloud computing.* 2011.
2. Wang, Q., et al., *Enabling public auditability and data dynamics for storage security in cloud computing.* Parallel and Distributed Systems, IEEE Transactions on, 2011. **22**(5): p. 847-859.
3. Xiao, Z. and Y. Xiao, *Security and privacy in cloud computing.* Communications Surveys & Tutorials, IEEE, 2013. **15**(2): p. 843-859.
4. Das, P., H. Classen, and R. Davé, *Cyber-Security threats and privacy controls for cloud computing, emphasizing software as a service.* The Computer & Internet Lawyer, 2013. **30**: p. 20-24.
5. Grobauer, B., T. Walloschek, and E. Stöcker, *Understanding cloud computing vulnerabilities.* Security & privacy, IEEE, 2011. **9**(2): p. 50-57.
6. Sabahi, F. *Cloud computing security threats and responses*. in *Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on*. 2011. IEEE.
7. Zissis, D. and D. Lekkas, *Addressing cloud computing security issues.* Future Generation computer systems, 2012. **28**(3): p. 583-592.
8. Abbdal, S.H., et al. *Secure Third Party Auditor for Ensuring Data Integrity in Cloud Storage*. in *Ubiquitous Intelligence and Computing, 2014 IEEE 11th Intl Conf on and IEEE 11th Intl Conf on and Autonomic and Trusted Computing, and IEEE 14th Intl Conf on Scalable Computing and Communications and Its Associated Workshops*. 2014. IEEE.
9. Li, L., et al. *Study on the third-party audit in cloud storage service*. in *Cloud and Service Computing (CSC), 2011 International Conference on*. 2011. IEEE.
10. Rewadkar, D. and S.Y. Ghatage. *Cloud storage system enabling secure privacy preserving third party audit*. in *Control, Instrumentation, Communication and Computational Technologies (ICCICCT), 2014 International Conference on*. 2014. IEEE.
11. Hussain, M. and M.B. Al *Effective Third Party Auditing in Cloud Computing*. in *Advanced Information Networking and Applications Workshops (WAINA), 2014 28th International Conference on*. 2014. IEEE.
12. Venkatesh, M., M. Sumalatha, and C. SelvaKumar. *Improving public auditability, data possession in data storage security for cloud computing*. in *Recent Trends In Information Technology (ICRTIT), 2012 International Conference on*. 2012. IEEE.
13. Han, S. and J. Xing. *Ensuring data storage security through a novel third party auditor scheme in cloud computing*. in *2011 IEEE International Conference on Cloud Computing and Intelligence Systems*. 2011. IEEE.