# ANALYSIS OF SECURITY IN DIFFERENT CLOUD SERVICES

**Prince Gupta[1], Prof. Dr. Jayant Shekhar[2]**

*[1]Department of Computer Science & Engineering, [2]Director*

*Subharti Institute of Technology & Engineering (Meerut)*

## ABSTRACT

*There is a growing trend of using cloud environments for ever growing storage and data processing needs. However, adopting a cloud computing paradigm may have positive as well as negative effects on the data security of service consumers. Cloud Computing presents an added level of risk because essential services are often outsourced to a third party, which makes it harder to maintain data security and privacy, support data and service availability, and demonstrate compliance. In this paper, we describe various service and deployment models of cloud services and identify major security issues.*

***Keywords: Cloud Computing, Security Issues, Security Threats, Attackers and Risk in Cloud Computing.***

## I. INTRODUCTION

As per the definition provided by the National Institute for Standards and Technology (NIST), "cloud computing is a model for enabling 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".

Cloud Computing enables 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.

While moving from traditional local computing paradigm to the cloud computing paradigm, new security and privacy challenges emerge because of the distributed nature of cloud computing. Some of these security vulnerabilities leave open doors, which stem from the existing computing models; and some of them, inherent from cloud-based models. As a result, malicious users force these doors to attack the system, and they attack on end-users' private data; processing power, bandwidth or storage capacity of the cloud network. Cloud computing organizations have to provide a high quality service and protect the users' sensitive data. To prevent these attackers, firewall mechanism and/or Intrusion Detection System (IDS) are effective solutions to resist them. They can provide additional protection mechanisms on the cloud systems' distributed environments. IDS can identify suspicious activities by monitoring network traffic changes, configuration of the system, logs files, and actions of end-users. When such a suspicious event is detected, IDS sends an alert message to a person or monitoring console to trigger some actions for preventing these attacks. In this paper, it is aimed to provide

definitions and properties of different attack types in cloud computing and to introduce intrusion detection and prevention models to resist these types of Security.

## II. ARCHITECTURE OF CLOUD COMPUTING

### 2.1 Specification of Cloud Computing

There are five essential characteristics of Cloud Computing :

On-demand Service: A user can be provided by oneself with computing abilities such as server time and network storage whenever it is needed without any provider and human interaction.

Wide Network Accessibility: Cloud computing has to be held abilities, which are standardized on the network and can be accessed by different kinds of devices (mobile phones, tablets, laptops, workstations etc.).

Resource Pool: The provider's computing resources such as a storage area, processing power, network bandwidth and memory must be in a physical or virtualized pool, can be allocated dynamically or according to demand of the end users and can be served multitenant at the same time. Users do not need to have any authority on the resources and do not know where the resources are.

Rapid Elasticity: Opportunities and abilities have to be provided, unserved and scaled interior or exterior in an elastic way. These services are introduced to end-users generally unlimited and provided as much as the requests.

Regular Service: Among to services, which are provided in cloud computing systems; resource usage can be monitored, controlled, reported; resource usage amounts can be determined and providers can serve these to users transparently.

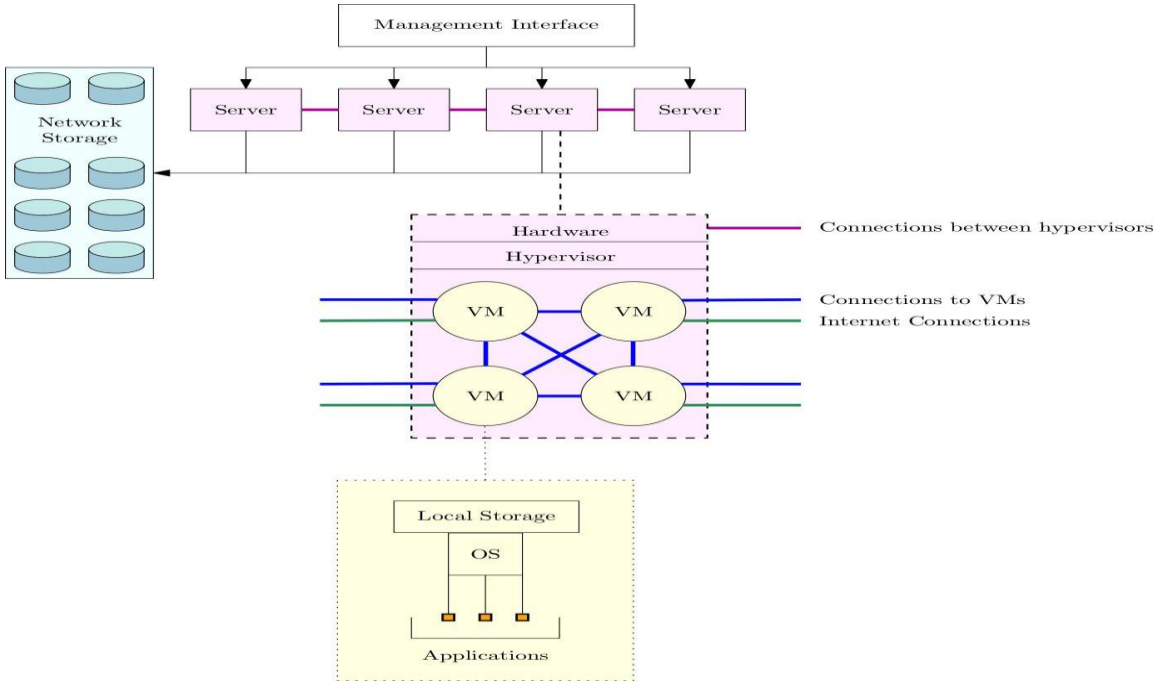


**Fig. 1: The Standard Architecture of Cloud Computing Infrastructure. Note This Same Infrastructure Can Be Used to Provide Infrastructure as a Service (Iaas), Platform as a Service (Paas), And Software as a Service (Saas).**

While every type of cloud service has these characteristics at its core, the various service models differ drastically in both form and function. We focus on three main service models: infrastructure as a service, software as a service, and platform as a service. Infrastructure as a service (IaaS) is the most basic service model for delivering cloud capabilities. Typically the consumer is given access to processing, storage, networks, and other resources necessary to run and/or deploy arbitrary software in a form that is close to having on-demand access to an arbitrary number of network-connected servers. An arbitrary number of "virtual servers" are multiplexed onto the providers' fixed number of physical hosts, generally using virtual machines (VMs) running on hypervisors.

An example of IaaS is Amazon's Elastic Compute Cloud (EC2) service: the consumer is given access to an EC2 "instance" (a VM) for a period of time to be used as a resource for whatever purpose the consumer wishes. Another example of IaaS would be Amazon's S3 service: the consumer is given access to low-latency data storage that is accessible from any location via the Internet.

With Platform as a Service (PaaS), the consumer has access to computational platforms including operating systems, programming language execution environments, databases, web servers, etc. These combined services are mainly used by developers who use the provided platform to run and test their software solutions on a cloud infrastructure without the overhead of maintaining the underlying software or hardware. Google App Engine [2] is an example of PaaS.

### 2.2 Structure of Cloud Computing Architecture

Cloud computing architecture contains some types of actors, which can be either an individual or an organizational unit who attend cloud services/tasks. NIST defines five main actors :

Consumer uses the cloud computing service and can be either an individual or an organizational unit. A consumer chooses the most appropriate service or services, which are provided by the cloud provider. Besides, the services are charged against to the agreement that is signed between the consumer and the provider.

Provider is an entity that is responsible for developing resources and services, which are used by individuals, organizations or consumers. Provider manages software, platform or infrastructure that is needed by consumers, and it builds obligatory technical infrastructure and provides specified service levels (mostly trust and security levels).

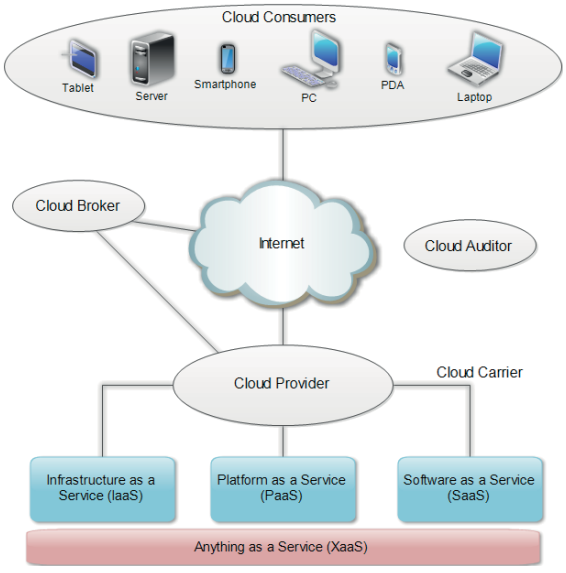

**Fig. 2 Service Models and Actors in Cloud Computing**

Auditor inspects whole information technology processes, performance and security issues independently within predefined criteria. Auditor must be a third party and can be either an individual or an organizational unit.

Broker: Manageability of cloud systems is very complicated because of its nature. Consumers can use cloud services not only get in contact with the provider directly but also broker. Broker organizes the connection between provider and consumer, and also manages performance and availability of the system.

Carrier realizes connection, communication and transfers between provider and consumer, and also it enables consumers can access to the services over communication infrastructure and other devices such as desktops, laptops or any mobile devices.

Distribution of the cloud services can be realized via network and communication infrastructure or communication agents, which have high storage capacity opportunities.

### 2.3 Service Models in Cloud Computing

About the services, which are served over cloud computing systems there is a definition as Anything as a Service (XaaS). The word anything defines the service, and it can take part as the type of the service like; Communication as a Service (CaaS), Network as a Service (NaaS) or Monitoring as a Service (MaaS). However, there are three fundamental service types to describe and define the service contents. They are Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) [5]. These three main service models/actors of the cloud computing are shown in Figure 1 and detailed as follows.

Infrastructure as a Service (IaaS): With this ability, users can access processing power, storage area, network and other computing resources through opportunity and ability of the provider, also use every kind of software including operating system (OS) and applications. Users are not responsible for controlling and managing the cloud infrastructure, they only have authority on OS, storage, distributed software and network components which are going to be used.

Platform as a Service (PaaS): Users can develop and run software over cloud computing infrastructure via programming languages, libraries, services and with the tools that are supported by provider. Users are not responsible for controlling and managing network, server, OS and storage areas which are founded in cloud computing infrastructure, they can only interfere limited configuration changes.

Software as a Service (SaaS): All the infrastructure, by the provider. Users can access to service based applications via different devices and interfaces as thin clients and network browsers. There are only some limited configurations authorities over the service based applications that can be made by users.

## III. SECURITY IN CLOUD COMPUTING

This section addresses the core theme of this paper, i.e., the security and privacy-related challenges in cloud computing. There are numerous security issues for cloud computing as it encompasses many technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management. Therefore, security issues for many of these systems and technologies are applicable to cloud computing. For example, the network that interconnects the systems in a cloud has to be secure. Furthermore, virtualization paradigm in cloud computing leads to several security concerns. For example, mapping the virtual machines to the physical machines has to be carried out

securely. Data security involves encrypting the data as well as ensuring that appropriate policies are enforced for data sharing. In addition, resource allocation and memory management algorithms have to be secure. Finally, data mining techniques may be applicable for malware detection in the clouds – an approach which is usually adopted in intrusion detection systems (IDSs).

There are six specific areas of the cloud computing environment where equipment and software require substantial security attention (Trusted Computing Group's White Paper, 2010). These six areas are: (1) security of data at rest, (2) security of data in transit, (3) authentication of users/applications/ processes, (4) robust separation between data belonging to different customers, (5) cloud legal and regulatory issues, and (6) incident response.

For securing data at rest, cryptographic encryption mechanisms are certainly the best options. The hard drive manufacturers are now shipping self-encrypting drives that implement trusted storage standards of the trusted computing group (Trusted Computing Group's White Paper, 2010). These self-encrypting drives build encryption hardware into the drive, providing automated encryption with minimal cost or performance impact. Although software encryption can also be used for protecting data, it makes the process slower and less secure since it may be possible for an adversary to steal the encryption key from the machine without being detected.

Encryption is the best option for securing data in transit as well. In addition, authentication and integrity protection mechanisms ensure that data only goes where the customer wants it to go and it is not modified in transit. Strong authentication is a mandatory requirement for any cloud deployment. User authentication is the primary basis for access control. In the cloud environment, authentication and access control are more important than ever since the cloud and all of its data are accessible to anyone over the Internet. The trusted computing group's (TCG's) IF-MAP standard allows for real-time communication between a cloud service provider and the customer about authorized users and other security issues. When a user's access privilege is revoked or reassigned, the customer's identity management system can notify the cloud provider in real-time so that the user's cloud access can be modified or revoked within a very short span of time.

### 3.1 Threat Vectors- What to Worry About in Security

How does the landscape of threats to security and privacy change as organizations shift to cloud-based systems, storage and applications? New vectors are introduced, and old ones can be exploited in new ways. In the following, we briefly discuss some of the threats, highlighting what is genuinely different and new in a world of cloud hosting, what threats are similar to the dominant model of local applications and in-house IT management but will manifest in different ways.

Before categorizing new threats, it is important to acknowledge that the structure of many cloud architectures can mitigate or negate some current security threats. If data are kept in the cloud, for example, then a lost or stolen laptop is much less likely to put sensitive information at risk. Standardized interfaces could make security management easier (ENISA, 2009), while the scale of a provider hosting many parties can generate more information for better threat monitoring. Centralized security management and monitoring can be more effective than local efforts by IT professionals with limited security experience. Still, moving critical systems and data to a network-accessible framework introduces new classes of vulnerabilities in and of itself, by creating new surfaces to attack and new interfaces to exploit. When those network resources are built on systems, platforms and applications shared with others, another set of threat vectors is introduced. The control mechanisms itself

can be attacked, breaking down isolation between users, potentially allowing another user to access data or resources. Even without direct access, a providers' other clients can learn valuable transaction data about an organization .The shared architecture also puts a cloud user at risk from other cloud users if their bad behavior draws attention from either law enforcement or media, leading to hardware seizure or bad publicity (Molnar & Schechter, 2010). Some threat vectors are not new to cloud, but have somewhat different dynamics. In classic IT architecture, PCs inside the organization may be at risk of compromise through a host of attack vectors exploiting local applications such as browses or documents viewers. If less data is stored locally, less is immediately at risk, but now the attacker could compromise credentials to gain access to the user's cloud privileges. A compromise to an entire Gmail database probably began with a compromised PC.

Similarly, in an attack on the Twitter management team in 2009, a compromised email password led to exposure of a wide range of other important documents in other cloud infrastructures. Shared authentication tokens can lead to brittle defenses.

Organizations must be careful to safeguard data as they move it around their organization, even without the benefit of cloud computing. When they no longer need data, it must be properly deleted, or else risk leaking sensitive data to the outside. When relying on a cloud service to handle data, appropriate care must be made to arrange for appropriate security management practices, such as encryption and appropriate deletion.

### 3.2 Security Issues in Cloud Computing

Security in the cloud is achieved, in part, through third party controls and assurance much like in traditional outsourcing arrangements. But since there is no common cloud computing security standard, there are additional challenges associated with this. Many cloud vendors implement their own proprietary standards and security technologies, and implement differing security models, which need to be evaluated

on their own merits. In a vendor cloud model, it is ultimately down to adopting customer organizations to ensure that security in the cloud meets their own security polices through requirements gathering provider risk assessments, due diligence, and assurance activities (CPNI Security Briefing, 2010).

Thus, the security challenges faced by organizations wishing to use cloud services are not radically different from those dependent on their own in-house managed enterprises. The same internal and external threats are present and require risk mitigation or risk acceptance. In the following, we examine the information security challenges that adopting organizations will need to consider, either through assurance activities on the vendor or public cloud providers or directly, through designing and implementing security control in a privately owned cloud. In particular, we examine the following issues:

• The treats against information assets residing in cloud computing environments.
• The types of attackers and their capability of attacking the cloud.
• The security risks associated with the cloud, and where relevant considerations of attacks and countermeasures.
• Emerging cloud security risks.
• Some example cloud security incidents.

### 3.3 Cloud Security Threats

The threats to information assets residing in the cloud can vary according to the cloud delivery models used by cloud user organizations. There are several types of security threats to which cloud computing is vulnerable.

Table 1 provides an overview of the threats for cloud customers categorized according to the confidentiality, integrity and availability (CIA) security model and their relevance to each of the cloud service delivery model.

**Table 1: A List of Cloud Security Threats**

| Threat | Description |
|---|---|
| Confidentiality | |
| Insider user threats:<br><br>• Malicious cloud provider user<br>• Malicious cloud customer user<br>• Malicious third party user<br>(Supporting either the cloud provider or customer organizations) | The threat of insiders accessing customer data held within the cloud is greater as each of the delivery models can introduce the need for multiple internal users:<br><br>SaaS – cloud customer and provider administrators<br>PaaS- application developers and test environment managers<br>IaaS- third party platform consultants |
| External attacker threats:<br>•Remote software attack of cloud infrastructure.<br>•Remote software attack of cloud Applications.<br>•Remote hardware attack against the cloud.<br>•Remote software and hardware attack against cloud user organizations' endpoint software and hardware.<br>• Social engineering of cloud provider users, and cloud customer users. | The threat from external attackers may be perceived to apply more to public Internet facing clouds, however all types of cloud delivery models are affected by external attackers, particularly in private clouds where user endpoints can be targeted. Cloud providers with large data stores holding credit card details, personal information and sensitive government or intellectual property, will be subjected to attacks from groups, with significant resources, attempting to retrieve data. This includes the threat of hardware attack, social engineering and supply chain attacks by dedicated attackers. |
| Data leakage:<br><br>• Failure of security access rights across multiple domains.<br>• Failure of electronic and physical transport systems for cloud data and backups | A threat from widespread data leakage amongst many, potentially competitor organizations, using the same cloud provider could be caused by human error or faulty hardware that will lead to information compromise. |
| Integrity | |

| | |
|---|---|
| Data segregation:<br>• Incorrectly defined security perimeters<br>• Incorrect configuration of virtual machines and hypervisors | The integrity of data within complex cloud hosting environments such as SaaS configured to share computing resource amongst customers could provide a threat against data integrity if system resources are effectively segregated. |
| User access:<br>• Poor identity and access management Procedures. | Implementation of poor access control procedures creates many threat opportunities, for example that disgruntled ex-employees of cloud provider organizations maintain remote access to administer customer cloud services, and can cause intentional damage to their data sources. |
| Data quality:<br>• Introduction of faulty application or infrastructure components | The threat of impact of data quality is increased as cloud providers host many customers' data. The introduction of a faulty or misconfigured component required by another cloud user could potentially impact the integrity of data for other cloud users sharing infrastructure. |
| Availability | |
| Change management:<br>• Customer penetration testing impacting other Cloud customers.<br>• Infrastructure changes upon cloud provider, customer and third party systems impacting Cloud customers. | As the cloud provider has increasing responsibility for change management within all cloud delivery models, there is a threat that changes could introduce negative effects. These could be caused by software or hardware changes to existing cloud services. |
| Denial of service threat:<br>• Network bandwidth distributed denial of Service.<br>• Network DNS denial of service.<br>• Application and data denial of service | The threat of denial of service against available cloud computing resource is generally an external threat against public cloud services. However, the threat can impact all cloud service models as external and internal threat agents could introduce application or hardware components that cause a denial of service. |
| Physical disruption: | |

| | |
|---|---|
| • Disruption of cloud provider IT services through physical access<br>• Disruption of cloud customer IT services through physical access<br>• Disruption of third party WAN providers Services | The threat of disruption to cloud services caused by physical access is different between large cloud service providers and their customers. These providers should be experienced in securing large data center facilities and have considered resilience among other availability strategies. There is a threat that cloud user infrastructure can be physically disrupted more easily whether by insiders or externally where less secure office environments or remote working is standard practice. |
| Exploiting weak recovery procedures:<br>• Invocation of inadequate disaster recovery or business continuity processes. | The threat of inadequate recovery and incident management procedures being initiated is heightened when cloud users consider recovery of their own in house systems in parallel with those managed by third party cloud service providers. If these procedures are not tested then the impact upon recovery time may be significant. |

### 3.4 Types of Attackers in Cloud Computing

Many of the security threats and challenges in cloud computing will be familiar to organizations managing in house infrastructure and those involved in traditional outsourcing models. Each of the cloud computing service delivery models' threats result from the attackers that can be divided into two groups as depicted in Table 2.

**Table 2: A list of Attacks on Cloud Computing Environments**

| | |
|---|---|
| Internal Attackers | An internal attacker has the following characteristics:<br>a) Is employed by the cloud service provider, customer or other third party provider organization supporting the operation of a cloud service.<br>b) May have existing authorized access to cloud services, customer data or supporting infrastructure and applications, depending on their organizational role.<br>c) Uses existing privileges to gain further access or support third parties in executing attacks against the confidentiality integrity and availability of information within the cloud service. |
| External Attackers | An external attacker has the following characteristics:<br>a) Is not employed by the cloud service provider, customer or other third party provider organization supporting the operation of a cloud service.<br>b) Has no authorized access to cloud services, customer data or supporting infrastructure and applications.<br>c) Exploits technical, operational, process and social engineering vulnerabilities to attack a cloud service provider. |

Although internal and external attackers can be clearly differentiated, their capability to execute successful attacks is what differentiates them as a threat to customers and vendors alike. In the cloud environment, attackers can be categorized into four types: random, weak, strong, and substantial .Each of these categories is based on ability to instigate a successful attack, rather than on the type of threat they present (i.e., criminal, espionage or terrorism):

• Random- The most common type of attacker uses simple tools and techniques. The attacker may randomly scan the Internet trying to find vulnerable components. They will deploy well known tools or techniques that should be easily detected.

• Weak – Semi-skilled attackers targeting specific servers/cloud providers by customizing existing publicly available tools or specific targets. Their methods are more advanced as they attempt to customize their attacks using available exploit tools.

• Strong – Organized, well-financed and skilled groups of attackers with an internal hierarchy specializing in targeting particular applications and users of the cloud. Generally this group will be an organized crime group specializing in large scale attacks.

• Substantial – Motivated, strong attackers not easily detected by the organizations they attack, or even by the relevant law enforcement and investigative organizations specializing in e Crime or cyber security. Mitigating this threat requires greater intelligence on attacks and specialist resources in response to detection of an incident or threat.

## IV. CLOUD SECURITY RISKS

The security risks associated with each cloud delivery model vary and are dependent on a wide range of factors including the sensitivity of information assets, cloud architectures and security control involved in a particular cloud environment. In the following we discuss these risks in a general context, except where a specific reference to the cloud delivery model is made. Table 4 summarizes the security risks relevant in the cloud computing paradigm.

**Table 3: A List of Security Risks in Cloud Computing**

| Risk | Description |
|---|---|
| Privileged user access | Cloud providers generally have unlimited access to user data, controls are needed to address the risk of privileged user access leading to compromised customer data. |
| Data location and segregation | Customers may not know where their data is being stored and there may be a risk of data being stored alongside other customers' information. |
| Data disposal | Cloud data deletion and disposal is a risk, particularly where hardware is dynamically issued to customers based on their needs. The risk of data not being deleted from data stores, backups and physical media during decommissioning is enhanced within the cloud. |
| E-investigations and Protective monitoring | The ability for cloud customers to invoke their own electronic investigations procedures within the cloud can be limited by the delivery |

| | |
|---|---|
| | model in use, and the access and complexity of the cloud architecture. |
| Assuring cloud security | Customers cannot easily assure the security of systems that they do not directly control without using SLAs and having the right to audit security controls within their agreements. |

## V. ASSESSING THE SECURITY OF A THIRD PARTY CLOUD PROVIDER

One of the most significant challenges for vendor cloud customers in particular is assurance over the security controls of their cloud provider .This is exacerbated by the fact that there is currently no common industry cloud computing security standard from which customers can benchmark their providers. Customers are primarily concerned with the following issues:

• Defining security requirements – The customers' information security requirements are derived from the organization's own policy, legal and regulatory obligations, and may carry through from other contracts or SLAs that the company has with its customers.

• Due diligence on cloud service providers – Prospective cloud customers should undertake proper due-diligence on providers before entering into a formal relationship. Detailed due-diligence investigations can provide an unbiased and valuable insight into a providers' past track record, including its financial status, legal action taken against the organization and its commercial reputation. Certification schemes such as ISO27001 also provide customers with some assurances that a cloud provider has taken certain steps in its management of information security risks.

• Managing cloud supplier risks – The outsourcing of key services to the cloud may require customer organizations to seek new and more mature approaches to risk management and accountability. While cloud computing means that services are outsourced, the risk remains with the customer and it is therefore in the customer's interest to ensure that risks are appropriately managed according to their risk appetite. Effective risk management also requires maturity both in vendor relationship management processes and operational security processes.

## VI. CONCLUSION

Cloud Computing is a rapidly emerged technology and it is a widely accepted computing paradigm all around the world by its advantages on quick deployment, cost efficiency (on setting up and improvement), large storage space, and easy access to system anytime and anywhere. Apart from these advantages it has some disadvantages on security and privacy concerns, which are seen as the primary obstacles to wide adoption. At the same time, because of the distributed nature of the system, there is a risk of security attacks on services and resources in cloud computing. These attacks can be both outside and inside the cloud provider's network. In this paper, we have discuss the security issues of cloud computing and in terms of attack types and their defense mechanism by means of intrusion detection and prevention systems.

Nevertheless, cloud providers are very tempting targets for attackers, particularly sophisticated ones. If they can get control of a cloud provider's infrastructure, whether through external or internal interfaces, they can control the fates of thousands of cloud customers and millions of individual users.

## REFERENCES

[1] P. Mell and T. Grance, "The NIST definition of cloud computing," NIST special publication 800-145, September 2011.

[2] Google Inc., "Google app engine – google developers," https://developers.google.com/ appengine/, accessed on March 24, 2013.

[3] Amazon Inc., "AWS elastic beanstalk," https://aws.amazon.com/elasticbeanstalk/, accessed on March 24, 2013.

[4] U. Oktay and O.K. Sahingoz, "Attack Types and Intrusion Detection Systems in Cloud Computing**"** et al 6th INTERNATIONALINFORMATION SECURITY & CRYPTOLOGY CONFERENCE.

[5] Gehana Booth, Andrew Soknacki, and Anil Somayaji, "Cloud Security: Attacks and Current Defenses", et al 8th ANNUAL SYMPOSIUM ON INFORMATION ASSURANCE (ASIA'13), JUNE 4-5, 2013, ALBANY, NY.

[6] Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina and Eduardo B Fernandez, "An analysis of security issues for cloud computing", Hashizume et al. Journal of Internet Services and Applications 2013, 4:5.

[7] Amit Sangroya, Saurabh Kumar, Jaideep Dhok, and Vasudeva Varma, " Security and Privacy Issues in Cloud Computing", et al Jaydip Sen Innovation Labs, Tata Consultancy Services Ltd., Kolkata, INDIA.

[8] Towards Analyzing Data Security Risks in Cloud Computing Environments @research.iiit.ac.in, vv@iiit.ac.in.

[9] URL: http://www.atis.org.

[10] URL: http://status.aws.amazon.com/s3-20080720.html

[11] URL: news.cnet.com/2010-1030_3-6102793.html.

[12] URL: http://www.nrf-arts.org.

[13] http://csrc.nist.gov/publications/drafts/800-146/Draft-NIST-SP800-146.pdf (Accessed on: November 20, 2012).

[14] Bertion, E., Paci, F., & Ferrini, R. (2009). Privacy-Preserving Digital Identity Management for Cloud Computing. IEEE Computer Society Data Engineering Bulletin, pp. 1-4, March 2009.

[15] Biggs & Vidalis (2009). Cloud Computing: The Impact on Digital Forensic Investigations. In Proceedings of the 7th International Conference for Internet Technology and Secured Transactions (ICITST'09), London, UK, November, 2009, pp.1-6,Blaze, M., Kannan, S., Lee I., Sokolsky, O., Smith, J. M., Keromytis, A.D., & Lee, W. (2009).

[16] http://www.cpni.gov.uk/Documents/Publications/2010/2010007-ISB_cloud_computing.pdf.

[17] Cloud Security Alliance (CSA)'s Security Guidance for Critical Areas of Focus in Cloud Computing (2009). CSA, April 2009. Available Online at: https://cloudsecurityalliance.org/csaguide.pdf (Accessed on: November 29, 2012).

[18] URL: http://www.itu.int/ITU-T.

[19] URL: http://www.ietf.org.

[20] URL:http://www.oasis-open.org.

[21] J.Q.Anderson, L. Rainie, "The Future of Cloud Computing", http://pewinternet.org/~/ media//Files/Reports/2010/ PIP_Future_of_the_ Internet_cloud_computing.pdf

[22] M. Weiser, "The Computer for the 21st Century," Scientific American Special Issue on Communications, pp. 94-104, 1991.

[23] Llanos, D.R.: Review of Grid Computing Security by Anirban Chakrabarti,Queue 5, 45 (2007).