IJSEAT International Journal of Science Engineering and Advance Technology

Probity And Speculations Yielding Model For Multi Clouds

Mantravadi Gayithri #1, R Pitchiah #2

#1Student of M.Tech,#2 Associate Professor Dept. of Computer Science

Universal college of Engineering &Technology, Dogiparru

ABSTRCT:

Cloud computing is a latest trend in present scenario. Cloud computing definitely makes sense if your own security is weak, missing features of understanding and privacy. The cloud acts as a big black box, nothing inside the cloud is visible to the clients.Clients have no idea or control over what happens inside a cloud. Even if the cloud provider is honest, it can have malicious system admins who can tamper with the VMs and violate confidentiality and integrity. However cloud is not proving security,privacy,authentication because of retrievable problem.So In this paper we providing great integrity technique on clouds it solves the problem of retrivevable.our experimental results shows better and efficiency of clouds.

Keywords:Privacy,security,retrivability,integration, authenication,multi clouds.

I INTRODUCTION:

“Cloud computing is a compilation of existing techniques and technologies, packaged within a new infrastructure paradigm that offers improved scalability, elasticity, business agility, faster startup time, reduced management costs, and just-in-time availability of resources.

Explosive growth in applications: biomedical informatics, space exploration, business analytics, web 2.0 social networking: YouTube, Facebook.Extreme scale content generation: e-science and e-business data deluge. Extraordinary rate of digital content consumption: digital gluttony: Apple iPhone, iPad, Amazon Kindle .Exponential growth in compute capabilities: multi-core, storage, bandwidth, virtual machines (virtualization).Very short cycle of obsolescence in technologies: Windows Vista→ Windows 7; Java versions; C→C#; Phython.Newer architectures: web services, persistence models, distributed file systems/repositories (Google, Hadoop), multi-core, wireless and mobile. Diverse knowledge and skill levels of the work force. You simply cannot manage this complex situation with your traditional IT infrastructure.

II PROBLEM STATEMENT:

The use of hybrid clouds is an emerging trend in cloud computing ability to exploit public resources for high throughput.Yet, better able to control costs and data privacy Several key challenges.

Data Design: how to store data in a hybrid cloud[1]?Solution must account for data representation used (unencrypted/encrypted), public cloud monetary costs and query workload characteristics.Query Processing: how to execute a query over a hybrid cloud[2]?Solution must provide query rewrite rules that ensure the correctness of a generated query plan over the hybrid cloud[3].Also a massive concentration of risk expected loss from a single breach can be significantly larger.concentration of “users” represents a concentration of threats[4],[5].“Ultimately, you can outsource responsibility but you can’t outsource accountability.” Trusting vendor’s security model Customer inability to respond to audit findings

- Obtaining support for investigations
- Indirect administrator accountability
- Proprietary implementations can’t be examined
- Loss of physical control

Data dispersal and international privacy laws,EU Data Protection Directive and U.S. Safe Harbor program.Exposure of data to foreign government and data subpoenas.Data retention issues,Need for isolation management,Multi-tenancy ,Logging challenges Data ownership issues ,Quality of service guarantees.

III PROPOSED WORK:

We propose a novel architecture that integrates cloud database services with data confidentiality and the possibility of executing concurrent operations on encrypted data.This is the first solution supporting geographically distributed clients to connect directly to an encrypted cloud database, and to execute concurrent and independent operations including those modifying the database structure. The proposed architecture has the further advantage of eliminating intermediate proxies that limit the elasticity, availability, and scalability properties that are intrinsic in cloud-based solutions. Secure DBaaS provides several original features that differentiate it from previous work in the field of security for remote database services.

ADVANTAGES OF PROPOSED SYSTEM:

The proposed architecture does not require modifications to the cloud database, and it is immediately applicable to existing cloud DBaaS, such as the experimented PostgreSQL Plus Cloud Database, Windows Azure and Xeround . There are no theoretical and practical limits to extend our solution to other platforms and to include new encryption algorithm.It guarantees data confidentiality by allowing a cloud database server to execute concurrent SQL operations (not only read/write, but also modifications to the database structure) over encrypted data.It provides the same availability, elasticity, and scalability of the original cloud DBaaS because it does not require any intermediate server.

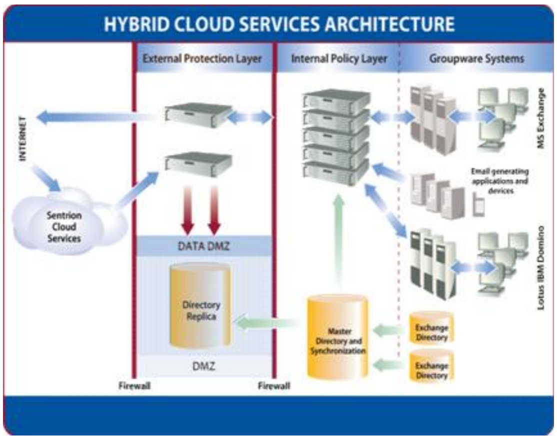

Fig1: secure integration of clouds

IV conclusion:

Cloud computing is sometimes viewed as a reincarnation of the classic mainframe client-server model However, resources are ubiquitous, scalable, highly virtualized Contains all the traditional threats, as well as new onesIn developing solutions to cloud computing security issues it may be helpful to identify the problems and approaches in terms of Loss of control, Lack of trust and Multi-tenancy problems, The PPDA tasks analyzed in the paper can be reduced to evaluation of a single function. Now, the question is how to analyze whether a PPDA task is in DNCC if it is reduced to a set of functions. In other words, is the composition of a set of DNCC functions still in DNCC? We will formally answer this question in the future. Another important direction that we would like to pursue is to create more efficient SMC techniques tailored towards implementing the data analysis tasks that are in DNCC. Even though privacy-preserving data analysis tech- niques guarantee that nothing other than the final result is disclosed, whether or not participating parties provide truthful input data cannot be verified. In this paper, we have investigated what kinds of PPDA tasks are incentive compatible under the NCC model. Based on our findings, there are several important PPDA tasks that are incentive driven. As a future work, we will investigate incentive issues in other data analysis tasks, and extend the proposed theorems under the probabilistic NCC model.

5 References

[1] B. Sotomayor, R. S. Montero, I. M. Llorente, and I. T. Foster,“Virtual infrastructure management in private and hybrid Clouds,” IEEE Internet Computing, vol. 13, no. 5, pp. 14–22, 2009.

[2] G. Ateniese, R. C. Burns, R. Curtmola, J. Herring, L. Kissner, Z. N. J. Peterson, and D. X. Song, “Provable data possession at untrusted stores,” in ACM Conference on Computer and Communications Security, P. Ning, S. D. C. di Vimercati, and P. F. Syverson, Eds. ACM, 2007, pp. 598–609.

[3] A. Juels and B. S. K. Jr., “Pors: proofs of retrievability for Large files,” in ACMConference on Computer and Communications Security, P. Ning, S. D. C. di Vimercati, and P. F. Syverson, Eds. ACM, 2007, pp. 584–597.

[4] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, “Scalable and efficient provable data possession,” in Proceedings of the 4th international conference on Security and privacy in Communication netowrks, SecureComm, 2008, pp. 1–10.

[5] C. C. Erway, A. K¨upc¸ ¨u, C. Papamanthou, and R. Tamassia, “Dynamic provable data possession,” in ACM Conference on Computer and Communications Security, E. Al-Shaer, S. Jha, and A. D. Keromytis, Eds. ACM, 2009, pp. 213–222.

[6] H. Shacham and B. Waters, “Compact proofs of retrievability,”in ASIACRYPT, ser. Lecture Notes in Computer Science, J. Pieprzyk, Ed., vol. 5350. Springer, 2008, pp. 90–107.

[7] Q. Wang, C.Wang, J. Li, K. Ren, and W. Lou, “Enabling public Verifiability and data dynamics for storage security in cloud Computing,” in ESORICS, ser. Lecture Notes in Computer Science, M.
Backes and P. Ning, Eds., vol. 5789. Springer, 2009, pp. 355–370. [8] Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S. S. Yau, “Dynamic audit services for integrity verification of outsourced Storages in clouds,” in SAC, W. C. Chu, W. E. Wong, M. J. Palakal, and C.-C.
Hung, Eds. ACM, 2011, pp. 1550–1557.

[9] K. D. Bowers, A. Juels, and A. Oprea, “Hail: a high-availability and integrity layer for cloud storage,” in ACM Conference on Computer and Communications Security, E. Al-Shaer, S. Jha, and A. D. Keromytis, Eds. ACM, 2009, pp. 187–198.

[10] Y. Dodis, S. P. Vadhan, and D. Wichs, “Proofs of retrievability via hardness amplification,” in TCC, ser. Lecture Notes in Computer Science, O. Reingold, Ed., vol. 5444. Springer, 2009, pp. 109–127.

[11] L. Fortnow, J. Rompel, and M. Sipser, "On the power of multiprover Interactive protocols," in Theoretical Computer Science, 1988, pp. 156–161.

[12] Y. Zhu, H. Hu, G.-J. Ahn, Y. Han, and S. Chen, "Collaborative Integrity verification in hybrid clouds," in IEEE Conference on the 7th International Conference on Collaborative Computing: Networking,Applications and Worksharing, CollaborateCom, Orlando, Florida, USA, October 15-18, 2011, pp. 197–206.

Authors:

MANTRAVADI GAYITHRI Is A Student Of Computer Science Engineering From Universal college of Engineering &Technology, Dogiparru. Presently pursuing M.Tech From This College. She received MCA From IGNOU In The Year Of 2010.

R PITCHIAH received his M.Tech in computer science Engineering from JNTU K. He is a good researcher. He is working as Associate Professor and gained 16 years' Experience on Teaching.