Volume 5, No. 4, April 2014 (Special Issue)

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

# Imperial Analysis of Threats and Vulnerabilities in Cloud Computing

Ruchita D.Londhe
Bhartiya Mahavidyalaya,
Amravati, India
ruchita1603@gmail.com

Swati S. Sherekar
Sant Gadge Baba Amravati
University, Amravati, India
ss_sherekar@rediffmail.com

V. M. Thakare
Sant Gadge Baba Amravati
University, Amravati, India
vilthakare@yahoo.com

***Abstract :*** Data security is one of the most crucial and a major challenge in the digital world. Security, privacy and integrity of data are demanded in every operation performed on internet. Whenever security of data is discussed, it is mostly in the context of secure transfer of data over the unreliable communication networks. Some common security techniques that can be employed to enhanced the security of the database against some known attacks and security threats. Its main objective is to provide secure, quick, convenient data storage and net computing services, with all computing resources visualized as services and delivered over the Internet.
The main contribution of this paper is that to identify the main vulnerabilities and threats in Cloud Computing environment. This paper focuses on various threats and vulnerabilities ultimately we are able to improve the security.

***Keywords:*** - Cloud Computing, Multitency, Security Issues, Threats, Vulnerability.

## I. INTRODUCTION

Cloud computing provides countless benefits and opportunity to spread servers across the world without upfront investments or even operating a single data centre. It is an innovative computing paradigm for storing data and running applications. Cloud computing appears to attract all sphere of computing [1, 2]. Cloud Computing enables ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources such as networks, servers, storage, applications, and other services that can be rapidly provisioned and released with minimal management effort or service provider interaction [3].

Cloud Computing appears as a computational paradigm as well as distribution architecture and its main objective is to provide secure, quick, convenient data storage and net computing service, with all computing resources visualized as services and delivered over the Internet [3, 4]. Cloud providers and cloud users are two main platform of cloud computing. Basic Cloud provider like Amazon is to Provide computing resources, such as storage (Amazon S3), CPU (Amazon EC2), or databases, as web services that can be subscribed to and consumed on a pay-as-you-go model without contracts [2].In cloud computing security is concerns and relate to risk areas such as external data storage, dependency on the public internet, lack of control, multi-tenancy and integration with internal security [3].

A threat is a potential attack that may lead to a misuse of information or resources, and the term vulnerability refers to the flaws in a system that allows an attack to be successful. Vulnerability is the probability that an asset will be unable to resist the actions of a threat agent. Vulnerability exists when there is a difference between the force being applied by the threat agent, and an object's ability to resist that force [6]. The current adoption of cloud computing is associated with numerous challenges because users are still sceptical about its authenticity [4].

## II. TYPES OF CLOUD COMPUTING

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources such as networks, servers, storage, applications, and services that can be rapidly provisioned and released with minimal management effort or service provider interaction[5]. There are four types of cloud computing public cloud, private cloud, community cloud, and hybrid cloud. In figure 1[6] visualizes the four cloud computing types and their relationships. Each of these cloud types offers different advantages to the cloud users. An organization can use one or more types of cloud computing to realize its organizational goals [8].

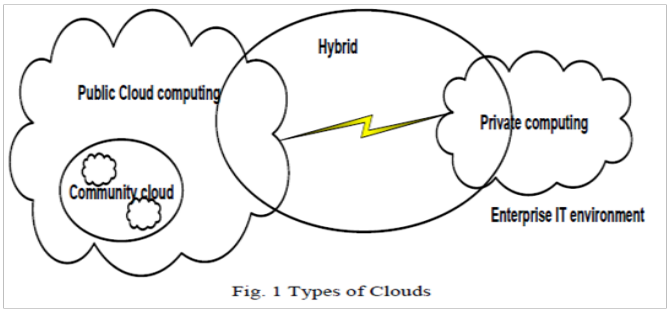


Fig. 1 Types of Clouds



CONFERENCE PAPER
Two day National Conference on Innovation and Advancement in Computing
Organized by: Department of IT, GITAM UNIVERSITY Hyderabad (A.P.) India
Schedule: 28-29 March 2014

### *A. Public Cloud:*

In public cloud computing, computer resources such as CPU, storage, bandwidth, databases, and load balancers are made available to the public by cloud service provider such as Amazon Web Services and Google's App Engine [8]. These resources may be provided for free or based on a pay-as-you-go model. Public clouds assure the major benefits of cloud computing [9].

### *B. Private cloud:*

A private cloud is hosted in the data centre of a company and provides its services only to users inside that company or its partners. A private cloud provides more security than public clouds [8].

### *C. Community Cloud:*

In this cloud services are provided to a specific group of organizations that share common goals or missions such as security requirements, policy, or compliance considerations. The cost of running the cloud services is shared among the participants. Community clouds can leverage service compliance to provide highly secure cloud environments among trusted communities [8].

### *D. Hybrid Cloud:*

This is a combination of private, public, or community clouds. Hybrid clouds allow organizations to find an optimal balance between cost of IT operations and inherent security risks by running highly confidential applications on private clouds and utilizing public clouds for peak loads or other computations [8, 9].

### *E. Grid Computing :*

Computing grids are ancestors of clouds, and where built by connecting hundreds of servers in one or more data centers to provide aggregated computing power for long-running and computationally intense tasks (like scientific computations, such as weather or DNA folding simulations), which run multiple hours or days at a time.

### *F. Utility Computing:*

Utility computing is another ancestor of cloud computing and has been inspired by how public utilities, such as electricity, water, and gas, are billed based on usage. Utility computing was developed after grid computing and provided computing resources to users through metered billing models. In grids, computing resources were often wasted, as users did not have incentives to control their resource usage.

## III. SECURITY ISSUES IN CLOUD COMPUTING

Security concerns relate to risk areas such as external data storage, dependency on the "public" internet, lack of control, multi-tenancy and integration with internal security. The security issues in Cloud Computing identifying the main vulnerabilities for clouds, and the most important threats in clouds. Various cloud service model are affected by many vulnerabilities and threats. Categorization of security issues for Cloud Computing focused in the SPI model (SaaS, PaaS and IaaS)[10]. The cloud model provides three types of services:

***(a). Software as a Service (SaaS)-*** The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser.

***(b). Platform as a Service (PaaS) -*** The capability provided to the consumer is to deploy onto the cloud infrastructure his own applications without installing any platform or tools on their local machines. PaaS refers to providing platform layer resources, including operating system support and software development frameworks that can be used to build higher-level services.

***(c). Infrastructure as a Service (IaaS)-*** The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications.

### *A. Software-as-a-service (SaaS) security issues:*

SaaS provides application services on demand such as email, conferencing software, and business applications. SaaS users have less control over security among the three fundamental delivery models in the cloud[11]. The adoption of SaaS applications may raise some security concerns such as:

#### *a. Application security:*

These applications are typically delivered via the Internet through a Web browser. However, flaws in web applications may create vulnerabilities for the SaaS applications. Attackers have been using the web to compromise user's computers and perform malicious activities such as steal sensitive data.

#### *b. Multi-tenancy:*

In a multitenancy environment, multiple customers share the same application, running on the same operating system, on the same hardware, with the same data-storage mechanism. The distinction between the customers is achieved during application design, thus customers do not share or see each other's data[12].

#### *c. Data security:*

Data security is a common concern for any technology, but it becomes a major challenge when SaaS users have to rely on their providers for proper security. In SaaS, organizational data is often processed in plaintext and stored in the cloud. The SaaS provider is the one responsible for the security of the data while is being processed and stored.

### *B. Platform-as-a-service (PaaS) security issues:*

PaaS facilitates deployment of cloud-based applications without the cost of buying and maintaining the underlying hardware and software layers Infrastructure-as-a-service (IaaS) security issues IaaS provides a pool of resources such as servers, storage, networks, and other computing resources in the form of virtualized systems, which are accessed through



CONFERENCE PAPER
Two day National Conference on Innovation and Advancement in Computing
Organized by: Department of IT, GITAM UNIVERSITY Hyderabad (A.P.) India
Schedule: 28-29 March 2014

the Internet. Users are entitled to run any software with full control and management on the resources allocated to them.

***a. Third-party relationships:***

Moreover, PaaS does not only provide traditional programming languages, but also does it offer third-party web services components such as mashups. Mashups combine more than one source element into a
single integrated unit. Thus, PaaS models also inherit security issues related to mashups such as data and network security .

***b. Development Life Cycle:***

From the perspective of the application development, developers face the complexity of building secure applications that may be hosted in the cloud. The speed at which applications will change in the cloud will affect both the System Development Life Cycle (SDLC) and security . Developers have to keep in mind that PaaS applications should be upgraded frequently, so they have to ensure that their application development processes are flexible enough to keep up with changes.

*c.* ***Underlying infrastructure security:***

In PaaS, developers do not usually have access to the underlying layers, so providers are responsible for securing the underlying infrastructure as well as the applications services. Even when developers are in control of the security of their applications, they do not have the assurance that the development environment tools provided by a PaaS provider are secure [13].

***C. Infrastructure-as-a-service (IaaS) security issues:***

IaaS provides a pool of resources such as servers, storage, networks, and other computing resources in the form of virtualized systems, which are accessed through the Internet. Users are entitled to run any software with full control and management on the resources allocated to them. With IaaS, cloud users have better control over the security compared to the other models as long there is no security hole in the virtual machine monitor. They control the software running in their virtual machines, and they are responsible to configure security policies correctly

***a. Virtualization:***

Virtualization means to create a virtual version of a device or resource, such as a server, storage device, network or even an operating system where the framework divides the resource into one or more execution environments. Virtualization allows users to create copy, share, migrate, and roll back virtual machines, which may allow them to run a variety of applications.

***b. Shared resource:***

VMs located on the same server can share CPU, memory, I/O, and others. Sharing resources between VMs may decrease the security of each VM. For example, a malicious VM can infer some information about other VMs through shared memory or other shared resources without need of compromising the hypervisor.

***c. Virtual networks:***

Network components are shared by different tenants due to resource pooling. As mentioned before, sharing resources allows attackers to launch cross-tenant attacks. Virtual Networks increase the VMs interconnectivity, an important security challenge in Cloud Computing[14].

***d. Virtual machine monitor:***

The Virtual Machine Monitor (VMM) or hypervisor is responsible for virtual machines isolation; therefore, if the VMM is compromised, it s virtual machines may potentially be compromised as well. The VMM is a low-level software that controls and monitors its virtual machines, so as any traditional software it entails security flaws.

***D. Staff Security Screening*:**

Most organizations employ contractors as part of their workforce. A cloud provider must be able to provide its policy on background checks and document that all of its employees have had a background check performed as per the policy. The contract between the user and cloud provider should bind the cloud provider to require the same level of due diligence with its contractors.

***E. Data location*:**

When clients running the data location, they probably won't know exactly where their data are hosted. Distributed data storage is a usual manner of cloud providers that can cause lack of control and this is not good for customers who have their data in local machine before moving from local to cloud.

***F. Recovery:***

If a cloud provider broke or some problems cause failure in cloud sever what will happen to users' data? Can cloud provider restore data completely? Moreover clients prefer don't get permission to third-party companies to control their data. This issue can cause an impasse in security[15].

***G. Investigative support*:**

Cloud services are not easy to support the investigation, because logging and data for multiple customers may be co-located and may also be spread across an ever-changing set of hosts and data centers.

***H. Long-period viability*:**

Cloud computing run business, it needs o ensure that data is adequately protected and can be restored in a timely fashion and get acquired by a larger company with maybe new policies. But clients must be sure their data will remain available even after such an event[16].

***I. Data segregation*:**

Data in the cloud is typically in a shared environment alongside data from other customers. Encryption is effective but isn't a cureall. Encryption and decryption is a classic way to cover security issues but heretofore it couldn't ensure to provide perfect solution for it[17].



CONFERENCE PAPER
Two day National Conference on Innovation and Advancement in Computing
Organized by: Department of IT, GITAM UNIVERSITY Hyderabad (A.P.) India
Schedule: 28-29 March 2014

### *J. Policy Integration:*

Different cloud servers can use different tools to ensure the security of client data. So integration policy is one of the major concerns of Security [15].

## IV. VULNERABILITIES IN CLOUD COMPUTING

Vulnerability is a cyber-security term that refers to a flaw in a system that can leave it open to attack. Vulnerability "is a weakness in the security system" that could be exploited to cause harm. Vulnerability to an attack is the use of denial-of-services. Web applications and services, virtualization, and cryptography is a core technologies in cloud computing have vulnerabilities that are either intrinsic to the technology or prevalent in the technology's [6].Some of these vulnerabilities are as follows:

### *A. Insecure interfaces and APIs:*

Cloud computing providers expose a set of software interfaces or APIs that customers use to manage and interact with cloud services. Provisioning, management, orchestration, and monitoring are all performed using these interfaces. Cloud Computing providers expose a set of software interfaces or APIs that customers use to manage and interact with cloud services. Provisioning, management, orchestration, and monitoring are all performed using these interfaces. The security and availability of general cloud services is dependent upon the security of these basic APIs[16]. From authentication and access control to encryption and activity monitoring, these interfaces must be designed to protect against both accidental and malicious attempts to circumvent policy.

### *B. Data-related vulnerabilities:*

Data can be collocated with the data of unknown owners such as competitors, or intruders with a weak separation.

a. Data may be located in different jurisdictions which have different laws
b. Data cannot be completely removed.
c. Data backup done by untrusted third-party providers.
d. Information about the location of the data usually is unavailable or not disclosed to users.
e. Data is often stored, processed, and transferred in clear plain text[4].

### *C. Vulnerabilities in Virtual Machines* :

Unrestricted allocation and de allocation of resources with VMs.VMs can be migrated from one server to another server due to fault tolerance, load balance, or hardware maintenance .VMs can be copied in order to provide flexibility, which may lead to data leakage. VMs have IP addresses that are visible to anyone within the cloud - attackers can map where the target.

### *D. Vulnerabilities in Virtual Machine Images:*

Uncontrolled placement of VM images in public repositories.VM images are not able to be patched since they are dormant artefacts

### *E. Vulnerabilities in Hypervisors:*

Flexible configuration of VMs or hypervisors to meet organization needs can be exploited. Vulnerabilities in the hypervisor that allow the execution of arbitrary code on the host with the privileges of the hypervisor that allow an attacker to control all virtual machines and the host itself.

### *F. Vulnerabilities in Virtual Networks:*

Virtual network significantly affects the VMs interconnectivity which is one of the biggest security challenges in the design of cloud computing platform. The more secure way to isolate each VM is using dedicated physical channel for each host-V M link.

### *G. Unauthorized access to management interface:*

The cloud characteristic on-demand self-service requires a management interface that's accessible to cloud service users. Unauthorized access to the management interface is therefore an especially relevant vulnerability for cloud systems[17]..

### *H. Internet protocol vulnerabilities:*

The cloud characteristic ubiquitous network access means that cloud services are accessed via network using standard protocols. In most cases, this network is the Internet, which must be considered untrusted.

### *I. Data recovery vulnerability:*

The cloud characteristics of pooling and elasticity entail that resources allocated to one user will be reallocated to a different user at a later time. For memory or storage resources, it might therefore be possible to recover data written by a previous user.

### *J. Metering and billing evasion:*

The cloud characteristic of measured service means that any cloud service has a metering capability at an abstraction level appropriate to the service type such as storage, processing, and active user accounts. Metering data is used to optimize service delivery as well as billing. Relevant vulnerabilities include metering and billing data manipulation and billing evasion [6].

## V. THREATS IN CLOUD COMPUTING

A threat, in the context of computer security, refers to anything that has the potential to cause serious harm to a computer system. A threat is something that may or may not happen, but has the potential to cause serious damage. Threats can lead to attacks on computer systems, networks and more. Threats can include everything from viruses, trojans, back doors to outright attacks from hackers. Often, the term blended threat is more accurate, as the majority of threats involve multiple exploits. For example, a hacker might use a phishing attack to gain information about a network and the person breakdown a network. Some common threats are:

### *A. Account or service hijacking:*

An account theft can be performed by different ways such as social engineering and weak credentials. If an attacker gains access to a user's credential, he can perform malicious



CONFERENCE PAPER
Two day National Conference on Innovation and Advancement in Computing
Organized by: Department of IT, GITAM UNIVERSITY Hyderabad (A.P.) India
Schedule: 28-29 March 2014

activities such as access sensitive data, manipulate data, and redirect any transaction. Account or service hijacking is not new. Attack methods such as phishing, fraud, and exploitation of software vulnerabilities still achieve results. Credentials and passwords are often reused, which amplifies the impact of such attacks [17].

### *B. Data scavenging-*

Since data cannot be completely removed from unless the device is destroyed, attackers may be able to recover this data. Data scavenging is the technique of piecing together information from found bits of data. There are two common types of data-scavenging attacks:

- ***a. Keyboard Attacks*** - Data scavenging through the resources that are available to normal system users who are sitting at the keyboard and using normal utilities and tools to glean information.
- ***b. Laboratory Attacks -.*** Data scavenging by using very precise electronic equipment; these are planned, orchestrated attacks.

### *C. Data leakage*:

Data leakage happens when the data gets into the wrong hands while it is being transferred, stored, audited or processed. There are many ways to compromise data. Deletion or alteration of records without a backup of the original content is an obvious example. Unlinking a record from a larger context may render it unrecoverable, as can storage on unreliable media. Loss of an encoding key may result in effective destruction. Finally, unauthorized parties must be prevented from gaining access to sensitive data[4].

### *D. Denial of Service:*

It is possible that a malicious user will take all the possible resources. Thus, the system cannot satisfy any request from other legitimate users due to resources being unavailable. is an attempt to make a machine or network resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of efforts to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet. As clarification, DDoS (Distributed Denial of Service) attacks are sent by two or more person

### *E. Customer-data manipulation:*

Users attack web applications by manipulating data sent from their application component to the server's application.

### *F. Virtual Machine (VM) escape :*

It is designed to exploit the hypervisor in order to take control of the underlying infrastructure. As the name suggests, an exploit that enables VM Escape allows a hacker who compromises a specific virtual server to escalate his attack from the virtual server to take control of the underlying hypervisor [13].

### *G. VM hopping* :

It happens when a VM is able to gain access to another VM. Similar to VM Escape, VM Hopping allows an attack to move from one virtual server to compromise other virtual server on the same physical hardware

### *H. Malicious VM creation:*

An attacker who creates a valid account can create a VM image containing malicious code such as a Trojan horse and store it in the provider repository. The level of background checks providers perform will likely differ compared to how enterprises usually control data center access for support. The staff may not be located in the geographic region (e.g., India versus USA) and privacy laws will be different. Companies need to perform a supplier assessment and outline a level of employee screening.

### *I. Sniffing/Spoofing virtual networks:*

A malicious VM can listen to the virtual network or even use ARP spoofing to redirect packets from other VMs. VMs share the "virtual" hub to communicate network, in which a VM is able to sniff the virtual network by using sniff tool such as "Wireshark" In the route mode, route plays a role as a "virtual switch". The virtual switch uses a dedicated virtual interface to connect each VM. In this case, a VM can do an Address Resolution Protocol (ARP) poofing, redirecting packets to them and be able to sniff packets going to and coming from other VMs[19].

### *J. Shared Technology Vulnerabilities:*

Misconfiguration can be duplicated across an environment where many virtual servers share the same configuration. Understanding patch management and configuration management from the vendor becomes crucial.

## VI. ANALYSIS AND DISCUSSION

Cloud computing offers some exciting opportunities for increased collaboration, working remotely and globally, and cost savings. While there are risks associated with moving to the cloud, the risks are no greater than when services are hosted internally. The main difference is that the cloud presents attackers with a new landscape in which to attack. The rapid growth in field of "cloud computing" also increases severe security concerns. Security has remained a constant issue for Open Systems and internet, because of this security cloud really suffers. Lack of security is the only barrier in wide adoption of cloud computing. Cloud computing is surrounded by many security issues like securing data, and examining the utilization of cloud by the cloud computing vendors. Threats are potentials for vulnerabilities to turn into attacks on computer systems, networks, and more. They can put individual's computer systems and business computers at risk, so vulnerabilities have to be fixed so that attackers cannot infiltrate the system and cause damage.

Cloud Computing leverages many existing technologies such as web services, web browsers, and virtualization, which contributes to the evolution of cloud environments. Therefore,



CONFERENCE PAPER
Two day National Conference on Innovation and Advancement in Computing
Organized by: Department of IT, GITAM UNIVERSITY Hyderabad (A.P.) India
Schedule: 28-29 March 2014

any vulnerability associated to these technologies also affects the cloud, and it can even have significant impacts that cloud security includes. Such as network and other infrastructural vulnerabilities, user access, authentication and privacy and also novel concerns derived from new technologies adopted to offer the adequate resources, services and auxiliary tools.

## VII. CONCLUSION

Cloud Computing is a relatively new concept that presents a good number of benefits for its users however, it also raises some security issues which may slow down its use. This paper focuses on vulnerabilities and threats based on security issues about clouds. In cloud environments traditional security mechanisms will not work well because it is a complex architecture that is composed of a combination of different technologies. There are various security vulnerabilities that the database suffers from and the need to control these vulnerabilities to improve security.

## VIII. REFERENCES


[1] Nelson Gonzalez, Charles Miers, Fernando Red´ıgolo, Marcos Simpl´ıcio, Tereza Carvalho,Mats N¨aslund and Makan PourzandiPg, "A quantitative analysis of current security concerns and solutions for cloud computing", Journal of Cloud Computing: Advances, Systems and Applications, Springer,vol 1,issues 11,Pg no 1-18 2012.

[2] Greg Goth, "Mobile Security Issues Come to the Forefront", 1089-7801, IEEE, published by the IEEE computer society, pg 7-9, 2012.

[3] Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina and Eduardo B Fernandez, "An analysis of security issues for cloud computing",Springer, Journal of Internet Services and Applications,vol 4,issues 5, Page 1- 13, 2013.

[4] Kuyoro S. O., Ibikunle F. & Awodele O, "Cloud Computing Security Issues and Challenges",International Journal of Computer Networks (IJCN), Volume 3,Issue 5 , pg 247-255,2011.

[5] elisa bertino, fellow, and ravi sandhu, "database security—concepts,approaches, and challenges" IEEE transactions on dependable and secure computing, vol. 2, no. 1, 1545-5971,pg 2-19,2005.

[6] Bernd Grobauer, Tobias Walloschek, and Elmar Stöcker "Understanding Cloud Computing Vulnerabilities", copublished by the ieee computer and reliability societies, 1540-7993, pg 50-57, 2011.

[7] Ifeanyi P. Egwutuoha, Daniel Schragl, Rafael Calvo, "A Brief Review of Cloud Computing, Challenges and Potential Solutions", Parallel and cloud computing,Vol. 2 Issues. 1, Pg no. 7-14, Jan. 2013.

[8] Kevin Hamlen, Murat Kantarcioglu, Latifur Khan, "Security Issues for Cloud Computing", 10.4018/jisp. 2010040103, International Journal of Information Security and Privacy,vol 4,issues 2,page no. 39-51, April-June 2010.

[9] John Harauz, Lori M. Kaufman, bruce Potter, "Data Security in the World of Cloud Computing", IEEE ,1540-7993,copublished by the IEEE computer & reliability societies, Pg No 61-64, 2009.

[10] Florin,"Cloud computing security issues", journal of Defense Resources Management,vol 3,issues 2(5),pg 141-148, 2012.

[11] Hashizume, Journal of Internet Services and Applications 2013, vol 4,issues 5

[12] Alexandru Iosup, Simon Ostermann, M. Nezih Yigitbasi, Radu Prodan, Thomas Fahringer, Dick H.J. Epema, "Performance Analysis of Cloud Computing Services for Many-Tasks Scientific Computing", IEEE 1045-9219,VOL. 22, NO. 6,pg 931-945 JUNE 2011.

[13] R Lakshman naik & s. S. V. N. Sarma,"A framework for mobile cloud computing", international journal of computer networking, Wireless and mobile communications (ijcnwmc), Issn 2270-1768,Vol. 3, issue 1,Pg No. 1-12,2013.

[14] Han Qi, Abdullah Gani, "Research on Mobile Cloud Computing: Review,Trend and Perspectives",pg no 1-8,2003.

[15] Atul Gonsai, Rushi Raval, "Mobile Cloud Computing: A Tool for Future", International Journal of Computer Science & Engineering Technology (IJCSET), ISSN: 2229-3347, Vol. 4 No. 07 Pg No.1084-1094, 2013.

[16] A. Muthukumaravel, D S. Prasanna, S. Deepa, "Supporting Various Techniques to optimize and secure application performance in a Cloud Computing Security in a effective manner",International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, Volume 3, Issue 4, pg 778-781 April 2013.

[17] K.Sravani, K.L.A.Nivedita," Effective Service Security Schemes In Cloud Computing",International Journal Of Computational Engineering Research ijcer Vol. 3,Issue 3,Issn 2250-3005, March 2013.




CONFERENCE PAPER
Two day National Conference on Innovation and Advancement in Computing
Organized by: Department of IT, GITAM UNIVERSITY Hyderabad (A.P.) India
Schedule: 28-29 March 2014