Harmony: A Resource Management Technique for Better Cooperation between Cloud Service Providers

G.Bandavi,

M.Tech Student, Dept of CSE, JNTUACEA, Andhra Pradesh, India.

bandavichowdary@gmail.com

***Abstract*—Cloud computing turned into a standout amongst the most imperative stage for the cloud suppliers so as to introduce the cloud suppliers in the virtual way through the internet. Cloud customers throughout the world exchange their information with high scope of computing resources, optional level of information stockpiling with high bandwidth. Subsequently the progressing interest for the versatile resources is widely expanding between the cloud clients. Along these lines single cloud server couldn't able to distinguish and unite with high scope of ability to the application among run time. Subsequently the specialists are in need to fabricate virtual environment for interfacing the numerous cloud servers accordingly leads the researchers to the collaborative Cloud computing (CCC). This paper uses an effective resource sharing platform called Harmony and also uses the Neural Networks (NN) for suitable resource selection. Further the trust management is implemented and optimal time period for resource selection is enhanced.**

Keywords: Cloudcomputing, collaborative computing, Resource Management, Trust management.

I.INTRODUCTION:

Cloud computing is a rising innovation, it is advancement of the parallel computing, circulated computing, and grid computing, utility computing. Cloud computing is considered as the future model for the computing. It gives the client ability to store data and access data utilizing web.

It included services like Software-as-a-service (SaaS), Infra structure-as-service (IaaS), Platform-as-a service (PaaS) [2].To clients, cloud computing is a Pay-Per-Use-On-Demand that helpfully access and shared resources through web. In these cloud computing there are distinctive cloud like public cloud, private cloud, community cloud and hybrid cloud. Researchers think about the cloud computing as a security on technical level, here mainly concentrate on the attacks and hacking attempts. Many Business and industry proprietors are attracted to cloud computing idea because of many features which includes:

1. Lower Investment.
2. Scalability.
3. Reliability and Security.
4. Faster Deploy.

In SaaS, a premade application, along with any obliged software, operating framework, hardware, and system are given. In PaaS, an operating framework, hardware and system are given, and the client installs or builds up its own software and applications. In IaaS model gives only the hardware and system, the client installs or builds up its own operating frameworks, software and applications.

Where in the collaborative cloud clients can pick private, public and dynamic clouds to support discrete services, here clients can achieve more value by integrating third party (TP) applications. Private clouds are claimed and operated by TP se,,rvices supplier, Public cloud is an open wide to everyone, Hybrid cloud is a structure of two or more particular cloud infrastructure, community cloud is a provisioned for select use by a particular group of customers from organizations that have shared concerns. Clients can pick a private, open or hybrid cloud support distinct services including:

1. Fabricate with cloud-grade applications and infra structure.
2. Manage part or all of your communications applications and infra structure.
3. Convey services through public and private clouds.
4. Enable service suppliers to convey cloud services.

Collaborative cloud computing

Collaborative cloud computing (CCC), where globally scattered distributed cloud resources belong to dissimilar organizations or individuals are collectively used in cooperative manner to provide services to customers.

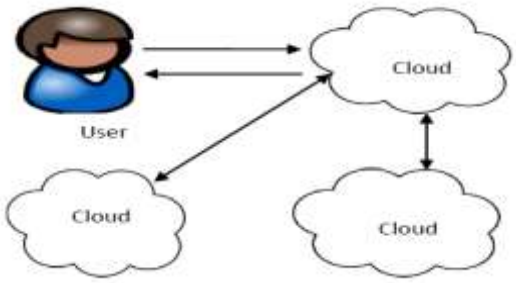


Figure 1: Collaborative Cloud Computing Structure

Collaborative cloud computing (CCC) platform is which interconnects the physical resources that allow sharing the resources in the middle of clouds and suppliers with immense amount of resources to clients, when a cloud doesn't have adequate resources then it will utilize resources structure different clouds which they want.

II.RELATED WORK:

In paper [4] CTrust framework addressed for the security reason by interfacing various sorts of Virtualization Technology (VT) transform keeping in mind the end goal to access resources like storage, system, and software. Secure Hypervisor Framework (SecHYPE) makes the root trust for the cloud running application. Right now cloud computing methods generally utilized as a part of e-trade, web auctioning companies despite the fact that cloud computing joining distinctive sorts of framework without regarding basic architecture of PC framework security issues is the major threat in the cloud computing. The National Institute of Standards and Technology (NIST) makes the research in the field of security as a primary concern on the cloud computing. Software abstraction has been utilized to create hardware and operating framework coupling each other all together the cloud applications. This paper gives the detailed information about security analysis, framework analysis, and cryptographic key management.

In paper [5] makes the detail contemplates about web security issues, the major security issues are worms, spam and phishing attacks. With a specific end goal to conquer the accompanying issue they proposed Unified Threat Management (UTM) which is utilized to module and associate distinctive sorts of systems. Interruption Detection System (IDS) advanced rapidly to the Distributed Denial of Service (DDoS) strings for recognizing the signature ventures to distinguished infections. Collaborative Network Security Management System (CNSMS) creates the new integrated environment for creating Unified Threat Management (UTM). This paper mainly concentrates on the security community for the traffic data analysis and procedure to store large amount of data.

In paper [6] Collaborative Cloud Computing is utilized to bolster exceptionally encouraging patterns in cloud information extraction systems. Recovering of information from the distinctive client is not that much conceivable and easy subsequently we could access data straightforwardly from the storage gadgets by utilizing Neural Network (NN) based framework. Artificial Neural Network (ANN) mechanism has a tendency to activate the inputs capacity with the assistance of yield values this procedure used to get the information at the same time with no sort of additional endeavors. This paper makes utilization of the learning framework based on the Neural Network which lessens single point failure and uproots all the issues lying in the cloud computing henceforth it gives out effective and successful extraction of information for the collaborative cloud computing.

In paper [7] Use of cloud computing with the collaboration of Multi cloud environment where cloud suppliers access software, platform, and infrastructure as the pay per use basis and gaining enormous attention according to industrial expectations. The client used to gain the access to the cloud services yet at the same time client gets seller secure along these lines client as to access particular cloud service suppliers for ease management to authentication to multi service suppliers. Security issues generated with the mash up revolve ought to be around the service suppliers while executing hubs on the cloud server. The main issues in the multi cloud environment performing task on the conveyed service henceforth the collaboration framework for multi cloud framework can be executed. Diverse sorts of intermediary systems like intermediary based framework, cloud facilitated intermediary, Peer to Peer intermediary and on – premise intermediary are utilized for the security issues. This paper portrays various research parameters on the multi cloud environment so as to give minimal effort functionalities.

In paper [8] cloud computing suppliers gives the greater open door keeping in mind the end goal to send complex information strategy as the infrastructure to the end client. Along these lines cloud service needs extremely solid cloud control frame work which can orchestrate cloud resources like utilization, configuration, provisioning and decommissioning around physical resources. Infrastructure as a Service (IaaS) environmental model gives Virtual Machine (VM) as an operating framework and consequently make cloud server as the

sophisticated joining virtual private cloud instance. This paper used to advocate a data driven approach for the cloud resource orchestration. Orchestration data format are structured and characterized by utilizing transactional semantic

All the above mention literature work has been tabulated with their respective advantages and dis-advantages in table 1:

Table 1: Comparison of various methods

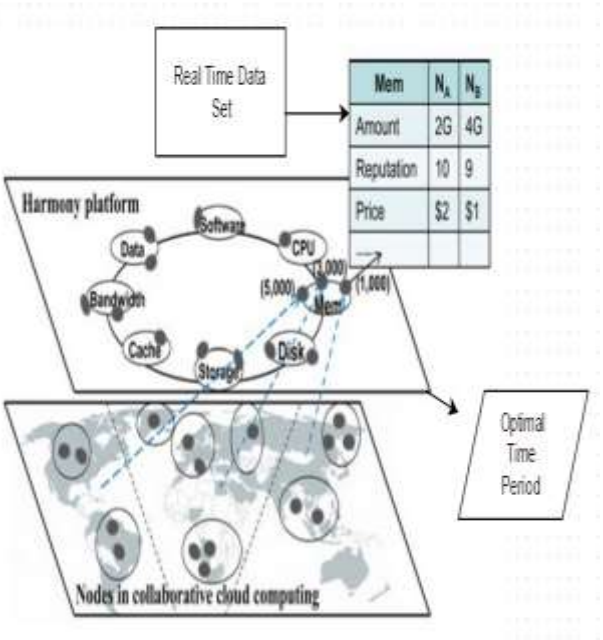
Ref.No	Technique used	Advantages and Disadvantages
[4]	CTrust frame Secure Hypervisor framework (SecHYPE)	**Advantages:** 1. Cloud computing allows multiple users to divide their information. 2. CTrust helps to expand sanctuary paradigm. 3. SecHYPE structure provides safety implementation. **Disadvantages:** 1. High Security risk provides obstruction to the client.
[5]	Distributed Denial of Service (DDoS). Unified Threat Management (UTM). Collaborative Network Security Management System (CNSMS)	**Advantages:** 1. CNSMS utilized for the resist calculate assault in the dispersed manner. 2. Find large quantity of gathered data utilizing CNSMS. 3. UTM used to analyze the data in circulated manner. **Disadvantages:** 1. System traffic is all that much congested over the hubs. 2. High security occasions.
[6]	Collaborative Cloud Computing (CCC). Neural Network (NN). Quality of Services (QoS)	**Advantages:** 1. Integrated retrieval of information management. 2. Interactions between dependable resources and effective among clouds. 3. High caliber of QoS is measured. **Disadvantages:** 1. Recovering of the information from distinctive client is all that much troublesome.
[7]	Elastic Compute Cloud (EC2). Software as a Service (SaaS). Virtual Machine (VM).	**Advantages:** 1. Gives scalability, adaptability for the storage of data. 2. Gives the client paying cash to the amount data has been utilized. 3. Data focus utilizes Virtual Machine (VM) for the isolation process. **Disadvantages:** 1. Organization of VM is all that much costlier. 2. Virtual infrastructure decides procurement over/under performance.
[8]	Data centric management framework. Infrastructure as a Service (IaaS).	**Advantages:** 1. Advanced cloud services used to share complex operation like storage management, fault management, image management and so forth. 2. Orchestration creates management and manipulation of the resources. 3. Data Centric Management Framework (DMF) gives very much characterized semantic

		to accessing the data. **Disadvantages:** 1. Sophisticated cloud services needs dynamic orchestration for the service abstraction.

III.PROPOSED MODEL

This paper used the idea of a coordinated resource administration platform called Harmony, to this model two extra functionalities are added one is to figure the ideal time period and another is to limit the un-authorized access.

The proposed model gives collaboration between distinct public clouds and gives trust administration to accessing



required files. The proposed model is dpicted in figure2.

Figure 2: Proposed Model Architecture

As the architecture represents that the harmony platform comprises of four major parts:

- Resource Management
- Trust Management
- Resource Selection
- Optimal time period calculation

The major part is the resource management where the service supplier or data proprietor will upload the data into the obliged or intrigued cloud server. The decision of cloud server is chosen by the client.

3.1: Resource Management:

Before uploading the data client has to create a VM with pre described edge for data restrain in cost assisted manner.

This paper utilizes a trust manger as the base to check the client character and to maintain the collaboration between the clouds. The figure 3 portrays the stream of the Resource management

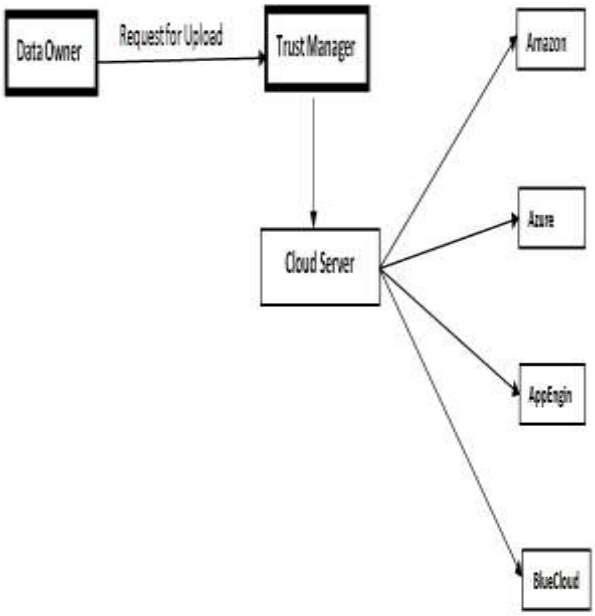


Figure 3: Resource Management phase.

The algorithm for trust management is as per the following:

1. User creates the VM in any one of 4 clouds with required size and a threshold limit for storing the data.
2. Then user logins to that cloud using the login credentials, if the credentials are not matched then user will be rejected.
3. Then user uploads his data into the cloud, if the threshold exceeds then upload will fail.
4. Else file will be stored in the desired cloud.

Then the trust manager keeps the required information about the file and a trusted key is generated for each file and stored in three places:

- Trust manager
- Cloud server
- Data Owner

Then the resources are efficiently placed in the required cloud and the process of resource management ends with the successful completion of the Owner request.

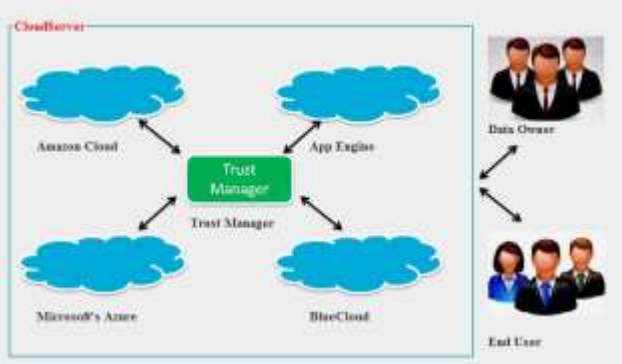


Figure 4: Resource Management Structure

The figure 4 portrays 4 virtual clouds created for resource sharing and the Trust Manager as the central base for the proprietor and client demands.

3.2. Trust Management:

As the paper defines a trust worthy resource sharing a trust management process is required to authenticate the user requests for the resources. The user will request the trust manager with his credentials for the proper resources. The trust management works as depicted in figure 5:

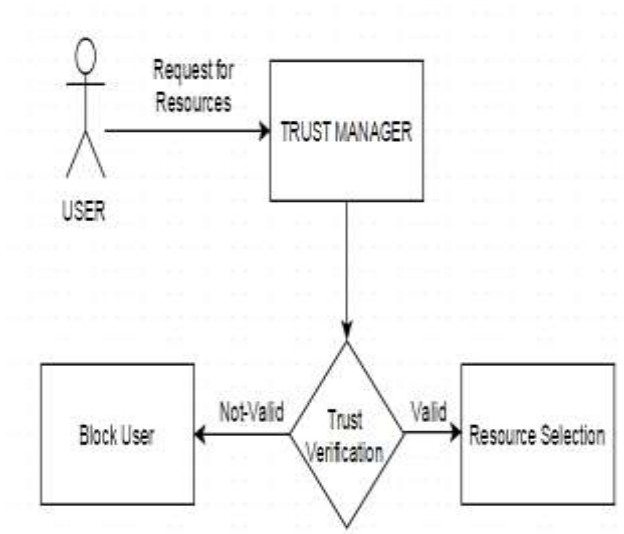


Figure 5: Trust Management

The user sends a request to the trust manger for the required resources along with the credentials and a secret key. The trust manager then verifies the trust composition of the user if the trust value is valid then the trust manager forwards the request to the resource selection else the user is blocked and notified.

3.3 Resource Selection:

Resource selection is the procedure of discovering where the actual resource is located and acquiring that record utilizing cloud collaboration. The Neural Network (NN) model is utilized to choose the appropriate resources. The resource determination procedure utilizes a QoS-Oriented Resource Selection for better cloud collaboration. The NN process searches all the clouds for the obliged resources and brings the conceivable one and gives to the client.

The NN procedure gets a set of parameters as input and those inputs are the clouds file index values and the values are given to the summation function and the activation function decides the winning value. The winning assessment defines that the required resource is located at that particular cloud. The process of NN is depicted in Figure 6.

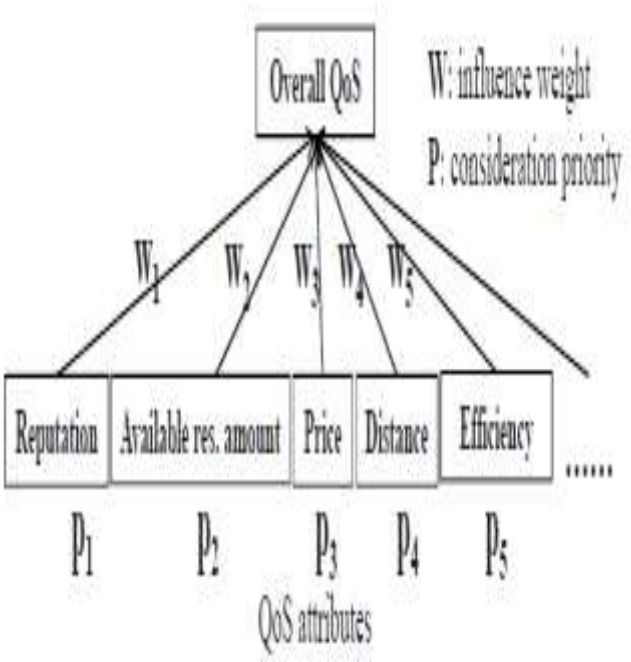


Figure 6: Resource Selection using NN

As the depicts portrays that the {W1, W2,Wn} speaks to the weight value and the {P1, P2,Pn} characterizes the need values.

The input for the resource choice is the QoS parameters and the yield will be the resource location.

3.4 Optimal Time Period Calculation:

The enhancement to the Harmony is to find out the optimal time period for resource selection. The NN process starts searching the required resources throughout the clouds using the cloud collaboration. The time required to search and fetch a request must be calculated to do so a triggering function is incorporated into the trust manager.

The triggering function is triggered when the process of searching starts and the stopped after receiving the resources back to the user. The optimal time period is calculated in Milli seconds.

IV.ANALYSIS:

The proposed model is tested under various resource management and resource selection conditions. The main metrics considered for the analysis are:

- Successful resource selection VS failures
- Waiting Time

The first measurement defines the total number of resource requests and the number of successful resource selection vs the failure requests due to delay.

The comparison is made with the Power Trust [9] algorithm. Figure 7 shows the successful resource selection for groups of 5-20 requests by each method. The black color represents delayed successful requests that have waited in the queue before being processed, and the grey color represents successful requests with no delay. As the graphs depict that the PowerTrust generates a large number of delayed successful requests, while the proposed methods generate no delayed requests.

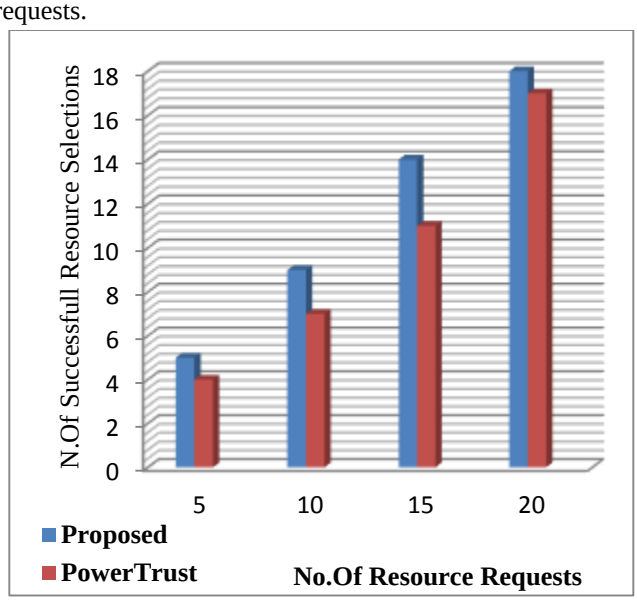


Figure 7: Successful Resource Selections

As the figure clearly depicts that the proposed system outperforms the PowerTrust with minimum number of failures.

The next metric to analyze is the waiting time to complete a resource request. Again the proposed system is compared with the PowerTrust for the efficient analysis.

Figure 8 shows the total waiting time for each group 5-20 requests, including failed requests. We see that PowerTrust generates high delay for a request, while the proposed method produces little or no delay, which is consistent irrespective of the number of requests. This is because PowerTrust always chooses the highest overall reputed nodes as resource providers without considering node load. These nodes receive too many requests, causing many to wait in the queues. Since proposed method select lightly loaded nodes as resource providers, they generate few delayed requests.

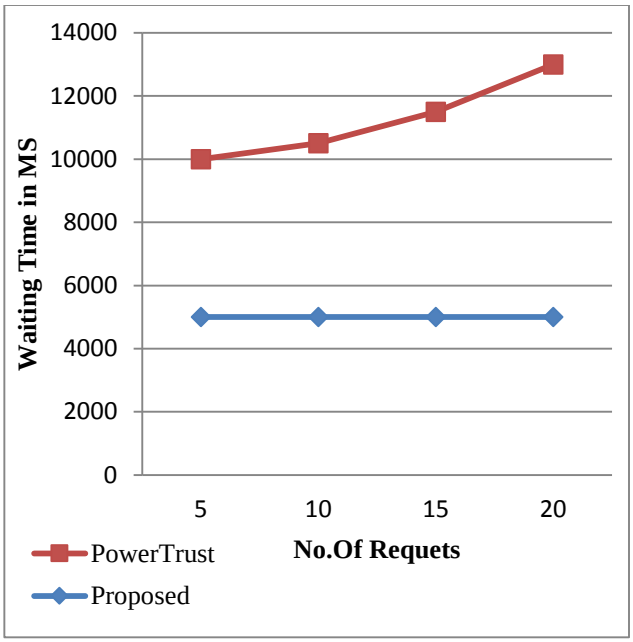


Figure 8: Waiting Time delay

The figure clearly depicts that the time taken by the PowerTrust is more compared to the proposed method.

V.CONCLUSION:

This paper proposed an efficient resource selection algorithm called Harmony and added some functionality like optimal time period and unauthorized request blocks for efficient trust management. The resource management and QoS resource selection provides efficient collaboration between the cloud users. The NN phase takes less waiting time to complete the requests with higher success rates. Further the trust manager maintains all the sensitive information related to the resources and kept confidential among the cloud users.

REFERENCES:

[1] Haiying Shen, Guoxin Liu, "An Efficient and Trustworthy Resource Sharing Platform for Collaborative Cloud Computing", IEEE Transactions On Parallel And Distributed Systems, VOL. 25, NO. 4, APRIL 2014, pp.862-875.

[2] Ch Chakradhara Rao, Mogasala Leelarani, Y Ramesh Kumar, "Cloud: Computing services and deployment models". International Journal of Engineering and computer science, vol. 2, Dec 2013.

[3] Avaya Collaborative Cloud from, http://www.Avaya.com.

[4] CTrust: A Framework for Secure and Trustworthy Application Execution in Cloud Computing. (Satyajeet Nimgaonka, Srujan Kotikela and Mahadevan Gomathisankaran) ISBN 978 – 1 – 62561 – 001 - 0.

[5] Cloud Computing – based Forensic Analysis for Collaborative Network Security Management System. (Zhen Chen, Fuye Han, Junwei cao, Xin Jiang, and Shuo Chen) TSINGHUA SCIENCE and TECHNOLOGY ISSN 1007 - 0214 05/12 pp 40-50 Volume -18, no - 1, Feb 2013.

[6] An Efficient Information Retrieval Approach for Collaborative Cloud Computing. (B.Hema Mrs.R.Hemalatha) ICMACE-14.

[7] A Review of Collaboration of Multi-Cloud- An Effective Use of Cloud Computing. (Swaraj P.Thakre, and Prof R.Chopde) IJAIEM Volume 2, Issue 3, Mar 13.

[8] Cloud Resource Orchestration: A Data Centric Approach. (Chanbin Liu, Yun Mao, Jacobus E. Vander Merwe, and Mary F.Fernandez) CIDR 11 Jan 9-12, 2011.

[9] R. Zhou and K. Hwang, "PowerTrust: A Robust and Scalable Reputation System for Trusted Peer-to-Peer Computing," IEEE Trans. Parallel and Distributed Systems, vol. 18, no. 4, pp. 460-473, 2008.

Selected Paper from International Conference on Computing (NECICC-2k15)