ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 2, Issue 3, March 2013

# Cloud Computing: An Architecture, its Security Issues & Attacks

**Kalpana N. Meher, Prof. P. S. Lokhande**

***Abstract* — Every day new things are added in old and those things should have to be preserve for managing the future, new things are always come with the major question that where should keep the things safely? This concept is applicable for both the regular household things as well as the computer data. Day by day storage requirements are increasing but storage space is the same for preserving the data securely. For storing extra data the computer users may invest extra cost on separate storage devices or choose the newly added feature in IT environment is 'Cloud Computing'.**

**Cloud computing has extended feature of the distributed computing; it is a way to increase the capacity or add capabilities without investing in new infrastructure, training new personal or licensing new software.**

**This paper mainly focused on the architecture of cloud computing; survey of the different security issues that has emanate due to the nature of the service delivery module of cloud computing system and type of attacks in cloud computing environment.**

***Keywords* — Cloud computing, cloud security, cloud providers, cloud standards, cloud attacks, software as a service (SaaS), platform as a service (PaaS), infrastructure as a service (IaaS)**

## I. INTRODUCTION

Cloud computing is extended feature of distributed computing, the evolutionary growth of many existing technologies and approaches most basic computing, separates applications and information resources from the underlying infrastructure and mechanisms used to deliver them with the addition of flexible scale and utility mode of allocation. Also the cloud computing enhances collaboration, agility, scale, ability and helps in the cost reduction though optimized and efficient computing.

Because of unpredictable need of data; the storage requirements in personal computing as well as in industries is increased rapidly. Storage requirements can be manageable in small-scale industries or in personal computer; but still they have to manage the storage periodically. Some times needs extra investment on storage.

Cloud describes the use of a collection of service, applications; information and infrastructure comprise of pools of computer, network, information, storage resources. These components can be rapidly arranged, provisioned, implemented and decommissioned also scale up or scale down as per the demand.

By using cloud components, the small and medium business companies are realizing that by investing very small amount in to the cloud they can gain fast access to business applications or can increase their infrastructural resources.

For providing a cloud services cloud computing involves a provider delivering a verity of it enable resources to consumer as a service over internet. At the front end there are client computers and the application require to access the cloud computing system and at the back end there are various computers, servers and data storage systems that creates the 'cloud' services. As these services provided by the cloud user need not have any knowledge or expertise in system that support them, or Indeed any control over those systems.

## II. ARCHITECTURE

### *A. The NIST (National Institute of Standards and Technology) Definition of Cloud Computing*

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.[1]

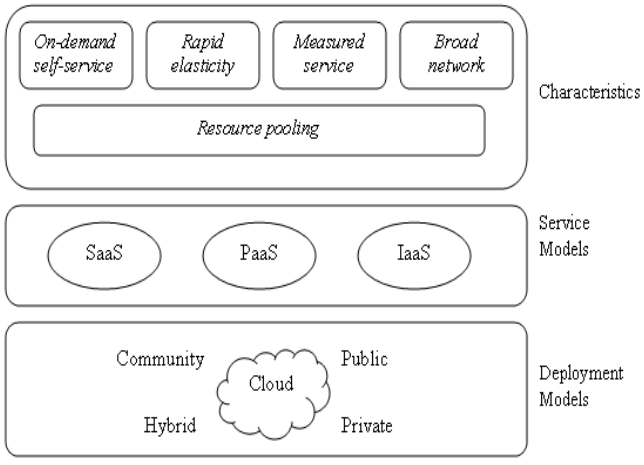


Figure 1 NIST Architecture of cloud

*B. Essential Characteristics cloud architecture*

*(a) On-demand self-service*

As per requirements of consumer, each service provider can unilaterally provide computing capabilities, such as server time, storage network as needed automatically without requiring human interaction.

*(b) Broad network access*

This characteristic allows the variable characteristics over network and access through standard mechanism supported by the thin or thick client platforms.

*(c) Resource Polling*

The provider to server pools all the resources that may be physical or virtual to multiple consumers using a multi tenant model. Pooled resources dynamically assigned or reassigned according to the consumer demand.

Cloud provides sense of location independence in that customer generally have no controls over the exact location of provided resources. Examples of resources including memory, processing, storage and network bandwidth.

*(d) Rapid Elasticity*

On the demand of consumers, capabilities can be elastically provisioned and released in some cases automatically. Cloud has the capabilities to make available unlimitedly and can be appropriate in any quantity, at any time as per the provisioning offer appear from consumer.

*(e) Measured Services*

As per the type of services and duration; the cloud system automatically control and optimize resources. Cloud provides the metering capabilities with the some level of abstraction, these metering capabilities at some level of abstraction appropriate to the type of service (e.g. Storage, Processing, Bandwidth and Active user accounts).

The usage of resources can be monitored, controlled and reported providing transparency for both the provider and consumer of the utilized service.

*C. Service Models*

*(a) Software as a Service (SaaS):*

Instead of investing in licensed software as per the requirement of consumer that may get costly, cloud provides a capability to the consumer is to use provider's applications running on cloud infrastructure. The application can be accessible from various client devices such as either Thin Client i.e. Web browser or a program interface. Due to the capability of the cloud, there is no need to think about computer specification for software installation, servers, operating systems, storage or even individual application capabilities with the possible exception of limited user specific application configuration settings. The consumer does not manage all the above infrastructural controls.

*(b) Platform as a Service (PaaS):*

Applications created by the consumers are deploy on to the cloud infrastructure in this capability provided by the cloud.

Consumer created applications using programming languages, libraries, services and tools supported by the provider for deploying the applications.

Cloud infrastructure including network servers, operating systems or storage neither manage nor controlled by consumer but consumer has control over the configuration settings for the application-hosting environment & the deployed application.[3]

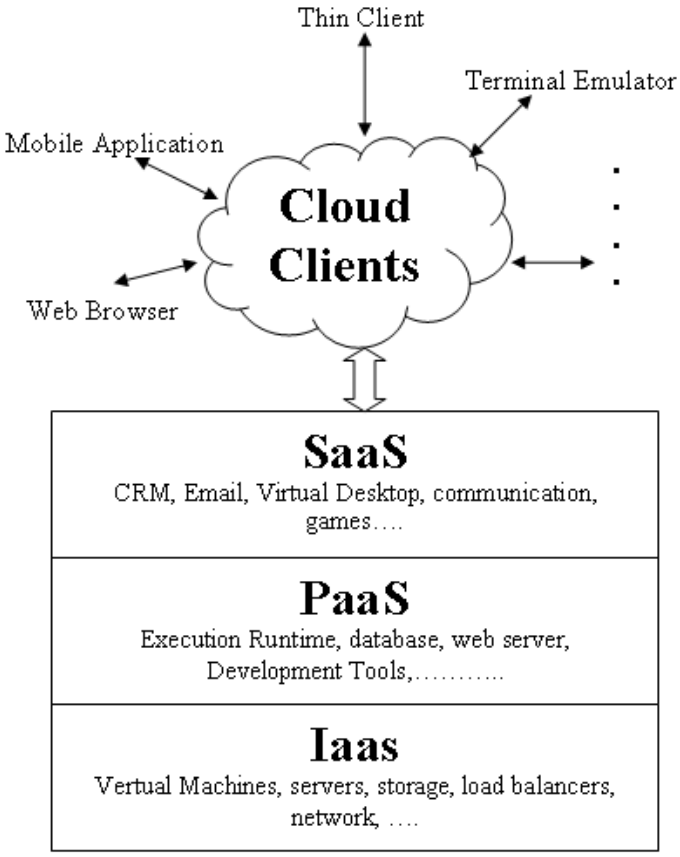


Fig.2 Cloud Srvice Models

*(c) Infrastructure as a Service (IaaS):*

Consumer has a capability to provision processing, storage, networks & other fundamental computing resources where the consumer is able to deploy and sun arbitrary software, which can include operating systems and applications. Underlying cloud infrastructure neither manages nor control by the consumer, but has control over operating systems, storage and deploys applications and possibly also has limited controls of selected networking components (e.g. Host Firewalls).[4]

*D. Deployment Models*

*(a) Private Cloud*

Private cloud computing architecture provides hosted services to limited members of people. It is exclusively use by a single organization includes multiple customers. It may be own, manage and operate by an organization, a third party or combination of them. It may exist on or off premises. It is also known as internal or corporate cloud.

*(b) Community Cloud*

This cloud infrastructure exclusively used by a specific community of consumers from an organization that have shared concerns (e.g. Mission, Security requirements, Policy and Compliance considerations). It may own, manage and operate by one or more of the organization in the community, a third party or some combinations of them and it may exists on or off premises.[1]

*(c) Public Cloud*

Anyone from public can access the cloud in this infrastructure. It may own, manage and operate by a business, academic or government organization or some combinations of them and it may exist on premises of the cloud provider. The benefits of using public cloud services are

- Easy and inexpensive setup because hardware, application and bandwidth cost are covered by the provider
- No wastage of resources because you pay for what you used
- Scalability to meet needs

*(d) Hybrid Cloud*

Hybrid cloud designed as per the consumer request, it is a composition of two or more distinct cloud infrastructures that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability.

Hybrid cloud typically offered in one of two ways; a vendor has a private cloud and forms partnership with a public cloud provider, or a public cloud provider forms a partnership with a vendors that provides private cloud platforms.[6]

Ideally, the hybrid approach allows a business to take advantages of scalability and cost effectiveness that a public cloud community environment offers without explosion mission critical applications and data to third party vulnerability.

## III SECURITY ISSUES IN SERVICE MODEL

*A. Security in SaaS*

In SaaS Client is depending on the provider for proper security measures. As we know multiple users are connected to cloud the provider has to keep multiple data hidden from each other. Because of the same, it is so difficult to user to insure the right security measures are in place and assure for the application which will be available whenever it needed.[14]

While developing and deploying a SaaS application the following security element should have to be carefully considered which are:

- Data Segregation
- Data security
- Data integrity
- Data access
- Network security
- Authentication
- Authorization
- Data Locality
- Web application

*(a)Data Security*

Traditionally all the applications are developed in the premises of the enterprise, because of limited boundary access of application it is easy to make software secure physically, logically, providing personal security to the software and securing application data by the access control policies.

However, data resides in SaaS model the limited boundary crosses the enterprise and enterprise data is share outside the enterprise boundary, which is at the SaaS vendor. Now the SaaS vendor provides security of data. Because of multiple user vendor must adopt the additional security checks for ensure the data security and prevent unauthorized data access due to security vulnerabilities. For securing data strong encryption techniques are used and different authorized access control mechanisms are implemented.

For security check at the SaaS vendor the following assessments tests are used:

- Hidden field manipulation
- Insecure storage
- Cookie manipulation
- Cross site scripting
- Access control weakness
- Insecure configuration
- Cross site request forgery
- OS and SQL injection clause

During test if any vulnerability detected this test can be avoid access to sensitive enterprise data and which causes a financial lost to enterprise.

*(b)Network Security*

In cloud, the strong network connection is a backbone of the cloud infrastructure. Whenever enterprise using a SaaS development model the processing sensitive data is obtained from enterprise processed by the SaaS application and stored at the SaaS vendor end. For this, data flow network is needed. For preventing leakage of sensitive

data network should be highly secured. For Security, network strong network traffic encryption techniques are used such as Secured Socket Layer (SSL) and Transport Layer Security (TLS).

In whatever extends,

- Network penetration And packet analysis
- Insecure SSL trust configuration
- Session management weaknesses

During these test if any vulnerability detected, test can be exploited to hijack active session, gain access to user credentials and sensitive data.

*(c) Data Locality*

By using cloud environment customer can process there business data by using applications provided by the SaaS. Because of virtual locality of cloud customer can't predict the actual location of data in network. Sometimes it may be issue because of business policies and rules of various countries for data privacy. Also the locality of data decides level of abstraction which is also important in much enterprise architecture.[7]

*(d) Data Integrity*

For storage of data, database systems are used. In standalone system data integrity is easily maintained; because of single database. In standalone database, system manages data integrity through database constraints and transactions. All the database transactions should have to follow the ACID (atomicity, consistency, isolation and durability) which ensures the data integrity.

In cloud distributed systems are used, multiple databases are located on various locations instead of same location along with multiple applications are together used for data storage. Because of distributed database, multiple users can simultaneously access the data and multiple transactions are simultaneously performed. Because of multiple transactions over multiple data sources it is need to be handle correctly without misplaced the any single bit of data; central global transaction manager does this. For integrate the data in distributed network each application should be able to participate in global transaction via a resource manager. This can be achieved using two-phase commit protocol.

*(e) Data Segregation*

One of the characteristic of cloud is multi-tendency in which multiple users can store their data using applications provided by SaaS. Because of multiple users, store data at same location there might be a more chances to get access to any other user's data by another. These loopholes in application can make possible that type of intrusion either by hacking or by injecting client code into SaaS system. By injecting masked code into the application written by the client, if the code gets executed by application without verification, then there is high potential of intrusion into others data. For the same SaaS model has to restrict or ensure a clear boundary for each users data.[15] This boundary is ensures at physical as well as logical level. Provider has to provide intelligent services to segregate the data from different users. Application vulnerabilities give chance to the malicious users by the own coded parameter they can bypass the security checks and other users sensitive data can be access by other tenants. Data segregation of the SaaS vendor can be test and validate by following assessments:

- SQL injection flaws
- Data validation
- Insecure storage

*(f) Data Access*

Each user has different rights in organization for data access. Data access is mainly focus on those security policies provided to the user for data access. In traditional systems, small business organization sets their own security policies for the set of data which employee can have. These access policies to access the data sets are decided by organizations. There unauthorized users should reflect security policies in cloud to avoid intrusion of data.

Cloud providers should restrict organizational data boundary for distinguish between multiple organizational data.

To handle the security policies forwarded by the organizational the cloud SaaS model should be flexible.

*(g) Authentification and authorization*

In small and medium business organizations, Light Weight Direction Access protocol (LDAP) or Active Directional scheme used for maintaining employee information. While most of the organizations now adapt to the SaaS, they most likely to use AD scheme tool for managing users. Now by using SaaS all employee information shared outside the company environment. SaaS providers only provides the service they are dependent on the SaaS customer for remove / disable accounts as per employee leave the organization & create / enable accounts as per new joining.

*(h) Data confidentiality issue*

Today the bulk of data is shared via internet of it is store at remote places through cloud. Cloud allows sharing data with many other services such as data storage sites, video sites, tax preparation sits, personal health record websites and list go on. This complete information may handle by a single cloud provider or many providers. Whenever an individual, a business, a government agency or any other entity shares information in cloud, the first question arises is about privacy or confidentiality of the data. Some of the issues related to the data confidentiality as discussed below:

- For some categories of cloud users and for some type of information, whenever a user discloses information to a cloud provider the status of information or user is

changed, some privacy or confidentiality rights, obligations may change.

- Because of unpredictable location for data storage, information in cloud may have significant effects on the privacy and confidentiality protections of information and on the privacy obligations of those who process or store the information.
- For monitoring or examine criminal activities the cloud provider may access the user information for collecting the evidence which oblige the cloud laws.
- Cloud computing has significant implication for the privacy of personal information as well as for the confidentiality of business and governmental information.
- Data mirroring is done for recovery of data in accidental loss of it; that is information in cloud may have more than one legal location at the same time with differing legal consequences.
- Cloud allows storing of the data outside organizational boundary. The location of stored data may add legal uncertainties to access the status of information, which make it difficult.
- As per the variations in terms of services and privacy policies established by cloud providers, user's privacy and confidentiality risks varies significantly.

*i) Web application*

By using SaaS model, the commercially available software deployed beyond the organizational boundaries and customers access that software via internet. This characteristic includes network-based access to, and management of software and managing activity from central location and customer access the application remotely via web. Because of application, access via web if any security holes in web application it causes the vulnerability to the SaaS application. The traditionally used network security solutions such as network firewalls, network intrusion detection system (IDS/IPS) cannot adequately address the problem of web applications. Security risks added with the web applications cannot be defended effectively at network layer and do require application level defense. Because of tightly coupled relationship between SaaS model and web application most of the security threads are inherently added with SaaS model.

*B. Security in PaaS*

In PaaS, the provider might give some control to the people to build applications on top of the platform. But any security below the application level such as host and network intrusion prevention will still be in the scope of the provider and the provider has to offer strong assurances that the data remains inaccessible between applications. PaaS is intended to enable developers to build their own applications on top of the platform. As a result it tends to be more extensible than SaaS, at the expense of customer-ready features. This tradeoff extends to security features and capabilities, where the built-in capabilities are less complete, but there is more flexibility to layer on additional security.

Applications sufficiently complex to leverage an Enterprise Service Bus(ESB) need to secure the ESB directly, leveraging a protocol such as Web Service(WS) Security[8]. The PaaS environments never have the ability to segment the ESBs. The effectiveness of the application security programs can be access through in place metrics. Among the direct application, security specific metrics available are vulnerability scores and patch coverage. Quality of application coding can be indicating by those metrics. Attention should be paid to how malicious actors react to new cloud application architectures that obscure application components from their scrutiny. Hackers are likely to attack visible code, including but not limited to code running in user context. They are likely to attack the infrastructure and perform extensive black box testing. The vulnerabilities of cloud are not only associated with the web applications but also vulnerabilities associated with the machine-to-machine Service- Oriented Architecture(SOA) applications, which are increasingly being deployed in the cloud.

*C. Security in IaaS*

With IaaS the developer has better control over the security as long as there is no security hole in the virtualization manager. Also, though in theory virtual machines might be able to address these issues but in practice there are plenty of security problems.[9] The other factor is the reliability of the data that is stored within the provider's hardware. Due to the growing virtualization of 'everything' in information society, retaining the ultimate control over data to the owner of data regardless of its physical location will become a topic of utmost interest. To achieve maximum trust and security on a cloud resource, several techniques would have to be applied.[10] The security responsibilities of both the provider and the consumer greatly differ between cloud service models. Amazon's Elastic Compute Cloud(EC2).[11] infrastructure as a service offering, as an example, includes vendor responsibility for security up to the hyper visor, meaning they can only address security controls such as physical security, environmental security, and virtualization security. The consumer, in turn, is responsible for the security controls that relate to the IT system including the OS, applications and data.[12]

## IV. CLOUD COMPUTING ATTACKS

### A. Distributed Denial of Service Attack

Many users sheared a common medium of data access in cloud infrastructure, because of the same cloud is more vulnerable to DoS attacks. The common sharing medium makes DoS attacks much more damaging. Whenever high workload is noticed on the flooded service, Cloud computing operating system starts to provide more computational power to cope with the additional work load. By providing more computational power cloud system trying to work against the attacker till the server hardware boundaries but actually to some extends even supports attacker by enabling them to do most possible damage.

### B. Side Channel Attacks

With the growth of Cloud Computing Environment, one of the service module of cloud computing which software-as-a-service (SaaS) is in also rise with web 2.0 applications. Software-as-a-service has also significantly raised the possibility of side-channel attacks on the web, even when transmissions between a web browser and server are encrypted (e.g., through HTTPS or WiFi encryption), according to researchers from Microsoft Research and Indiana University[13]. By placing, a malicious virtual machine in close proximity to a target cloud server an attacker then launches the side channel attack. Those kinds of attacks are mainly part of security thread targeting system implementation of cryptographic algorithms.

### c) Cross side scripting

This type of attack is occurred when user enters a correct URL of web side and hacker on the other site redirect the user to its own website and hack the credential.

Cross-Site Scripting (XSS) attacks occur when:

1. Data enters a Web application through an untrusted source, most frequently a web request.
2. The data is included in dynamic content that is sent to a web user without being validated for malicious code.[13]

### d) Cloud Malware Injection Attack

Cloud Malware Injection Attack aims to inject a spiteful service, application or virtual machine in between authorized communication medium tries to damage the cloud infrastructure. Once attacker succeeds enter spiteful software in cloud structure as he cares for the spiteful software as legitimate request. If authorized user asks for spiteful software which is shown as legitimate, by accessing those software virus enters in cloud infrastructure and tries to damage user related information. Whenever user gives request for this spiteful software uploaded virus is spread throw internet and tries to infect more and more files by replicating itself or by external attachment. Finally infection flooded in to the cloud structure and cloud infrastructure may majorly damages if infection is so long undetected.

### e) Authentication Attack

Most frequently targeted part of cloud is Authentication which is weakest in hosted and virtual service. Methods and mechanisms used for secure the authentication are frequently targeted by the attacker. As per architectural configuration of cloud infrastructure cloud provide types of service models SaaS, PaaS and IaaS out of those three only IaaS offering these kinds of information protection and data encryption. For securing data communication, most suitable architecture is IaaS for highly confidential data for any enterprise. In addition, the user side (enterprises) to instead of the service providers for those data belonged to the enterprises but stored on the service provider's side must authorize the authorization of data process or management. Various forms of secondary authentication (such as site keys, virtual keyboards, shared secret questions, etc.) are used by some financial institutions to protect the system by more difficult for popular phishing attacks but still some of them uses simple most user-facing services which is username and password type of knowledge-based authentication.

### f) Man in the Middle Attack

It is also very crucial attack, whenever to authorized parties are communicating with each other attacker places himself between two users. This type of attacks can be possible if configuration of Secure Socket Layer (SSL) is not properly done.

## V. CONCLUSION

Evolution of cloud computing opened the doors to achieve the growth of many existing technologies. An e-commerce industry, which is having online presence and focus on customer service need more scalable architecture. Cloud has the capability to accommodate all the features that are in demand. As the use of technology increases, obviously they are prone to have various attacks. These attacks pose threat to the integrity of cloud system. In this paper we tried to address various security issues and concerns may arise. There is a need to address the security issues in service model, in development model to defend against the various attacks on cloud computing formulation of strong designing with good architecture is required. Various attacks such as cross side scripting, SQL injection, authentification attack may be avoided with strong foundation of full proof architecture designing.

## VI. REFERENCES

[1] Peter Mell and Timothy Grance, "The NIST Definition of Cloud Computing," Special Publication 800-145, September 2011, pages2—3,http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf. Short NIST document defining cloud computing models and services.

[2] "NIST Cloud Computing Reference Architecture," Special Publication 500-292, September 2011, pages 15—17, http://collaborate.nist.gov/twiki-cloud-computing/pub/CloudComputing/ReferenceArchitectureTaxonomy/NIST_SP_500-292_-_090611.pdf. NIST document describing security expectations in a cloud computing environment.

[3] By John Panagulias, "Cloud Computing: Platform As A Service Defined", Wednesday, August 5, 2009, http://cloud.kendallsquare.com/article/cloud-computing-platform-as-a-service-defined

[4] Ian O'Rourke,"Being Too Glib About Cloud" , October, 20012, http://www.elucidateit.net/?p=608

[5] Defense Engineering, Inc.Partnering Technology with Business Needs, "Cloud Computing ,http://www.defenginc.com/solutions/cloud_computing

[6] Cloud Computing Ireland,"Hybrid Cloud", Nov 2012, http://cloudireland.ie/?page_id=9

[7] Pradnesh Rane, Persistent System White Paper, "Securing SaaS Applications A cloud security perspective for Application Providers"

[8] Oracle Wiring through an Enterprise Service Bus, 2009 /http://www.oracle.com/technology/tech/soa/mastering-soa-series/part2.html [accessed on:19Feb- February 2010].

[9] Gajek S, Liao L, Schwenk J. Breaking and fixing the inline approach. In: SWS '07, Proceedings of the ACM workshop on secure web services. New York, NY, USA: ACM; 2007. p. 37–43.

[10] Descher M, Masser P, Feilhauer T, Tjoa AM, Huemer D. Retaining data control to the client in infrastructure clouds. In: International conference on availability, reliability and security, ARES '09, 2009, p. 9–16.

[11] Amazon. Amazon Elastic Compute Cloud (EC2), 2010 /http://www.amazon.com/ ec2/S [accessed: 10December2009].

[12] Seccombe A, Hutton A, Meisel A, Windel A, Mohammed A, Licciardi A, et al. Security guidance for critical areas of focus in cloud computing, v2.1. Cloud Security Alliance, 2009, 25 p.

[13] Differential Power Analysis, P. Kocher, J. Jaffe, B. Jun, appeared in CRYPTO '99.https://www.owasp.org/index.php/Cross-site_Scripting_(XSS) retrieved January 12, 2013

[14] P S Lokhande, D R Ingle, B B Meshram , "Consideration of critical elements, Active-X security concerns and risks for web development" RTSCIT-09, Jan 9-10, 2010, IEEE Infrastructural conference on recent trends in soft computing & information technology.

[15] P S Lokhande, B B Meshram , "Learning from the past intrusion attacks: Digital Evidence collection to make E-commerce system more secure" ; International conference – Interactive Computer Aided Learning (ICL 2009), September 23-25,2009, Page 824 Villach, Austria.

**Kalpana N. Meher**

Perusing M.E. Computer Engineering from MGM's College of Engineering and Technology, Navimumbai, India. Working as Lecturer at MGM's College of Engineering and Technology, Navimumbai, India. Having 4 years of Teaching Experience.

**Prof. P S Lokhande**

Working as Head Dept of IT at MGM's College of Engineering and Technology, Navimumbai, India. Having 14 years of Teaching and Industry Experience. Published more than 20 paper in various National, International conferences and Journals. His basic area of interest is Web Engineering, E-Commerce, E-Commerce Security, Digital Evidence Collection etc.