International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Survey on Improved Cloud Computing Security: From Single to Distributed-Clouds

Neha N. Latpate[1], S. B. Waykar[2]

[1]Sinhgad Institute of Technology, Lonavala

[2]Professor, Sinhgad Institute of Technology, Lonavala

Abstract: ***It is the actual concern of the cloud's, due to it's simple nature as a shared resource, identity management, privacy and access management.it is further confidential issue provide offer|to supply|to produce} correct security and totally different in all probability vulnerable areas became a priority for organizations getting with a cloud computing provide,.and it's regarding With extra organizations exploitation cloud computing and associated cloud suppliers for data operations. On one cloud provider, If crucial information and applications are depends, you will feel affected in your ability to negotiate through business disagreements thereupon provider in an exceedingly worst-case situation, from running your software or accessing company information, the provider could block your accounts and stop you. during this case, to operating with multiple cloud providers provides you additional flexibility for each negotiations and information access . This paper surveys recent analysis associated with single and multi-cloud security and addresses doable solutions. it's found that the analysis into the utilization of multi-cloud providers to take care of security has received less attention from the analysis community than has the utilization of single clouds. owing to its ability to minimize security risks that have an effect on the cloud computing user, this work aims to push the employment of multi-clouds.***

Keywords: cloud computing, security, single to distributed cloud

1. Introduction

Because of the service provider will access the information that's on the cloud at any time Cloud computing poses privacy considerations. It might accidentally or deliberately alter or perhaps delete data. if necessary for functions of law and order even while not a warrant, several cloud suppliers will share data with third parties. that's permissible in their privacy policies that users have to be compelled to comply with before they begin victimization cloud services. Solutions to privacy embrace policy and legislation similarly as finish users' selections for a way information is keep.

Dealing with ―single cloud" as a result of potential issues like service accessibility failure and also the chance that there are malicious insiders within the single cloud, suppliers is changing into less fashionable customers. In recent years, there has been a move towards ―multi-clouds", ―inter-cloud" or ―cloud-of-clouds"..

The cloud computing model consists of 5 characteristics, 3 delivery models, and 4 preparation models. The 5 key characteristics of cloud computing are: location-independent resource pooling, on-demand self-service, fast snap, broad network access, and measured service.

The three key cloud delivery models are infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). Infrastructure as a service is taking the physical hardware and going utterly virtual (e.g. all servers, networks, storage, and system management all existing within the cloud). this can be the love infrastructure and hardware within the ancient (non-cloud computing) methodology running within the cloud. In different words, businesses pay a fee (monthly or annually) to run virtual servers, networks, storage from the cloud. for an information center, heating, cooling, and maintaining hardware at the native level, this may mitigate the requirement. Platform as a service is cloud computing service that provides the users with application platforms and databases as a service. this can be equivalent to middleware within the ancient (non-cloud computing) delivery of application platforms and databases.The software-as-a-service (SaaS) service-model involves the cloud provider putting in and maintaining code within the cloud and users running the software from their cloud clients over the net (or Intranet). The users' client machines need no installation of any application-specific code - cloud applications run on the server (in the cloud). SaaS is scalable, and system administration might load the applications on many servers.

Cloud deployment models embrace public, private, community, and hybrid clouds. a public cloud, could be a cloud environment that's accessible for multi-tenants and is available to the general public. a non-public cloud is on the market for a selected cluster, whereas a community cloud is changed for a selected cluster of consumers. composition of 2 or additional clouds (private, community, or public cloud) is termed Hybrid cloud infrastructure. This model represents the third layer within the cloud environment design.

By adopting a multi-cloud strategy, that is, by running your cloud-based deployments on different cloud providers, redundancy is taken to a full new level. By choosing information centers from completely different providers to host our cloud servers, we are able to effectively eliminate the danger related to the business continuity of the infrastructure supplier, likewise as risks associated with electricity suppliers, networking suppliers and different "data center" problems, since every cloud provider can typically operate individually.

Other risks related to having one provider reduces a multi-cloud strategy: to Illustrate somebody discovers a vulnerability on the virtualization platform that your current

infrastructure provider uses. If you're deploying on multiple clouds, you'll be able to merely shut down the servers on the vulnerable provider with very little or no impact to your operations. a similar mentality applies if suddenly your provider decides to extend its costs, or perhaps modification its terms of service: stop working your servers, and move your business to somebody else.

Multi-cloud strategy is that the use of 2 or a lot of cloud to reduce the danger of service accessibility failure, Loss and corruption of knowledge, loss of privacy, seller lock-in and also the chance of malicious insiders within the single cloud. The service inconvenience will occur owing to breakdown of hardware, code or system infrastructure. A multi-cloud strategy may also improve overall enterprise performance by avoiding "vendor lock-in" and exploitation completely different infrastructures to satisfy the requirements of numerous partners and customers. the price of exploitation multiple clouds are going to be more than that of single clouds. so unless and till there's a style which might build use of multi-clouds while not increasing price, the implementation are going to be extremely impractical.

2. Literature Survey

D. Agrawal, A. El Abbadi, F. Emekci and A. Metwally, "Database Management as a Service: Challenges and Opportunities",. The technical contributions of this paper is the establishment and development of a framework for effi- - cient fault-tolerant scalable and theoretically secure privacy preserving data outsourcing that supports a diversity of database operations executed on different types of data, which can even leverage publicly available data sets.

G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson and D. Song, "Provable data possession at untrusted stores",They present two provably-secure PDP schemes that are more efficient than previous solutions, even when compared with schemes that achieve weaker guarantees. In particular, the overhead at the server is low (or even constant), as opposed to linear in the size of the data.

A. Bessani, M. Correia, B. Quaresma, F. André and P. Sousa, "DepSky: dependable and secure storage in a cloud-of-clouds", In this paper we present DEPSKY, a system that improves the availability, integrity and confidentiality of information stored in the cloud through the encryption, encoding and replication of the data on diverse clouds that form a cloud-of-clouds.

C. Cachin, R. Haas and M. Vukolic, "Dependable storage in the Intercloud", We discuss the design of Intercloud storage, which we currently are implementing, as a primer for dependable services in the Intercloud. Intercloud Storage precisely addresses and improves the CIRC attributes (confidentiality, integrity, reliability and consistency) of today‘s cloud storage services.

C. Cachin and S. Tessaro, "Optimal resilience for erasure-coded Byzantine distributed storage",Theyanalyze the problem of efficient distributed storage of information in a message-passing environment where both less than one third of the servers, as well as an arbitrary number of clients, might exhibit Byzantine behavior, and where clients might access data concurrently.

A.J. Feldman, W.P. Zeller, M.J. Freedman and E.W. Felten, "SPORC: Group collaboration using untrusted cloud resources",Conceptually, SPORC illustrates the complementary benefits of operational transformation (OT) and fork* consistency. The former allows SPORC clients to execute concurrent operations without locking and to resolve any resulting conflicts automatically.

K.D. Bowers, A. Juels and A. Oprea, "HAIL: A high-availability and integrity layer for cloud storage", In this paper, they introduce HAIL (High-Availability and Integrity Layer), a distributed cryptographic system that permits a set of servers to prove to a client that a stored file is intact and retrievable. HAIL strengthens, formally unifies, and streamlines distinct approaches from the cryptographic and distributed-systems communities. Proofs in HAIL are efficiently computable by servers and highly compact—typically tens or hundreds of bytes, irrespective of file size. HAIL cryptographically verifies and reactively reallocates file shares. It is robust against an active, mobile adversary, i.e., one that may progressively corrupt the full set of servers. They propose a strong, formal adversarial model for HAIL, and rigorous analysis and parameter choices.

C. Cachin, R. Haas and M. Vukolic, "Dependable storage in the Intercloud", In this paper, They argue for the Intercloud as the second layer in the cloud computing stack, with the goal of building more dependable cloud services and systems. In the Intercloud layer, they foresee client-centric distributed protocols to complement more provider-centric, large scale ones in the (Intra)cloud layer. These client-centric protocols orchestrate multiple clouds to boost dependability by leveraging inherent cloud heterogeneity and failure independence.

C. Cachin and S. Tessaro, "Optimal resilience for erasure-coded Byzantine distributed storage", In this paper, They analyze the matter of economical distributed storage of knowledge in an exceedingly message-passing atmosphere where each but one third of the servers, likewise as associate discretional range of purchasers, might exhibit Byzantine behavior, and wherever purchasers would possibly access information at the same time. specifically, they provide a simulation of a multiple-writer multiple-reader atomic read/write register during this setting which uses erasure-coding for storage-efficiency and achieves optimum resilience. to boot, they offer the primary implementation of non-skipping timestamps that provides optimum resilience andwithstands Byzantine clients; it's supported threshold cryptography.

3. Proposed Approach Framework and Design

3.1 Architecture

At Present a virtual storage cloud system known as DepSky that consists of a mix of various clouds to make a cloud-of-clouds are used. The DepSky system addresses the provision and also the confidentiality of information in their storage

system by victimisation multi-cloud providers, combining Byzantine assemblage system protocols, science secret sharing and erasure codes DepSky is one such design style that overcomes all the restrictions of multi-clouds by eliminating the need of code execution within the servers (i.e., storage clouds). it's still economical because it needs solely 2 communication round-trips for every operation. Also, it deals with knowledge confidentiality and reduces the quantity of information keep in every cloud. It uses associate degree economical set of Byzantine assemblage system protocols, cryptography, secret sharing, erasure codes and also the diversity that comes from exploitation many clouds. The DepSky system model contains 3 parts: readers, writers, and 4 cloud storage providers, wherever readers and writers square measure the client_s tasks. The DepSky protocols give consistency proportional linguistics, i.e., the linguistics of an information unit is as sturdy because the help clouds permit, from ultimate to regular consistency linguistics. to make sure confidentiality of keep knowledge on the clouds while not requiring a key distribution service, we tend to use a secret sharing theme.

The DepSky design consists of 4 clouds and every cloud uses its own explicit interface. The DepSky rule exists within the clients‘ machines as a software package library to speak with every cloud (Figure 2). These four clouds square measure storage clouds, thus there aren't any codes to be executed. The DepSky library permits reading and writing operations with the storage clouds.

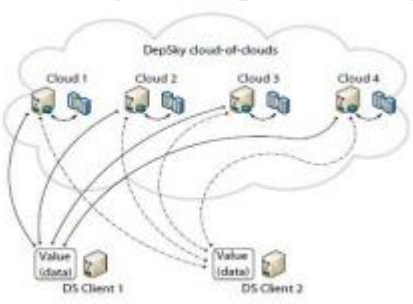

Figure 2: DepSky Architecture

4. Algorithm

A. Algorithm for Data Integrity Verification
Step 1: Start
Step 2: TPA Generates a random set
Step 3: CSS computes root hash based on the filename/blocks input
Step 4: CSS computes the originally stored value.
Step 5:TPA decrypts the given content and compares with generated root hash.
Step 6: after verification, the TPA can determines whether the integrity is breached.
Step 7 : Stop.

B. Algorithm for Updating and Deleting Data Present in CSS
Step 1: Start.
Step 2: Client generates new Hash for tree then sends it to CSS.
Step 3:CSS updates F and computes new R‘.
Step 4: Client computes R.
Step 5: Client verifies signature, If it fails output s false.
Step 6: Compute new R and verify the update and
Step 7: Stop.

5. Mathematical Model

The mathematical implementation of Cloud Computing security algorithm can be understood with the help of a simple example. The generalized idea is as follow:

We choose at random (k-1) coefficients i.e. a1…ak-1 We divide our secret data 'S' by picking a random degree polynomial

$$q(x) = a0 + a1x1 + a2x2 + \cdots + ak - 1xk - 1$$

Where a0='S' (i.e the data).

Now if we wish to divide the data into n parts, we will substitute 'n' different values of x in the polynomial q(x) and obtain 'n' such sets of (x, y), here y is nothing but our polynomial q(x).The essential idea of Adi Shamir's threshold scheme is that 2 points are sufficient to define a line, 3 points are sufficient to define a parabola, 4 points to define a cubic curve and so forth. That is, it takes "k" points to define a polynomial of degree "k-1".

Select "k" such sets, any k combination of the available n parts will generate the same result. The value in these sets are meaningless alone, it is only when 'k' sets are brought in together and further worked upon that we get our secret back. These "k" instances of original polynomial are processed using Lagrange polynomials

The Lagrange basis is:

$$I0 = \frac{X-X1}{X0-X1}.\frac{X-X2}{X0-X2}$$

$$I1 = \frac{X - X0}{X1 - X0} \cdot \frac{X - X2}{X1 - X2}$$

$$I2 = \frac{X - X0}{X2 - X0} \cdot \frac{X - X1}{X2 - X1}$$

Substitute the values of x from the selected 'k' sets into the Lagrange basis and we obtain 'k' fractional equations for the same. Finally on taking summation of the equations obtained from Lagrange basis and y form the selected 'k' sets, we get back our original polynomial. Thesummation can be represented mathematically as:

$$f(x) = \sum_{j=0}^{2} y_j \, .I_{j\,(x)}$$

The above explanation helps in understanding the working of the secret sharing algorithm. When done manually the entire calculation can be done in minutes, while on implementation, as the microprocessor technology has elevated its level to a new high, thousands of such calculations can be done in seconds.

6. Work Done

In this section we are discussing the practical environment, scenarios, performance metrics used etc.

6.1 Input

In this user signature is the input for our practical experiment.

6.2 Hardware and Software Configuration

Hardware Requirements

- Processor : Pentium IV 2.6 GHz
- RAM :512 MB DDR RAM
- Hard Disk : 20 GB

Software Requirements

Front End : Java
Tools Used : NetBeans
Operating System : Windows 7/8
Database : Mysql

7. Conclusion and Future Work

The use of cloud computing has been quickly augmented however the most important issue within the cloud computing environment continues to be in thought. from malicious corporate executive within the cloud, the users perpetually wish their information to be secure . several drawback for an oversized range of consumers recently caused by the loss of service convenience. what is more, for the users of cloud computing information intrusion leads to several issues. Our main purpose is to understand concerning security risks and solutions of single clouds and multi-clouds There search has been done to make sure the safety of the only cloud and cloud storage wherever multi-clouds have received less attention within the space of security. we tend to support the migration to multi-clouds as a result of its ability to decrease security risks that have an effect on the cloud computing user.

References

[1] (NIST),http://www.nist.gov/itl/cloud/.
[2] I. Abraham, G. Chockler, I. Keidar and D. Malkhi, "Byzantine disk paxos: optimal resilience with Byzantine shared memory", Distributed Computing, 18(5), 2006, pp. 387-408.
[3] H. Abu-Libdeh, L. Princehouse and H. Weatherspoon, "RACS: a case for cloud storage diversity", SoCC'10:Proc. 1st ACM symposium on Cloud computing, 2010, pp. 229-240.
[4] D. Agrawal, A. El Abbadi, F. Emekci and A. Metwally, "Database Management as a Service: Challenges and Opportunities", ICDE'09:Proc.25thIntl. Conf. on Data Engineering, 2009, pp. 1709-1716.
[5] M.A. AlZain and E. Pardede, "Using Multi Shares for Ensuring Privacy in Database-as-a-Service", 44th Hawaii Intl. Conf. on System Sciences (HICSS), 2011, pp. 1-9.
[6] Amazon, Amazon Web Services. Web services licensing agreement, October3,2006.
[7] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson and D. Song, "Provable data possession at untrusted stores", Proc. 14th ACM Conf. on Computer and communications security, 2007, pp. 598-609.
[8] A. Bessani, M. Correia, B. Quaresma, F. André and P. Sousa, "DepSky: dependable and secure storage in a cloud-of-clouds", EuroSys'11:Proc. 6thConf. on Computer systems, 2011, pp. 31-46.
[9] K. Birman, G. Chockler and R. van Renesse,"Toward a cloud computing research agenda", SIGACT News, 40, 2009, pp. 68-80.
[10] K.D. Bowers, A. Juels and A. Oprea, "HAIL: A high-availability and integrity layer for cloud storage", CCS'09: Proc. 16th ACM Conf. on Computer and communications security, 2009, pp. 187-198.
[11] C. Cachin, R. Haas and M. Vukolic, "Dependable storage in the Intercloud", Research Report RZ, 3783, 2010.
[12] C. Cachin, I. Keidar and A. Shraer, "Trusting the cloud", ACM SIGACT News, 40, 2009, pp. 81-86.
[13] C. Cachin and S. Tessaro, "Optimal resilience for erasure-coded Byzantine distributed storage", DISC:Proc. 19thIntl.Conf. on Distributed Computing, 2005, pp. 497-498.
[14] M. Castro and B. Liskov, "Practical Byzantine fault tolerance", Operating Systems Review, 33, 1998, pp. 173-186.
[15] G. Chockler, R. Guerraoui, I. Keidar and M. Vukolic, "Reliable distributed storage", Computer, 42, 2009, pp. 60-67.
[16] Clavister, "Security in the cloud", Clavister White Paper, 2008.
[17] A.J. Feldman, W.P. Zeller, M.J. Freedman and E.W. Felten, "SPORC: Group collaboration using untrusted cloud resources", OSDI, October2010, pp. 1-14.
[18] S.L. Garfinkel, "Email-based identification and authentication: An alternative to PKI?", IEEE Security and Privacy, 1(6), 2003, pp. 20-26.
[19] S.L. Garfinkel, "An evaluation of amazon‘s grid computing services: EC2, S3, and SQS", Technical Report TR-08-07, Computer Science Group, Harvard University, Citeseer, 2007, pp. 1-15.
[20] E. . Goh, H. Shacham, N. Modadugu and D. Boneh, "SiRiUS: Securing remote untrusted storage",NDSS: Proc. Network and Distributed System Security Symposium, 2003, pp. 131–145.
[21] G.R. Goodson, J.J. Wylie, G.R. Ganger and M.K. Reiter, "Efficient Byzantine-tolerant erasure-coded storage",DSN'04: Proc.Intl. Conf. on Dependable Systems and Networks,2004, pp.1-22.
[22] E. Grosse, J. Howie, J. Ransome, J. Reavis and S. Schmidt, "Cloud computing roundtable", IEEE Security & Privacy, 8(6), 2010, pp. 17-23.
[23] J. Hendricks, G.R. Ganger and M.K. Reiter, "Lowoverhead byzantine fault-tolerant storage", SOSP'07: Proc. 21st ACM SIGOPS symposium on Operating systems principles, 2007, pp. 73-86.
[24] A. Juels and B.S. Kaliski Jr, "PORs: Proofs of retrievability for large files", CCS '07: Proc. 14th ACM Conf. on Computer and communications security, 2007, pp. 584-597.
[25] S. Kamara and K. Lauter, "Cryptographic cloud storage", FC'10: Proc. 14thIntl.Conf. on Financial cryptograpy and data security,2010, pp. 136-149.

[26] H. Krawczyk, M. Bellare and R. Canetti, "HMAC: Keyed-hashing for message authentication", Citeseer, 1997, pp. 1-11.
[27] P. Kuznetsov and R. Rodrigues, "BFTW 3: why? when? where? workshop on the theory and practice of byzantine fault tolerance", ACM SIGACT News, 40(4),2009, pp. 82-86.
[28] L. Lamport, R. Shostak and M. Pease, "The Byzantine generals problem", ACM Transactions on Programming Languages and Systems, 4(3), 1982, pp. 382-401.
[29] P.A. Loscocco, S.D. Smalley, P.A. Muckelbauer, R.C. Taylor, S.J. Turner and J.F. Farrell, "The inevitability of failure: The flawed assumption of security in modern computing environments", Citeseer, 1998, pp. 303-314.
[30] P. Mahajan, S. Setty, S. Lee, A. Clement, L. Alvisi, M. Dahlin and M. Walfish, "Depot: Cloud storage with minimal trust", OSDI'10: Proc. of the 9th USENIX Conf. on Operating systems design and implementation, 2010, pp. 1-16.
[31] U. Maheshwari, R. Vingralek and W. Shapiro, "How to build a trusted database system on untrusted storage", OSDI'00: Proc. 4thConf. on Symposium on Operating System Design & Implementation, 2000, p. 10.
[32] D. Malkhi and M. Reiter, "Byzantine quorum systems", Distributed Computing, 11(4),1998, pp. 203-213.
[33] J.-P. Martin, L. Alvisi and M. Dahlin, "Minimal byzantine storage", DISC '02: Proc. of the 16thIntl. Conf. on Distributed Computing, 2002, pp. 311- 325.
[34] H.Mei, J. Dawei, L. Guoliang and Z. Yuan, "Supporting Database Applications as a Service", ICDE'09:Proc. 25thIntl.Conf. on Data Engineering, 2009, pp. 832-843.
[35] R.C. Merkle, "Protocols for public key cryptosystems", IEEE Symposium on Security and Privacy, 1980, pp. 122-134.
[36] E. Mykletun, M. Narasimha and G. Tsudik, "Authentication and integrity in outsourced databases", ACM Transactions on Storage (TOS), 2,2006, pp. 107-138.
[37] C. Papamanthou, R. Tamassia and N. Triandopoulos, "Authenticated hash tables", CCS '08: Proc. 15th ACM Conf. on Computer and communications security, 2008, pp. 437-448.
[38] M. Pease, R. Shostak and L. Lamport, "Reaching agreement in the presence of faults", Journal of the ACM, 27(2), 1980, pp. 228-234.
[39] R. Perez, R. Sailer and L. van Doorn, "vTPM: virtualizing the trusted platform module", Proc. 15th Conf. on USENIX Security Symposium,2006, pp. 305-320.