Enhancing Secured and Balanced Centralized Multiservice Cloud System

Lida John [1*], Prof. P Mohamed Shameem[2*]
[1*] PG Scholar, Dept. of computer science and engineering
[2*] Professor, Dept. of computer science and engineering
TKM Institute of Technology, Kollam, India

***Abstract*— In Centralized Cloud-based Multimedia System(CMS), massive data goes through the Centralized system i.e. Resource Manager which in turn creates a chance for heavier load. Thus the load balancing is done by calculating the cost of transmission to each cluster head based upon the traffic load and network proximity. Then the Cluster Head chooses the optimal server using Genetic Algorithm without violating the maximal load on each server. The proposed scheme checks whether the optimal cluster head is consistent or not for the particular request using Reply Attestation Scheme. Our experimental results shows that each client can optimally utilize the resources with minimum response time and resource cost based upon each client request**.

Keywords: Cloud Computing, Genetic Algorithm, Integrity attestation, Signature Authentication.

I.INTRODUCTION

Cloud Computing is an emerged computing paradigm that can provide computation, storage, and communication resources as per users demands in a scalable and virtualized manner. With the explosive growth of multimedia applications over the internet such as image, video, audio retrieval and sending to host, intensive computation, real-time conferencing, video on demand etc causes heavier load in the cloud. Multimedia cloud contains several heterogeneity based challenges. They are:

a) Multimedia and service heterogeneity
b) Qos heterogeneity
c) Network heterogeneity
D) Device heterogeneity.

Multimedia Cloud [1] focuses on how cloud can provide Quality of service with this heterogeneity and also provisioning for multimedia application and services. However, in such a Multimedia Cloud environment there is a challenging issue i.e. how the requested clients required resources in shortest time. Mainly in centralized system without a proper load-balancing scheme, cause heavier load in the connected nodes which will eventually cause a bottleneck in the system's service quality.

This paper considers a Centralized Cloud Based Multimedia System (CMS).In the systematical concern of the centralized system consists of Resource Manager, Cluster Head and Servers connected to it. RM receives requests from each client and transmitted to appropriate Cluster Head. Subsequently, the cluster head of each sever cluster distributes the assigned task to optimal server within the cluster. Here the challenging issue is the uncontrollable load in the RM. Load balancing is the process of reassigning the total load to the individual nodes of the collective system. It makes resource utilization effective and improves the response time of the job. And also the cloud computing field is a flourishing industry that comes with its own set of new security challenges. A cloud infrastructure is the result of a constant three-way negotiation among service organizations, cloud service providers (CSPs), and end users to ensure productivity while maintaining a reasonable degree of security. The CSP should keep data safe from security threats and yet give the client access anywhere with an Internet service. A client organization also needs to verify that the cloud computing enterprise is contributing to its business goals and to its objectives.

The rest of the paper is organized as follows: Section II explains the related works about the topic. Section III contains the problem description having the system model and parameter explanation. Section III defines the algorithm and working details. Section IV presents the performance evaluation of each parameter. Section V summarizes the result.

II. REALATED WORK

Load Balancing in wireless networks has been studied extensively in previous literature.eg, multiple-factor load balancing [2], load balancing with policy mechanism [3], load balancing based on game theory [4], load balancing in WLANs [5], multiservice load balancing [6] and soft load balancing [7], and scheduling [8] in heterogeneous wireless networks. By considering the CMS in [9] distributing the load in RM to each cluster head and then to optimal servers without violating the maximal load in servers.

The integer linear programming problem will occurred when the server cluster only handle a specific type of multimedia service task, and each client request different multimedia services. That can be solved by using a heuristics approach i.e. here we use Genetic algorithm [10]. Here an integrated service integrity attestation framework is provided for the multiservice cloud systems. It provides a practical service integrity attestation scheme, that does not trusted entities on third party service provisioning sites or require application modifications. This is scalable and efficient distributed service integrity attestation framework can be used on large scale cloud

computing infrastructures. Although our experimental results have shown that it can achieve better scalability and higher detection accuracy.

Here the signature developed by the sender for each packet with private key known signing, after that receiver checks the integrity of each packet using public key known as verifying. If both the process succeeds then the received packet is authentic. Note that the RSA [11], which is expensive on signing and verifying. All the schemes in [12] are indeed computationally not efficient since each receiver needs to verify only one signature for a block of packets. In the existed scheme not implement a efficient consistency checking of each nodes. In addition they not concern about the overhead produced in the centralized system.

II.PROBLEM DESCRIPTION

In the centralized system in [13] is based upon only the selection process in the connected nodes. Here the selected nodes may be malicious or not. Thus there is a chance of creating overhead in the RM. According to that whole system will damage. So by extending this model with these concerns, the first section gives the system overview and then formulates our concerned problem.

A. System Model

The representative network architecture of CMS is illustrated in Figure 1.Three different network levels can be defined as follows:

- Resource Manager (RM): Each time it receives and manages the client request of service tasks and also to the server cluster.
- Cluster Head (CH): Among from all the cluster heads, the CH having minimum will undergo for attestation scheme. The consistent CH was selected for further transmission of particular request.
- Server Clusters: Based upon the characteristics of different service request, it will be transmitted to servers in server clusters.

In this Centralized System with genetic algorithm imposed some overhead due different iterated values on each timestamp. However the above CMS with attestation scheme providing reliable and easier transmission rate.

B. General Architecture

Our system model involves the Resource Manager, Cluster head and servers connected to it. A typical

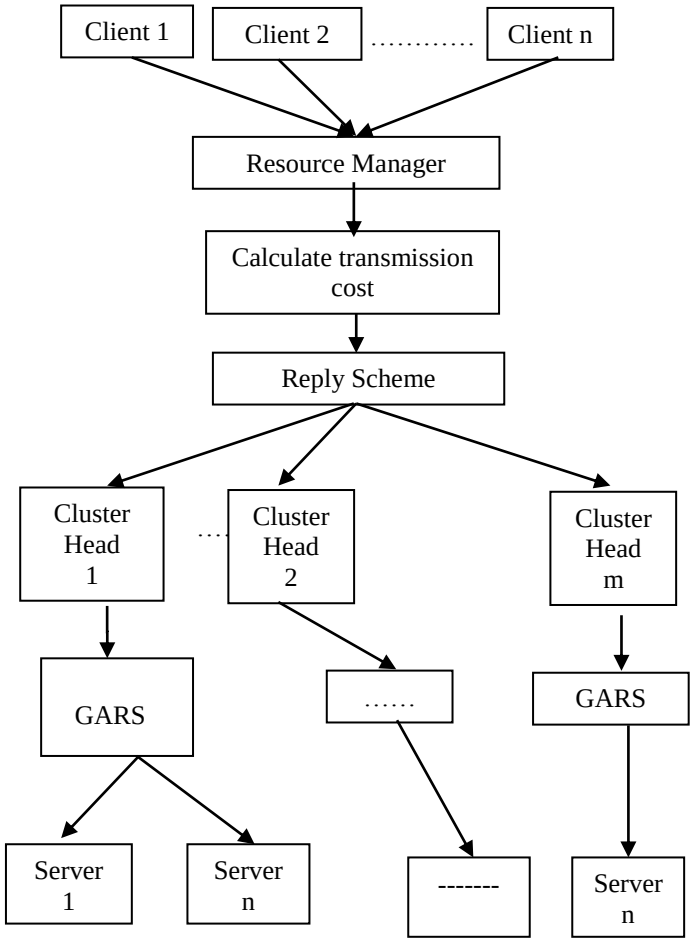

Fig1. Illustration of Secured Centralized Cloud based Multiservice System.

configuration of our system architecture shown in Fig. 1. The diagrammatic representation shows the transmission flow of each request.

Multiple client requests is received in the Resource Manager and there is chance for creating bottleneck due to frequent transmission. So the basic concept of calculating transmission cost to each cluster head and select the cluster head which having minimum cost while computing with other nodes. Then that node will take for further transmission. After that, the reply scheme will performed in each selected nodes like cluster head and also the connected servers which will lead to find out the malicious nodes in between them. For finding the optimal node to a particular request here use the iteration value using genetic algorithm performed in all servers and nodes connected to it.

C . Problem Formulation

In CMS, each client will assigned a particular link related to the characteristics of request they send. Let before the assigning of links to each request want to satisfy the condition given below:

$$\mu_i = \emptyset_j \qquad (1)$$

Where, μ_i indicates the request send by the client and $\emptyset_j$ indicates the resource provide by the client will be equal. Otherwise repeatedly we have to check all the nodes with an optimum resource. And also the quality of service provide by particular server will be higher than the given request. Otherwise cannot provide a successful transmission of data. i.e.

$$s_i \geq w_j \quad (2)$$

Where, s_i is the Qos provided by the server and w_j is the Qos requested by the client. The goal is to help increase local resource allocations during increase demands. Our scheme should satisfy the resource requirements based upon the availability. The cost for transmitting multimedia data between server cluster *i* and client *j* at a particular time step, which is defined as follows:

$$T_c = \begin{cases} \infty & if\ l_{ij} \to \infty \\ l_{ij}\, t_{ij} & otherwise \end{cases} \quad (3)$$

Where, l_{ij} is the network proximity between server cluster *i* and client *j*, t_{ij} is the traffic load of the link between server cluster *i* and client *j* that is defined as follows:

$$t_{ij} = \sum_{n \in N_i} S_{inj}\, C_{in} \quad (4)$$

Where N_i is the set of servers in server cluster *i*; S_{inj} is the server utilization ratio of server *n* in server cluster *i* due to client *j*, and C_{in} is its capacity. Based upon the above condition calculate the value for selecting the nodes which optimal for particular request. The server cluster can be created using the distributed binning method[13]. This method is helpful for cluster level configuration in the system.

III. DESIGN AND ALGORITHMS

A. Calculation of Transmission Cost

The GARS specifying both the Genetic and Reply Scheme on selected clusters which satisfying below conditions. While satisfying the conditions a set of optimal nodes and apply the given algorithm on it where *r* represents request send by the client.

1. **for** *r* = 1,2… **do**
2. remove the links violating eq(1) and eq(2)
3. remove the nodes which are out of bin
4. obtain the set of available cluster for request *r*
5. for each *r*, do
6. measure the traffic load to each cluster using (4)
7. measure the transmission cost of each client request using (3)
8. end for
9. end for

B. Data Reply Scheme

In order to detect service integrity attack, a data reply method with the function value is used in the processing service nodes. Different malicious activity that attempts to track or attack the information of system resources or the information of each nodes. Due to this the system undergo through a *consistency check* method to detect is it malicious or not. The different level nodes ie, cluster heads and severs send their own functions based upon the data send to the client. Most probably each nodes send same functions for a particular request. The reply function of each data is checked by the provider. The function send by the malicious is different from the other nodes for particular request. Thus the malicious attackers cannot be avoiding the risk of detected when they produce false results on the original data.

Here for the reply scheme use a batch signature verification for achieving the functional values of each data. The problem here is based on the sender-favored approach and a receiver-oriented approach by taking into account the heterogeneity of the receivers. In particular, when a receiver collects n packets:

$$p_i = \{m_i, \sigma_i\}, i=1,\ldots n,$$

Where m_i is the data payload, σ_i is the corresponding signature, and i can be any positive integer, it can input them into an algorithm

$$\text{Batch Verify } (p_1 p_2 \ldots p_n) \in \{True, False\}.$$

If the output is *True*, when the receiver knows the *n* packets are authentic, and otherwise not. If the batch packets are signed by the sender, the verification value will be true. Otherwise the verification value will be false due to some unauthenticated packets. The parametric calculation for signature verification method,

Definition:

p, a prime longer than 512 bits.
q, a 160-bit prime divisor of p _ 1.
g, a generator value with order q, $g^q = 1 \bmod q$.
x, the private key of the signer, $0 < x < q$.
y, the public key of the signer, $y = g^x \bmod p$.
h(), a hash function generating an output.

Given a message m, the signer generates a signature by:

1. randomly selecting an integer k with $0 < k < q$,
2. computing h = h(m),
3. computing $r = n (g^k \bmod p) \bmod q$, and
4. computing $s = rk - hx \bmod q$.

Therefore, the signature value verified by the receiver with a function value given by the sender. Based upon the reply data, receiver checks the consistency of the node. Moreover, the same processing is occurring in receiver for verification.

C. Working Principle of Genetic Algorithms (GAs)

The genetic algorithms (GAs) are based survival of the fittest. Genetic algorithms (GAs) may contain a set

of chromosome (selection process related to the solution), grouping of chromosome population, check fitness with fitness function, mutation and survival. Genetic algorithms (GAs) begin with a set of solutions represented by chromosomes, called population. Solutions from one population are taken and used to form a new set of population, which is motivated by the possibility that the new population will be better than the old population.

Here in this transmission between nodes, each routing path is encoded by string of positive integers that represent the IDs and path which they pass etc. These string represent the order of a nodes. The iteration goes on the nodes which are not malicious. In our algorithm the corresponding routing path is randomly generated for each chromosome in the initial population.

I. Create random population of chromosomes, with suitable solution based upon the parameter value given above. Here denoted by £ .

II. Calculate the fitness of each chromosome in the population.

$$\text{Fitness } (C_i) = \begin{cases} 1 & \text{if } i \text{ is fiitted for solution} \\ 0 & \text{Otherwise} \end{cases}$$

III: The new population created based upon the fitness value subjected to binary encoding of each strings.

a) Select two parent chromosomes from the pool a based upon their fitness. Better the fitness chromosomes taken as parental chromosomes.

b) The chosen individual chromosomes taken for crossover process. At this stage, a value of k bit streams is generated based on nodes selected.

c) In the mutation process, each locus value generated related to the solution with a probability. Mutation process is done when the bit stream values not satisfy the solution.

IV: Checking if the end condition is satisfied or not. Based upon the value stop the iteration process otherwise repeat it.

V: Return the best solution in current population.

VI. PERFORMANCE EVALUATION

To the best of our understanding, there are no previous works that studied on this concerned problem. As a result, here we have implemented an attestation signature verification on each nodes. By the consistency check on each node, overhead created in the whole system can be reduced thereby increasing the accuracy rate. In addition to that we can increase the throughput rate according to the number of tasks. From the simulation result in fig.2 and fig.3 the accuracy rate and throughput rate are justified.

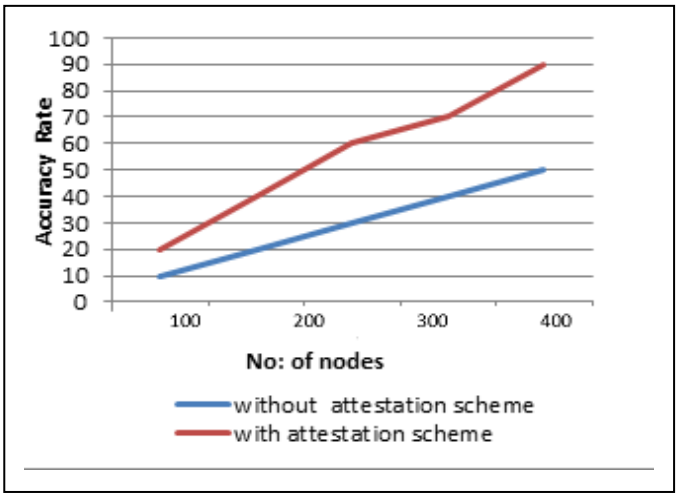

Fig 2. Average rate of accuracy increase in number of nodes

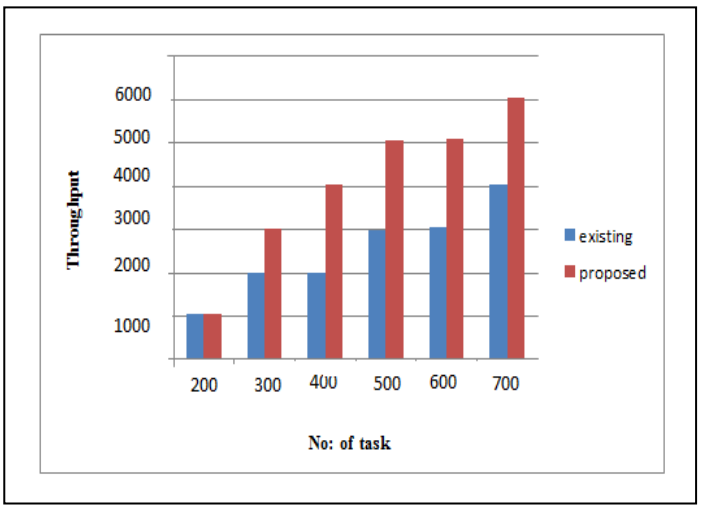

Fig 3. Increase of throughput in the number of task.

V. CONCLUSION

In Centralized Multiservice System, secured transmission is an inevitable to reduce the overhead in Resource Manager. The main difference from the previous model is that we considered a reply attestation scheme on each node to check whether it is malicious or not. The security proof and efficiency evaluations are illustrated in this paper. The attestation with batch signature value purely provides a highly secured transmission scheme which increases the accuracy rate of each data packet. The simulation result shows this scheme can achieve higher pinpointing accuracy than the existing alternative schemes and also reduces the overhead created by the malicious attackers.

REFERENCES

[1] W. Zhu, C. Luo, J. Wang, and S. Li, "Multimedia cloud computing: An emerging technology for providing multimedia services and applications," IEEE Signal Process. Mag., vol. 28, no. 3, pp. 59–69, May 2011.

[2] C.-F. Lai, Y.-M. Huang, and H.-C. Chao, "DLNA-based multimedia sharing system over OSGI framework with extension to P2P network," IEEE Syst. J., vol. 4, no. 2, pp. 262–270, Jun. 2010.

[3] W. Hui, H. Zhao, C. Lin, and Y. Yang, "Effective load balancing for cloud-based multimedia system," in Proc. Int. Conf. Electron. Mech. Eng. Inform. Technol., 2011, pp. 165–168.

[4] C.-Y. Chen, H.-C. Chao, S.-Y. Kuo, and K.-D. Chang, "Rule-based intrusion detection mechanism for IP multimedia subsystem," J. Internet Technol., vol. 9, no. 5, pp. 329–336, 2008.

[5] L. J. Wu, A. E. AL Sabbagh, K. Sandrasegaran, M. Elkashlan, and C. C. Lin, "Performance evaluation on common radio resource management algorithms," in Proc. 24th IEEE Int. Conf. Advanced Information Networking Appl. Workshops, Mar. 2010, pp. 491–495.

[6] R. Yavatkar, D. Pendarakis, and R. Guerin, "A framework for policy based admission control," Internet Requests for Comments, RFC Editor, RFC 2753, 2000.

[7] D. Niyato and E. Hossain, "Integration of Wi=0MAX and WiFi: Optimal pricing for bandwidth sharing," IEEE Commun. Mag., vol. 45, no. 5, pp.140–146, May 2007.

[8] C.-Y. Chang, T.-Y. Wu, C.-C. Huang, A. J.-W. Whang, and H.-C. Chao, "Robust header compression with load balance and dynamic bandwidth aggregation capabilities in WLAN," J. Internet Technol., vol. 8, no. 3, pp. 365–372, 2007.

[9] J. Sun, X. Wu, and X. Sha, "Load balancing algorithm with multiservice in heterogeneous wireless networks," in Proc. 6th Int. ICST Conf. Commun. Networking China (ChinaCom), 2011, pp. 703–707.

[10]H. Cheng and S. Yang, "Genetic algorithms with immigrants schemes for dynamic multicast problems in mobile ad hoc networks," *Eng. Appl.Artif. Intell.*, vol. 23, no. 5, pp. 806–819, 2010.

[11] J. Du, X. Gu, and T. Yu, "On Verifying Stateful Dataflow Processing Services in Large-Scale Cloud Systems," Proc. ACM Conf. Computer and Communications Security (CCS), pp. 672-674, 2010.

[12] C.K. Wong and S.S. Lam, "Digital Signatures for Flows and Multicasts," Proc. Sixth Int'l Conf. Network Protocols (ICNP '98), pp. 198-209, Oct. 1998.

[13] H. Cheng and S. Yang, "Genetic algorithms with immigrants schemes for dynamic multicast problems in mobile ad hoc networks," *Eng. Appl. Artif. Intell.*, vol. 23, no. 5, pp. 806–819, 2010.

[14] H. Takabi, J. B. D. Joshi, and G. J. Ahn, "Security and privacy challenges in cloud computing environments," *IEEE Security Privacy*, vol. 8, no. 6, Nov.–Dec. 2010.

[15] J. Idziorek, M. F. Tannian, and D. Jacobson, "The insecurity of cloud utility models," IEEE Cloud Comput., pp. 14–18, May–June 2013.

.