IPHV7I20020X
International Journal Of Advanced Research and Innovation -Vol.7, Issue .II
ISSN Online: 2319 – 9253
Print: 2319 – 9245

To Enforce And Emplane The De Facto And Anticipated Security Threats In Cloud Computing

B.Viswanath Reddy,
Dept of Computer Science & Engineering
Sri Krishnadevaaraya University, Anantapur
Andhra Pradesh

Dr.V.Raghunatha Reddy,
Assistant Prof. Dept of CSE
Sri Krishnadevaaraya University, Anantapur
Andhra Pradesh

Abstract- Security attacks in the cloud computing environment are starting to mirror those that have traditionally taken place in physical environments with a rise of volume of problems which are identified by those who were going to try to keep them at bay. The security issues of public and private cloud and in addition to this the common misconceptions that are mostly listed as a foremost reason why enterprises are leery of the cloud. Anytime you move to a new technology, there are lot of concerns about the results of that change. With public cloud, talking about a cogent change of compute to move towards becoming this shared utility. There is a lack of visibility from the context of a customer -- businesses and enterprises -- do not have control over the IT assets any longer. **Both the** ***Security and compliance go hand in hand when cloud computing is involved. As the cloud consumers, enterprises are responsible for defining security policies, authorizing end-user use along with understanding cloud compliance requirements. But entire burden doesn't fall alone on enterprise IT. Cloud service providers must share this burden by maintaining the physical security of data centers, ensuring sufficient controls are in place for multi-tenancy environments and also must provide efficient authentication mechanisms. This paper proposes such embark issues i.e., one way to launch data security is provided through the cloud security certifications.***

Index terms- Cloud security, Public cloud, SLA's, Service organization control.

I. INTRODUCTION

Cloud computing security is the set of control-based technologies and policies designed to adhere to regulatory compliance rules and protect information, data applications and infrastructure associated with cloud computing use. Because of the cloud's very nature as a shared resource, identity management, privacy and access control are of particular concern. With more organizations using cloud computing and associated cloud providers for data operations, proper security in these and other potentially vulnerable areas have become a priority for organizations contracting with a cloud computing provider. Cloud computing[3] security processes should address the security controls the cloud provider will incorporate to maintain the customer's data security, privacy and compliance with necessary regulations. The processes will also likely include a business continuity and data backup plan in the case of a cloud security breach. The infrastructure that exists between the client and the cloud computing server, as well as the cloud computing server infrastructure itself, presents opportunities for other types of specifically targeted attacks. For example, DoS and DDoS attacks against either the cloud computing service provider or the cloud computing client. DoS attacks can be launched at the cloud computing service provider when the client may be the real target. Within the client server farm infrastructure, one server may become compromised and other good servers may suddenly become busy, resulting in anycast directing cloud computing requests to the rogue server and preventing legitimate connections to the client servers. If the cloud computing service provider is the target, all client servers within the provider's infrastructure could be rendered unavailable by flooding the cloud computing environment's entry points with connection requests. The problem is exacerbated by the geographically distributed nature of cloud computing. When the server farms span multiple data centers and nations, there are no guarantees that each server is configured and managed identically. Though centralized policy management is available for massively distributed environments, it is not always implemented correctly; few customers demand proof of how policy conformance is implemented by their CC providers. Furthermore, if any server were to be compromised, the company policies must be reconciled with the host nation's cyber laws. Robust centralized management of server configurations can help prevent DoS and ensure all servers in the cloud respond according to the same accepted baseline. Moreover, there are network and perimeter devices available to detect malicious traffic, such as DoS floods, that will mitigate this type of attack and ensure legitimate traffic continues to be processed.

Cloud computing is providing computing resources (Software, Platform and Infrastructure) as a service over the network. Cloud computing users can use the services provided by the Cloud Computing service provider without taking the trouble of planning, procuring, building, configuring and maintaining the infrastructure. Cloud is a metaphor used for Internet. cloud computing is using computing resources managed by provider and “pay as per usage”. The service provider will take care of infrastructure management and user needs to pay only for services used. Further cloud computing largely divided in two types, Private clouds and Public Cloud.

i) Private Cloud- In case of Private Clouds, cloud services are maintained for one client. It may be managed internally or externally by Internal IT or third-party. This gives organization little edge on security but same time because of small scale they won’t able to cost benefits of virtualization. A private cloud, because it functions independently for an organization and that too behind firewall settings does prove to be accessible. By stating this, we mean that a private cloud[5] cannot be accessed from anywhere and at any point of time. It is completely managed by the users working for an organization. As far as the scalability factor is concerned, private cloud gives scalable business environment. It also offers flexibility to expand as per users’ requirement. A private cloud tends to be more secure since it resides on your local system, and all of your data is protected by your local firewall. Another argument in favor of the private cloud is that many large organizations already have extensive data centers so they might as well use their current infrastructure as opposed to letting it go to waste. The major argument against private cloud is that these are fully responsible for the management, maintenance and updating of data centers. Servers get old and need to be replaced, which can get very expensive. With the public cloud, these aren’t responsible for the maintenance and updating of data centers. The cloud provider from which you’re purchasing your public cloud is.

ii) Public Cloud- A public cloud is constructed with a view to offer unlimited storage space and increased bandwidth via Internet to all businesses. It is usually an open system that is available for free to general public via World Wide Web or Internet. Some of the popular examples of public clouds include Amazon Elastic Cloud Compute, Google App Engine, Blue Cloud by IBM and Azure services[7] Platform by Windows. Public Cloud architecture is built with the view to create an accessible business environment that can be shared and accessed from anywhere and at any time of the hour. Even though, it poses security risks, public cloud is considered more useful than its counterpart because of several reasons: Initial cost is minimal, but if data is stored for a long period of time, it proves to be expensive. However, the cloud acts as an excellent source for different types of data than a particular type of it. Public Cloud is extension of private cloud with additional cost-benefit due to service-provider orients low cost cloud storage to enterprise. Public Cloud like Microsoft Windows Azure passed the benefit of shared infrastructure and automation in term of low-cost. More accessible than the private cloud as it can be accessed from anywhere round the globe. Availability and reliability are the two factors that make public cloud computing service more popular. The reason being, it is available to users via web installed at a given server off-premises.

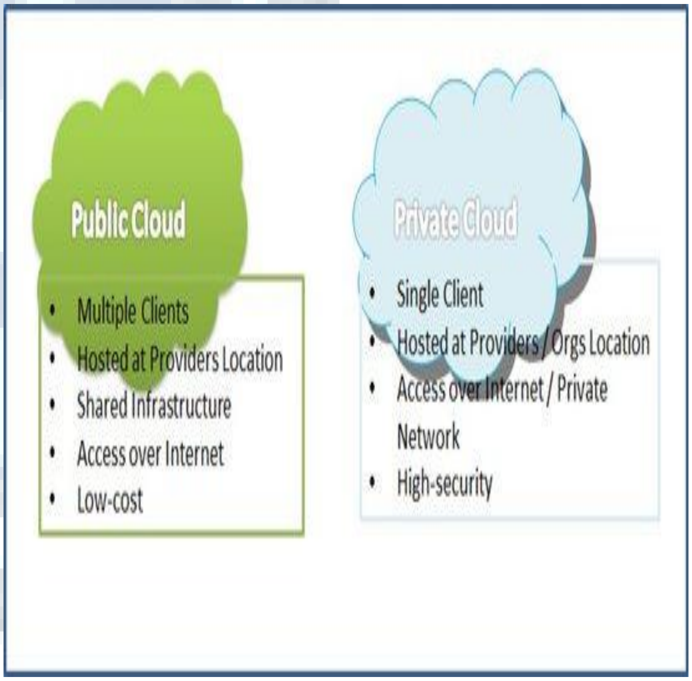

Fig.1 Comparison of public cloud and private cloud

In order to understand what properties make a decision of a cloud computing environment there is a need to differentiate between the two clouds.

i) Public cloud is used as a service via Internet by the users, whereas a private cloud, as the name conveys is deployed within certain boundaries like firewall settings and is completely managed and monitored by the users working on it in an organization.

ii) Users have to pay a monthly bill for public cloud services, but in private cloud money is charged on the basis of per Gb usage along with bandwidth transfer fees.
iii) Public cloud functions on the prime principle of storage demand scalability, which means it requires no hardware device. On the contrary, no hardware is required even in private cloud, but the data stored in the private cloud can only be shared amongst users of an organization and third party sharing depends upon trust they build with them. It is also entirely monitored by the business entity where it is running.

II. RELATED WORK

Cloud computing promises to serve enterprise computing needs while providing cost savings, particularly in the areas of capital hardware, data center management and software development. The cost-benefit argument goes something like this: Why pay for software, custom-development and hardware when infrastructure expenses and management overhead can be transferred to a cloud computing provider? It's no wonder that as cash-strapped companies scramble for ways to cut costs, many of them are looking to the cloud. While cloud computing provides compelling benefits, it's highly distributed. A service-based model will also render many of today's existing security architectures obsolete. Security architects will need to re-examine assumptions and derive a security model that can be implemented in a distributed, cloud infrastructure. The traditional "defense-in-depth" approach to security must be expanded beyond on-premise controls to distributed and federated ones that are portable enough to work in a variety of cloud architectures. Rethinking zones is also in order. Protective zones around servers, applications and even individual pieces of data must extend beyond the physical control of the in-house corporate network.
Although some risk can be transferred to the cloud, all of the issues related to accountability and responsibility for protection of sensitive data still rests with the original steward of that data. Understanding how the cloud computing provider builds its services and manages the data is critical because it can mean the difference between real cost savings and false economy. Infrastructure is defined as those services that make clouds and cloud services available to end-user clients and the transport mechanisms to the cloud(s) and between the various components within the cloud(s).
This illustration represents the common elements within a typical shared cloud computing infrastructure architecture.

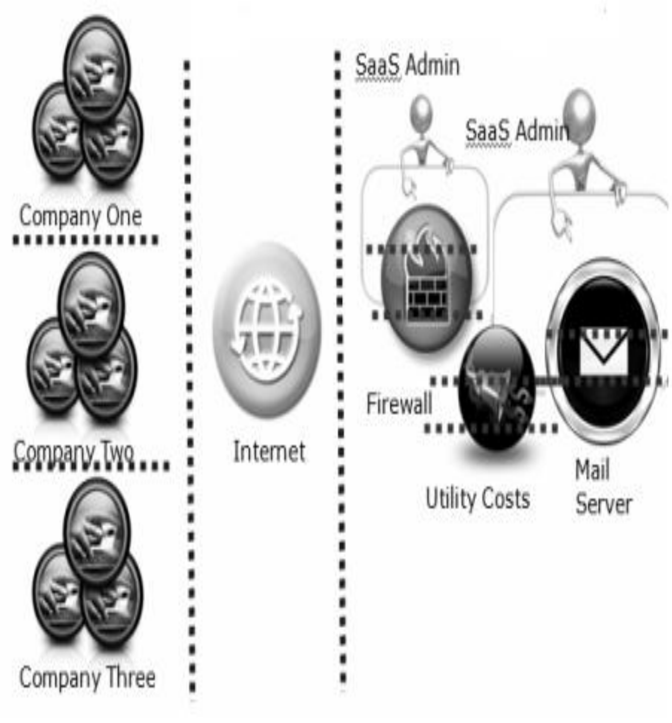

Fig.2 SaaS conceptual architecture-Shared

Cloud computing takes advantage of the fact that many services and data processes are repeatable. Rather than writing a unique piece of software for each customer, cloud computing enables a single instance of the software, on shared or single-purpose hardware, to be delivered as a service to multiple customers. This saves software developers time because the same code or application can be reused for multiple customers. Commercial off-the-shelf software, for example Microsoft's Exchange Server, provides the same reuse benefit. But cost is incurred by the end-user enterprises that purchase the software and the hardware it will run on, and then pay professionals to manage it.

Much like a global software library where certain repeatable procedures are stored and accessed by many, the cloud computing architecture transfers storage and management of applications -- and the hardware on which they run -- to a set of data centers, thereby creating a virtual software library of sorts. Traditional software libraries reside on a host's operating system. Cloud applications and application mash-ups reside in virtual libraries across multiple host systems and can interact with multiple clouds. These large data centers and server farms supply business services and data management for multiple customer clients, creating a mature "client/server" model for the masses. Most public cloud storage services provide details of the service levels that users can expect on their websites and these will likely be the same for all users. However, an enterprise establishing service with a private cloud storage provider may be able to negotiate a more customized deal. In this case an SLA might include specifications for retention policies, the number of copies that will be retained, storage locations and so on. It's important to read an SLA closely and examine the ramifications. For example, 99.9% uptime, a common stipulation, translates to nine hours of outage per year. For some mission critical data, that may not be adequate.

Even when business is booming, smart companies always have an eye on the bottom line. Security is not usually one of the first places companies look to trim expenses, but some IT professionals believe that they can easily lower costs by eliminating third-party Secure Sockets Layer (SSL) Certificate Authorities (CAs) from the budget equation. Although spending money on SSL security for external facing sites—such as the company home page or e-commerce pages—still seems necessary, some IT professionals think that self-signed SSL certificates are an acceptable alternative for internal sites. They believe that, since only internal employees have access to servers that host internal-facing sites such as intranet portals and wikis, self-signed certificates provide adequate protection at practically no cost. A cloud storage[7] SLA is a service-level agreement between a cloud storage service provider and a customer that specifies details of the service, usually in quantifiable terms.A service-level agreement (SLA) is a contract between a network service provider and a customer that specifies, usually in measurable terms, what services the network service provider will furnish. Many Internet service providers (ISP)s provide their customers with an SLA. More recently, IS departments in major enterprises have adopted the idea of writing a service level agreement so that services for their customers (users in other departments within the enterprise) can be measured, justified, and perhaps compared with those of outsourcing network providers.

Some metrics that SLAs may specify include:

- What percentage of the time services will be available
- The number of users that can be served simultaneously
- Specific performance benchmarks to which actual performance will be periodically compared
- The schedule for notification in advance of network changes that may affect users
- Help desk response time for various classes of problems
- Dial-in access availability
- Usage statistics that will be provided.

IV. IMPLEMENTATION & ANALYSIS RESULTS

A typical cloud storage SLA articulates precise levels of service – such as, for example, 99.9% uptime – and the recourse or compensation that the user is entitled to should the provider fail to provide the service as described. Another normal cloud storage SLA detail is service availability, which specifies the maximum amount of time a read request can take, how many retries are allowed and so on. The SLA should also define compensation for users if the specifications aren't met. Cloud storage service providers usually offer a tiered service credit plan that gives users credits based on the discrepancy between SLA specifications and the actual service levels delivered. Most public cloud storage services provide details of the service levels that users can expect on their websites and these will likely be the same for all users. However, an enterprise establishing service with a private cloud storage provider may be able to negotiate a more customized deal. In this case an SLA might include specifications for retention policies, the number of copies that will be retained, storage locations and so on. It's important to read an SLA closely and examine the ramifications. For example, 99.9% uptime, a common stipulation, translates to nine hours of outage per year. For some mission critical data, that may not be adequate. You should also check to see how terms are defined. Terri McLure, a senior analyst at Enterprise Strategy Group in Milford, Mass., explains: "I know of one vendor SLA, for example, that offers 99.9% uptime. It sounds pretty good. But they don't count downtime unless the client can't access applications for more than 10 minutes. A nine-minute outage is not considered downtime for them in their SLA."

Some certifications are designed to address the requirements of a broad range of users, such as Service Organization Controls 1 (SOC 1) and International Organization for Standardization 27001 (ISO 27001) certifications. Other certifications narrowly target particular types of end users, such as Payment Card Industry Data Security Standard (PCI DSS), which applies to businesses using payment cards and the Federal Information Security Management Act (FISMA), which addresses the needs of U.S. government federal agencies. Because these standards include general best practices, you may benefit from a cloud provider that meets these standards -- even if your business does not use payment cards or doesn't need to comply with FISMA. Cloud providers offer a wide range of services, but the quality of those services isn't immediately known. The SOC 1 report helps to address the actual implementation of those services corresponds to what the cloud provider claims. This report covers the presentation of services from a cloud computing service provider, the design of systems for implementing those services and the effectiveness of operational controls for maintaining those services. The American Institute of CPAs has detailed documentation on SOC 1 and related reports, including information on the SSAE 16 report -- an auditor-to-auditor report about compliance. Self-signed certificates are inherently less trustworthy than those signed by leading CAs(Certificate Authorities).Reputable third-party CAs have robust processes in place to help ensure that their encryption keys, especially their highly sensitive private “root” keys, are kept safe. For these CAs, security is always a top priority: Personnel are rigorously vetted and highly trained, and these CAs have strict policies concerning where private keys are stored. In fact, if a CA wants to be approved by mainstream web browsers, these keys must be kept on non-extractible storage on smart cards. To offer strong SSL security[9], a CA must also provide high-availability and failover mechanisms to prevent system failure. This helps to ensure that it can provide the proper authentication on demand whenever users need it. Replicating this infrastructure to match the high security standards in place at leading CAs requires a number of costly components. First, an organization must have high-availability (HA) replication of the SSL system and data. A second, related requirement is that this replication must be achieved using two different secure rooms in two different data centers in two separate locations. This helps to ensure that if one data center goes down, due to power loss or other unforeseen factors, the other will be there to provide backup authentication. Without replication across data centers, servers and browsers would not be able to complete the authentication process and vital SSL-protected transactions.

i) First, an organization needs to carefully control who has the authority to create and sign certificates for its domains, and establish processes for ensuring that this is done according to established policies. Such policies would include requiring that only personnel of sufficient tenure and trust have authority to create and sign certificates, and that they are adequately trained in best practices, standards, and technologies. This authority should not be given lightly, and a clear audit trail is needed in case an investigation is ever required.

ii) Second, leading third-party CAs typically offer web-based applications with easy-to-use management interfaces that automate and accelerate many processes, including delegating authority for creating certificates and approving certificates for signing by the CA. Certificate Signing Requests (CSRs) must eventually be approved by someone vested with authority for a particular domain. Trusted CAs have robust automated procedures in place to help ensure that all of this occurs as prescribed.

iii)Third, if an organization decides to use self-signed certificates, it will need processes similar to those described above. Some businesses attempt to automate the SSL security workflow by writing custom software, but many simply attempt to manually manage the processes. This takes a considerable amount of time and effort from highly skilled and trusted staff—which may mean more highly paid senior employees.

iv) Fourth, without the management tools and alerts that often come with certificates from a trusted CA, organizations will not be notified when certificates expire. The expiration of self-signed certificates—as well as their renewal—will need to be tracked manually, an extremely time consuming task that can take skilled personnel away from other mission-critical work. The cost of expired SSL Certificates is unacceptably high; “rogue” certificates can create an uneven patchwork of security, leading to warning messages that may negatively impact customers and internal stakeholders alike.

v) Finally, with software-only encryption, visibility into status can be severely limited. Unless the keys are stored in hardware, organizations cannot guarantee that it knows how many keys exist and who has had access to them. If the network is compromised, a company has no way of knowing if a key was copied off-site and is being compromised as well.

There are different existing algorithms like the Genetic algorithm (GA) is used for searching large solution space. On other hand, simulated Annealing (SA)[11] is an iterative technique that considers only one possible solution for each meta-task at a time. Ant Colony Algorithm (ACO) is the latest entrant to this field. ACO algorithm can be interpreted as parallel replicated Monte Carlo (MC) systems. MC systems are general stochastic simulation systems, that is, techniques performing repeated sampling experiments on the model of the system under consideration by making use of a stochastic component in the state sampling and/or transition rules. Experimental results are used to update some statistical knowledge about the problem. In turn, this knowledge can be also iteratively used to reduce the variance in the estimation of the described variables and directing the simulation process toward the most interesting state space regions.

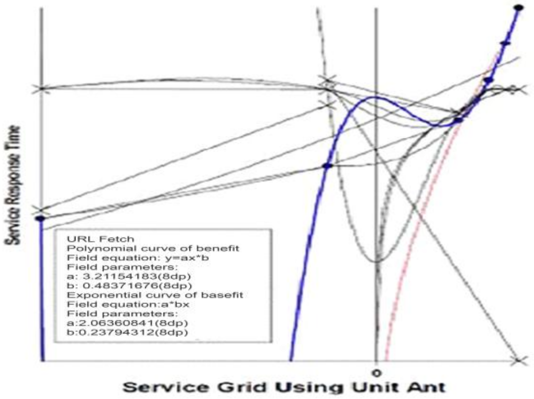

Fig. 3 Cloud services under ACO

Analogously, in ACO algorithms the ants sample the problem's solution space by repeatedly applying a stochastic decision policy until a feasible solution of the considered problem is found. The sampling is realized concurrently by a collection of differently instantiated replicas of the same ant type.

The use of each cloud model among respondents is fairly evenly split, with 40% using public cloud, 30% using private cloud and another 30% of respondents reporting the use of hybrid cloud services. And all three cloud models will see increased use over the next six months, as survey results show in figure 4a and 4b. In figure 4, for example, 90 respondents using public cloud currently have 25% to 50% of their data center infrastructure in the cloud.

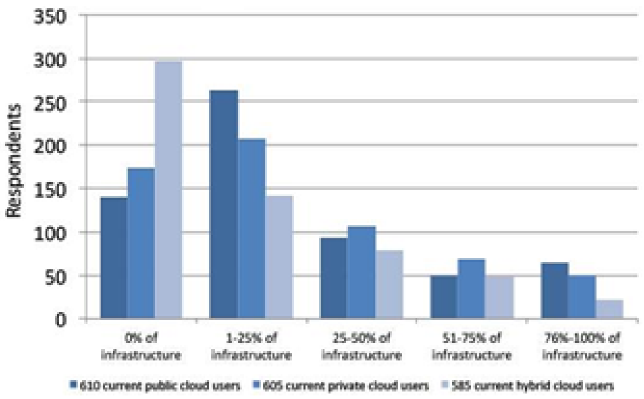

Fig. 4(a)

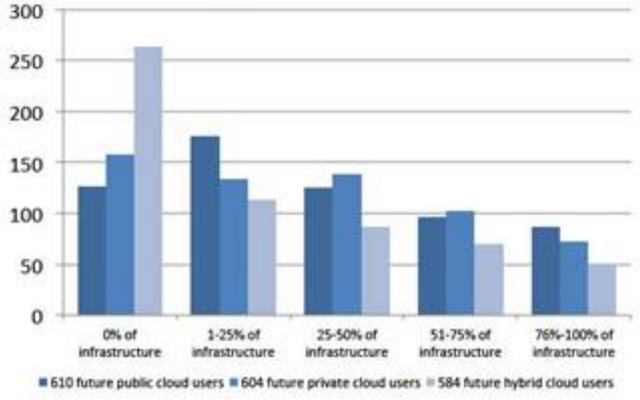

Fig. 4(b)

Fig. 4(a) & 4(b) Levels of cloud adoption by model.

V. CONCLUSIONS

Cloud computing promises reduced costs and increased agility, but there is a critical need to provide training and certification of professionals to ensure the model is implemented securely. The main concern that people have in enterprises now is if your systems are being operated by a third party -- especially a massively well-trafficked third party, such as a major cloud provider -- there can be a potential for bad actors potentially accessing your information or hacking into your systems. That's always been true, but the concern is more front-of-mind right now because these systems are so very public in terms of their visibility and their brand. Cloud security certifications such as these are not only helpful, they're often required when working with cloud providers. Certifications attest to the state of security practices within a cloud provider and can help enterprises meet compliance reporting requirements. In some cases, such as with federal agencies, at least one of these certifications may be required before you can do business with a cloud service provider.

It's important to understand that certifications do not alleviate your responsibilities as a cloud consumer. Poor in-house security practices can undermine the benefits of sound cloud security practices of an established cloud service provider. For example, if you do not have a data-classification scheme in place and you have weak internal controls over authorizations to access and manipulate data, your data may be at risk even if it's stored with a cloud provider that holds a number of certifications. Using a provider that adheres to specific cloud certifications can help enterprises meet some compliance requirements in the cloud. And sharing this burden with a cloud provider means enterprises have more time to address other internal security requirements.

REFERENCES

[1] I. Foster, C. Kesselman. "Globus: A Metacomputing Infrastructure Toolkit", Intl J. Supercomputer Applications, 11(2):115-128, 1997.

[2] I. Foster, C. Kesselman, C. Lee, R. Lindell, K. Nahrstedt, A. Roy. "A Distributed Resource Management Architecture that Supports Advance Reservations and Co-Allocation", Intl
Workshop on Quality of Service, 1999.

[3] I. Foster, C. Kesselman, S. Tuecke. The anatomy of the Grid: Enabling scalable virtual organization. The Intl. Jrnl. of High Performance Computing Applications, 15(3):200--222, 2001.

[4] I. Foster. What is the Grid? A Three Point Checklist, July 2002.

[5] I. Foster, C. Kesselman, and S. Tuecke, The Anatomy of the Grid-Enabling Scalable Virtual Organizations, The Globus Alliance, http://www.globus.org/research/papers/anatomy.pdf.

[6] I. Foster, H. Kishimoto, A. Savva, D. Berry, A. Djaoui, A. Grimshaw, B. Horn, F. Maciel, F. Siebenlist, R. Subramaniam, J. Treadwell and J. Von Reich, The Open Grid Services Architecture, Version 1.0, http://forge.gridforum.org/projects/ogsa-wg, January 2005.

[7] S. Tuecke, K. Czajkowski, I. Foster, J. Frey, S. Graham, C. Kesselman, T. Maquire, T. Sandholm, D. Snelling, and P. Vanderbilt, Open Grid Services Infrastructure (OGSI) Version 1.0, Global Grid Forum, http://www.ggf.org, June 2003.

[8]"What is cloud computing?" http://searchcloudcomputing.techtarget.com/sDefinition/0sid201gci1287881,00.html.

[9] L.M. Vaquero, L.R. Merino, J. Caceres, and M. Lindner, "A break in the clouds: towards a cloud definition," ACM SIGCOMM Computer Communication Review, Vol. 39, No. 1, 2009. "MammoGrid", http://mammogrid.vitamib.com.

[10]. "DDGrid", http://www.ddgrid.ac.cn.

[11]. Erico Guizzo, "Robots with their heads in the cloud", IEEE Spectrum, 2011.

[12]. "Panda Cloud", http://www.cloudantivirus.com.

[13]. R. Buyya, D. Abramson and J. Giddy, "Nimrod/G: An Architecture for a Resource Management and Scheduling System in a Global Computational Grid", IEEE Intl. Conf. on High Performance Computing (HPC ASIA), 2000.

AUTHOR'S INFROMATION:

Mr. Viswanath Reddy Bontha is pursuing PhD. from Sri Krishnadevaraya University, Anantapur. His main research interest includes "cloud computing".

Dr.V.Raghunatha Reddy is working as Assistant Professor in the Department of Computer Science & Technology. He published nearly 14 Papers in International Journals. He has 10 years of teaching experience at University level. He did his Ph.D. from the Department of Computer Science & Technology of S.K.Univerity, Anantapur, India.