Concomitant ammunition for the counterfeit multi-cloud enumeration

Author:
Sunny H. Bhadlawala
M.Tech, B.E., MCP, MCTS,

***Abstract*— In this research paper, I have analyse on the multi-cloud Computing Time, budget, geographic reach, data protection, and the small number of companies that have already implemented cloud computing have shaped the level of detail in these research findings.**

The second in this paper of the multi-cloud, I have implemented a proposed structure to replicate servers and their data as and when needed.

However, consistency with applied research methods increases credibility and enriches the knowledge and insight generated in this study.

***Keywords*—cloud computing, multi-cloud computing, cryptography, Security, Authentication, Protocols.**

I. INTRODUCTION

Cloud computing has become a popular buzzword; it has been widely it are the focus of the IT industry.

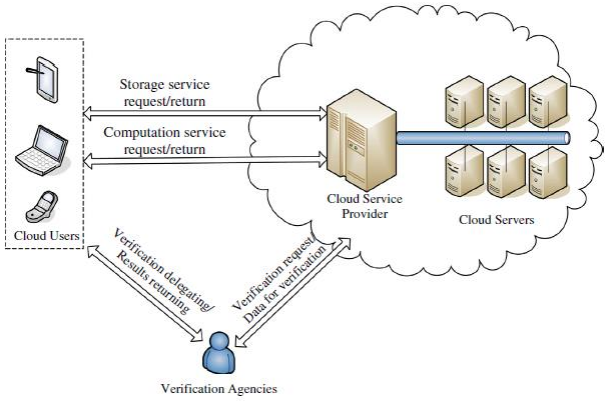

Fig.1 Protocol based cloud computing.

1.1. *Cloud Confidentiality*

Large organizations that own massive computing infrastructures in-house is most demanding now a days but management for that is very difficult for that cloud offering better solutions with the very minimal management of resources.

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

It makes it possible to utilizing cloud and industry resources which their effective usage, with no or minimal up-front costs.

All these operations can be performed and billed simply by entering the payment details through online only.

In this case, users subscribe to the service and establish with

1.2. *Layers and security issue in cloud*

Cloud computing seems really simple to the consumers of a cloud as in access cloud, place or retrieves required data that's all.

But the internal cloud as per master and slave is as per Fig 2. Illustrates various layers of cloud computing pyramid.

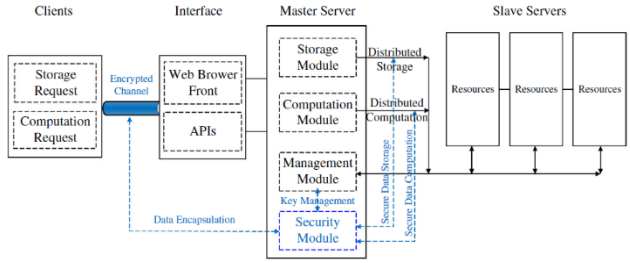

Fig.2 The cloud master and slave servers

1.2.1 *Service layer authorization*

Here with the fewer management and less hassles without worries regarding the installation of an application, software and it's updating of the apps such like company's Salesforce.com, Impel CRM, and Microsoft Dynamics etc.

II. PREVIOUSPAPERS STUDY

In base paper [1], approach to ensure data security in cloud computing:

It is an authenticated based approach to maximize the capacity and the capabilities vigorously without investing

in new infrastructure, nurturing new personnel or licensing new software.

III. PROPOSEDAPPROACH

Proposed algorithm for that I have used cloud sim library for practical implementations using following steps and mathematical equivalence.

1. Start using of the library with the following parameters.
   - 1.1. Number of users
   - 1.2. Calendar
   - 1.3. Trace flag
2. Create Datacentres Resources
   - 2.1. Create a Power Datacentre:
     1. Create storage in each machines
     2. Each machine should content at least 1 PEs.
     3. Generate PEs
     4. Generate Host
        - Number of machines
        - Memory: 1024 (MB)
        - Storage: 10000kb
        - Band width: 10000kb
     5. Generate a Datacentre warehouse with the operating systems, Machines, space.
        - Architecture: x86
        - OS: Linux
        - VM: Xen
        - Time zone: based on system location
     6. Shared Data Network to access Datacentres.
3. Create Brokers
4. Broker set link to datacentres
5. Create one Cloudlet
   - 5.1. Submit virtual machine list to the broker
6. Starts the simulation
7. Print the results

Each different type exercitation of simulation in CloudSim for that follows the steps in programming language code from configuration to simulation.

1. Set number of users.
2. Start the simulation.
3. Generate CIS.
4. Generate data centre.
5. Generate machines.
6. Generate broker.
7. Generate VMs.
8. Submitting data centre.
9. Generate cloudlets.
10. Submitting broker.
11. Start the simulation.
12. Stop the simulation.
13. Printing the results of the simulation.

Here Initialization can be generated by three parameters I^3it has two groups

$e^{\wedge}:S_1$& S_2

Where e = lim (1+1/x) x, x→∞)

S: $\{0, 1\}^* \rightarrow X_q^4$, S1: $\{0, 1\}^* \rightarrow G_1$

S2: $\{0, 1\}^* \rightarrow X_q^*$,

S_3: $S_2 \rightarrow X_q$.

User Registration: sk_{ID} = s Q_{ID}.

Storage space: X = {x1, x2,….,xn} ∈ Xq

$K_{I,SC} = S_3 (e^{\wedge}(sk_I, Z_{SC}))$

$K_{I,AV} = S_3 (e^{\wedge}(sk_I, Z_{AV}))$

$K_{I,SC} = S_3 (e^{\wedge}(sk_{CS}, Z_I))$.

$\sum_i = e^{\wedge} (U_i + S_2 (U_i || m_i || i_i) Z_{ID}, sk_{sc})$

$e^{\wedge}(U_A, sk_{av}) = \sum`_A$

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

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

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

IV. SIMULATION

Cloudlet ID	Status	Data Centre ID	VM	Time	Start Time	Finish Time
16	SUCCESS	7	5	100	90	100
44	SUCCESS	7	4	80	60	70
75	SUCCESS	7	9	160	101	102
18	SUCCESS	7	11	02	0	14
22	SUCCESS	7	12	102	15	16
33	SUCCESS	7	17	03	02	07
66	SUCCESS	7	16	01	0	1
97	SUCCESS	7	36	400	350	366
.	.	.	.	.	.	.
.	.	.	.	.	.	.
.	.	.	.	.	.	.
n^{th}	SUCCESS	7	n	$t+t^n$	t	t^n

Table - I: Cloud simulation

V. CONCLUSION

Therefore, I have utilized the CloudSim with the tools for research lab and then, I have implemented a proposed algorithm and executed the code based on mathematical equation and generated out comes with show that concept executed properly with the minimal strategies.

V. REFERENCES

[1].Nancy J. King, V.T. Raja, "Protecting the privacy and security of sensitive customer data in the cloud", computer law & security review28(2012)308e319

[2]. Abhishek Mohta ,Ravi Kant Sahu,Lalit Kumar Awasthi, "Robust, Volume 2, Issue 2, February 2012."

[3]. Ronnie D. Caytiles and Sunguk Lee, "Security Considerations for Public Mobile Cloud Computing ", international Journal of Advanced Science and Technology Vol. 44, July, 2012

[4].Abdul K., Samee K., Sajjad Contents lists available at Sci. Verse Science Direct Future Generation Computer Systems

[5].J. Han, W. Future Generation Computer Systems, vol. 29, no. 3, pp. 673–681, 2013.

[6].L. M. Kaufman, "Data security in the world of cloud computing," Security & Privacy, IEEE, vol. 7, no. 4, pp. 61–64, 2009.

[7].P. Kumar and H. S. Arri, "Data location in cloud computing," International Journal for Science and Emerging Technologies with Latest Trends, vol. 5, no. 1, pp. 24–27, 2013.

[8]."IBM-Uncovers-Encryption-Scheme-That-Could-Improve-Cloud-Security," http://www.eweek.com/c/a/Security/IBM-Uncovers-Encryption-Scheme-/ That-Could-Improve-Cloud-Security-Spam-Filtering-135413.

[9]. Advances in Networks and Services, vol 7 no 1 & 2, year 2014.