JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

SURVEYING AND ANALYZING SECURITY CHALLENGES AND DATA INTEGRITY IN CLOUD COMPUTING

Patel Kajal Miteshbhai

Abstract*— Cloud computing is almost similar distributed computing over a network and means the power to run a program on many connected computers at the same time. The word is also, more commonly used to refer to network-based services which seems to be provided by real server hardware, which really are served up by virtual hardware, simulated by software running on one or more real machines. Such type of virtual servers do not physically exist and can therefore be moved around and scaled up or scale down on the fly without affecting the end user - arguably, rather like a cloud. Cloud computing is a model to achieve more reliable, on-demand access to a shared pool configurable computing resources. In cloud computing, IT related abilities are provided as services, accessible without requiring brief information of the underlying technologies, and with minimal management effort. It provides more efficient computing by centralizing storage, bandwidth and memory processing. Adopting cloud computing can result in both negative and positive effects on data security. This paper provides an overview of cloud computing, and discusses related security challenges. We emphasize that even there are many techniques that can improve cloud security, there are in present no one-size fits- all solutions, and future work has to undertake challenges such as service level agreements for security, as well as holistic schemes for insure accountability in the cloud.

Keywords: **Privacy and security; Cloud computing; formatting; security challenges; security strategies.**

I. INTRODUCTION

The rapid development of the computer technology and network technology brings growing computing demands and storage demands. Many companies, organizations and individuals choose to outsource their computing demands and storage demands. Cloud computing and cloud storage are proposed to satisfy these requirements.

Nowadays storing the data in remote servers (cloud environment) becomes natural and also essential. Cloud is a large shared resource pool and the users move towards them with respect to their needs. It offers amenities for data storage, data access and other computational capabilities in a reliable manner. But, security becomes the major concern for both cloud service provider and the clients who are using the cloud resources. Meanwhile, it reduces the

Overhead of cloud users in maintaining their crucial data in a secured manner. But in those cases, the provider must ensure that their infrastructure is secure enough to protect clients' data and its applications and the customer on the other hand, must be able to attest that the provider has taken proper security measures to protect their crucial information. Although cloud architecture has its own security.

Integrity is the core process to ensure storage security in cloud. In case of compromise by service provider at any cost, entrusting cloud side is of no use. Also at the same time, data must not be tampered by cloud server.

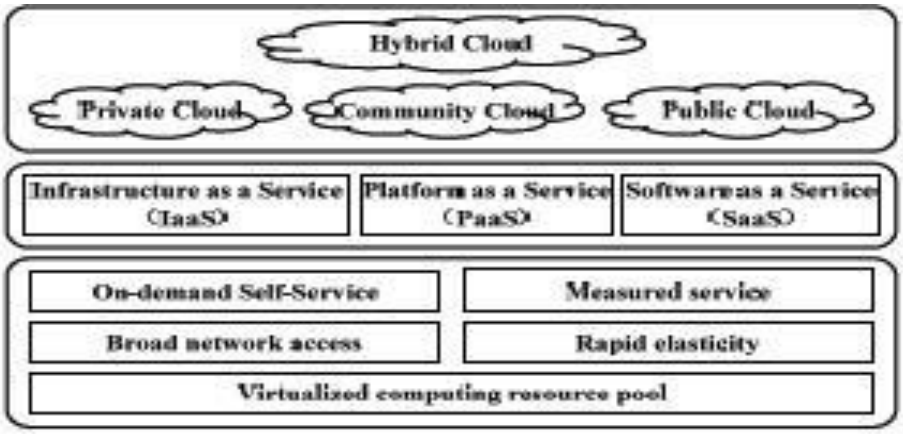


Fig. 1. the NIST's definition model of cloud computing[1]

Cloud computing is a computing model, where resources such as computing power, storage, network and software are abstracted and provided as services on the internet in a remotely accessible fashion. Billing models for these services are generally similar to the ones adopted for public utilities. [2]

"Cloud" is a virtualized pool of computing resources. It can:

• Manage a variety of different workloads, including the batch of back-end operations and user-oriented interactive applications.

• Rapidly deploy and increase workload by speedy providing physical machines or virtual machines.

• Support for redundancy, self-healing and highly scalable programming model, so that workload can be recover from a variety of inevitable hardware/software failure.

• Real-time monitor resources usage, rebalance the allocation of resources when needed. [2] On-demand availability, ease of provisioning, dynamic and virtually infinite scalability are some of the key attributes of cloud computing.

II. MODELS OF CLOUD COMPUTING

Public Cloud

IT activities/functions are provided "as a service," over the Internet

- **Key features:**
  - **Scalability**
  - **Automatic/rapid provisioning**
  - **Standardized offerings**
  - **Consumption-based pricing.**
  - **Multi-tenancy**

Hybrid Cloud: Hybrid Cloud means either two separate clouds joined together (public, private, internal or external) or a combination of virtualized cloud server instances used together with real physical hardware. The most correct definition of the term "Hybrid Cloud" is probably the use of physical hardware and virtualized cloud server instances together to provide a single common service. Two clouds that have been joined together are more correctly called a "combined cloud". [3]

Private Clouds: Private clouds describe offerings that deploy cloud computing on private networks. It consists of applications or virtual machines in a company's own set of hosts. They provide the benefits of utility computing shared hardware costs, the ability to recover from failure, and the ability to scale up or down depending upon demand. [3]

III. SERVICE MODEL OF CLOUD COMPUTING

Software-as-a-Service (SaaS): Software as a service is software that is deployed over the internet and/or I deployed to run behind a firewall in your local area network or personal computer. This is a "pay-as-you go"

model and was initially widely deployed for sales force automation and Customer Relationship Management (CRM). [4] **Platform-as-a-Service (PaaS):** Platform as a service, another SAAS, this kind of cloud computing provide development environment as a service. You can use the middleman's equipment to develop your own program and deliver it to the users through Internet and servers. [4]

Infrastructure-as-a-Service (IaaS): Infrastructure as service delivers a platform virtualization environment as a service. Rather than purchasing servers, software, data centre space or network equipment, clients instead buy those resources as a fully outsourced service. [4]

Hardware-as-a-Service (HaaS): According to Nicholas Carr, "the idea of buying IT hardware or even an entire data centre as a pay-as-you-go subscription service that scales up or down to meet your needs. But as a result of rapid advances in hardware virtualization, IT automation, and usage metering and pricing, I think the concept of hardware-as-a-service, let's call it HaaS, and may at last be ready for prime time." This model is advantageous to the enterprise users, since they do not need to invest in building and managing data centres. [4]

IV. THE COMMON SECURITY ISSUE OF CLOUD COMPUTING

4.1. Seven Security Issues of Cloud Computing Respectively by CSA and Gartner: Cloud Security Alliance (CSA) has published a white paper titled *Top Threats to Cloud Computing* by summarizing various security concerns of cloud computing in March, 2010 [7]. In this white paper, CSA has described seven security risks of cloud computing: 1) *abuse and nefarious use of cloud*, 2) *insecure interfaces and APIs*; 3) *malicious insiders*; 4) *shared technology issues*; 5) *data loss or leakage*; 6) *account or service hijacking*; 7) *unknown risk profile*. Gartner, a global authoritative IT research and analyst firm, has made a widespread investigation, and summarized seven security risks of cloud computing [8]: 1) p*rivileged user access*; 2) r*egulatory compliance*; 3) d*ata location*; 4) d*ata segregation*; 5) r*ecovery*; 6) *investigative support*; 7) l*ong-term viability*.

4.2. Three Parties' Security Issues of Cloud Computing: We analyze the security risks of cloud computing from the perspective of customer, service provider and government as follows.

- *The security risks confronted by customers*

The security risks that customers need to confront in cloud computing environment include:

1) The downtime of cloud computing environment that brings great depress to the confidence of customers cannot be avoided totally; 2) The leak of commercial secrets that means a nightmare for customer cannot be avoided totally; 3) How to face the privilege status of cloud service provider and the security concerns such as fault elimination, damage compensation and business migration etc.

• *The security risks confronted by service providers*

The security risks that service providers need to confront in cloud computing environment include: 1) How to assure the long-term secure operation of the cloud data center and isolate the fault to reduce its influence to a smallest extent are the security risks that service providers have to face with; 2) How to fight against the numerous and aggressive network hackers is a disturbing security problem; 3) For customers with various demands, how to effectively and securely manage these customers and identify and block the malicious customers is another unavoidable task.

• *The security risks confronted by government*

The security risks that government administrators need to confront in cloud computing environment include: 1) How to enhance the security protection of a mass-scale data center is one important concern; 2) How to securely manage the numerous and various scale cloud service providers; 3) How to evaluate and rank the security level of cloud service providers and the security credit of cloud customers, and publish the proactive alarm of malicious programs.

V. PROBLEM DEFINITION

The proposed scheme has four important features:

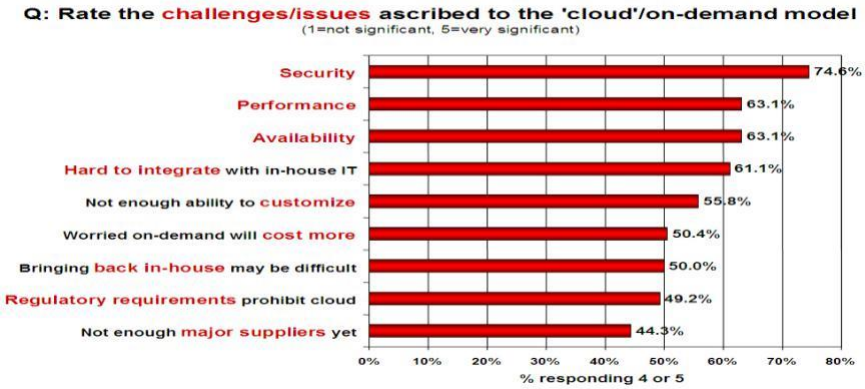
1) it allows the owner to outsource sensitive data to a CSP, and perform full block-level dynamic operations on the outsourced data, i.e., block modification, insertion, deletion, and append,

2) it ensures that authorized users (i.e., those who have the right to access the owner's file) receive the latest version of the outsourced data,

3) it enables indirect mutual trust between the owner and the CSP, and

4) it allows the owner to grant or revoke access to the outsourced data.

VI. NEED FOR RESEARCH Factors Affecting Cloud Model



Security Challenges

Cloud Servers are not fully trustable:

Data Integrity

Data could be corrupted or even deleted in the cloud.

Data integrity in the Cloud system means to preserve information integrity (i.e., not lost or modified by unauthorized users). As data is the base for providing Cloud Computing services, such as Data as a Services, Software as a Service, Platform as a Service, keeping data integrity is a fundamental task.

Furthermore, Cloud Computing system usually provides massive data procession capability. Herein, massive data means many Tera Bytes (TB) data or even Peta Bytes (PB) data in volume. The challenges for data integrity associated with data storage in the Cloud Computing system are as follows. Firstly, in terms of the current development of state for hard disk drivers (or solid state disks or tapes), their capacity increases are not keeping pace with the data growth. Therefore, to scale up the data storage in the Cloud Computing systems, vendors need to increase the population of hard drives (or solid state disks or tapes). This may consequently result in increased high probability of either node failure or disk failure or data corruption or even data loss. Secondly, disk drives (or solid state disks) are getting bigger and bigger in terms of their capacity, while not getting much faster in terms of data access. [3]

Data Access control

Data may be given access to unauthorized users.

As the critical data is situated in the cloud provider infrastructure, the data may be changed without the owner's consent. The modified information may then be retrieved and processed by the owner to make serious decisions. The authenticity of the information in this case is very essential, and therefore needs to be guaranteed. However, general standards to ensure data
integrity do not exist.

Need for Data Integrity Proofs.

- Storing the data to the cloud provider
- Cloud provider may change or corrupt your data
- Client does not know about its confidential data

Auditing as a Service

Checking On Retrieval is not adequate:

- Not sufficient: random sampling cannot cover large size of data
- Not convenient: overhead is too high
- A service to check the cloud data integrity
- Conducted by a Third Party Auditor

Why Third Party Auditing?

A third party auditor can

- Provide unbiased auditing results
- Benefit for both data owners and service providers
  - Data Owners – be ensured data integrity
  - Service Providers – Build good reputation
  - Able to do a good job efficiently
  - essional Expertise
  - Computing Capabilities

VII. RESEARCH ISSUES

- Privacy Preservation

Keep the data confidential against the auditor

- Dynamic Auditing

Allow dynamic updates of data in the cloud

- Batch Auditing

Combine multiple auditing tasks together to improve efficiency **Architecture of 3rd Party Auditing**

Initialization: Data owner sends 1) encrypted data & verification tags to server, and 2) data index to auditor

- **Challenge:** Auditor sends *Challenge* to cloud server
- **Proof:** Server responses with *Proof*
- **Verification:** Auditor verifies correctness of the *Proof*

VIII. **COMPARATIVE STUDY OF DIFFERENT SYMMETRIC BLOCK CIPHERS** There are so many symmetric block ciphers algorithms are there. The mostly used algorithms are AES, DES, 3DES, Blowfish, RC5 and RC6. In this approach, there are so many options are there in choosing the most secure and speedy algorithm.

Table 3.1: Comparison of algorithms based upon the four characteristics, [32]

Characteristics / Algorithms	Block Size	Key Size	Speed	Security
AES	128	128,192 and 256	High	More secure
DES	64	56	Low	Less secure when speed increases
3DES	128	112 or 168	Low	Less Secure
Blowfish	64	32 to 448	Faster except when changing keys	More secure
RC5	32,64 and 128	0 to 255	fast security	High
RC6	32	32	fast	Secure

Here in this table, there are comparison of these algorithms in parameters of:

- Block size
- Key size
- Speed

Security

REFERENCES

[1] S. Haider, *"Security Threats in Cloud Computing,"* no. December, pp. 11–14, 2011.

[2] J. Yang, Z. Chen, and A. Definition, *"Cloud Computing Research and Security Issues,"* pp.10–12, 2010.

[3] 3. P. Hemant, A. Sonule, and H. Wani, *"DEVELOPMENT OF SERVERS IN CLOUD COMPUTING TO SOLVE ISSUES RELATED TO SECURITY AND BACKUP,"* 2011.

[4] L. Guoman*,"Research on Electronic Data Security Strategy Bas ed on Cloud Computing,"* pp. 5–8, 2012.

[5] D. Chen, *"Data Security and Privacy Protection Issues in Clo ud Computing,"* no. 973, pp. 647–651, 2012.

[06] M. Zhou, R. Zhang, W. Xie, W. Qian, and A. Zhou, *"Security and Privacy in Cloud Computing"* 2010 Sixth International Conference on Semantics, Knowledge and Grids,: A Survey," pp. 105–112, Nov. 2010.

[7] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, *"Provable data possession at untrusted stores,"* Proceedings of the 14th ACM conference on Computer and communications security - CCS '07, p. 598, 2007.

[8] A. Juels and B. S. K. Jr, *"PORs : Proofs of Retrievability for Large Files."* 2007

[09] K. D. Bowers, A. Juels, and A. Oprea, *"Proofs of Retrievability : Theory and Implementation,"* 2009.

[10] M. W. Storer, K. Greenan, D. D. E. Long, and E. L. Miller, *"Secure data deduplication,"* Proceedings of the 4th ACM international workshop on Storage security and survivability - StorageSS '08, p. 1, 2008.

[11] S. Halevi, D. Harnik, B. Pinkas, and A. Shulman-peleg, *"Proofs of Ownership in Remote Storage Systems ⁎,"* pp. 1–13, 2011.

[12] Y. Deswarte and J. Quisquater, *"How to Trust Files Stored on Untrusted Servers,"* 2002.

[13] G. Ateniese, *"Proofs of Storage from Homomorphic Identification Protocols,"* pp. 1– 14.-2008.

[14] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, *"Scalable and Efficient Provable Data Possession Categories and Subject Descriptors."-2008.*

[15] R. Curtmola, O. Khan, R. Burns, and G. Ateniese, *"MR-PDP: Multiple-Replica Provable Data Possession,"* 2008 The 28th International Conference on Distributed Computing Systems, pp. 411–420, Jun. 2008.

[16] C. Erway, A. Küpçü, C. Papamanthou, and R. Tama ssia, *"Dynamic provable data possession,"* Proceedings of the 16th ACM conference on Computer and communications security - CCS '09, p. 213, 2009.

[17] T. S. S. J and E. L. Miller, *"UC Santa Cruz Postprints,"* 2006.

[18] Francesc Sebe, Josep Domingo-Ferrer, Antoni Martınez-Balleste, Yves Deswarte, JeanJacques Quisquater, *"Efficient remote data possession checking in criti cal information infrastructures"* , IEEE Trans. on Knowl. and Data Eng., pp.1034-1038, 2007.

[19] Lanxiang Chen, Gongde Guo, *"An Efficient Remote Data Possession Checking in Cloud Storage"*, JDCTA: International Journal of Digital Content Technology and its Applications, Vol. 5, No. 4, pp. 43-50, 2011.

[20] Xiao Da, Shu Jiwu, Chen Kang, Zheng Weimin, *"A Practical Data Possession*

[21] *Checking Scheme for Networked Archival Storage"* , Journal of Computer Research and Development, 46(10):1660- 1668, 2009.

[22] Charalampos Papamanthou, Roberto Tamassia, *"Time and space efficient algorithms for two-party authenticated data structures"* , In: Proc. of ICICS'07, pages 1–15, 2007.

[23] S. Ni-Na and Z. Hai-Yan, *"On Providing Integrity for Dynamic Data Based on the Third-party Verifier in Cloud Computing,"* 2011 First International Conference on Instrumentation, Measurement, Computer, Communication and Control, pp. 521–524, Oct. 2011.

[24] N. Y. Lee, *"Hybrid Provable Data Possession at Untrusted Store s In Cloud Computing,"* 2011.

[25] F. Liu, D. Gu, H. Lu, and C. Chris, *"AN IMPROVED DYNAMIC PROVABLE DATA POSSESSION MODEL,"* pp. 1–6, 2011.

[26] P. Varalakshmi and H. Deventhiran, *"Integrity checking for cloud environment using encryption algorithm,"* 2012 International Conference on Recent Trends in Information Technology, pp. 228–232, Apr. 2012.

[27] B. Chen, *"Robust Dynamic Provable Data Possession, "* 2012.

[28] P. Golle, S. Jarecki, and I. Mironov. *Cryptographic primitives enforcing communication and storage complexity. In Financial Cryptography*, pages 120–135, 2002.
[29] Q. Wang, S. Member, C. Wang, and K. Ren, *"Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing,"* pp. 1–13.-2009.
[30] F. Sebe, A. Martinez-Balleste, Y. Deswarte, J. Domingo-Ferrer, and J.-J. Quisquater. *"Time- bounded remote file integrity checking."* Technical Report 04429, LAAS, July 2004.
[31] H. Shacham, *"Compact Proofs of Retrievability,"* no. 2006, pp. 1–36, 2008.
[32] R. Curtmola, O. Khan, and R. Burns, *"Robust remote data checking,"* Proceedings of the 4th ACM international workshop on Storage security and survivability - StorageSS
'08, p. 63, 2008.
[33] K.VetriVel , Dr.C.Senthamarai *" A Study of Comparison of various Block Ciphers in Symmetric Key Encryption Algorithm".* International Journal of Computer Information Systems, Vol. 1, No. 5, 2010
[34] J. Guo, S. Ling, C. Rechberger, and H. Wang, "A dvanced Meet-in-the-Middle Preimage Attacks : First Results on Full Tiger, and Improved Results on MD4 and SHA-2," pp. 1– 20.

Book

Cloud computing for Dummies
The Basics about cloud computing

Web References

[1] http://en.wikipedia.org/wiki/Comparison_of_cryptographic_hash_functions
[2] http://www.cryptopp.com/benchmarks.html