IJITKM 0973-4414 Volume-8, Number-2 Jan-Jun 2015 pp. 43-49

Security Protocol Based Algorithm in Cloud Computing Infrastructure

Shivani & Dr. Dheerendra singh
Shaheed Udham singh college of Engg. & Technology, Tangori, Punjab
shivani.dudeja90@gmail.com, professordsingh@gmail.com

ABSTRACT
Cloud Computing is one of the illustrious innovation in which all computing assets like equipment, programming and stages for creating applications are given as administrations to the clients through web. Clients don't need to contribute money to buy, oversee, keep up and scale the physical base. The clients can take obliged assets on interest from the cloud suppliers and pay for it as they utilize. This exploration assignment concentrates on the execution of dynamic and secured burden adjusting in the cloud computing environment. The proposed work is looked at focused around the parameters expense and execution time. The parameters in the proposed methodology are giving better, ideal and viable results in different cloud situations.
Keywords: Cloud Security, Secured Load Balancing, Cloud Computing.

INTRODUCTION

The administrations that are given by the cloud suppliers are comprehensively characterized into three classifications:
Infrastructure as-a-Service (IaaS): In Infrastructure as a Service show, the administration supplier possesses the gears including stockpiling, equipment, servers and systems administration segments and is given as administrations to the customers. The customer commonly pays on every utilization premise. Amazon flexible Compute (EC2) and Simple Storage Service (S3) are regular samples for IaaS.

Platform as-a-Service (PaaS): In Platform as a Service demonstrate, the administration supplier gives virtualized server, working framework and improvement devices as administration. Utilizing these administrations, clients can create, test, convey and oversee new applications in a cloud domain or run existing applications. These applications are conveyed to clients by means of the web. Google App Engine is an ordinary illustration for PaaS.
Software as-a-Service (SaaS): In Software as a Service demonstrate, the administration supplier gives programming as an administration over the Internet, dispensing with the need to purchase, introduce, keep up, overhaul and run the application on the client's own particular PCs. Google Docs is a normal sample.

A cloud administration has four different attributes as takes after:

i. It is flexible : A client can alertly scale up and scale down assets as they need at any given time.

ii. Pay Per Usage : Usage is metered and client pays just for what they expend.

iii. Operation: The administration is completely overseen by the supplier.

iv. Self-administration: Users can include another CPU, a server example or additional stockpiling utilizing the comfort offered by the cloud supplier.

CHARACTERISTICS OF CLOUD COMPUTING

The few of the characteristics of cloud computing is mentioned below : -

1) It is virtual, which means there are large numbers of servers which are placed along data centre. This server becomes massive pool of resources this pool is divided into various multiple virtual servers which lead to the creation of _cloud‘.

2) It is flexible and scalable, which means it gives whatever the user need within a moment. It also spins up the server in a moment and take it down just as easily.
3) It is open or closed, in open cloud it can be easily moved around without been locked into one provider or a closed, proprietary technology.
4) It can be secured, for maintaining the security there cloud be a creation of private cloud on the working hardware, but an appropriate security measures must be put on these cloud.
5) It can be affordable, a good cost saving could be made on public cloud, whereas in virtual servers runs on physical servers that are shared with other customers.

CLOUD COMPUTING SECURITY ARCHITECTURE

Security inside cloud registering is a particularly troubling issue as a result of the way that the gadgets used to give administrations don't have a place with the clients themselves. The clients have no control of, nor any learning of, what could happen to their information. This is an awesome concern in situations when clients have significant and individual data put away in a cloud figuring administration. Clients won't trade off their protection so cloud processing administration suppliers must guarantee that the clients' data is protected. This, on the other hand, is getting to be progressively difficult in light of the fact that as security advancements are made, there dependably is by all accounts somebody to make sense of an approach to debilitate the security and exploit client data. A percentage of the essential parts of Service Provider Layer are SLA Monitor, Metering, Accounting, Resource Provisioning, Scheduler& Dispatcher, Load Balancer, Advance Resource Reservation Monitor, and Policy Management. A portion of the security issues identified with Service Provider Layer are Identity, Infrastructure, Privacy, Data transmission, People and Identity, Audit and Compliance, Cloud uprightness and Binding Issues. A portion of the essential segments of Virtual Machine Layer makes number of virtual machines and number of working frameworks and its checking. A portion of the security issues identified with Virtual Machine Layer are VM Sprawl, VM Escape, Infrastructure, Separation between Customers, Cloud legitimate and Regularity issues, Identity and Access administration Some of the imperative parts of Data Center (Infrastructure) Layer contains the Servers, CPU's, memory, and capacity, and is from this time forward regularly indicated as Infrastructure-as-a-Service (IaaS). A percentage of the security issues identified with Data Center Layer are secure information very still, Physical Security: Network and Server.

A few associations have been concentrating on security issues in the cloud processing. The Cloud Security Alliance is a non-benefit association framed to advance the utilization of best practices for giving security certification inside Cloud Computing, and give training on the employments of Cloud Computing to help secure all different types of processing. The Open Security Architecture (OSA) is an alternate associations concentrating on security issues. They propose the OSA design, which example is an endeavor to outline center cloud works, the key parts for oversight and danger moderation, cooperation crosswise over different interior associations, and the controls that require extra accentuation. Case in point, the Certification, Accreditation, and Security Assessments arrangement increment in significance to guarantee oversight and confirmation given that the operations are being "outsourced" to an alternate supplier. Framework and Services Acquisition is pivotal to guarantee that procurement of administrations is overseen effectively. Possibility arranging serves to guarantee an agreeable comprehension of how to react in the occasion of intrusions to administration conveyance [14]. The Risk Assessment controls are essential to comprehend the dangers connected with administrations in a business connection. National Institute of Standard and Technology (NIST), USA (http :/www.nist.gov/) has started exercises to advance norms for cloud processing [39]. To deliver the difficulties and to empower cloud figuring, a few guidelines gatherings and industry consortia are creating proving ground gatherings are Cloud Security Alliance (CSA), Internet Engineering Task Force (IETF), Storage Networking Industry Association (SNIA) and so on. On the other side, a cloud API gives either an utilitarian interface or an administration interface (or both). Cloud administration has various angles that can be institutionalized for interoperability. Some conceivable principles are Federated security (e.g., character) crosswise over clouds, Metadata and information trades among clouds, Standardized yields for observing, examining, charging, reports and warning for cloud applications and administrations, Cloud-autonomous representation for arrangements and administration and so forth.

PRESENT WORK

In the proposed work and implementation, an effective algorithmic approach is devised and deployed for the dynamic secured environment. The proposed approach improves the classical approach mentioned in the base paper [1] for the optimized results.

3.3 PROBLEM FORMULATION

In cloud data centers, a number of resources are required to be balanced in terms of the server and power requirements. This work focus on developing a new algorithm for effective load balancing with secured environment.

We have simulated the work using MATLAB and CloudSim. Using MATLAB, the improved load balancing is implemented and CloudSim is used for secured environment simulation.

Cloud Data centre are vulnerable to assorted attacks. It is required for the cloud service providers to ensure the secured data transmission in the cloud framework. The proposed algorithmic approach shall make use of encryption based on the hash keys to secure the data centre and cloudlets.

Assumptions

For the implementation of dissertation various assumptions are : -

- Creation of multiple datacenters, Virtual Machines
- Multiple Cloud brokers shall be used
- One host each in the datacenters
- Execution of cloudlets of two users on them.
- Hash Keys shall be used

Parameters

- Turnaround Time
- Delay
- Execution Time without hash keys
- Execution Time with implementation of hash keys
- Security improvement percentage.

RESULTS AND DISCUSSION

4.1 RESULTS AND DISCUSSION
PROPOSED WORK WITH IMPROVED SERVER ALLOCATION AND LOAD BALANCING

In the results, it is evident that the server allocation is effective in terms of equal and consistent assignment of resources. In case of existing approach, the resource allocation is not effective.

Table 4.1:Simulation and Comparative Results

Existing Approach	Improved Algorithm
42	66
45	51
35	86
41	51
42	59
33	71
36	78
33	89
45	53
35	80

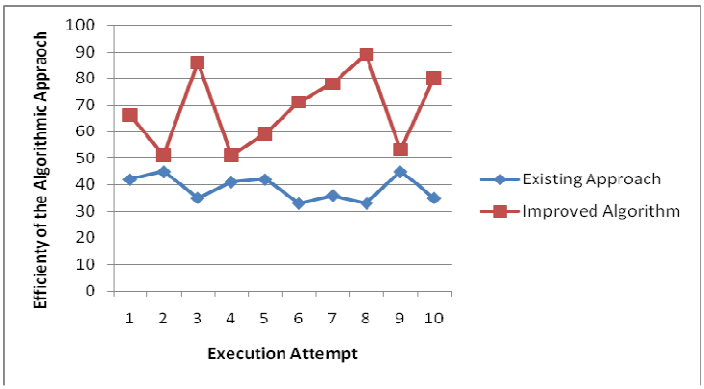

Figure 4.1 Comparison between classical and proposed approach

The figure shows the comparative analysis between classical and proposed approach. It is clear from the results that the proposed approach is giving better results as compared to the classical in terms of efficiency and integrity.

Table 4.2 Simulation and Comparative Results

Existing Approach	Improved Algorithm
2.2	1.5232
3.2	2.1212
3.43	2.112
3.245	2.6
4.2323	3.3111
4.2112	3.2323
2.3232	2.1212
3.2637	2.35235
3.6211	2.32323
4.2222	3.221

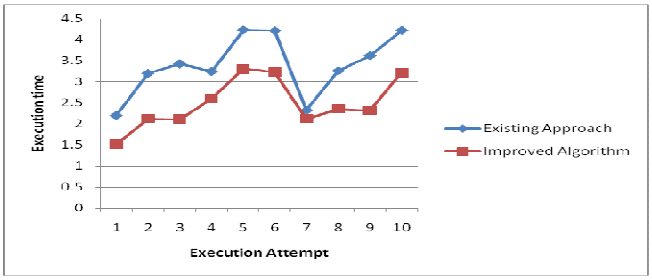

Figure 4.2 Bar comparison between existing and proposed approach

COMPARISON OF EXECUTION TIME IN EXISTING AND PROPOSED APPROACH

Table 4.3 represents the major differences in the classical and proposed approach in terms of execution time. It is evident from the results specified in Table 4.3 that the execution time of proposed approach is very less as compared to the classical approach because the proposed approach is making use of parallel execution as compared to the sequential implementation in the existing approach. The proposed algorithmic approach is simulated in number of iterations which is mentioned here as Simulation Attempt.

Table 4.3 - Comparison Table of Classical and Proposed Approach in terms of Execution Time

Simulation Attempt	Proposed Approach	Existing Approach
1	1316	2724
2	1242	2914
3	1113	2367
4	1192	2300
5	1281	2971
6	1804	2359
7	1483	2613
8	1286	2096
9	1855	2700
10	1090	2049
11	1415	2939
12	1376	2588
13	1005	2151
14	1039	2485
15	1340	2797
16	1828	2755
17	1680	2132

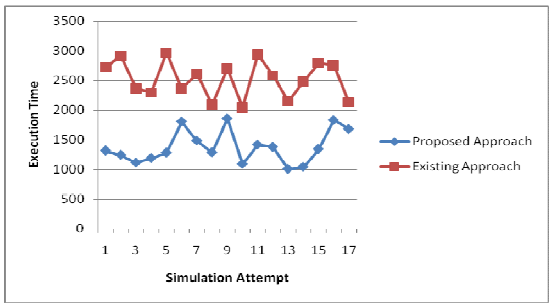

Figure 4.4 – Comparison between Existing and Proposed Approach

COMPARISON TABLE FOR SECURITY PARAMETER

Table 4.4 depicts the comparative analysis of proposed and existing approach in terms of security enhancement. It is clear from the results and Figure 4.4 that the results are efficient in the proposed approach.

Table 4.4 - Comparison Table of Classical and Proposed Approach in terms of Security

Simulation Attempt	Existing	Proposed
1	10	37
2	10	32
3	15	32
4	16	38
5	15	33
6	16	39
7	17	38
8	18	33
9	11	33
10	12	40
11	16	39
12	15	31

13	11	40
14	11	34
15	18	30
16	20	38
17	10	33
18	19	34
19	16	37
20	10	36

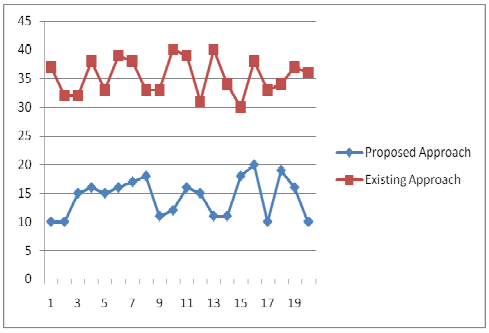

Figure 4.5 – Line Graph Comparison between Existing and Proposed Approach

CONCLUSION AND FUTURE SCOPE

This work mainly focuses on the security as well as load balancing aspects in the cloud computing infrastructure. The existing algorithmic approaches are not effective by which the security can be enhanced. In the proposed approach, the improvements in the classical algorithms are implemented and effective results are found. The proposed approach gives optimized cost as well as the execution time that is directly proportional and related.

The tolerance power of proposed model may be checked by implementing and penetrating various attacks. After the tolerance test we may come to a conclusion about its robustness in terms of confidentiality, integrity and authenticity.

- The combination of access control techniques and cryptographic techniques may be used to maintain more privacy and security of data within the cloud.
- The QOS (quality of service) of proposed model may be determined in terms of availability, throughput and delay.
- The actual physical implementation and testing of proposed model required to detect its fault tolerant power and Data availability.
- The work can be enhanced using metaheuristics techniques including
- Genetic Algorithms
- Ant Colony Optimization
- Neural Networks
- HoneyBee Algorithm

REFRENCES

[1] Abhay Bhadani , Sanjay Chaudhary, “Performance Evaluation of Web Servers using Central Load Balancing Policy over Virtual Machines on Cloud”, Proceedings of the Third Annual ACM Bangalore Conference, Article No. 16, ISBN: 978-1-4503-0001-8, January 2010, DOI: 10.1145/1754288.1754304.

[2] Anthony T.Velte, Toby J.Velte, Robert Eisenpeter, “Cloud Computing: A Practical Approach”, Tata McGraw-Hill Publishers, 1st Edition, 2009, ISBN: 0071626948.

[3] Argha Roy, Diptam Dutta, “Dynamic Load Balancing: Improve efficiency in Cloud Computing”, International Journal of Emerging Research in Management Technology, pp 78-82, Vol 2, Issue 4, ISSN:2278-9359, April 2013.

[4] Arzuaga, E., and Kaeli, D. R., 2010, Quantifying load imbalance on virtualized enterprise servers,

Proceedings of the first joint WOSP/SIPEW international conference on Performance engineering, pp. 235–242.

[5] Barrie Sosinsky, "Cloud Computing Bible", Wiley publishers, 1st edition, December 2010, ISBN: 978-0-470-90356-8.

[6] Bellur, U., Rao C., and Kumar, M., 2010, Optimal Placement Algorithms for Virtual Machines, Proceedings of CoRR, pp.103-110.

[7] Bobroff, N., Kochut, A., and Beaty, K., 2007, Dynamic Placement of Virtual Machines for Managing SLA Violations, Proceedings of the 10th IFIP/IEEE Symposium on Integrated Network Management, pp. 119-128.

[8] Che-Lun Hung, Hsiao-hsi Wang, Yu-Chen Hu, "Efficient Load Balancing Algorithm for Cloud Computing Network", International Conference on Information Science and Technology (IST 2012), pp 251-253, April 28-30, 2012.

[9] Chandrasekaran, B., Purush, R., Douglas, B., and Schmidt, D., 2007, Virtualization Management Using Microsoft System Center and Dell OpenManage, Dell Power Solutions, pp. 40-44.

[10] Uddalak Chatterjee, "A Study on Efficient Load Balancing Algorithms in Cloud Computing Environment", International Journal of Current Engineering and Technology, pp 1767-1770, Vol 3, ISSN 2277-4106, December 2013.

[11] Vaidehi. M, Rashmi. K. S, Suma. V, "Enhanced Load Balancing to Avoid Deadlock in Cloud", International Journal of Computer Applications on Advanced Computing and Communication Technologies for HPC Applications, pp 31-35, June 2012.

[12] Van, H., and Tran, F., 2009, Autonomic resource management for service host platforms, Proceedings of Workshop on Software Engineering Challenges in Cloud Computing, pp. 1-8.

[13] Verma, A., Ahuja, P., and Neogi, A., 2008, pMapper: Power and Migration Cost Aware Application Placement in Virtualized Systems, Proceedings of the 9th ACM/IFIP/USENIX International Conference on Middleware, pp. 243-264.

[14] W Kleiminger, E Kalyvianaki, P Pietzuch, "Balancing Load in Stream Processing with the Cloud", 27th IEEE International Conference on Data Engineering Workshops[ICDEW], Zurich, Switzerland, pp 16-21, 11-16 April 2011, DOI: 10.1109/ ICDEW.2011.5767653.

[15] Wood, T., Shenoy, P., and Arun, 2007, Black-box and gray-box strategies for virtual machine migration, NSDI 2007, pp. 229–242.

[16] Xu, J., and Fortes, J., 2010, Multi-objective Virtual Machine Placement in Virtualized Data Center Environments, Proceedings of the 2010 IEEE/ACM Conference on Green Computing and Communications, pp. 179-188.

[17] Yi Lu, Qiaomin Xie, Gabriel Kliot, Alan Geller, James R Larus, Albert Greenberg, "Join-Idle-Queue: A Novel Load Balancing Algorithm for Dynamically Scalable Web Services", Elsevier, Journal on Performance Evaluation, pp 1056-1071, Vol 68, Issue 11, Nov 2011, DOI: 10.1016/j.peva.2011.07. 015.

[18] Zhao, Y., and Huang, W., 2009, Adaptive Distributed Load Balancing Algorithm based on Live Migration of Virtual Machines in Cloud, Proceedings of 5th IEEE International Joint Conference on INC, IMS and IDC, pp. 170-175.

[19] Gallery Images For (Basic Cloud Architecture) URL - http://imgarcade.com/1/basic-cloud-architecture

[20] Tziritas, Nikos, Cheng-Zhong Xu, Thanasis Loukopoulos, Samee Ullah Khan, and Zhibin Yu. "Application-aware Workload Consolidation to Minimize both Energy Consumption and Network Load in Cloud Environments." In Parallel Processing (ICPP), 2013 42nd International Conference on, pp. 449-457. IEEE, 2013.