An Efficient Technique for Energy Consumption in Distributed Cloud Network Using ANT Technique

Priya Dubey [1], Mr. Saurabh Jain [2]
M.Tech Scholar [1], Assistant Professor [2]
Department of Computer Science and Engineering
Oriental College of Technology
Bhopal – India

ABSTRACT
Cloud Computing enables various users to send their data over cloud and also in distrusted manner. But during the transmission of data over distributed network in cloud, energy consumption is more and hence network becomes unstable and costly. Hence various techniques are implemented for the energy consumption in cloud network, but the technique implemented so far is not an efficient and stable technique for the energy consumption as well as execution time. Here an efficient technique is implemented for the energy consumption as well as for the less execution of data transmission and overload over cloud network using Ant based shortest path.

Keywords:- Cloud, Security, Multi-Keyword, Cloud Computing.

I. INTRODUCTION

Cloud Computing means a remote server that access through the internet which helps in business applications and functionality along with the convention of system software for respective web application. Cloud computing concept saves capital that cloud users pay out on annual or monthly payment. Due to advantage of cloud services, more and more sensitive information are being centralized into the cloud servers, such as confidential videos and photos, various emails, personal health records information, corporation business data, government documents, etc. So as to privacy problem, data privacy [1] and data loss will be increase in certain circumstances. When users outsource their private onto cloud, the cloud service provider able to monitor the communication between the users and cloud at will trust or untrusted. As cloud computing is promising development in computing concept the confidence increase becomes very important aspect. There are mainly two parameters which can help to get better the confidence on the cloud services. One is to improve efficiency and another for improving security. To improve the efficiency the keyword search method is enhanced as it makes available two way communications between cloud server and the cloud customer. But while deploying security the burden on cloud server gets increased unexpectedly. Consequently it is extremely significant to maintain these two factors so that to improve overall efficiency of the cloud services [2]. Also the world is of mobile devices, so everyone wants to use cloud services on their mobile devices and if the computational cost goes to elevated then it effects into important resource utilization, which is not appropriate for mobile devices. So current scenario is having need of a proficient method is cloud services in the expectations.

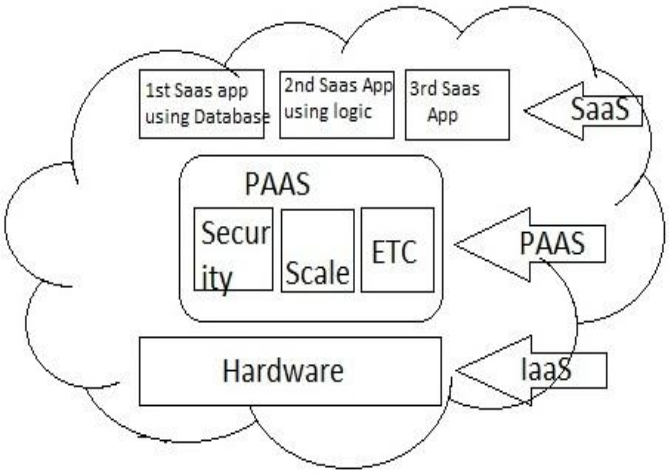

Figure 1. Architecture of the Cloud Computing

Cloud is a service which can be accessed from everywhere if arranged in that way at any path. It causes lots of parties or persons using it for their purpose. In such case the data Various parties may contribute to within them on the cloud server can be secret. In addition every cloud user who uses cloud services doesn't like to get followed. In such cases it is very important to maintain their privacy [3]. Thus to maintain their privacy the files and even the search requests are encrypted as soon as the request is sent to the server. This encryption may also affect the efficiency of searching techniques as the search should go on in encrypted manner.

Besides, in cloud computing data owners may allocate their outsourced data with a number of cloud users, who strength want to only get back the data files they are paying attention in cloud server. One of the most fashionable ways to do so is throughout keyword-based retrieval. It is like better to get the retrieval outcome with the most significant content of the users which matches with the ranked in order to fill the user's

interest. To develop security exclusive of give up effectiveness, methods here in [4], [5], give you an idea about that they sustain top-k single keyword retrieval under different circumstances. To protect data privacy, confidential data has to be encrypted before outsourcing, so as to provide end-to-end data confidentiality assurance in the cloud. Clouds enable customers to remotely store and access their data by lowering the cost of hardware ownership while providing robust and fast services [6]. The importance and necessity of privacy preserving search techniques are even more pronounced in the cloud applications. Due to the fact that large companies that operate the public clouds like Google or Amazon may access the sensitive data and search patterns, hiding the query and the retrieved data has great importance in ensuring the privacy and security of those using cloud services. We aim to achieve an efficient system where any authorized user can perform a search on a remote database with multiple keywords, not including exposing neither the keywords he/she searches for, nor the pleased of the documents he/she get backs. The main confront of cloud storage is guaranteeing have power over, and the essential integrity and confidentiality of all stored cloud data.

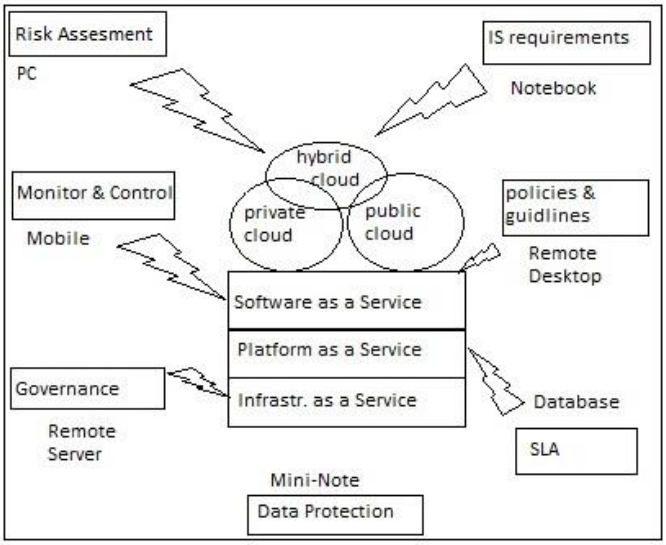

Figure 2. Various Models of Cloud Computing

Benefits of Cloud Computing

- Although the infrastructures under the cloud are much more powerful and reliable than personal computing devices, they are still facing the broad range of both internal and external threats for data integrity.
- Second, there do exist various motivations for CSP to behave unfaithfully toward the cloud users regarding their outsourced data status.
- In particular, simply downloading all the data for its integrity verification is not a practical solution due to the expensiveness in I/O and transmission cost across the network. Besides, it is often insufficient to detect the data corruption only when accessing the data, as it does not give users correctness assurance for those unaccessed data and might be too late to recover the data loss or damage.
- Encryption does not completely solve the problem of protecting data privacy against third-party auditing but just reduces it to the complex key management domain. Unauthorized data leakage still remains possible due to the potential exposure of decryption keys.

II. LITERATURE REVIEW

2014- A. Q. Lawey et. al. they introduced energy efficient cloud computing services design framework over IP/WDM core networks. They analyzed distribution of clouds, impact of demand, cloud capability, access frequency content popularity along with no. of switches, routers, servers, storage required in cloud [7]. They examined cloud content delivery, virtual machines and storage as a service (StaaS).they developed mixed integer linear programming (MILP) to enhance services of cloud content delivery by replicating content into multiple clouds on which they developed energy efficient cloud content delivery heuristic DEER-CD. They increased power savings by migrating content according to access frequency and by optimizing placement of virtual machines by breaking them into smaller virtual machines and placing them in proximity. They termed replicating content into multiple clouds based on content popularity as OPR scheme. With the help of these schemes they were able to save 92% and 43% network and total power savings respectively. They obtained power savings are by placing Virtual machines using a heuristic (DEER-VM) developed to copy the model behavior in real time [7].

2014 – V. Mathew et. al. identified the operational costs of Internet scale distributes systems(IDS).they proposed a demand response technique in which pricing signals from smart grid makes the system to reduce energy usage [8]. The load is deferred from elastic requests to later time periods reducing server demand and energy usage. They proposed optimal offline algorithm and showed that cost savings can be achieved without increasing in bandwidth cost of IDS .the approach used by them for elastic requests like background downloads, software updates etc. does not require continuous services. The algorithm proposed by them achieved 12% of savings on time of use electricity pricing. They presented a future plan to move load to near data centers for energy saving [8].

2013- S. Zaman et. al. analyzed that the cloud computing resources were provisioned to different virtual machine instances allocated to users for specific period of time which is not efficient allocation economically due to fixed price allocation [9]. They proposed combinatorial auction based allocation which described that user's demand is taken into account while making provisioning decisions and VM allocation because the existing mechanism do not consider user's demand. They evaluated the mechanism through simulation experiments which improved utilization of resources of clouds and increased the revenue of cloud

provider. They designed mechanism CA-PROVISION which effectively captured market demand, provisioned the computing resources and generated higher revenue as compared to CA-GREEDY [9].

2013- K. Qazi et. al. observed that virtual machines(VM) rent computational resources like memory, network bandwidth etc. to data center owners [10]. They stated that the physical machine that make up cloud termed as machine farms should optimally use these resources without being overload at a point and also minimum machine should continue running. They observed the pattern to help arrange the VM on physical machines. They proposed a framework PoWER that predicts the behavior of cluster and distributes VM in cluster turning off unused physical machines to save energy. They tested PoWER on tested cluster and analyzed its performance resulting in better results compared to FFT based time series method [10].

III. PROPOSED WORK

Max-min algorithm

Pseudocode for the Negamax version of the minimax algorithm (using an evaluation heuristic to terminate at a given depth) is specified below. .

1. Generate construction graph
2. Set the range of pheromone value to α_{min}, α_{max} where $\alpha_{min}>0$
3. Set m ants at randomly chosen vertices on the construction graph
4. Initialize trails to α_{max}
5. Ant arbitrary moves on the graph to constructs its solutions
6. If iteration completed then the pheromone trails consisting of the best solution will be updated
7. The pheromone trail constructs $\alpha_{min,}<= \alpha_{(i,j)}<=\alpha_{max}$ where $\alpha_{(i,j)}$ shows the pheromone trails for the connection
8. It will be imposed such the
   If $\alpha_{(i,j)}<\alpha_{min}$ then $\alpha_{min,}= \alpha_{(i,j)}$
   If $\alpha_{(i,j)}>\alpha_{max}$ then $\alpha_{max}= \alpha_{(i,j)}$
9. Continues till the termination criteria is not met.

Fuzzy rule based system

1. Obtain a problem & represent it as a graph so that it is covered by ants
2. Assign a heuristic preference to each choice that the ant has to take in each step to generate the solution
3. Initialize the pheromone value
4. Define fitness function
   Do for each ant
   Calculate the fitness value of the ant f_a

/*updating ants best fitness value so far*/

If f_a is better than a_{best} then set current value as the new a_{best}

/*updating population best fitness value so far*/

Set g_{best} to the best fitness value of all ants

5. Repeat until the termination criteria is not met

2013- G. Lahoti et. al. stated that fine grained energy usage data can leak customer information and due to use of this data by online service providers for effectiveness of smart grid technologies ,the sharing of data is increasing [11]. They proposed privacy enhanced framework to store, manage and share such data. The mechanism used by them stated that the customer can control the usage information showing to service providers which will be convinced by its authenticity. They implemented a prototype using Green Button data model. Their prototype worked allowing redaction of Green Button data model while sharing data with third party service provider. The presented data can be used for billing and accounting purpose as it can be authenticated and verified by third party using Green Button data model. They planned to work on the working prototype of the model of demand response aggregation service [11].

Rank based Algorithm

1. Generate construction graph
2. Initialize pheromone value
3. While not stop condition
4. Generate m ants for a tour
5. Perform sorting on ants by their length such that $l_1<=l_2<=l_m$
6. An ant to the trail update is weighted according to the rank R of the ant
7. The n best ant is chosen based on the rank R
8. If W is the weight of the trail level involvement of the best tour length than it should not be exceeded by any other ant weight.

Proposed Methodology

The model is fully distributed, i.e. every node behaves separately as well as each ant or agent, and this denotes that every node or ant is autonomous. Figure represents the table attached to each node or ant. In the model, each node contains a table that includes information about other nodes in the system. At the initial state, the table entries are Null. In each ant tour, the ant will carry the updated information about all nodes that the ant has been passed throughout. Upon arrival of the ant at every node, the following events will be done:

Assume a network is setup and a number of packets send from source to destination and the value of pheromone deposited at each nodes and shortest path is selected using Max-Min, Rank based and Fuzzy System.

1. Suppose ‘N’ of packets to be send from Source ‘S’ to destination ‘D’.
2. Initialize all the pheromone table of the node to zero.
3. When first packet is send from one node to another pheromone value is updated accordingly at that node and update all the tables of the network.
4. Proposed methodology uses the limitation s of the existing ant based techniques; hence at each node of the network the possibility of various

paths from that node to next node is computed and updated.

5. After first iteration the value of the value of pheromone is calculated at each node of the network.
6. More value of pheromone attracts more ants, hence the next packet is send to that particular nodes where pheromone value is maximum.

```
If N → pkts send from one node to other nodes
Compute next node based on Max-min ();
Compute next node based on Rank();
Compute next node based on Fuzzy();
Repeat till 'N' packets send from source to destination
For each N → pkt to traverse from nod1-> nod2
If Vpher → nod2 == Vpher → nod3v && If Rnod2 > Rnod3 && Rnod4<Rnod3
Stores the path from nod2 → nod3
End
End
Repeat for each N → pkt from 'S' to 'D'
Call Max-Min();
Call Rank();
Call Fuzzy();
Traverse the nod1 → nod2 based on stored path.
End
End
End
```

Here in the proposed methodology the shortest route from source to destination will depends on the stored routes from Max-Min, Rule based and Fuzzy based System.
At each step of the node in the network instead of checking of only two nodes the next possible path from 3 ant based techniques is checked and if the chances of traversing fails to apply then the next traversing path is stored, which is then used in the proposed methodology.
The proposed methodology uses the wrong traversed routes from one to another where the decision is based on only values from one node to another.

IV. RESULT ANALYSIS

The table shown below is the analysis of Load balancing when various parameters are applied on the cloud environment. The analysis is done for various datacenters and brokers and cloudlets on the basis of which an average Load is computed and makespan time is calculated.

# Data Centers	# Brokers	# Cloudlets	# VM	Average Load	Makespan Time
3	1	5	1	4781	25.564
3	1	10	1	3482	5.1735
3	1	15	1	8149	28.385
3	1	20	1	3851	5.695
3	1	25	1	2895	4.33
3	1	30	1	4737	8.197

Table 1. Load Balance on various cloud parameters

The table shown below is the analysis of Load balancing when various parameters are applied on the cloud environment. The analysis is done for various datacenters and brokers and cloudlets on the basis of which an average Load is computed and makespan time is calculated.

# Data Centers	# Brokers	# Cloudlets	# VM	Average Load	Makespan Time
5	2	5	2	3225	6.043
5	2	10	2	1000	11.635
5	2	15	2	9723	66.324
5	2	20	2	4128	8.179
5	2	25	2	10271	70.329
5	2	30	2	5813	14.551

Table 2. Load Balance on various cloud parameters

The table shown below is the analysis and comparison of various load balancing techniques on the basis of number of packets send from cloudlet to data centers. The proposed methodology is more efficient as compared to the existing techniques of load balancing.

# of packets	Max-Min	Rank based	Fuzzy Rule based	Proposed
10	7538	6281	5493	4016
20	8015	7329	6283	5002
30	8519	8015	7012	6183
40	9253	8428	8025	6519
50	10163	9712	8581	7153
60	10582	10126	9273	8129
70	11283	11172	10273	9012
80	12263	11428	11239	10176
90	13527	12439	12103	11193
100	14328	13230	12382	11386

Table 3. Comparison of Computational Time

The figure shown below is the analysis and comparison of various load balancing techniques on the basis of number of packets send from cloudlet to data centers. The proposed methodology is more efficient as compared to the existing techniques of load balancing.

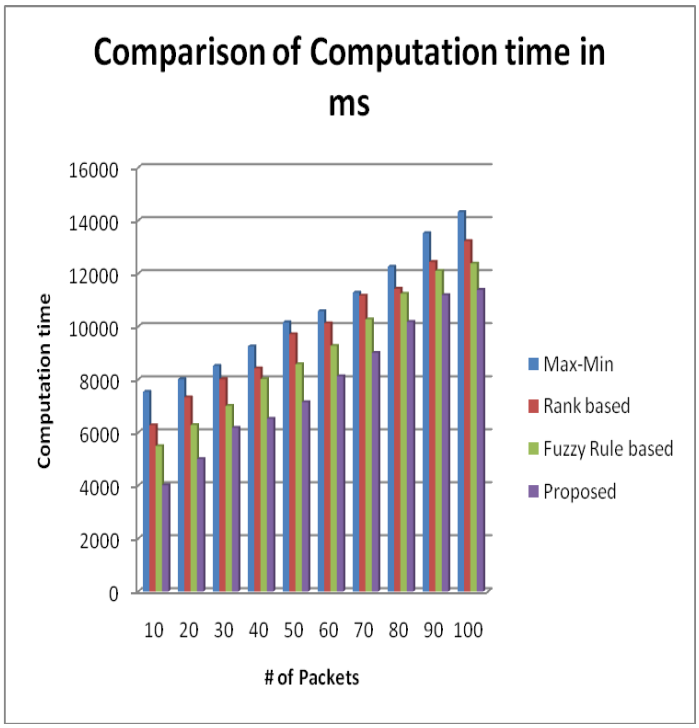

Figure 3. Computational Time in ms

V. CONCLUSION

The proposed methodology implemented here for the energy consumption in distributed cloud network using ant based techniques provides an efficient way of overloading on all the datacenters using brokers. The experimental results shows that the proposed methodology implemented here provides less energy consumption as compared to the existing technique implemented for the distributed core networks in cloud computing.

REFERENCES

[1] Cloud Security Alliance, "Top Threats to Cloud Computing," http://www.cloudsecurityalliance.org, 2010.

[2] Kui Ren, Cong Wang and Qian Wang, "Toward Secure and Effective Data Utilization in Public Cloud", IEEE Network, November/December 2012.

[3] Cong Wang, Sherman S.M. Chow, Qian Wang, Kui Ren, and Wenjing Lou, " Privacy-Preserving Public Auditing for Secure Cloud Storage", IEEE Transactions on Computers, Vol. 62, No. 2, February 2013.

[4] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-Preserving Multikeyword Ranked Search over Encrypted Cloud Data," Proc.IEEE INFOCOM, 2011.

[5] H. Hu, J. Xu, C. Ren, and B. Choi, "Processing Private Queries over Untrusted Data Cloud through Privacy Homomorphism," Proc. IEEE 27th Int'l Conf. Data Eng. (ICDE), 2011.

[6] L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner. A break in the clouds: towards a cloud definition. SIGCOMM Comput. Commun. Rev., 39:50{55, December 2008.

[7] Ahmed Q. Lawey, Taisir E. H. El-Gorashi, and Jaafar M. H. Elmirghani," Distributed Energy Efficient Clouds Over Core Networks", JOURNAL OF LIGHTWAVE TECHNOLOGY, VOL. 32, NO. 7, APRIL 1, 2014".

[8] Virnal Mathewt, Rarnesh K. Sitararnan t and Prashant Shenoy," Reducing Energy Costs In Internet-Scale Distributed Systems Using Load Shifting", 978-1-4799-3635-9/14/$31.00 ©2014.

[9] Sharrukh Zaman," A Combinatorial Auction-Based Mechanism for Dynamic VM Provisioning and Allocation in Clouds", IEEE TRANSACTIONS ON CLOUD COMPUTING,2013.

[10] Kashifuddin Qazi, Yang Li, and Andrew Sohn," PoWER - Prediction of Workload for Energy Efficient Relocation of Virtual Machines", ACM 978-1-4503-2428-1/13/10.

[11] Gaurav Lahoti," Customer-centric Energy Usage Data Management and Sharing in Smart Grid Systems", 2013 ACM 978-1-4503-2492-2/13/11.