International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 3 | ISSN : 2456-3307

Intercloud Promising Second Layer in Cloud Computing Stack and Dependable Storage

S.Hendry Leo Kanickam*[1], K. Arun Kumar[2]
*[1]Assistant Professor, Department of Information Technology, St.Joseph's College, Trichy, Tamilnadu, India
[2]M.Sc CS, Department of Information Technology, St.Joseph's College, Trichy, Tamilnadu, India

ABSTRACT

Cloud computing has a potential to transform a way of outsourcing and sharing business activities in a dynamic world. The current cloud computing enables clients to interact with servers and it provides infinite scalability and depends on availability towards changing of systems and services. However, cloud-computing proliferations have not lived and come in the enterprise segment. Often issues including in these computing be confidentiality and integrity, but also reliability and consistency. In this paper, we discuss the Intercloud occupies as the second layer in the cloud computing stack, offering a goal of building in services and systems are more dependable. Intercloud layer, client-centric distributed protocols complement are more provider-centric, large scale ones in the Intracloud layer. Client-centric protocols having a multiple clouds for dependability by leveraging inherent cloud heterogeneity and failure independence. We also argue the design of Intercloud storage, which is currently are implementing, dependable services in the Intercloud. Intercloud Storage precisely addresses and improves the CIRC attributes which means confidentiality, integrity, reliability and consistency of cloud storage services.

Keywords: Intercloud, CIRC, Client-Centric Protocols.

I. INTRODUCTION

Cloud computing act as promising model to the client, infinite scalability and always-on availability, that makes renders in appealing of data for use and computation outsourcing for services and systems, both for consumers want to share their pictures with friends and for enterprises world to reduce their IT budgets and costs. They obvious on dependability and security concerns associated potentially under untrusted third party. Even though some cases if the cloud provider is itself trusted by the client, issues may be occurs be like multi-tenancy entail vulnerabilities. More specifically, a problem occurs in data confidentiality and integrity, but also reliability and consistency of the contracted service. We trust that a promising solution for improved cloud security and dependability be in the Intercloud1 , goes beyond adding perfection to single, the cloud of clouds in computing, isolated cloud computing. In this paper, we first discuss about Intercloud act as the second layer for the next-generation cloud. Upcoming Intercloud and single-provider clouds are two separate layers in the cloud-computing stack that complement each other. It offers promising solutions for enhanced dependability. Secondly, design of a service in the Intercloud, exploits the unique features of this model: storage service that is currently under development and addresses the CIRC dimensions through a layered architecture.

II. DEPENDABLE CLOUD COMPUTING STACK

First overview the single-domain cloud layer and its dependability limitations and then discussing focus at Intercloud for solutions.

2.1 Single-Domain Cloud and Limitations

Layer occupies the most part of the cloud computing systems to date that means updating, and consists of distributed protocols designed to make use of run in a single administrative domain, under the control of one service provider e.g., Amazon , Google Apps, N irvanix4. Distributed protocols used in this context are intended mostly in areas be like wide-area systems, with scalability offering very large number of clients to share of data and most important goals be high availability[18]. Dependability and security for an single-domain cloud, mainly towards integrity, confidentiality, and isolation for data and computations in a multi-tenant model are receiving increased attention (e.g., [5, 16]). Devising a dependable service relying on single cloud provider named as P has its inherent limitations, while all trusting system reduces to trusting of provider P. The service offered by cloud provider P as well, that works immediately only by defeats the benefits of encryption. Encryption creates keys to be managed, but if only a client can rely on offerings of provider P, it would immediately store encryption keys. Storing the encryption keys at fault-prone clients to be in unacceptable solution, after storing there will be losing of key, which implies losing of encrypted data. One of another limitations be relying on a single cloud provider's services related to data reliability and consistency and clouds are designed in highly available, out coming may be occur at any individual provider. In these part of networking cloud provider P remains only at single point of failure, most in the case of cloud providers P services and systems. Moreover, network connections are particularly locate when the client resides outside North America and Western Europe, while having of high-bandwidth connections but it may not be readily usable at the time. Finally, Single-cloud solutions give an incentive for a client to locally cache data, in order to avoid consistency problems. Only be complicates concurrent access to the service or outsourcing data to the cloud. To the other single-cloud dependability issues, we eye contact at the Intercloud.

2.2 Intercloud layer Secure Networking

In network communications, sharing of data services and systems passed only on the highest to the lowest layer, while each layer adding of more information, which means data, occupies information, reliability, depends on available services, etc. Security controls exist on many layers of the TCP/IP model.

Application Layer- Security control and connections will be established on each application. It provides high degree of controls and flexibility application.

Transport Layer-Security controls connection used to protect the data in a single transport flow between two hosts of services and systems. Transport Layer Security (TLS) [14] , Secure Sockets Layer (SSL) [15], said to be an cryptographic protocols in cloud computing that provides communication and security at the Transport Layer. Using TLS it modifies some applications, Sometimes called as well-tested protocol having of several implementations used for adding of many applications, so it is a relatively low-risk option compared to the application layer.

Table 1

	Network Layer	Transport Layer
1	Logical communication between the hosts	Logically communication between the process
2	Responsible for checking the data available in the session layer are error free	Responsible for translating the logical addresses in to the physical address
3	Protocols used in this	Protocols used in this

	layers are • IP(Internet protocol) • ARP(Address Resolution Protocol) • IGMS(Internet group Resolution Protocol)	layers are • TCP(Transmission Control Protocol) • UDP(User Datagram Protocol) • SCTP(Stream Control Transmission Protocol)
4	This layer control routing from end to end flow and error controls	This layer control routing from source to destination.
5	The third –lowest layer of the OSI Reference is model is the network layer	The fourth and the Middle layer of the OSI Reference model is the transport layer
6	It deliver packets from source to destination across multiple network	It deliver from source to destination to the entire message
7	It divides each message ion to logical to physical	It divides each message in to packets.

Network Layer-Security controls connection available at all applications and but not specific in application. All network communications differs two hosts or networks can be protected its own layer without modifying applications on the clients or the servers. In many environments, network layer controls such as IPSec [16] provides better solution than transport or application layer controls because it controls of adding of individual applications. Network layer controls provide less control and flexibility than application and transport layer.

Data Link Layer- security controls connections are available at all communications on a specific physical link. Compared at the other layers, data link layer controls are relatively simple, which makes them easier to implement, they support other network layer protocols IP. However, they are poor of protecting connections with multiple links over the Internet. However, they have been used frequent offering of securing communications over the Internet.

The most common use of IPSec implementations is Virtual Private Networking (VPN) [17] services. Used to built an existing physical networks that can provide a secure communications mechanism for data transmitted between networks. The existing networks, it slightly facilitate towards of secure data over trusted public networks such as intracloud and inter-cloud in our case.SSL-based VPN becomes a costeffective alternative provides a solution secure connectivity within a cloud moreover recently, Amazon using of VPN releases beta version of Amazon Virtual Private Cloud (Amazon VPC) [18], While having partial solution they did not address the issues completely.

The Intercloud layer does not replace the single-cloud layer, having greatly expands its scope. Depend intercloud will be client-centric first, where client-side can be in multiple clouds. Offers more services involving communication among different cloud services this is not easily possible today due to lack of standardization.

III. INTERCLOUD STORAGE

ICStore client consists of three layers that goals different dependability aspects:-

i) confidentiality, ii) integrity and iii) reliability and consistency (RC).

i) Confidentiality-The client performs a simple symmetric key (both sender and receiver having same keys) encryption of the data and received from the client. The challenge in this layer is to be an key management. When a key is split it share with secret shared [17]) upon encryption, and key shares are been in metadata to individual clouds. Shares of data needed then reconstruct the key is to be in

parameter that depends on the number of available clouds and reliability protocols.

ii) Integrity –This layer is against unauthorized data modification. When a single client accesses the untrusted cloud storage, data integrity can maintained the data, While multiple clients access some data maintained by ICstore.

iii) Reliability and Consistency (RC)- The RC layer consists of fault-tolerant distributed protocols that disperse data to the Intercloud. After the data can passes through the confidentiality and integrity layers. Support a variety of data dispersal protocols, which are to be selected depending on the goals of the end application.

In addition, of increased cost of such an approach, this raises issues regarding access control on base clouds. The trends are present in recent single-domain cloud storage implementations. The final stage of this implementation is planning to add an extra coding to client-driven storage protocols.

IV. CONCLUSION

Finally Intercloud act as an second layer of cloud computing stack and storage of intercloud issues solution can be maintained such as confidentiality, integrity, reliability and consistency. Future outcomes be incomplete the implementation of ICStore prototype and evaluate of its cost and benefits.

V. REFERENCES

[1]. H. Abu-Libdeh, L. Princehouse, and H. Weatherspoon, "RACS: A case for cloud storage diversity," in ACM SoCC, 2010.

[2]. E. Anderson, X. Li, A. Merchant, M. A. Shah, K. Smathers, J. Tucek, M. Uysal, and J. J. Wylie, "Efficient eventual consistency in Pahoehoe, an erasure-coded key-blob archive," in DSN, 2010.

[3]. M. Bjorkqvist, C. Cachin, R. Haas, X.-Y. Hu, ¨ A. Kurmus, R. Pawlitzek, and M. Vukolic, "Design ´ and implementation of a key-lifecycle management system," in Financial Cryptography and Data Security (FC 2010), pp. 160-174, 2010.

[4]. K. D. Bowers, A. Juels, and A. Oprea, "HAIL: A high-availability and integrity layer for cloud storage," in ACM CCS, pp. 187-198, 2009.

[5]. C. Cachin, I. Keidar, and A. Shraer, "Fail-aware untrusted storage," in DSN, pp. 494-503, June 2009.

[6]. C. Cachin, I. Keidar, and A. Shraer, "Trusting the cloud," SIGACT News, vol. 40, no. 2, pp. 81-86, 2009.

[7]. G. Chockler, R. Guerraoui, I. Keidar, and M. Vukolic, "Reliable distributed storage," ´ IEEE Computer, vol. 42, no. 4, pp. 60-67, 2009.

[8]. J. Hendricks, G. R. Ganger, and M. K. Reiter, "Low-overhead byzantine fault-tolerant storage," in SOSP, pp. 73-86, 2007.

[9]. F. Junqueira and K. Marzullo, "A framework for the design of dependent-failure algorithms," Concurrency and Computation: Practice and Experience, vol. 19, no. 17, pp. 2255-2269, 2007.

[10]. L. Lamport, "On interprocess communication," Distributed Computing, vol. 1, pp. 77-101, May 1986.

[11]. T. Dierks, E. Rescorla. The Transport Layer Security (TLS) Protocol, RFC 5246, August 2008.

[12]. N. Santos, K. P. Gummadi, and R. Rodrigues, "Towards trusted cloud computing," in HotCloud, 2009.

[13]. R. Thayer, N. Doraswamy, R. Glenn, (November 1998). IP Security Document Roadmap. IETF. RFC 2411, November 1998.

[14]. S. Nepal, J. Zic, S. Chen: A Contract Language for Service-Oriented Dynamic Collaborations. CollaborateCom 2008: 545-562.

[15]. D. Nurmi, R. Wolski, C. Grzegorczyk, G. Obertelli, S. Soman, L. Youseff, and D. Zagorodnov, "The Eucalyptus open-source

cloud-computing system," in CCGRID, pp. 124-131, 2009.

[16]. N. Santos, K. P. Gummadi, and R. Rodrigues, "Towards trusted cloud computing," in HotCloud, 2009.

[17]. W. Vogels, "Eventually consistent," Commun. ACM, vol. 52, no. 1, pp. 40-44, 2009.

Author's Profile

Mr.S.Hendry Leo Kanickam working as a Assistant Professor in Department of Information Technology ,St. Joseph's College (autonomous) Trichy, India. He received his M.Phil Degree in Bharathidasan University in 2008 and also He is pursuing Ph.D (Computer Science) in Bharathidasan University.

Mr. K.Arun Kumar is studying II M.Sc Computer Science in the Department of Information Technology ,St. Joseph's College (autonomous) Trichy, India