**Cloud Computing Security**

**Abstract**: In the field of Information Technology, Cloud Computing is one of the fundamental changes happening in the past few years. It has obvious advantage characters such as large-scale computation and data storage, virtualization, high expansibility, high reliability and low price service. However, it also brings great challenges in data security and privacy. This paper presents different aspects of security issues related with clouding computing and surveys the current technologies adopt in this field.

**I INTRODUCTION**

Clouds are actually easily usable and accessible virtualized resources. These resources can be dynamically re-configured to adjust to a variable load scale, allowing optimum resource utilization.It’s also a network-based environment that focuses on sharing computations and resources. Cloud providers use virtualization technologies combined with self-service abilities for computing resources via network infrastructure especially the Internet. In cloud environments multiple virtual machines hosted on the same physical server as infrastructure. Cloud computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the data centers that provide those services.

Based on this, cloud computing is nothing new because it uses approaches, concepts, and practices that have already been established before. From another perspective, everything is new because cloud computing changes how we develop, deploy, scale, update, maintain, and pay for applications and the infrastructure on which they run.

User now could use applications in cloud without installation and access their personal files from any computer with Internet access. This allows much more efficient computing by centralizing storage, memory, processing and bandwidth.

Amazon Simple Web Service (AWS) and Google APP Engine are both well-known example of Clouding Computing service. I will use them as examples to demonstrate most of my views in this paper.

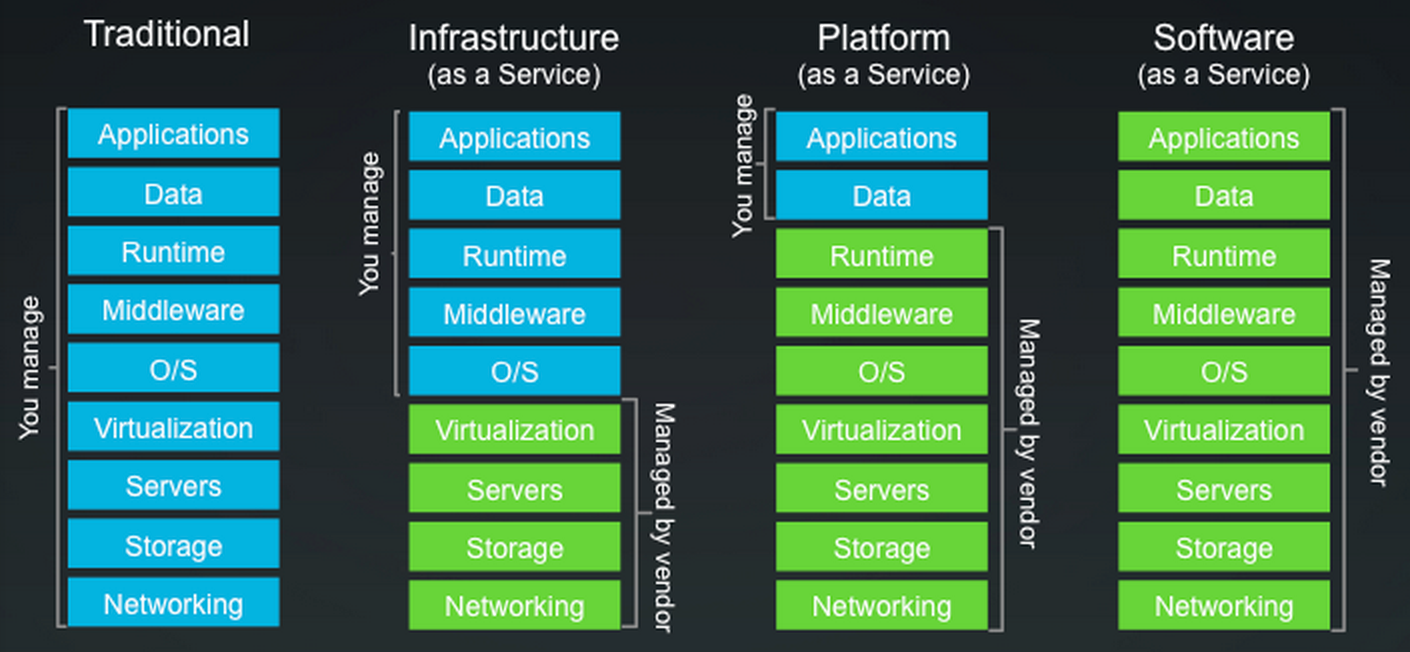
**II CLOUD COMPUTING MODELS**

Several fundamental models are offered by Cloud computing providers. They are infrastructure as a service (IaaS), platform as a service (PaaS), software as a service (SaaS), and network as a service (NaaS). IaaS is the most fundamental one and each higher model abstracts from the lower one.

**Fig.1 Cloud computing service models**

**Infrastructure as a Service (IaaS)**

It is the delivery of hardware, like server, storage and network, and associated software ,such as operating systems, virtualization technology, as a service. It is an evolution of traditional hosting that does not require any long-term commitment and allows users to increase resources on their demand. To deploy their applications, cloud users install operating-system images and their application software on the cloud infrastructure. In this model, the cloud user patches and maintains the operating systems and the application software.

For example, Amazon Web Services provides virtual server instances with unique IP addresses and blocks of storage on demand. Users use the provider's application program interface (API) to start, stop, access and configure their virtual servers and storage.

**Platform as a Service (PaaS)**

Platform as a Service (PaaS) is an application development and deployment platform to developers over the Web. It facilitates development and deployment of applications without the cost and complexity of buying and managing the underlying infrastructure. And provide all of the facilities required to support the complete life cycle of building and delivering web applications and services from the Internet. This platform consists of infrastructure software, normally includes a database, middleware and development tools. A virtualized and clustered grid computing architecture is often the basis for this infrastructure software. With some PaaS providers like Windows Azure, the underlying computer and storage resources scale automatically to match application demand so that the cloud user does not have to allocate resources manually.

**Software as a Service (SaaS)**

A SaaS provider typically hosts and manages a given application in their own data center and makes it available to multiple users over the Web. Cloud users do not manage the cloud infrastructure and platform where the application runs. And don’t need to install and run the application on the user's computers, which simplifies maintenance and support. Cloud applications are different from other applications in their scalability—which can be achieved by cloning tasks onto multiple virtual machines at run-time to meet changing work demand.

Supporters claim SaaS allows the potential to reduce IT operational costs by outsourcing hardware and software maintenance and support to the cloud provider. In addition, applications updates can be released on cloud without the need for users to install new software. One potential problem of SaaS is that the users' data are stored on the cloud server. As a result, there could be unauthorized access to the data. For this reason, intelligent third-party key management systems could be adopted to help secure their data.

**III CLOUD COMPUTING SECURITY STATUS ANALYSIS**

With the developing of cloud computing, the threats, risks and vulnerabilities with Cloud Computing are also evolving. To prevent a system from vulnerable attacks is considered as the system’s security. Some people argue that user data is more secure when managed internally, while others argue that cloud providers have a strong incentive to maintain trust and employ a higher level of security. It’s a fact of truth that in the cloud, your data will be distributed over these individual computers no matter where your base repository of data is ultimately stored.

With cloud computing, the impact, which a cyber-attack can have at this moment, is growing logarithmically. A completely interconnected and globalized world is nothing but a bigger cyber-attack surface from a hacker’s perspective. In a report titled "Assessing the Security Risks of Cloud Computing" ,Gartner says that Cloud computing has "unique attributes that require risk assessment in areas such as data integrity, reliability, and privacy”.

**Integrity**

Data integrity protection is one of the prime challenges in the cloud computing because the data is located in the third party server. We need to keep up data integrity for our cloud data in efficient manner for our own usage whenever there is a want for that and must have some integrity measurement for our data storage to protect data from internal and external attack including byzantine as well as malicious attack.

In a cloud computing model, the program efficiency and performance are addressed by the integrity. So it’s highly recommended for the cloud provider and user to adopt certain method to confirm the integrity of any retrieved data. One of the command method is based on hash values. A hash value is derived by condensing a set of data into a single unique value by way of a pre-defined algorithm. Since the hash value is derived from the original data itself, if the two hash values are not identical, it is an indicator that at least one of the two copies has been either altered or corrupted.

**Reliability**

Reliability also plays a major role in cloud computing since the needs of the users should be satisfied in time. Based on one research from the University of California, it was found that overload on the system caused programming errors resulting in system crashes and failures has happened to all of the major cloud suppliers. Due to the lack of backup recovery Apple, Google Gmail and Amazon s3 reported periods of unavailability ranging from 2 to 14hrs in a span of just 60 days. This could result in a loss of confidence among the users and the suppliers.

Servers in the cloud have the same problems as our own resident servers. They also experience downtimes and slowdowns. The difference is that users have a higher dependent on cloud service provider in the model of cloud computing. Natural disasters could also cause significant risks. A lightening strike at one of Amazon’s facilities in 2011 caused the service to go offline for approximately 4 hours. This component of the cloud was difficult to replace immediately and resulted in delays.

**Privacy**

Cloud computing poses great privacy concerns because the service provider can access the data that is on the cloud at any time. This access has the immense risk of data being disclosed either accidentally or deliberately.Different from the traditional computing model, users’ personal data may be scattered in various virtual data center rather than stay in the same physical location, even across the national borders, with virtual computing technology. at this time, data privacy protection will face the controversy of different legal systems. On the other hand, users may leak hidden information when they accessing cloud computing services. Attackers can analyze the critical task depend on the computing task submitted by the users.

Solutions to privacy in cloud computing include policy and legislation as well as end users' choices for how data is stored. The cloud service provider needs to establish clear and relevant policies that describe how the data of each cloud user will be accessed and used. Cloud service users could encrypt data that is processed or stored within the cloud to prevent unauthorized access.

**IV CLOUD COMPUTING SECURITY THREATS**

Cloud computing runs on the network structure. So it’s open to most of network type attacks. Below we present a selection of security issues related to Cloud Computing. Each one is explained briefly and accompanied with a short discussion on potential or real-world measured impacts.

**DDoS Attacks and Network Sniffing**

One of most common attacks is the distributed denial of service attacks(DDoS). Attacker could send a huge amount of nonsense requests to a certain service. As each of these requests has to be processed by the server in order to determine its invalidity, this causes a certain amount of workload per attack request, which, in the case of a flood of requests, usually would cause a Denial of Service to the server hardware. In the specific case of Cloud Computing systems, the impact of such a flooding attack is expected to be amplified drastically. To stop these attacks the use of SYN cookies and limiting users connected to a server could help stop a DDoS attack.

Another type of attack is network sniffing. sensitive data if unencrypted such as passwords and other web service related security configuration such as the UDDI (Universal Description Discovery and Integrity), SOAP (Simple Object Access Protocol) and WSDL (Web Service Description Language) files could be captured by the attacker with a packet sniffer. Port scanning is also another threat.Port 80 is always open due to it being the port that the web server sits on. However this can be encrypted easily. And there should be no intrusion s long as the server software is configured correctly.

**XML Signature Wrapping Attack**

XML Signature Element Wrapping is a well-known type of attacks on protocols using XML Signature for authentication or integrity protection. This also applies to Web Services and Cloud Computing.

The first case of wrapping attacks was discovered by Michael McIntosh and Paula Austel in 2005. Since then, a number of further variations, countermeasures and attacks circumventing these countermeasures have be published. For instance, a method called inline approach was introduced to protect some key properties of the SOAP message structure to hinder wrapping attacks. Due to the rare usage of WS -Security in applications these attacks remained theoretical and no real-life wrapping attack became public. Until in 2008, it was discovered that Amazon’s EC2 services were vulnerable to wrapping attacks. With a variation of the attack presented before an attacker was able to perform arbitrary EC2 operations on behalf of a legitimate user. In order to exploit the SOAP message security validation vulnerability of EC2, a signed SOAP request of a legitimate, subscribed user need to be intercepted. Since the vulnerability in the SOAP request validation allows interference in any kind of operation and has it executed, it does not matter what kind of request the attacker has at its disposal. The case of a virtual machine sending spam mails is just one example what an attacker can do, using the legitimated user’s identity

**Browser Security**

In a Cloud, computation is done on remote servers. The client PC is used as I/O device, and for authentication and authorization of commands to the Cloud. It thus make sense to develop platform independent client software. A standard Web browser is a ideal universal tool for such application. This trend has been observed and confirmed during the last years, and has been categorized under different names: Web applications, Web 2.0, or Software as a Service.

Modern Web browsers with their AJAX techniques (JavaScript, XMLHttpRequest, Plugins) are suited for I/O ideally. But, the security has always been a serious problem. After compared policies (with the notable exception of TLS) for the most important browser releases, this document[6] reveals many shortcomings of browser security, with a focus on the Same Origin Policy (SOP). If we additionally take into account TLS, which is used for host authentication and data encryption, these shortcomings become even more obvious.

**V CLOUD COMPUTING SECURITY MEASURES**

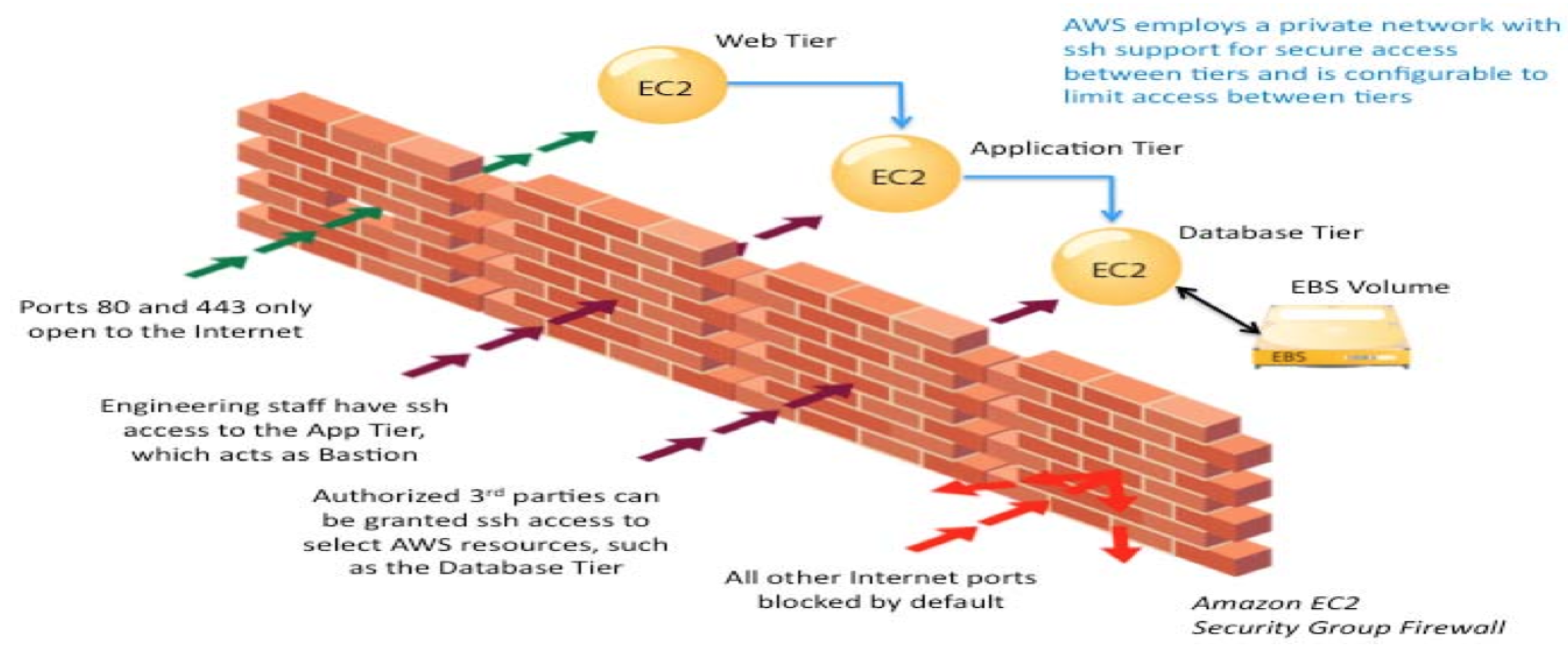
We need to come up with a security analysis process to secure the structure. This will include what type of assets need to be protected from a user point of view, what threats can be run against a them, what countermeasures can be adopted to stop these attacks. Normally, threats include failures in provider security, attacks by a user or hacker, availability and reliability issues.

Amazon is one of the leading company in the field of cloud computing. Below we are going Amazon as an example to analysis how to implement Clouding Computing security in real environment.

**Firewall Implementation in Cloud**

Firewall is a very important meausre for security. For example, Amazon EC2 provides a complete firewall solution; this mandatory inbound firewall is configured in a default deny mode. Users must explicitly open certain ports to allow inbound traffic. The traffic may be restricted by protocol, by service port, as well as by source IP address. The firewall can be configured in groups permitting different classes of instances to have different policies.

For instance, the group for the web servers would have port 80 (HTTP) and port 443 (HTTPS) open to the world. The group for the application servers would have port 8000 (application specific) accessible only to the web server group. The group for the database servers would have port 3306 (MySQL) open to the application server group. All three groups would permit administrative access on port 22 (SSH) only from the User’s corporate network. User can be deployed highly secure applications using this expressive mechanism. The firewall is controlled not by the host/instance itself. the users X.509 certificate and key are required to authorize changes, which adds an extra layer of security. In addition, AWS encourages user to apply additional per-instance filters with host-based firewalls such as IP tables. Both inbound and outbound traffic on each instance can be restricted by this method. The level of security implemented by the



**Fig.2 Amazon EC2 security group firewall**

firewall is a function of which ports are opened by the user, and for what duration and purpose.

**Private Cloud**

Private clouds is another solution to further increase the security of cloud computing. One example of this is the Amazon Virtual private Cloud (VPC). The idea of a private cloud is to allow a company to create a secure and seamless bridge between the company’s existing IT structure and the AWS cloud. Amazon VPC enables user to connect their existing infrastructure to a set of isolated AWS compute resources via a Virtual Private Network (VPN) connection, and to extend their existing security implementation such as security services, firewalls, and intrusion detection systems to include their AWS resources.

**Access Control**

Access to data stored in Amazon S3 is restricted by default; only bucket and object owners have access to the Amazon S3 resources they create (note that a bucket/object owner is the AWS Account owner, not the user who created the bucket/object). There are multiple ways to control access to buckets and objects: AWS IAM (Identity and Access Management) policies enable organizations with many employees to create and manage multiple users under a single AWS Account. IAM policies are attached to the users, enabling centralized control of permissions for users under your AWS Account. With IAM policies, you can only grant users within your own AWS account permission to access your Amazon S3 resources. ACLs is used to grant other AWS accounts (not specific users) access to your Amazon S3 resources. Bucket policies in Amazon S3 can be used to add or deny permissions across some or all of the objects within a single bucket. You can further restrict access to specific resources based on certain conditions. For example, you can restrict access based on request time (Date Condition), whether the request was sent using SSL (Boolean Conditions), a requester’s IP address (IP Address Condition), or based on the requester's client application (String Conditions). To identify these conditions, policy keys will be used.

**Data Transfer and Storage**

For maximum security, data is uploaded/downloaded to Amazon S3 via the SSL encrypted endpoints. The encrypted endpoints are accessible from both the Internet and from within Amazon EC2, so that data is transferred securely both within AWS and to and from sources outside of AWS.

Amazon S3 provides several options for protecting data stored at Cloud. For user who prefers to manage their own encryption keys, they can use a client encryption library like the Amazon S3 Encryption Client to encrypt data before uploading to Amazon S3. Alternatively, you can also use Amazon S3 Server Side Encryption (SSE). With Amazon S3 SSE, you can encrypt data on upload simply by adding an additional request header when writing the object. Decryption happens automatically when data is retrieved. SSE uses one of the strongest block ciphers available – 256-bit Advanced Encryption Standard (AES-256). Every protected object is encrypted with a unique encryption key. This object key itself is then encrypted with a regularly rotated master key. Additional security is provided by storing the encrypted data and encryption keys in different hosts.

**Data Durability and Reliability**

In order to achieved 99.999999999% durability and 99.99% availability of objects over a given year. Objects are redundantly stored on multiple devices across multiple facilities in an Amazon S3 region. Once stored, Amazon S3 maintains the durability of the objects by detecting and repairing any lost redundancy. It also regularly verifies the integrity of data stored using checksums. If corruption is detected, it is repaired using redundant data. In addition, Amazon S3 calculates checksums on all network traffic to detect corruption of data packets when storing or retrieving data. Amazon S3 provides further protection via Versioning. You can use Versioning to preserve, retrieve, and restore every version of every object stored in an Amazon S3 bucket. With Versioning, you can easily recover from both unintended user actions and application failures.

**Access Logs**

An Amazon S3 bucket can be configured to log access to the bucket and objects within it. The access log contains details about each access request including request type, the requested resource, the requestor’s IP, and the time and date of he request. When logging is enabled for a bucket, log records are periodically aggregated into log files and delivered to the specified Amazon S3 bucket.

**Cross-Origin Resource Sharing (CORS)**

AWS users who use S3 to host static web pages or store objects used by other web pages can ensure that content is loaded securely by configuring an S3 bucket to explicitly enable cross-origin requests. Modern browsers use the Same Origin policy to block JavaScript or HTML5 from allowing requests to load content from another site or domain as a way to ensure that malicious content is not loaded from a less reputable source (such as during cross-site scripting attacks). After enable Cross-Origin Resource Sharing (CORS) policy, assets such as web fonts and images stored in an S3 bucket can be safely referenced by external web pages, style sheets, and HTML5 applications.

**VI CONCLUSION**

Cloud computing offers real alternatives to user for improved flexibility and lower cost. With the increase in the growth of cloud computing, security needs to be analyzed more frequently. The Users should be aware of the potential risks and vulnerabilities present in the current cloud computing environment before being a part of the environment.

In this paper, we have discussed several major risks associated with cloud computing and the countermeasures adopted. From this study of current cloud computing practices and inherent risks involved, it is illustrated that major suppliers in this field, like Amazon and Google, have made a great effort to improvement the overall security of their Cloud Computing environment. However, there is a lack of a systematic risk analysis approach in the cloud computing environments. A proper risk analysis approach will be of great help to both the service providers and the users.

In this world where everyone is becoming a part of cloud computing, we believe that awareness among the people regarding the existence of risk, security mechanisms provided by the different cloud service providers to eliminate such risks and the introduction of new risk analysis approaches has significant importance and scope.

**VII REFERENCE**

[1]Amazon. *Amazon Web Services: Overview of Security Processes.* https://aws.amazon.com/security/, 2013.

[2]Arora, Pankaj, Rubal Chaudhry Wadhawan, and Er. Satinder Pal Ahuja. "Cloud Computing Security Issues in Infrastructure as a Service." *International Journal of Advanced Research in Computer Science and Software Engineering* 2, no. 1 (2012): 128.

[3]Chen, Kang, and Weimin Zheng. "Cloud Computing:System Instances and Current Research." *Journal of Software* 20 (2009): 1337-1348.

[4]Cloud Security Alliance. *Security guidance for critical areas of focus in cloud computing v3.0.* https://cloudsecurityalliance.org/, 2011.

[5]Feng, DengGuo, and Min Zhang. "Study on Cloud Computing Security ." *Journal of Software* 22 (2011): 71-83.

[6]Google. "Browser Security Handbook." 2013. https://code.google.com/p/browsersec/.

[7]Jensen, Meiko, Nils Gruschka, and Ralph Herkenhoner. "A Survey of Attacks on Web Services." *Computer Science - Research and Development* 24 (2009): 185-197.

[8]Liu, Wentao. "Research on Cloud Computing Security Problem and Strategy." *Consumer Electronics, Communications and Networks (CECNet), 2012.* Yichang: IEEE, 2012. 1216 - 1219.

[9]Mishra, Ankur, and Ruchita Mathur. "Cloud Computing Security ." *International Journal on Recent and Innovation Trends in Computing and Communication* 1, no. 1 (2013): 36-39.