

# Proposed Architecture For Implementing Privacy In Cloud Computing Using Grids And Virtual Private Network

N. Mahesh Kumar, K. Senthilkumar

PG scholar, Department of CSE, Paavai engineering college, Namakkal  
PG scholar, Department of CSE, Paavai engineering college, Namakkal  
mahesh.vcet@gmail.com, tissystems@gmail.com

**ABSTRACT:** Cloud computing technology use central server and provide applications as services to users. The organization can take advantage of reducing the cost of hardware and software ownership and maintenance. Many surveys proved cloud computing reduces total cost of ownership. But due to centralized server approach there is always risk to system security. All applications required by different set of users are stored in single CPU and there is a chance for attackers to hack important data. If organization implements separate central servers then it will again reduce the cost of hardware and software ownership. Our proposed system provides effective solution for this problem by placing grid in public cloud computing server. The grids are accessed only by authorized persons or organization with virtual private network. The applications and data's belonging to a set of users are placed inside the grids, the organizations or users from multiple locations are allowed to access the grids by using virtual network. If other user or any other resources in centralized public cloud server tries to access the grid environment, the system will deny the request. Our proposed system will secure private files and applications under public cloud environment using grid & virtual private network. Our proposed system is ideal to implement secured application in public cloud environment.

**Keywords:** Virtual Private Network (VPN), Community Cloud, Private and Public cloud.

## I. INTRODUCTION

Cloud Computing is a technology where applications or services are provided to all organization through hosted environment. The organization will use applications as a service through web browser or special software provided by the cloud service provider. Service provider use single server or group of server to provide services to all organization. In this case, the major issue is privacy among the different organizations, even though if a service provider provides dedicated server to the particular organization, still there is privacy issue among different departments or different project groups in organization. If organization uses virtual private network then practically it's not possible to access the public cloud server. Our proposed architecture provides solution to this privacy issue using grid services along with virtual private network.

## II. EXISTING

Grid computing concepts are mainly used by organizations that are distributed across the globe, but working for same project. Grid computing offers only storage service to distributed organization and there is no in built security mechanism among distributed organization. There is also no virtual network setup that may provide security between those distributed organizations. Virtual Private Network provides secured connection among different departments of same organization and also it secures the organization network from public network. It serves a reputed communication services between the organizations that are of same department that is spread across different location. It will not provide any other external service between them and it will not allow any other organization to interrupt them.

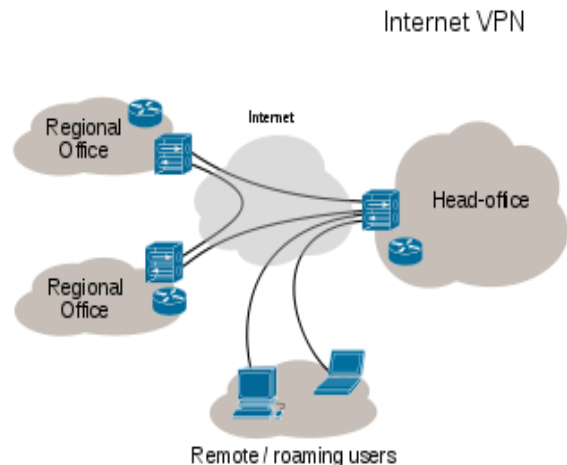


Fig 1 : VPN set up

The most emerging technology is the cloud computing technology. In this, people or an organization requires a network environment in which they can enable and utilize all the services that are required for them under the cloud environment. The departments of organization that is in same location can establish a private cloud for their own services. But if those departments of organization are in different location they are in need of communicating across public cloud which may lead to the cause in their communication privacy. It may also lead to the "loss of control".



Fig 2: cloud architecture

normally provided by the cloud are described in the following figure.

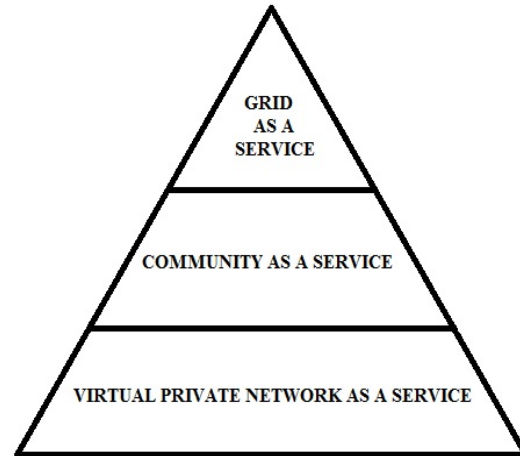


Fig 3: Services provided

### III. PROPOSED

#### a) *Creating a Grid:*

Generally a grid refers to frame like structure which is created for a particular group of departments in an organization and a cluster is loosely connected sub-organizations that are viewed as a single organization. This technique initially develops a cluster in which the departments that are belonging to the same organization are powered under that cluster. Then a frame is developed around that cluster which completely forms a grid for that department under the cloud environment. This will not allow other departments of organization to communicate with that grid. By means of this a trustable service is provided and an unwanted interruption among the department is avoided.

#### b) *Creating a Virtual Private Network:*

Virtual private network provides a secured connection across public network. It gives organization a secured way to use the internet pathways. Here the organizations department which is having the previously established grid for them in the cloud environment is directly linked with means of virtual private network. This virtual private network uses the concept of cryptography in which the encryption and decryption concept is followed while data sharing or service sharing under cloud environment. The virtual private network is established between the department of organization and its respective grid created under cloud to form a convincing infrastructure for their communication and for service sharing with the cloud.

#### c) *Support provided:*

This architecture provides the support for virtualization i.e., when different department or physically distributed branches of same organization is requesting for service in the cloud they can access simultaneously in the same grid that was created for them in the cloud environment. This technique not only provides the support for departments under a public cloud environment but also for the department of other organizations under private cloud environment. It provides a support for an organization against the issue regarding "loss of control". The services supported by this architecture other than the services

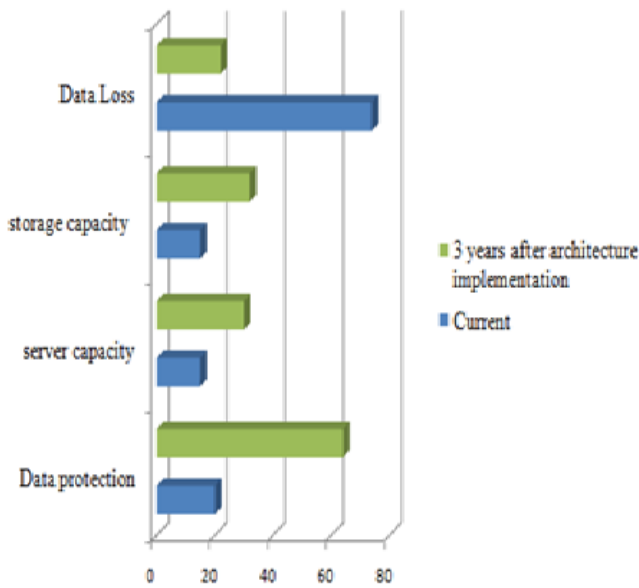
### IV. PURPOSE

#### a) *Trustable services:*

The organizations will feel free to work under their own private conditions without any interference. The information's shared between them will not be leaked out without the permission or support of the other entire department involved in that organization.

#### b) *Avoidance of loss of control:*

In general people or any other organizations that are using the cloud environment for the necessity of its services such as software or hardware are in need of depending upon the cloud providers. Similarly if an organization is developing a project under the help of cloud service and they are storing it under the cloud environment, they need to believe the service provider ensures integrity, but still there is no assurance that the data will be safe. Hence the factor "loss of control" with respect to the organizations data is made complex. But this proposed architecture overcomes this drawback by means of the departmental grid that is established for that organization in the cloud. Another factor that is giving additional confidence for their security is the virtual private network (VPN) that is established between the organization and the grid created for that organization in that cloud. So that not only a single organization but also a departments of organizations can be given room to use the secured environment to store their projects and hence the "loss of control" regarding the organizations data will be controlled enough under the cloud environment. From the following graph the observed result of this architecture is displayed. It shows the comparison between the current situation and the situation after the architecture implementation.



Graph 1: Future usage level

**V. IMPLEMENTATION**

This is a service oriented architecture in which the different modules that are involved are combined together by the following analysis to form a complete architecture.

From figure 4,

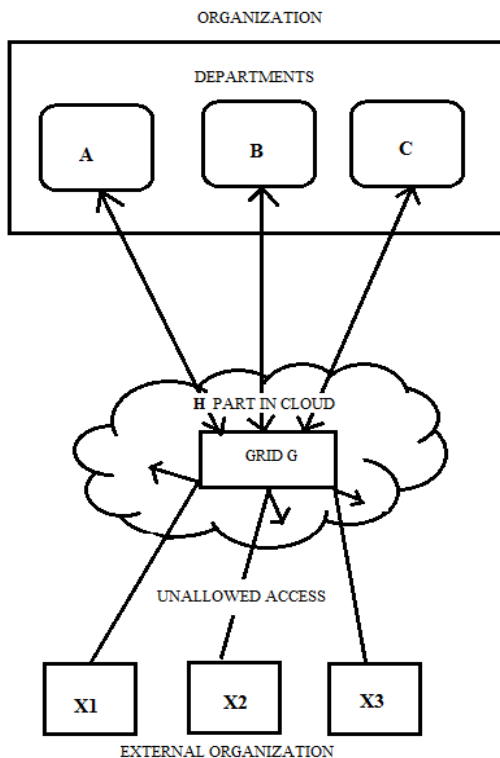


Fig 4: Architecture for implementing privacy cloud

Let us consider the departments as A, B and C under an organization X. Now a grid G is created inside the cloud environment P. Then a Virtual Private Network (VPN) is established between the organization X and the grid G. The remaining portion in the cloud other than the grid G is referred as H. The departments A,B and C inside the organization X can have direct contact with the grid G inside the cloud P by means of the pre-established VPN. But when an external organization such as X1, X2 and X3 are trying to access or communicate with grid G without establishing a virtual private network, then it will be considered as an unauthorized access and it will be automatically diverted to H part of the cloud or even from the P part of the cloud.

Let

$$X = \{A, B, C\} \text{-----} 1$$

$$P = \{G \cup H\} \text{-----} 2$$

$$G = \{A\} \cup \{B\} \cup \{C\} \text{-----} 3$$

Substitute Equation 3 in 1

We get,

$$P = \{A\} \cup \{B\} \cup \{C\} \cup \{H\} \text{-----} 4$$

The unauthorized access from the external organizations X1, X2 and X3 will be acceptable only by the H part of the cloud and it will be considered as an unknown access by the G portion inside the cloud P.

Hence from figure 4,

$$H = \{X1 \cup X2 \cup X3\} \text{-----} 5$$

$$P = \{H\} \cup \{G\} \text{-----} 6$$

Substituting 3 & 5 in 6 we get,

$$P = \{X1 \cup X2 \cup X3\} \cup \{A \cup B \cup C\} \text{--} 7$$

From Equation 7,

The cloud environment P will allow all the departments but, the authorization for grid G is provided only for A, B and C under the organization X. Similarly, The department A, B and C under the organization X will not communicate with the departments inside the organizations X1, X2 and X3. If the organizations X1, X2 and X3 want to communicate with the organization X, then they have to establish a new Virtual Private network among them along with the new grid (G1) inside the cloud environment P with the support of all the departments involved in those organizations.

**VI. CONCLUSION**

In this paper, an architecture is introduced for reducing the "loss of control" that was occurred during the service usage inside the cloud environment by an organization or by a department of organizations. This paper also describes the concept of secured infrastructure that was established

between the department of organizations and the cloud environment by means of Virtual Private Network (VPN). Here the Grid that was created inside the cloud for a particular organization or describes the need for privacy among the departments from same organization. The other services that are all provided by this architecture include Virtual Private Network as a service, Grid as a service and also a community as a service. This architecture also invokes the need for controlling the interruption by the other department of organization's and provide a control grid to avoid unauthorized access and hence the users of organization feel secured in public cloud server.

Comprehensive Guide to Secure Cloud Computing.  
Indianapolis, IN: Wiley, 2010.

## VII. REFERENCES

- [1] Armbrust, M., et al., 2010, A View of Cloud Computing, ACM, 53(4), pp. 50-58.
- [2] Papazoglou, M., Traverso, P., Dustdar, S., Leymann, F., 2007, Service-Oriented Computing: State of the Art and Research Challenges, IEEE Computer, 40(11), pp. 38-45.
- [3] Durkee, D., 2010, Why Cloud Computing Will Never Be Free, IT Professional, 53(5), pp. 62-69.
- [4] Joshi, B.D.J, Takabi, H., Ahn, G., Security and Privacy Challenges in Cloud Computing Environments, IEEE Security & Privacy, Nov/Dec, 2010.
- [5] Bianco, P., Kotermanski, R., Merson, P., Evaluating a Service-Oriented Architecture, SEI's tech report no. ESC-TR-2007-015.
- [6] Ali Babar, M., Chauhan, M. A., A Tale of Migration to Cloud Computing for Sharing Experiences and Observations, proceedings of the Software Engineering for Cloud Computing Workshop (SE-CLOUD), Collocated with ICSE 2011, Hawaii, USA.
- [7] SSL VPN security white paper at <http://www.cisco.com>, Steven Song, [http://www.cisco.com/web/about/security/intelligence/05\\_08\\_SSL-VPN-Security.html](http://www.cisco.com/web/about/security/intelligence/05_08_SSL-VPN-Security.html).
- [8] Cisco SAFE VPN IPsec Virtual Private Networks in Depth, Jason Halpern, et al., [http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/networking\\_solutions\\_white\\_paper09186a00801dca2d.shtml#wp48088](http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/networking_solutions_white_paper09186a00801dca2d.shtml#wp48088).
- [9] Briscoe, G.; Marinos, A., "Digital ecosystems in the clouds: Towards community cloud computing", Digital Ecosystems and Technologies, 2009. DEST '09.
- [10] International Engineering Consortium. *Digital Subscriber Line 2001*. Intl. Engineering Consortiu, 2001
- [11] P Plaszczak, R Wellner, *Grid computing*, 2005, Elsevier/Morgan Kaufmann, San Francisco.
- [12] Krutz, Ronald L., and Russell Dean Vines. "Cloud Computing Security Architecture." *Cloud Security: A*