Cloud Computing: Solving Availability Problem in Future Framework for e-Governance

Dileep Kumar Gupta
Department of IT
BIT Mesra
Ranchi, India

Abhishek Mishra
Department of IT
BIT Mesra
Ranchi, India

Dr. G. Sahoo Prof. & Head,
Department of IT
BIT Mesra
Ranchi, India

ABSTRACT

Cloud is a centralized system where all the software and hardware taken together that provides the services to the users as pay per use system. To compete the world, every time the organizations need to have the better technology and proper utilization of resources to improve the performance. The proper utilization of the available scarce resources needs proper management and implements the better strategies to accomplish the task. Mukherjee and Sahoo [1] have proposed an effective framework of e-Governance based on cloud computing concept, which would be intelligent as well as accessible by all. In this paper, we discussed the availability problem in the existing framework for e-Governance and also provide a better solution to solve this problem.

Keywords

Cloud computing, E-governance, Web services, Availability, Filtering mechanism

1. INTRODUCTION

E-governance is used for the governance activities such as administration, income taxes, pension services etc. to make easy use with the help of IT infrastructure. E-governance improves the efficiency of government functioning by removing redundancy at different levels.

Following are the four main categories of e-governance:

1. Government to government (G2G): Administration, policy formation etc.
2. Government to Business (G2B): Taxation & tender etc.
3. Government to Consumer (G2C): Land record, birth certificate etc.
4. Government to Employees (G2E): Income tax, pension etc.

The key of the success of e-governance framework is providing accessibility of different web services of e-Governance irrespective of locations and language barriers. In one of the existing models, Chandwick and May [4] have proposed an e-Governance framework have different problems. One of the major problems is unable to address all categories of users starting from rural urban to metropolitan citizens.

This problem is solved in the future framework for e Governance proposed by Mukherjee and Sahoo [1]. In this cloud computing based e-governance, the thin clients and other mobile nodes can access the e-governance web services by sending the request over a network which is cheaper to the clients. The existing framework of e-governance provides the access to the different web services of the e-governance to the variety of users from rural to metropolitan cities. In cloud computing,

the software layer is responsible for the distributed application which is known as Hadoop. The e-governance framework is categorized into three layers.

1. Knowledge base

2. Inference engine

3. User interface

The knowledge base consists of the rules and facts about the particular problem which is varied from problem to problem. The interface engine goes through the rules and facts, processes it and provides the result of the user's request. User interface is the medium through which user can communicate with the system by sending the request in the human understandable format.

Organization of the paper is as follows: Related work is discussed in section 2. Framework for e-governance has discussed in section 3. Availability problem has discussed in section 4. Types of attacks have discussed in section 5. Availability problem in framework has discussed in section 6. Proposed modified algorithm has discussed in section 7. Conclusion has discussed in section 8.

2. RELATED WORK

The research work in the cloud computing architecture is being growing continuously. The different researchers proposed different architectures. Previously, Chadwick and May [4] have proposed an e-governance framework based on the interaction between government and its users. They have discussed three heuristic models of interaction which was managerial, consultative and participative. Grant and Chau [8] have proposed a generic e-government framework that allows for the identification of e-government strategic agendas and key application initiatives that transcend country specific requirements. After that web technologies are used to integrate the government information and services proposed by Coursay and Norris [5]. After that the latest technologies is used for enhancing the performance of the web services. S.Adreozzi, et al. [2] presented a model for rigorous representation of service characteristics. D. Gouscos, et al. [7] presented a simple approach to model certain web service management attributes. J.P Thomas, et al. [12] has represented distributed web service by modeling the flow of messages and methods in a web service transaction. Tu, et al [11] has discussed design strategies to improve the performance of web service. Levy, et al [9] has presented architecture and prototype implementation of performance management system for cluster based web service. V. Cardellini, et al. [6] considered different categories of web applications, and evaluate how static, dynamic and secure web service request affects the performance and quality of service of distributed web sites. These web services are either server centric or device centric. Mukherjee and Sahoo [1] have proposed the future framework for e-governance which is based on all categories of users.

Minho Sung and Jun Xu [15] proposed "IP Traceback-Based Intelligent Packet Filtering:

A Novel Technique for Defending against Internet DDoS Attacks" which is based on the IP traceback schemes to obtain the information concerning whether a network edge is on the attacking path of an attacker ("infected") or not ("clean"). Sharon Yan Ping and Lee Moonchuen [13] proposed IP Traceback Marking Scheme Based Packets Filtering Mechanism which is used to defend against such attacks is to locate the attack source(s) and to filter out the attack traffic. Tao Peng, et al. [14] proposed "Protection from Distributed Denial of Service Attacks using History-based IP Filtering" which is a practical scheme to defend against Distributed Denial of Service (DDoS) attacks based on IP source address filtering.

3.FRAMEWORK FOR E-GOVERNANCE

Mukharjee and Sahoo [1] have proposed hadoop in their framework that contains four components. Each component functions its specific job. The different components of Hadoop are shown in fig 1. Where U.I., A.C., W.S.M., and J.S. stands for

1. U.I. (user Interface)

2. A.C. (Authentication Check)

3. W.S.M. (Web Service Mapping)

4. J.S. (Job Scheduler)

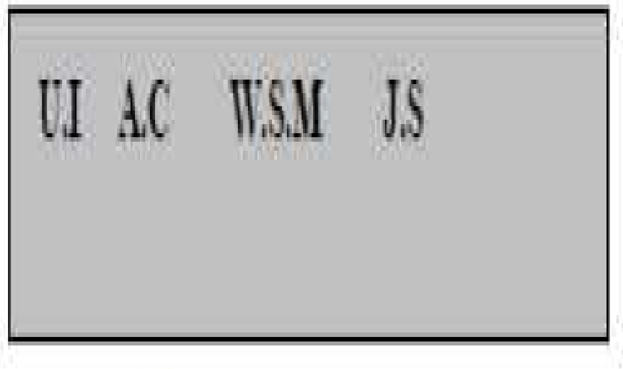

Fig 1: Components of Hadoop.

Users are the thin clients or mobile nodes. They are connected to the Hadoop and Hadoop is connected to the commodity hardware [10]. The commodity hardware are categorized as

a. Active Commodity Hardware

b. Passive Commodity Hardware

In this framework, user sends the request to the Hadoop for e-governance web services. ThenA.C. component of Hadoop check the authenticity of the user by the authentic server. Once the authentic server recognizes that the user is authentic then it checks that which type of service needs for this request by mapping in the WSM component.

After finding out the appropriate web service, it submits to the J.S. of the Hadoop which schedules the job to the grid of volunteer commodity hardware (PCs, clusters, supercomputers, mainframes etc.).

The J.S. sends the job to the idle commodity hardware. The idle commodity hardware processes the job and sends back the results to the Hadoop and Hadoop to thin clients or mobile users.

The optimized load balancing of the idle hardware is done by the J.S. The working of J.S. is based on the two tables, one is Job Queue and other is Node Controller. Job Queue is used for making the list of jobs according to its priority or the FIFO basis depending on the requirement. The job queue table is collection of 4 attributes as in the Table 1. These are IP, Job, Job Type, and Job Status, where IP is the IP address of the machine that job is coming from. Job is the name of Job. Job Type tells that what kind of server needs for this job and Job Status is Boolean type of attribute either 1 (for job is done) or 0 (job is not done).

IP	JOB	JOB TYPE	JOB STATUS
192.168.1.1	J1	Application	0
192.168.1.3	J2	Mail	1
192.168.1.7	J3	FTP	0

Table 1: Attributes of job queue.

The second table is the Node Controller Table has 3 attributes shown in the Table 2. These are

IP, Job Assign, Job Status. IP and Job Status is similar to the Job Queue Table while Job Assign tells that which job is assign to the given server.

IP	JOB ASSIGNED	JOB STATUS
192.168.1.1	J1	1
192.168.1.3	J2	1
192.168.1.7	J3	0

Table 2: Attributes of node controller.

But if user request needs the expert advice then the Hadoop uses the inference engine. It first selects the corresponding volunteer node for launching the inference engine and inference engine refers the corresponding knowledge base of the active commodity hardware. With the help of knowledge base, inference engine finds the result and sends back to the Hadoop and then to the end user. The inference engine exists into the WSM component which would use with the help Job Scheduler of the Hadoop.

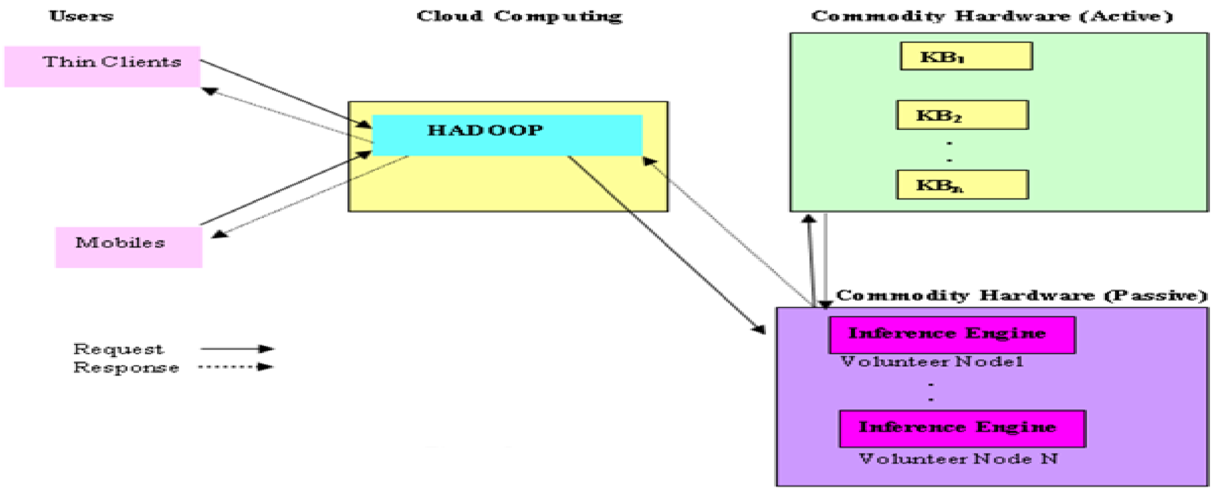

Fig 2: Framework for e-governance

4.AVAILABILITY PROBLEM

Availability states that the network resources (both hardware and software) are available to the authorized users all the time. Availability of services or resources are the one of the biggest challenge among the top 10 obstacles [3] in growth of the cloud computing.

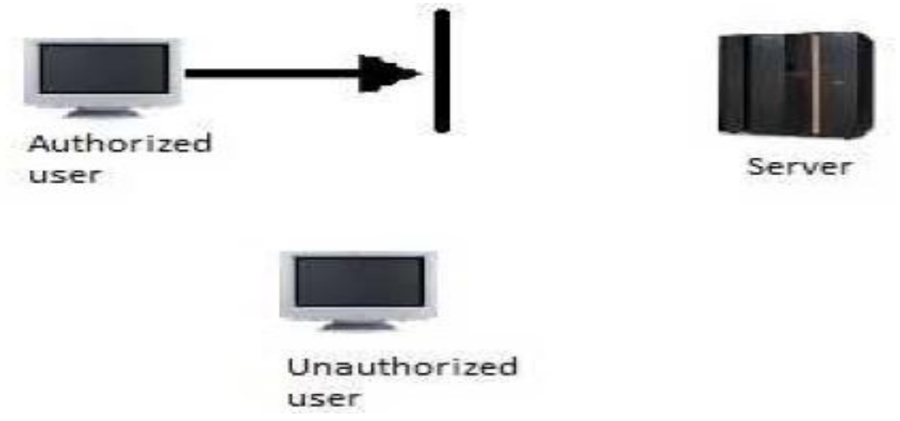

Fig 3: Availability Problem

In the fig 3, due to intentional action of the unauthorized client makes that server or its services are unavailable to the authorized users. This type of attack is known as Dos attack which causes unavailability of resources to the authorized users over the network.

5.TYPE OF ATTACKS

5.1. ICMP Flood

This attack is based on the sending the large amount of ICMP (ping) packet to the victim machine. If each machine is flooding the ICMP packet over the network and receivers send back to the sender node then the huge traffic generated over the network. This huge traffic makes unavailable the resources over the network. For example, normally when we ping any machine then the target machine replies 4 times 32 bytes packet to the sender machine to check the connection while if we write the ping command given below

```
ping 192.168.130.156 –t –l 32000
```

then target machine continuously sends packet of 32000 bytes which increases the traffic.

5.2. SYN Flood

In this type of attack, the attacker sends the lot of SYN requests to the target user to consume the server resources and make unavailable to the authorized users.

5.3. Teardrop attack

In this type of attack, the attacker uses the mangled packet. Such packets are lack of orders to confuse the target machine over the network which causes the DoS attack and makes the target machine unavailable to the authorized users.

6AVAILABILITY PROBLEM IN FRAMEWORK

In the framework, proposed by Mukherjee and Sahoo [1], if servers are not available to process the jobs, then the availability problem is arrived. Suppose user sends the request to Hadoop, first, it checks by A.C. component that verifies the coming request that comes from the authenticated user or not. Once Hadoop authenticates the user and mapping is done by W.S. M. component after that J.S. schedules the job and also launches the inference engine when the expert advice is needed to the request. In the whole process DoS attack can be at two points. First, at the A.C. component because lots of requests come from the network then it will take lot of time to check whether the request is coming from authentic user or not. Second, at job scheduling, although J. S. does its work very well that sends the job to the corresponding server (commodity hardware) at which the job will process but it never checks that, is each job coming from the same IP address because the attacker can easily spoofed the IP address of authenticated user and sends lot of request to the Hadoop which verifies the authenticity of user. Since the attacker spoofed the IP address, the A. C. will verify that request and consider it as coming from legitimate user. So that if massive requests come from a single source then there is two possibilities, first, this time only one user is active and sends request to the corresponding server and second, a user intentionally sends massive requests to corresponding server to make it unavailable to others. So, here availability problem occurs.

7.PROPOSED MODIFIED ALGORITHM

We have proposed here a new modified Model by adding one filtering module in the existing algorithm. Basically, DoS attacks are used for two purposes. First is to consume the resources and second is to consume the bandwidth of network. In both cases, either resources or bandwidth of network are scarce. The most difficult part to defend against DoS attack is that, how to differentiate between normal traffic and malicious traffic? DoS attack has two solutions. It blocks the packets either from the port numbers or by the IP addresses. When blocking of packets is done by port number then it will block all the packets coming from the particular port. For example, if we allow TCP packets to come into the network so that all UDP packets will drop and we cannot confirm that all TCP packets are coming from authenticated user so that we have used IP filtering mechanism to protect DoS attack. Thus, the major challenge is that how to differentiate the IP address either it is legal or malicious.

Thus, we have used the history based IP filtering mechanism [14] to find either the IP address is legal or not.

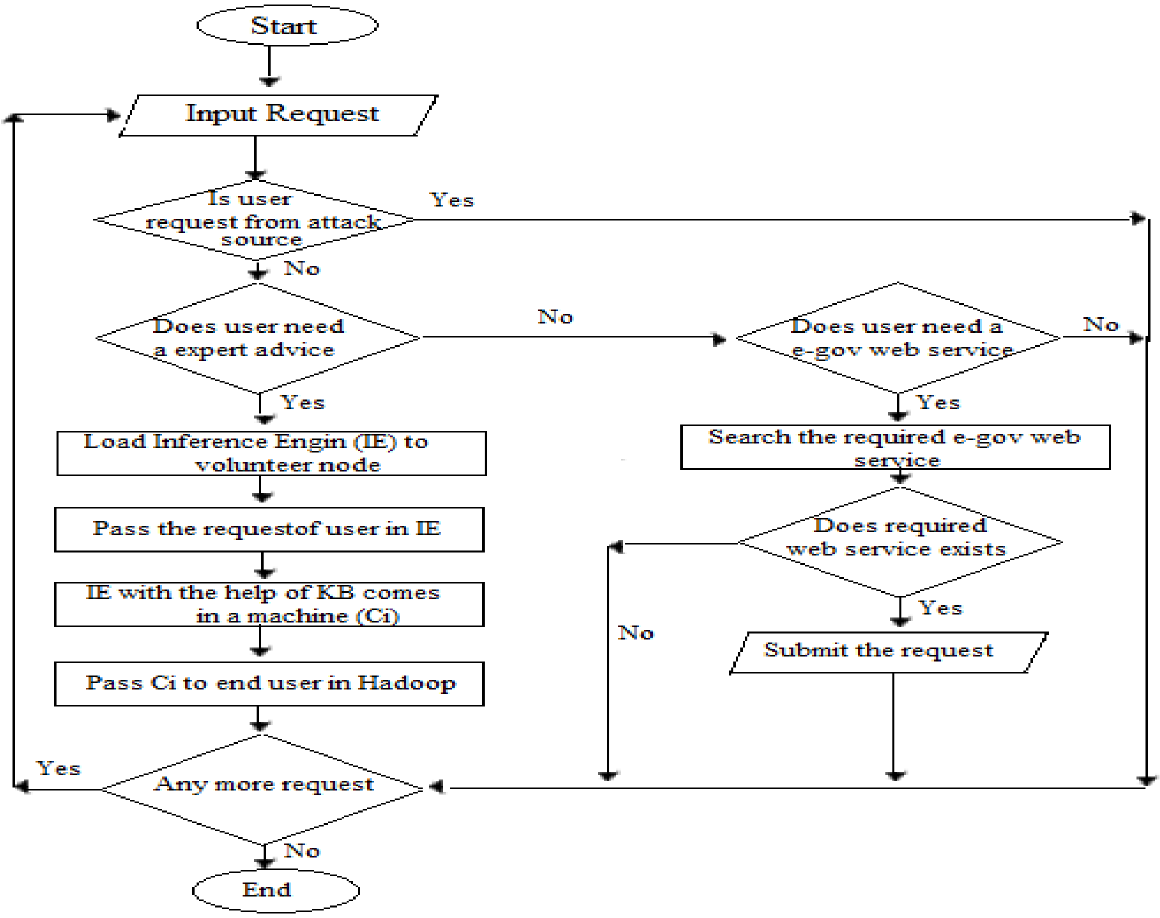
Start
Input Request
Is user request from attack source
Yes
No
Does user need a expert advice
No
Does user need a e-gov web service
No
Yes
Yes
Load Inference Engin (IE) to volunteer node
Search the required e-gov web service
Pass the requestof user in IE
Does required web service exists
IE with the help of KB comes in a machine (Ci)
Yes
No
Submit the request
Pass Ci to end user in Hadoop
Yes
Any more request
No
End

Fig 5: The proposed algorithm for processing the entire user request

8.CONCLUSION

Today cloud computing is one of the most emerging technology and widely accepted because Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable and reliable computing resources (e.g., networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal consumer management effort or service provider interaction. Due to pay per use facility, numbers of users are tremendously increased so that lots of requests are increased over the network and the servers are heavily loaded. In our proposed algorithm we handle the requests and manage the traffic over the network to make availability of server or services to the end users.

REFERENCE

[1] Mukherjee and Sahoo, "Cloud Computing: Future Framework for e-Governance" International Journal of Computer Applications (0975 – 8887) Volume 7– No.7, October 2010

[2] Adreozzi, S., Ciancarini, P., Montesi, and D., Moretti R., "Towards a model for quality of web and grid service" InProc 13th IEEE international Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WET ICE'04) page 271-276, 2004**.**

[3] Armbrust, M., Fox, A., Griffith, R., Katz, R., Konwinski, A., Lee,G., Patterson, D., Rabkin, A., Stoika, I., Zaharia,M., "Above the Clouds: a Berkeley view of Cloud Computing", Technical report, available at http://abovetheclouds.cs.berkeley.edu

[4] Chanwick, A. and May, C., "Interaction between states and Citizens in the age of the internet: E-Government in the United States, Britain and the European Union, Governance" An International Journal of policy,Administration and Institutions, volume 16, Number 2, pp 271-300, year 2003

[5] Coursey, D. and Norris, D. "Models of e-Government; Are they correct? An empirical assessment" , Public Administration, Review, volume 68, Number 3, pp 523-536,2008

[6] Cardellini, V., Casalicchio, E., and Colajanni,, M., " A performance study of distributed architectures for the quality of Web services", in Proceeding 34th Annual Hawaii International Conference on System Sciences,2001.

[7] Gouscos, D., Kalikakis, M., and Georgiadis, P. "An approach to modelling Web service QoS and provision price ", in Proceeding 3rd International Conference on Web Information Systems Engineering Workshops, pages 121- 130, 2003.

[8] Grant, G., and Chau, D., "Developing a Generic Framework for E-Government", Journal of Global Information Management, Volume 13, Number 1, pp 1-30, year 2005

[9] Levy,R., Nagarajaro, J., Pacific, G., Spreitzer,M., Tantawi, A., and Youssef, A., "Performance management for cluster based Web services", in Proceeding IFIP/IEEE 8th International Symposium on Integrated Network Management, pages 247-261, 2003

[10] L.F.G Sarmenta, "Volunteer Computing", Ph.D. Thesis in "Massachusets Institute of Technology", March 2001

[11] Tu, S.,.Flanagin, M., Wu, Y., Abdelguerfi, M., Normand, E., Mahadevan, V. " Design Strategies to improve performance of GISWeb services", in Proceding International Conference on Information Technology : Coding and Computing(ITCC04),pages 444-448, 2004.

[12] Thomas, J.P., Thomas, M. and Ghinea, G. "Modeling of Web service flow", in Proceeding IEEE International Conference on E-Commerce (CEC 03), pages 391-398, 2003.

[13] Sharon Yan Ping, Lee Moonchuen, "IP Traceback Marking Scheme Based Packets Filtering Mechanism" 0-7803-8836-4/2004 IEEE.

[14] Tao Peng Christopher Leckie Kotagiri Ramamohanarao "Protection from Distributed Denial of Service Attacks Using History-based IP Filtering"

[15] Minho Sung and Jun Xu, "IP Traceback-Based Intelligent Packet Filtering: A Novel Technique for Defending against Internet DDoS Attacks" IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 14, NO. 9, SEPTEMBER