Simultaneous ammunition for the multi-cloud computing simulation

Mr. Sunny Bhadlawala[1], Prof (Dr.) S.S. Srivastava[2]

[1]Ph.D. (Pursing), M.Tech, B.E., MCP, MCTS, Research Scholar, Dept. of Computer Science & Engineering
AISECT UNIVERSITY,
[2]Dept. of Computer Science & Engineering, AISECT UNIVERSITY

***

Abstract— *In this research report, we analyze multi-cloud securities and optical networks. This decision was explained by the fact that the current spinal cord of cloud computing is based on many factors and techniques including the securities. Apart from that, we use the protocol and it is forced to transfer the web to a specialist in web transfers with nodes and broken networks in parts of the internet. The protocol is designed for server-to-server that transfers data over data and automates it for data transfer and synchronization.*

***Keywords*—cloud computing, multi-cloud computing, replica.**

1. INTRODUCTION

Cloud computing was in limited popularity; It is associated with the software as it has been commonly used in a variety of technologies, services and concepts that are often virtualized infrastructure or hardware-on-demand, utility computing, outsourcing, platforms and services, and many other things at the heart of the IT industry.

A cloud is a type of parallel and distributed system that includes the collection of the one and the virtualized computer that is dynamically deployed and based on the service level agreements established by the interaction between the service provider and the consumer is presented as a more unified computing resources.

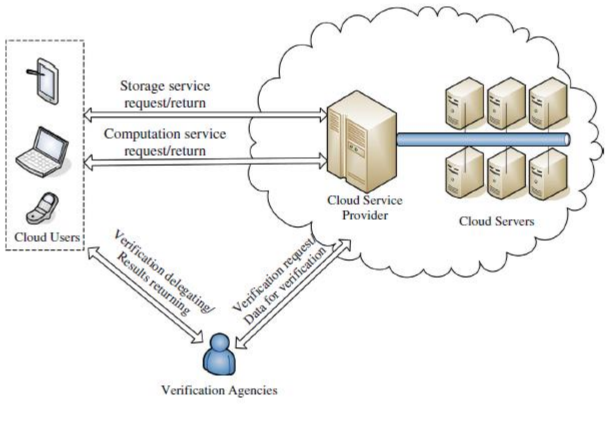
Storage service request/return
Computation service request/return
Cloud Service Provider
Cloud Servers
Cloud Users
Verification delegating/ Results returning
Verification request/ Data for verification
Verification Agencies

Fig.1 Protocol based cloud computing.

Cloud computing is a model for accessing the ubiquitous, practical on-demand network that accesses a shared pool of configurable computing resources such as networks, servers, storage, applications, and services.

This deployment can be fast and can be done with minimal management effort or interaction with the service provider.

As we can see in fig. Various network-enabled devices, such as Smartphone's, tablets, desktops and notebooks, use the cloud computing features of an Internet connection.

You can store your data such as important documents, training data, calendars, finances and many important documents.

In such a situation, the secure placement of parts and storage for advanced hacking techniques that are available today is essential.

Cloud computing is its utility-oriented approach. More than any other distributed computing trend, cloud computing is geared towards distributing services with a fixed pricing model, in most cases a pay-per-use strategy.

1.1. Cloud in house

The use of cloud-based in-house solutions is driven by the need to store sensitive information in an organization's premises. Companies like governments and banks prefer to create and use private or corporate clouds, such as high security requirements, privacy policies, and regulatory concerns

Large organizations that have a large computer infrastructure can copy cloud IT service delivery models from cloud computing.

This idea has led to the concept of private clouds as opposed to public clouds.

In the private cloud, all resources are tightly secured and available within the organization.

It enables the payment of online storage, the rental of virtual hardware or the use of development platforms and their effective use without any minimum or minimum cost. All of these operations can be billed to enter the credit card information and access the highlighted services via a web browser.

Although many cloud computing services are available independently to individual users, enterprise-class services are distributed according to a specific price plan. In this case, users subscribe to the service and use a service level agreement (SLA) to set up the service provider that defines the quality service standards under which services are provided.

1.2. Type of layers

Cloud computing is very easy for cloud customers like access cloud, retrieve storage or important data, all retrieved.

But internal clouds have been mentioned in three have been built on the very important layers of these layers as Software as Infrastructure as a Service (SaaS), Platform as a Service (PaaS) and a Service (IaaS). Different cloud service providers offer different types of services based on these layers.

The software, which is at the first level, has as its services various applications that provide an interface to eliminate the user. This layer usually allows access to internal data with some authentication mechanisms.

The second layer is a platform as a service, another assignment of users in this layer request for the resources required to cloud computing. Finally, the level of infrastructure in which most of the time are virtual machines and infrastructure that can request the user as show in Fig. 2. Cloud computing shows different pyramid layers.

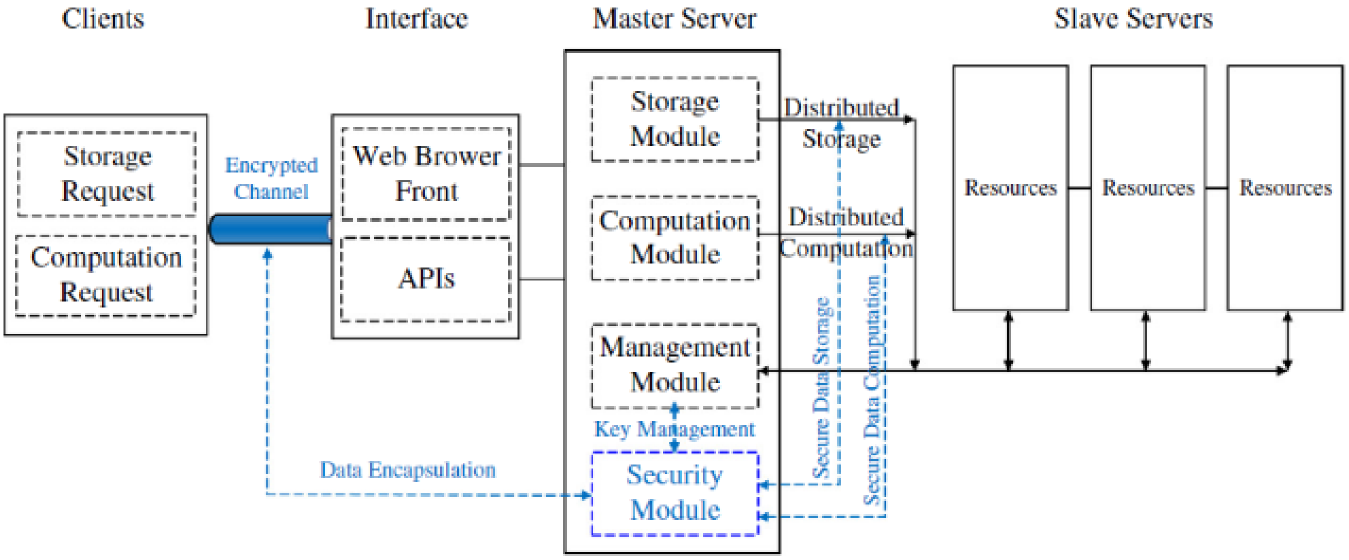

Fig.2 The cloud master and slave servers

Every layer of the cloud has its weaknesses. Similar to software in the form of a service, the layer uses an authentication mechanism to verify the identity of the owner on the document, but it can be corrupted if a person receives a security code that has been verified for authentication. Continuously.

1.2.1 Service layer

SaaS model allows users to use a software application as a service

It has full administrative powers for its application and is responsible for activities such as deployment, maintenance and updating; it is suitable for customers who want to have less administrative burden and concerns about setting up a management software and want to update it.

Applications that support productivity and collaboration are the best choice; For example,

Google Apps, online project management apps such as Zoho Mail, Dzieva CRM applications such as Salesforce.com Imple CRM and Microsoft Dynamics, etc.

Cloud services like SkyDrive, Google Docs and Dropbox. Small and Medium Enterprises (SMEs) / Small and Medium Businesses (SMB) User services such as ice-skating.

1.3. Cryptography

It is a branch of security that proposes hundreds of algorithms that can be used for secure communication between different users or that can securely store data on certain media.

This section provides methods for encryption, decryption, and verification for a different purpose. Encryption is meant to convert simple plain text into an encrypted text that is not easy to understand.

To recover text from cipher text, a reverse process of decryption encryption is performed. Different methods, algorithms can be optimized like many hash algorithms like AES, RSA, DES, Triple-DES and MD5.

It provides secure ways to generate a key that can be used for sender-side encryption and decryption to the receiver and with a secure mechanism for transmitting those keys.

2. PREVIOUSPAPERS STUDY

In a base paper [23], a common approach to ensuring data security in cloud computing:

Cloud computing is the impending revolution due to its performance, reach, low cost and many other luxury goods in the IT industry.

It is a certified approach to maximizing capacity and capabilities without investing in new infrastructure, promoting new employees, or licensing new software.

It provides huge storage for data and faster data processing for customers on the Internet. This essentially changes the database and application software for large data centers. The cloud, where the management of data and services cannot be completely reliable

As a result, businesses are reluctant to shut down their cloud computing business and therefore offer a wide range of luxuries. The security of data in the cloud is an obstacle to the implementation of cloud computing, one of the main problems.

In this publication, an overview of various techniques and special procedures has been proposed, which is sure to keep data from the beginning of the data to the end. From the owner to the cloud and then to the user, we can begin with the classification of data, the basis of the three cryptographic parameters presented by the user, i. privacy, ii. Availability and iii. Integrity

The privacy policy is to use various measures such as Secure Sockets Layer (SSL) 128-bit encryption and can be fetched for 256-bit encryption as needed, Mac (Message Authentication Code) Data Integrity Searchable encryption and division of data into three sections used in the cloud for storage

Provides extra protection and easy access to data in three sections of data sharing. The user who wants to access the data before he can enter the encrypted data for approval must provide the owner's login identity and password.

3. PROPOSED APPROACH

Provides extra protection and easy access to data in three sections of data sharing.

Before the data is accessed to access encrypted data and enable the requirement for enabling storage data, the user must enter the owner's login identity and password to log in.

Here are two groups of I3 it that can be started with three I3 it parameters.

$e\hat{}:G_1\& G_2$
Where $e = \lim (1+1/x)\, x, x\rightarrow\infty)$
$H: \{0, 1\}^* \rightarrow Z_q^{4}$, $H1: \{0, 1\}^* \rightarrow G_1$
$H2: \{0, 1\}^* \rightarrow Z_q^{*}$,
$H_3: G_2 \rightarrow Z_q$.
User Registration:$sk_{ID} = s\, Q_{ID}$.
Storage space: $M = \{m1, m2,....,mn\} \in Zq$

Data encapsulation: To guarantee the secure data transmissions, after identifying the cloud server or the verification agency, the cloud user pre-computes the session key
$key_{ID,CS}$ or $key_{ID,VA}$.

$key_{ID,CS} = H_3\, (e\hat{}(sk_{ID,}\, Q_{CS}))$
$key_{ID,VA} = H_3\, (e\hat{}(sk_{ID,}\, Q_{VA}))$
$key_{ID,CS} = H_3\, (e\hat{}(sk_{CS,}\, Q_{ID}))$.

Data receiving: After receiving the packets, CSP first decrypts them by its own session key to obtain the data-signature pairs {D,Ø} and checks the signatures by verifying secret key sk_{CS}:

$$\sum_i = e\hat{}\ (U_i + H_2\, (U_i || m_i || i_i)\, Q_{ID}, sk_{cs})$$

Considering the fact that the major communication and computation overhead comes from verification of the signatures, we introduce an advanced protocol to further reduce the computational and communication. The computational complexity based on the protocol is:

$$e\hat{\ }(U_A,sk_{va}) = \sum\grave{\ }_A$$

$$\Sigma'_A = \prod_{i=1}^{k}\prod_{j=1}^{n_i}\hat{e}(V_{ij}, Q_{VA}) = \hat{e}\left(\sum_{i=1}^{k}\sum_{j=1}^{n_i}V_{ij}, Q_{VA}\right)$$

$$= \hat{e}\left(\sum_{i=1}^{k}\sum_{j=1}^{n_i}(U_{ij} + H_2(U_{ij}\|m_{ij})Q_{ID_i}), sk_{VA}\right) = \hat{e}(U_A, sk_{VA}).$$

$$= \hat{e}\left(\sum_{i=1}^{k}\sum_{j=1}^{n_i}(r_{ij} + H_2(U_{ij}\|m_{ij}))sk_{ID_i}, Q_{VA}\right)$$

Here combination $\sum\grave{\ }_A$ and U_A can be performed incrementally with the computational cost but it almost measured by the expensive pairing operations as mentioned in the equation of e^.

4. SIMULATION

Cloudlet ID	Status	Data Centre ID	VM	Time	Start Time	Finish Time
1	SUCCESS	2	1	800	0	800
4	SUCCESS	2	1	801	0	801
7	SUCCESS	2	3	1601	1	1602
10	SUCCESS	2	3	802	801	1603
2	SUCCESS	2	7	802	1600	2402
3	SUCCESS	2	7	803	1600	2403
6	SUCCESS	2	6	801	3203	4004
9	SUCCESS	2	6	1600	3200	4800
. . .	. . .	. . .	. . .	. . .	. . .	. . .
n^{th}	SUCCESS	2	n	$t+t^n$	t	t^n

Table - I: Cloud simulation

CONCLUSION

In this research paper we have implemented cloud simulation and made number of app0..n to use cloudlet and make their copy in to data centre 2 along with their own id in that case the data centre will generate based on the requirement or create virtual machine(VM) allow to perform task of cloudlet or agents.

REFERENCES

[1]. SushmitaRuj, Milos Stojmenovic, Amiya Nayak, "Privacy Preserving Access Control with Authentication for Securing Data in Clouds", 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing-2012.

[2]. Ming Li, Shucheng Yu, Yao Zheng, Kui Ren, and Wenjing Lou, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 24, NO. 1, JANUARY 2013.

[3]. DananThilakanathan, Shiping Chen, Surya Nepal and Rafael A. Calvo, "Secure Data Sharing in the Cloud", security, Privacy and Trust in Cloud Systems 2014.

[4]. Anurag Porwal, RohitMaheshwari, B.L.Pal, Gaurav Kakhani, "An Approach for Secure Data Transmission in Private Cloud ", IAENGEngineeringLettersInternational Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-1, March 2012.

[5]. M.Sudha , M.Monica, "Enhanced Security Framework to Ensure Data Security in Cloud Computing Using Cryptography", Advances in Computer Science and its Applications 32 Vol. 1, No. 1, March 2012.

[6]. ParsiKalpana, SudhaSingaraju, "Data Security in Cloud Computing using RSA Algorithm",

ParsiKalpana ,et al, International Journal of Research in Computer and Communication technology,IJRCCT, ISSN 2278-5841, Vol 1, Issue 4, September 2012.

[7]. KawserWazedNafi, TonnyShekhaKar, Sayed AnisulHoque, Dr. M. M. A Hashem, " A Newer User Authentication, File encryption and Distributed Server Based Cloud Computing security architecture ",(IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 3, No. 10, 2012.

[8]. Ahmad Rashidi and NaserMovahhedinia, "A Model for User Trust in Cloud Computing", International Journal on Cloud Computing: Services and Architecture(IJCCSA),Vol.2, No.2, April 2012.

[9]. Mohammed A. AlZain, Ben Soh and Eric Pardede, "A New Approach Using Redundancy Technique to Improve Security in Cloud Computing", Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference on 26-28 June 2012.

[10]. DimitriosZissis, DimitriosLekkas, "Addressing cloud computing security issues", Future Generation Computer Systems 28 (2012) 583–592.

[11]. Mohammed A. AlZain, Eric Pardede, Ben Soh, James A. Thom, "Cloud Computing Security: From Single to Multi-Clouds", 45th Hawaii International Conference on System Sciences – 2012.

[12]. Lei Xu, XiaoxinWu,Xinwen Zhang, "CL-PRE: a Certificateless Proxy Re-Encryption Scheme for Secure Data Sharing with Public Cloud", ASIACCS '12 Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security.

[13]. Jianxin Li, Bo Li, Tianyu Wo, Chunming Hu, JinpengHuai, Lu Liu, K.P. Lam, "CyberGuarder: A virtualization security assurance architecture for green cloud computing", Future Generation Computer Systems 28 (2012) 379–390.

[14]. Deyan Chen, Hong Zhao, "Data Security and Privacy Protection Issues in Cloud Computing", International Conference on Computer Science and Electronics Engineering, 2012.

[15]. VeerrajuGampala, SrilakshmiInuganti, Satish Muppidi , "Data Security in Cloud Computing with Elliptic Curve Cryptography ", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-3, July 2012.

[16]. D.H. Patil, Rakesh R. Bhavsar, Akshay S. Thorve, " Data Security over Cloud ", International Conference on Emerging Frontiers in Technology for Rural Area (EFITRA) 2012 Proceedings published in International Journal of Computer Applications® (IJCA).

[17]. EmanM.Mohamed, Hatem S. Abdelkader, "Enhanced Data Security Model for Cloud Computing", The 8th International Conference on INFOrmatics and Systems (INFOS2012) - 14-16 May.

[18]. K. R. C. Wang, Q. Wang and W. Lou, "Ensuring data storage security in cloud computing," in Proc. 17th International Workshop on Quality of Service (IWQoS '09), pp. 1–9, 2009. N. I. of Standards and Technology (NIST). http://www.nist.gov/itl/cloud/.

[19]. Boyang Wang, Baochun Li, and Hui Li, "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud", Cloud Computing, IEEE Transactions on (Volume:2 , Issue: 1), Jan.-March 2014.

[20]. W. Liu, "Research on cloud computing security problem and strategy," in Consumer Electronics, Communications and Networks (CECNet), 2012 2nd International Conference on, pp. 1216–1219, IEEE, 2012.

[21]. A. Reed, C. Rezek, and P. Simmonds, "Security guidance for critical areas of focus in cloud computing v3. 0," Cloud Security Alliance, 2011.

[22]. S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," Journal of Network and Computer Applications, vol. 34, no. 1, pp. 1–11, 2011.

[23]. S. K. Sood, "A combined approach to ensure data security in cloud computing," Journal of Network and Computer Applications, vol. 35, no. 6, pp. 1831–1838, 2012.

[24]. Z. Mahmood, "Data location and security issues in cloud computing," in Emerging Intelligent Data and Web Technologies (EIDWT), 2011 International Conference on, pp. 49–54, IEEE, 2011.

[25]. Ronald Petrlic, Christoph Sorge, "Privacy-Preserving DRM for Cloud Computing", 26th International Conference on Advanced Information Networking and Applications Workshops-2012.