©2016 IEEE. Reprinted, with permission, from M. Ben Haj Frej, J. Dichter, and N. Gupta, "Security in Cloud Computing Based on Third Party Auditor: A Survey." In Proceedings of 2016 Annual Connecticut Conference on Industrial Electronics, Technology & Automation (CT-IETA), Bridgeport, CT, 2016.

This material is posted here with permission of the IEEE. Such permission of the IEEE does not in any way imply IEEE endorsement of any of the University of Bridgeport's products or services. Internal or personal use of this material is permitted. However, permission to reprint/republish this material for advertising or promotional purposes or for creating new collective works for resale or redistribution must be obtained from the IEEE by writing to pubs-permissions@ieee.org. By choosing to view this document, you agree to all provisions of the copyright laws protecting it.

Security in Cloud Computing Based on Third Party Auditor: A Survey

Annual IEEE Connecticut Conference on Industrial Electronics, Technology & Automation
(CT-IETA 2016)

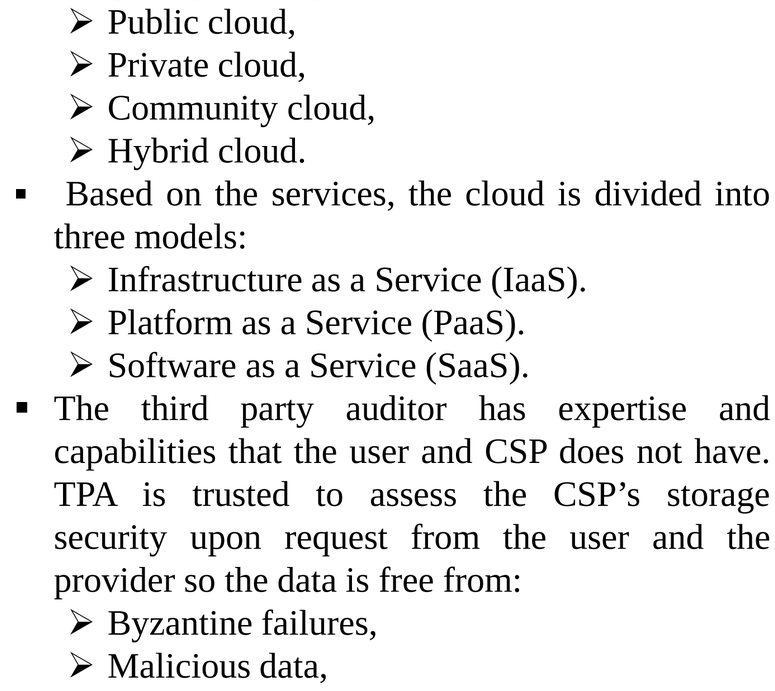
Mohamed Ben Haj Frej, Julius Dichter, Navarun Gupta
Department of Computer Science and Engineering
University of Bridgeport, Bridgeport, CT

Abstract

This Paper surveys security in cloud computing based on Third Party Auditor (TPA) also known as Trusted Third Party (TTP). There are various security models for safeguarding the client's data in cloud. TPA provides secure connections between the user and the cloud server. Cloud Service Provider (CSP) Provides the clients with cloud storage and service. TPA has access to the client's cloud data and all the critical information. There are many security models for making the TPA more reliable so the clients can trust the third party for storing their data. In this paper, we survey mostly the types of security models based on Third Party Auditing in cloud. We also discuss how these security models enable the third parties to gain the clients trust. The classification has been based on the adopted security method as well as on the kind of threats they are addressing.

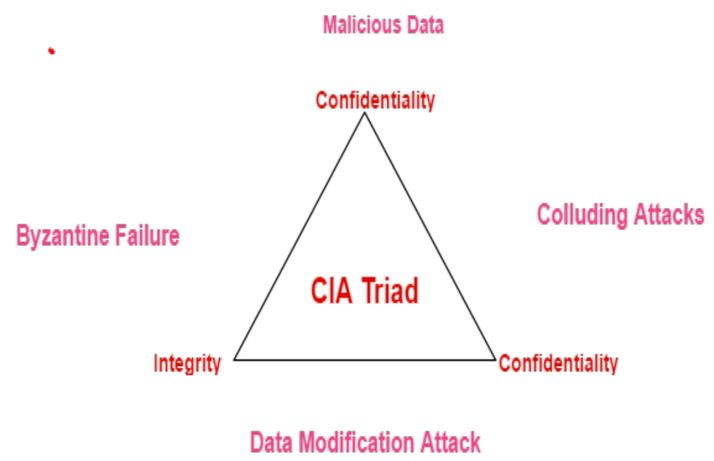
Introduction

- 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 has expertise and capabilities that the user and CSP does not have. TPA is trusted to assess the CSP's storage security upon request from the user and the provider so the data is free from:
  - Byzantine failures,
  - Malicious data,
  - Data modification attack
  - Server colluding attacks



Cloud Computing Based on Trusted Third Party

Security Threats:



Cloud Computing Vulnerabilities

- *Confidentiality*: only authorized parties or systems having the ability to access protected data.
- *Integrity*: assets can be modified only by authorized parties or in authorized ways.
- *Availability*: the property of a system being accessible and usable upon demand by an authorized entity.
- *Access Control*: the data is illegally accessed due to astringent access control, Authentication and Identification that is due to multi-tenancy resulting into interoperability defects.
- *Cloud Vulnerabilities*: for the third party management models, most security problems stem from:
  - Loss of control
  - Lack of trust
  - Multi-tenancy

Methods for improving security in TPA

RECAPITULATION TABLE

Security Model	Security Requirements	Threats	Advantages
Novel Third Party Auditor Scheme	• RSA: used for encryption algorithm and Bilinear Diffie-Hellman: used to secure the keys while exchanging them. • Bilinear Diffie-Hellman being the proper method to exchange keys which allows two entities to share secret keys without any prior knowledge.	• Data storage security.	• Complexity in computing is reduced. • Confidentiality of users in cloud environment. • Authentication is secure.
Proof of Retrievability Scheme (OPoR)	• The different entities present in this scheme are Client, Cloud Storage Server and Cloud Audit Server. • Files which are remotely stored are audited by using a cloud server which is independent of the storage server.	• Reset attacks occur during upload phase against storage.	• Significantly reduced computation overhead. • Both dynamic data operation and public verifiability is supported.
Layered Interleaving Technique	• To tolerate multiple failures, erasure correcting code is used. • TPA delegates the task of verification in order to save time on user's side. • Challenge token verification, correctness verification and data recovery are the steps involved in this technique.	• During data auditing TPA should not learn the user's data content.	• Highly efficient in recovering the singleton losses. • Recovering the bursty data losses.
Privacy Negotiation Language (PNL) Mechanism	• PNL mechanism is based on description logic. • To guarantee the availability, erasure code in file distribution is used. • Public auditing is required for stored data; hence TPA is used.	• Does not guarantee the security of user privacy data.	• Protects the user data from being misused. • Protects against byzantine failures by dynamic data operation and server colluding attacks in cloud.
Privacy-preserving Public Auditing for Shared Cloud Data	• Proxy re-signature scheme is used for outsourcing the updated operations. • Encryption is done by dynamic broadcast in order to distribute securely the private key to the dynamic group members.	• TPA consumes more time and bandwidth to achieve high error detection probability.	• Highly efficient for dynamic groups. • Public auditability and data dynamic for remote data integrity check.
Securing the cloud storage audit service	• It's based on feedback based audit scheme. • It's a light weight protocol and for the computational audit it adopts multi-TPAs. • Three phases: Setup, release and execute phase • User executes the final verification task.	• Processing proofs is required. • Running time analysis should be done.	• Frame and colluding attacks are prevented.

Conclusion

In this paper, we have surveyed the main security models and the techniques they are using to overcome the security issues. The focus is centered based on Third Party Auditor in cloud computing which does the auditing process on behalf of the client, establishes the secure connection and guarantees the integrity of the data. The classification has been based on:

- The adopted security methods
- The kind of threats these methods are addressing.

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.