

# Secure Cloud Service Management and its Resource Utilization of Server Using Volunteer Computing

Nirupadi Tidigol, Thrilochana Kumara Y.P, T.P.Lokesh,

nirupadi.tidigol@gmail.com thrilochankumaryp@gmail.com tplokeshp@gmail.com

EIT Ummathur, India, VVET Mysore India

**Abstract:** Cloud computing Delivers the computing resources to the user as a service over an internet. It uses wireless services with a user's data, software and computation. So spreaded over almost all IT sector and become a rich area of research. Cloud Computing composes of virtualization, on demand deployment. Here user has to pay for the application on which they want. So extensive and effective cloud security is provided by using kerberos to ensure the correctness of data, as the number of users increases cloud server may busy and failure to provide the services to the users, volunteer computing can be used to maintain the load balance of a cloud server

**Keywords:** Cloud computing, Dispatcher Algorithm, Kerberos, service models, secure cloud service, and Volunteer computing.

## I. INTRODUCTION

Cloud computing uses the computing resources that are delivered as a service over an internet. Cloud computing entrusts wireless services with the user's data, software and computation. It spreaded over almost all IT field and it become a rich area of research. Cloud is used as a metaphor for the internet based on how the internet is represented in the computer network diagrams and is an abstraction for the complex infrastructure

Cloud Computing composed of virtualization, on demand deployment. Cloud computing changes how we contrive, develop, deploy, scale, update, maintain and pay for application and the infrastructure on which the user used. Because of these benefits, Cloud Computing requires an effective and extensive security mechanism to ensure the correctness of user's data in the cloud.

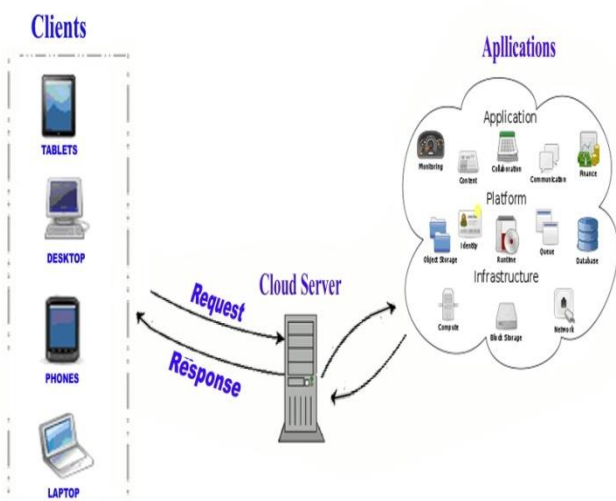


Fig 1 schematic diagram of Cloud Computing

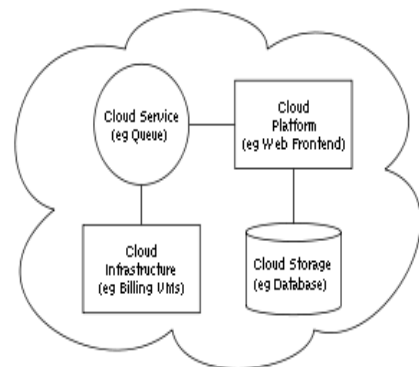


Fig 2 simple architecture of Cloud computing

The systems architecture of the software systems involved in the delivery of cloud computing, it involves multiple cloud components communicating with each other over a loose coupling mechanism such as a messaging queue.

The Inter cloud is an interconnected global "cloud of clouds" and an extension of the Internet.

*Advantages*

- Companies need to pay only for the storage actually they used, as it is also possible for companies by utilizing actual virtual storage features like thin clients.
- Companies do not need to install physical storage devices in their own datacenter or offices.
- Storage maintenance tasks, such as backup, data replication, and purchasing additional storage devices are offloaded to the responsibility of a service provider.
- Cloud storage can be used for copying virtual machine images from the cloud to on-premise locations or to import a virtual machine image from an on-premise to the cloud image library.

**II SERVICE MODELS**

Cloud computing models can be mapped with layers of business value pyramid as shown in below:

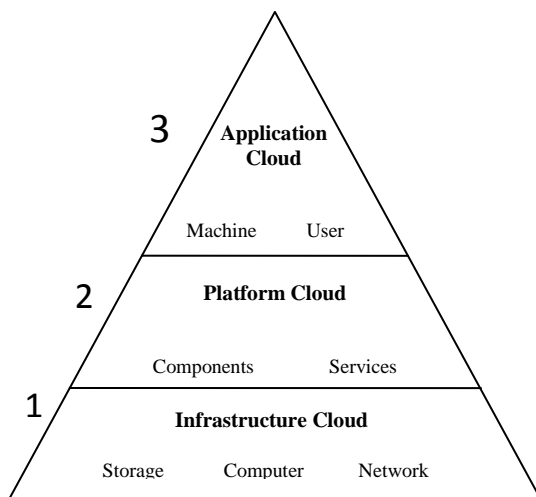


Fig 3 Cloud computing models can be mapped with layers of business value pyramid

Cloud computing providers offer their services according to the following three fundamental models:

1. Infrastructure as a service (IaaS)
2. Platform as a service (PaaS)
3. Software as a service (SaaS)

Where IaaS is the most basic and each higher model abstracts from the details of the lower models.

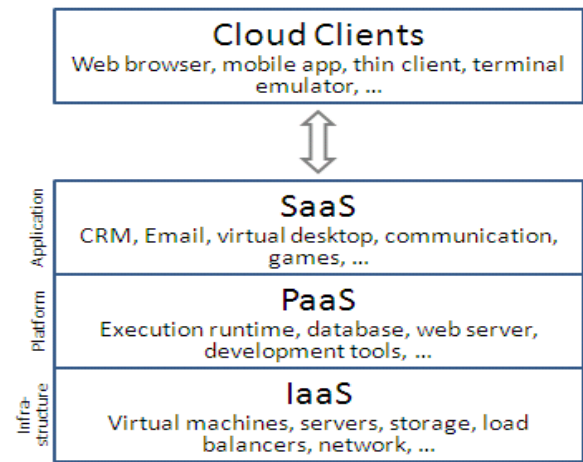


Fig 4. Layer architecture of models

*Infrastructure as a service (IaaS)*

It is the basic cloud service model, cloud providers offer computers, as physical or more often as virtual machines, and other resources. Examples: Amazon Cloud Formation (Amazon EC2) and Google Compute Engine.

*Platform as a service (PaaS)*

Here, cloud providers deliver a computing platform typically including operating system, programming language execution environment, database, and web server. Examples: Amazon Elastic Beanstalk, Google App Engine, and OrangeScope.

*Software as a service (SaaS)*

In this model cloud providers install and operate the application software in the cloud and cloud user access the software from cloud clients. The cloud users do not manage the cloud infrastructure and platform on which the application is running.

## III. DEPLOYMENT MODELS

*Public cloud*

In this model applications, storage and other resources are made available to the general public by a service provider. These services are free or offered on a pay.

*Community cloud*

Community cloud shares infrastructure between several organizations from a specific community with common concerns (security, compliance, jurisdiction, etc.), whether managed internally or by a third-party and hosted internally or externally.

*Hybrid cloud*

It is a composition of two or more clouds (private, community or public) that remain unique entities but they are bound together, offering the benefits of multiple deployment models.

*Private cloud*

Private cloud is operated solely for a single organization, whether managed internally or by a third-party and hosted internally or externally.

## IV. SECURE CLOUD SERVICES

While accessing the cloud Services from a service provider, privacy and security will play a major roll. Security model must be developed which ensures

CAI (confidentiality, availability and integrity). With the competence provided by the cloud systems, as the number of users enhances, the probability of cybercrime increases. Cloud computing is becoming a tempting target for cybercrime.

To overcome this problem we introduce Kerberos authentication mechanism to accessing the services securely.

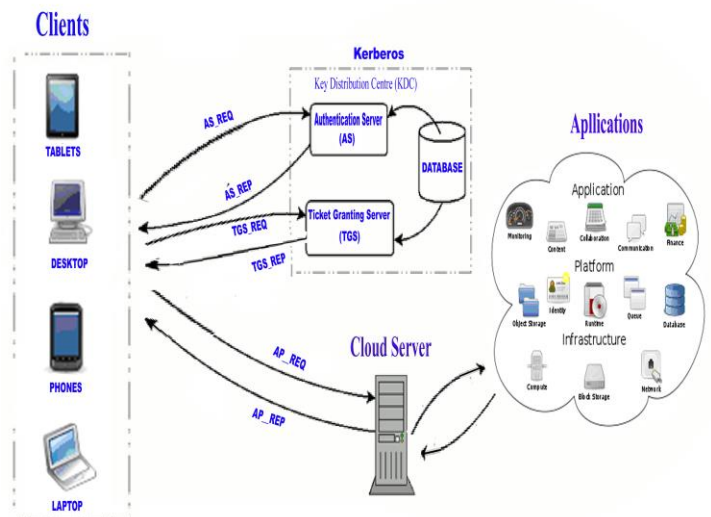


Fig.5. service access from the service provider through Kerberos Authentication

Kerberos is a computer network authentication protocol which works on the basis of "tickets" to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner. Its designers aimed primarily at a client-server model, and it provides mutual authentication for both user and the server verify each other's identity. Kerberos protocol messages are protected against eavesdropping and replay attacks.

*Algorithm for Secure cloud service access from service provider:*

- Step 1: start
- Step 2: select the input data (Services) to be accessed.
- Step 3: Client request to the AS in a KDC (AS\_REQ).
- Step 4: AS will take the information from the database in a KDC and response to the client request (AS\_REP).
- Step 5: Based on reply from the AS client will request TGS for TGT.
- Step 6: TGS will check client authentication from the Database in a KDC.
- Step 7: If authentication is valid TGS generate SK, SK will be encrypted by using client\_SK to create a TGT.
- Step 8: client decrypts the message to get the SK.
- Step 9: decrypted SK is used to create authenticator Containing user name, IP and Time stamp.
- Step 10: Authenticator request AP to get the result for input Services (AP\_REQ).
- Step 11: based on the request secure service is accessed from the server (AP\_REP) [Service provider].
- Step 12: End.

V. CLOUD SERVICE THROUGH VOLUNTEER COMPUTING

As the number of clients' increases, cloud server will get busy for providing services to the clients, to reduce this load we introduce volunteer computing. This application contains mainly to perform the operation of Watermarking effectively and with faster performance. The function to be performed will be sent to server and intern the server sends it to volunteers. Volunteer computing consist of three modules:

Cloud server, cloud clients and cloud volunteer.

Cloud Server

When client made a request regarding service from the cloud server, the function to be performed will

be sent to server and in turn the server sends it to volunteers.

Depending upon the time taken for the execution of the task by the volunteers, the server allots the task to perform. Here the cloud server uses Dispatching Algorithm to perform the task.

[Dispatching algorithm is to find the least load server for dispatching]

Cloud clients

Clients request cloud service to the server by providing Authentication after establishing connection with the server.

Cloud volunteer

Volunteer will perform the task assigned by the cloud server based on the client request. Volunteer will share the cloud applications from cloud server.

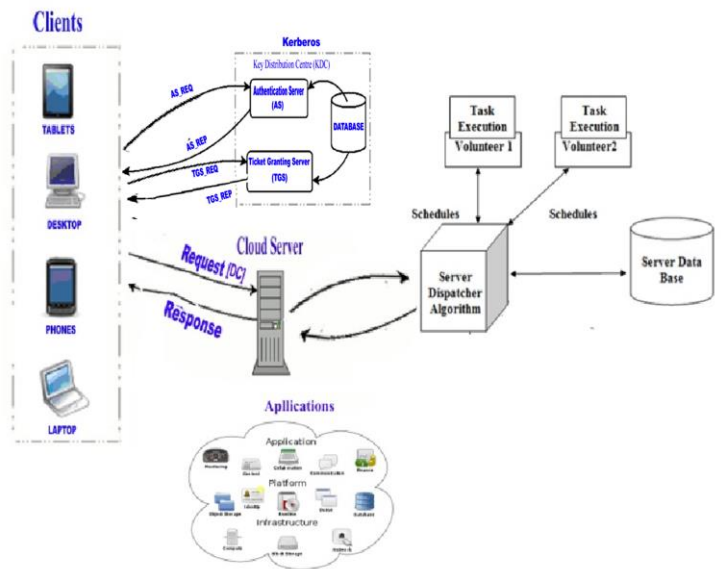


Fig 6. Cloud service through volunteer computing

## DISPATCHER ALGORITHM

- Step 1: Configuration of TCP
- Step 2: Checks the TCP connection table entry
- Step 3: Check if the incoming packets is in the range of Stateful service.
- Step 4: Check whether the packet is singleton or client activated method.
- Step 5: Directs the connection construction request to the least load server.
- Step 6: If the incoming method is indeed a stateful request, a session table is created.
- Step 7: Checks for expiration of the session.
- Step 8: Algorithm does TCP header rewriting to forward Packets, to and from the intended server of that Connection.
- Step 9: Stop.

## CONCLUSION

Using Kerberos cloud computing delivers the resources to the user securely. So it provides extensive and effective security to the cloud server as well as cloud clients. And also volunteer computing provides the solutions to reduce the server load balance. Hence speedy and secure services can be access by a client form the service provider.

## ACKNOWLEDGMENT

Acknowledge and express our sincere thanks to parents and family for their encouragement and support throughout this work. We also extend thanks to our friends and colleagues, who have encouraged us.

## REFERENCES

- [1] Udayan Banerji, "The evolution of cloud computing", 8<sup>th</sup> March 2011, <http://cloud-computing.sys-con.com/node/1714332>.
- [2] Current Trends in Cloud Computing. A Survey of Cloud Computing system By Harjith Singh. IJECSE, ISSN 2277-956 V1N3 1214-1219
- [3] Klems, M, Lenk, A, Nimis, J, Sandholm T and Tai S, 'What's inside the Cloud? An Architectural Map of the Cloud Landscape', IEEE Xplore, pp 23-31, viewed 21(2009)
- [4] Amazon. Amazon elastic compute cloud (amazon EC2). (2009). <http://aws.amazon.com/ec2/>
- [5] Cryptography and Network Security By Atul Kahate, 2<sup>nd</sup> edition, Published By The McGraw.Hill Companies.
- [6] Ellis Horowitz, Sartaz Sahani Fundamental of Computer Algorithms
- [7] Y.Lan, T.Yu (1995) "A Dynamic Central Scheduler Load-Balancing Mechanism", Proc. 14th IEEE Conf. on Computers and Communication, Tokyo, Japan, pp.734-740.
- [8] Guy Bernard, & Michel Simatic "A Decentralized and Efficient Algorithm for Load Sharing in Networks of Workstations

AUTHORS PROFILE



Nirupadi Tidigol received B.E in CSE,SJMIT,Chithradurga and 1995. M.Tech in CNE, NIE, Mysore,2011.

He is working as an Assistant Professor and Head, Department of Computer Science and Engineering in EIT,Ummathur, Chamarajanagara, India, 4Yrs. Experience as a Head,Department of CS&E VVET,Mysore, 1Yr. of Experience as a Head, Department of computer Science and engineering VVCE, 9 Yrs. Experience as Head/Lecturer Dept. of CS&E,SLN. presented, and attended the number of Conferences and workshops. His area of interests are Computer Networks and its Security , Data Mining, Cloud Computing ,wireless communication and Image Processing



**Thrilochana Kumara Y.P** received B.E in CSE, JVIT, Bangalore and 2005. M.Tech in IT, KSOU,Mysore, 2010.

He has 3Yrs. Experience as a Lecturer, Department of CS&E VVET,Mysore, 2Yr. of Experience as a Administrator VET,Bannur .He Presented, and attended the number of Conferences and workshops. His area of interests are Computer Networks, Data Mining and its Security, Cloud Computing, wireless communication, Software Engineering, Software Testing & Image Processing.



**T.P.Lokesh** received B.E in Electronics and Communication, M.Tech in Computer Network and Engineering and he is working as a Assistant Professor, Department of Electronics and Communication in VVET, Mysore. He has 8 years of teaching experience. He presented, attended the number of Conferences and workshops organized at various organizations.