IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-2, Feb 2019 E-ISSN: 2347-2693

# Cloud Computing and Data Security : AWS and Google Case Study

**Rajinder Singh**

Department of Computer Science and Applications PUSSGRC Hoshiarpur (Pb.)

*Corresponding Author: rajinderid@gmail.com

DOI: https://doi.org/10.26438/ijcse/v7i2.164171 | Available online at: www.ijcseonline.org

Accepted: 12/Feb/2019, Published: 28/Feb/2019

***Abstract*—** Cloud Computing is today's exciting technology**.** Cloud computing means delivering various computer resources over the internet. Main examples of cloud services are webmail, social networking sites and business applications**.** Depending upon the services clouds can be divided into three categories SaaS, PaaS and IaaS. Depending upon the location clouds can be divided into four parts public, private, hybrid and community. Cloud security is very important to organization because data is very important to organizations as well as for the individuals. Depending upon the type of cloud and types of services, security is the two way responsibility. Security is responsibility of both the cloud service providers and users. Three major organizations which provide the cloud service are Azure, Google and AWS. This study discusses various features of Google Cloud and AWS with respect to security. Both these organizations give high priority to the security of user's data. Both these organizations follow layer wise approach to protect user's data. These organizations also provide their own build tools for security and privacy of the data.

***Keywords*—** Cloud Security, Iaas, PaaS, SaaS, Data Encryption, DDoS ;

## I. INTRODUCTION

Cloud computing means delivering various computer hardware and software resources over the internet [1]. Mainly these resources are storage, servers, software and networking. These resources can also be delivered on demand as per user's requirement [2]. Companies which are providing these services are called cloud providers. Data is not stored or updated on the local hard disk but instead of it data is stored at another location and applications stored on the other locations are used. So cloud computing is delivering computing services and resources over the internet. In cloud computing various computing resources are shared over the internet instead of storing them on local personal devices. Main examples of cloud services are webmail, social networking sites, storing various file online and business applications. With the help of cloud computing-model users are able to access information and various computer resources from anywhere if he/she has a network connection. Main purpose of this technology is to decrease costs and helping users to concentrate on their own business instead of IT obstacles. Cloud computing technology provides users a shared pool of resources [3][4].

## II. CLOUD COMPUTING ARCHITECTURE

Main components of cloud computing architecture are: a) Front- end b) Back-end, each of these is connected through network. Client part of the cloud computing is Front end. Mainly these are interfaces and applications which are used to access cloud, e.g. web browsers. Back-end of cloud consists of virtual machines, data storage, security mechanism, services etc [5].

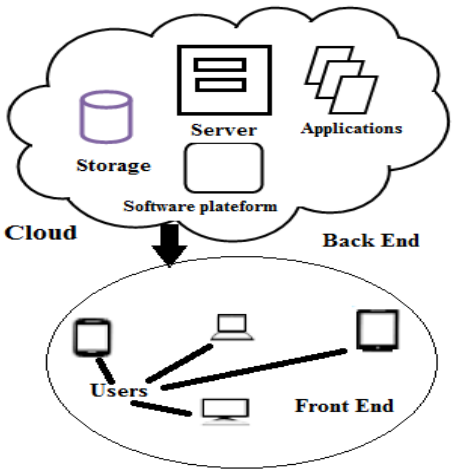


Figure 1 Cloud Computing Architecture

## III. CLOUD COMPUTING SERVICE MODELS

There are mainly three types of cloud computing models:

**a) Infrastructure as a service (IaaS):**

 

This is the main cloud computing service. It gives customers virtualized computing resources over the internet. Main resources consist of networks, storage, servers and management systems in the cloud [5][3]. With the help of these resources clients can build their own applications [6].

**b) Platform as a service (PaaS)**

It provides users computing platforms and helps users to develop their own applications and databases as a service. With the help of this service developers can develop, test, and deliver software applications in on-demand-environment [1][6].

**c) Software as a service (SaaS)**

This service provides their customers hosted applications. Main applications are Customer resource management (CRM), IT services management, video conferencing [1][6].

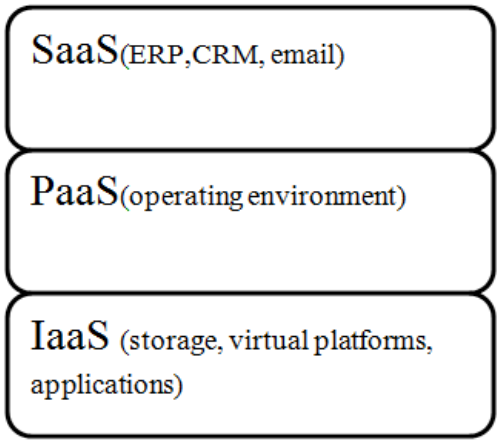


Figure 2 Cloud computing Services

## IV. TYPES OF CLOUD DEPLOYMENTS

**a) Public**

In this type of cloud various resources such as applications, storage and infrastructure are made public over the internet. One example of this type of cloud is IBM's Blue Cloud. Some advantages of public cloud are:

a) Ease of scalability: small and medium-sized organizations can use resources on demand.

b) Organizations can reduce their cost by using public cloud resources instead of investing on their own IT resources.

c) Wastage of the resources is also less [7][8].

**b) Private**

Public cloud also offers the same services as of public cloud but over private IT infrastructure. It is hosted within companies firewall. It is managed by the internal resources. Main advantage of private cloud over public cloud is more security and privacy as compared to public cloud.

Main advantages of private cloud computing are: a) greater control b) increase in performance c) more security and management flexibility.

With the help of private cloud companies can customize their operating environment according to their need and security.

**c) Hybrid**

In case of hybrid cloud, organizations use mixed services of public cloud and private cloud. Organizations can maximize their efficiency by using public cloud for non sensitive operation and using of private cloud if it has sensitive data.

In case of hybrid cloud computing different providers' teams up for providing both public and private services [9]. Hybrid cloud allows data and applications can be shared between public and private cloud [3].

**d) Community**

In case of community cloud infrastructure is shared between the various organizations for shared data [10].

## V. SECURITY AND PRIVACY

Data security is very important in cloud computing. In case of cloud computing, security and privacy of users and organization's data is very important because data is very important asset to organizations and to the users. Companies are not confidant because data is stored in service provider's data centers and it is scattered on different locations and on different machines [2].

When the data is stored in the public cloud it can be compromised in many ways such as a) when data is transferred from internal organizations network to public cloud. b) When data is stored in the cloud. c) When organizations backup the data d) when the data is restored back. Service providers must ensure that proper data security transfer protocols are used while transferring the data on the server.

Cloud computing is mainly defined in two ways a) based on the cloud location b) services that the cloud is offering. Based on the location there are four types of
clouds a) Public b)Private iii) Hybrid iv) Community and based on the services clouds are defined as IaaS, PaaS, SaaS.

 

Depending upon the type of the cloud or services cloud computing security must be done on two sides. a) Cloud providers level b) On user's level. At cloud providers level the cloud providers must maintain the security of infrastructure and client's data and applications are well protected. From user's side, users must use strong password and strong authentication algorithms. Cloud providers must make proper check for their employee to avoid any internal threats. In some cases it may happen that cloud service providers save more than one users data on the same server. So there is chance that one user can access other user's data, so proper isolation methods should be made by the users. If the cloud service providers are using virtualization then the virtualization layer must be properly configure, managed and secured. Further in case of cloud computing a number of traditional threats can be made. In addition to traditional threats other threats that can be made are side channel attack, vulnerabilities due to virtualization. So proper care related to these must be taken [11] [12]. Main Security layers in case of Cloud Computing and responsibilities are shown below:

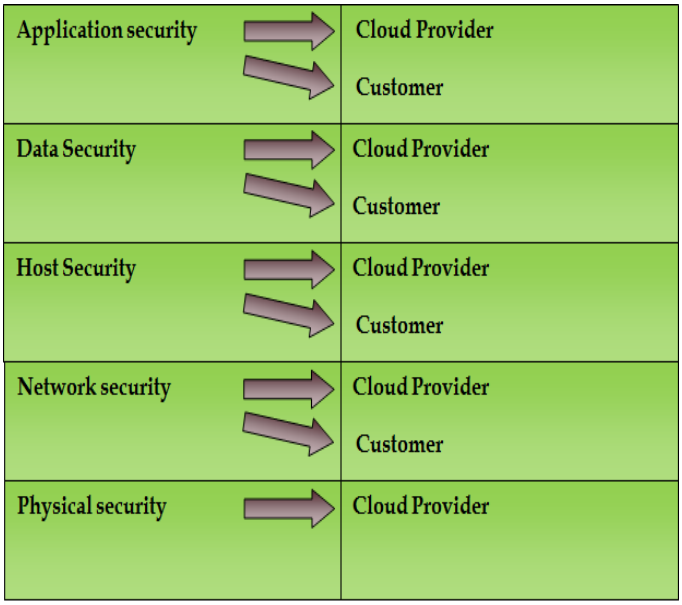


Figure 3 Cloud computing and Responsibilities

## VI. CASE STUDIES

Three major organizations which provide the cloud computing services are Azure, Google and AWS. In this paper various main features and security features of Google Cloud and AWS are discussed. Both of these service provider's have advantages as well as disadvantages.

### *A. AWS Security a Case Study*

AWS gives highest priority to its cloud security. Main security layers where AWS focus on are:

- Infrastructure Security:

Infrastructure security is cloud service provider's responsibility. In case of AWS, clients can create private networks using Network Firewalls and Web application firewalls, thus increasing the security. AWS WAF is used to protect user's web applications from common web threats. AWS WAF can be used to filter the traffic to block attack such as SQL injection attack. When data is transferred from one location to another, it is encrypted. Users can create private or dedicated connections as per their requirement.

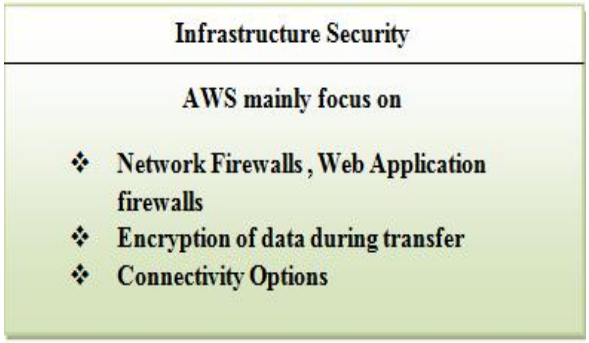


Figure 4 AWS Infrastructure Security

- Data Encryption (Data is at Rest):

AWS provides additional layer of security to user's data by using various encryption features. AWS data storage and databases available with AWS have data encryption capability. With the help of AWS key Management Service either user can manage encryption keys or AWS can manage keys. Sensitive data can also be encrypted with the help of Server – side encryption (SSE). With AWS CloudHSM hardware security module user can create and use their keys.

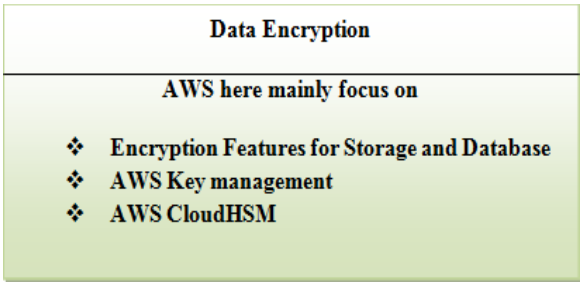


Figure 5 Data Encryption

- DDoS Mitigation:

In this case a combination of services available with AWS may be used to thwart DDoS attacks. These technologies are Amazon CloudFront, autoscaing and Amazon Route 53. These can be used to mitigate Distributed Denial of Service attacks.

 

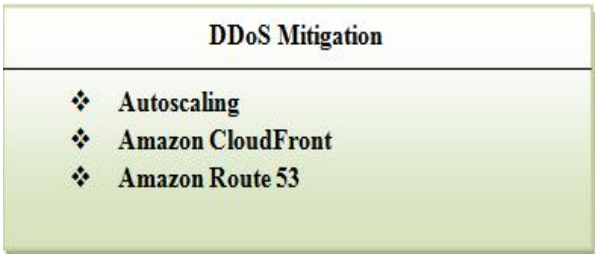


Figure 6 AWS DDoS Mitigation

- Monitoring and Logging:

AWS provides many tools for monitoring AWS environment. API calls can be checked through AWS CloudTrail. Various Alerts and Notifications can be generated by Amazon CloudWatch tool.

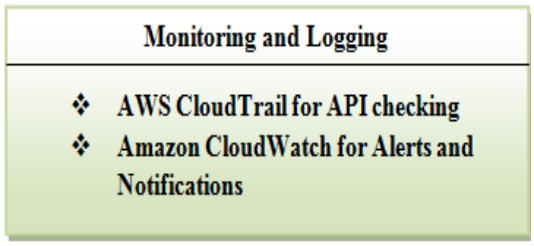


Figure 7 AWS Monitoring and Logging

- Identity and Access Control:

AWS allows defining user access policies. Identity and Access Management (IAM) tool allows defining individual user account. AWS Multi-Factor Authentication can be used for creating privileged account. AWS directory service can be used to reduce administrative overhead.

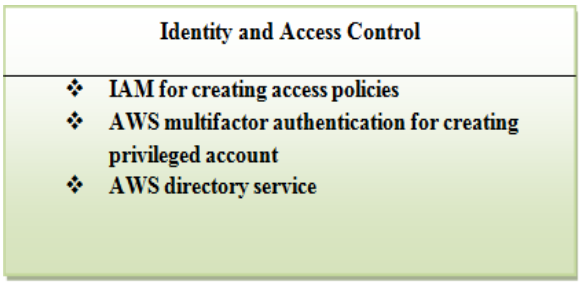


Figure 8 AWS Identity and Access Control

- Inventory and Configuration:

AWS offers many tools for ensuring that these resources are fit with organizational standards. Amazon Inspector tool can be used for checking vulnerabilities or deviations from best practices. Inventory and configuration management tools can identify resources and can be used to manage changes within these resources. AWS provides management tools and template definition e.g. AWS CloudFormation can be used to model the infrastructure components creating a template [13].

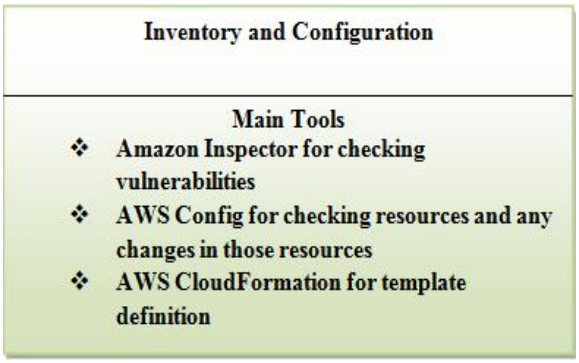


Figure 9 Inventories and Configuration

*B. Google Cloud Security:*

Security of user data is primary concern at Google cloud. Main areas where the Google focus on the security of its cloud are
a) Infrastructure Security
b) Network Security
c) Data Security
d) Application security
e) Identity and access management [14].

Google builds and design its own Data centres. These centres are protected through multiple layers of physical security. Data centres are physically secured using a layered security model. Networking equipments and servers are custom build. Google provide secure deployment of the services and secure communication between these services. Data is encrypted before it is stored on the physical device. For the security of a service on the internet Google Front End infrastructure service and TLS can be used [15].

Similarly custom designed OS is used in the servers. If a hardware component is not working properly then it is removed and proper checks are made that it does not contain any user data. In case of cloud networking only authorized services and protocols are used. To detect the malicious code and DDoS attack, traffic is routed through dedicated servers.

Beside this Google Operational Security is given below.

Google Operational Security:

Cloud security is primary concern for Google, because it runs on the same infrastructure that is made available to its customer. Protection of data is primary design criteria for Google. Google provides cloud security in the following ways[15-15].

 

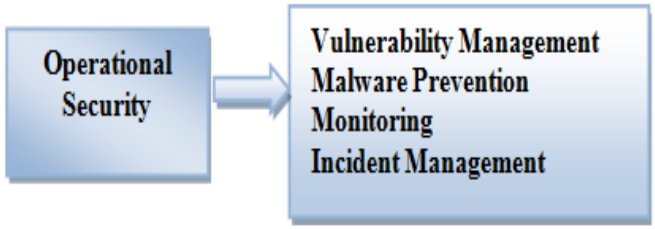


Figure 10 Inventory and Configuration

Operational Security:

In this area Google mainly focus on:

- Vulnerability Management

Google actively scans for various security threats by vulnerability management process. Vulnerabilities are tracked by using commercial as well as built- in -house tools, manual penetration process and quality assurance process etc.

- Malware Prevention

Google uses Safe Browsing technology to look for unsafe sites. Unsafe sites contain malicious code that gets installed on the user's machine when he /she visit it. This threat can lead data theft and compromising user's account. Google also use VirusTotal online technology for checking malicious code. Figure 11 and Figure 12 shows scanning for file and URL with the help of VirusTotal.

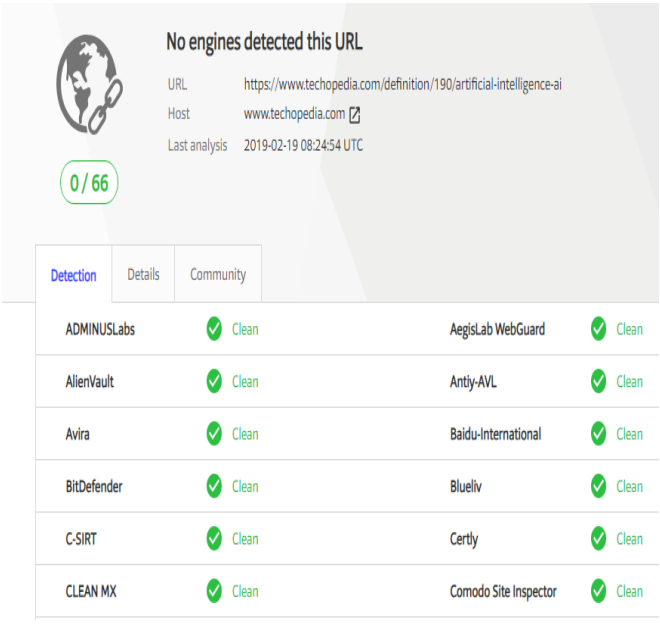


Figure 11 VirusTotel for scanning URL


Figure 12 VirusTotal for scanning file

- Monitoring

Internal network traffic is checked for any kind of suspicious activity like botnet connections. For this purpose a combination of third party and open source tools are used. System logs are examined for checking whether there is an attempt for accessing user data.

- Incident Management

Google use incident management process for checking security events. In case an incident occurs, its severity is checked. Key staff is used for testing the event for various cases.

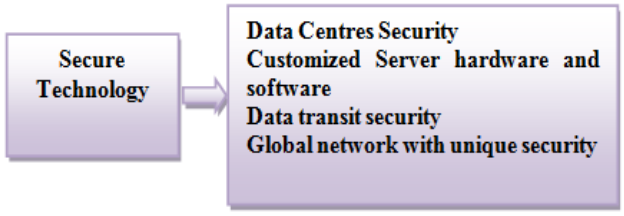


Figure 13 Secure Technology

- Secure Technology

For security, privacy, and compliance independent third-party audits are performed on a regular basis. ISO27001 is

 

used where systems and data centres use G suite. The SOC 1 is used for security, availability, integrity and confidentiality.

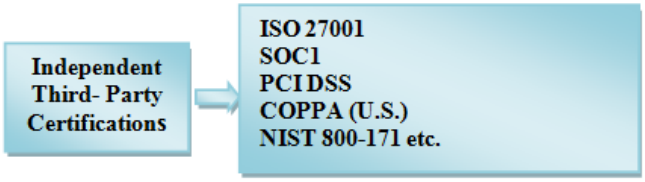


Figure 14 Independent Third-Party Certifications

Comparison at different security layers:

Key features of AWS Security are: Data encryption, secure infrastructure, Data availability, Network security with VPC and IAM.

Key features of Google Cloud Security are: Security of data centers, Data encryption during transit, data encryption during rest, IAM, using of GFE and use of HTTPs protocol.

Table 1

| Comparison of AWS and Google Cloud | | | |
|---|---|---|---|
| ***S.N.*** | ***Main Security Layers*** | ***AWS*** | ***Google Cloud*** |
| 1. | **Infrastructure Security** | a) Security of the data centre building.<br><br>b) Physical access to data centres is logged and audited.<br><br>c) Data is stored within multiple geographic regions and across multiple availability zones.<br><br>d) Using Amazon VPC, AWS AWF. | a) Security of physical premises, security of the Networking Equipment and Storage Hardware.<br><br>b) Secure deployment of services.<br><br>c) Security of the communicating devices |
| **2.** | **Security of Data** | a) Stored data is encrypted using AES-256 bit algorithm<br><br>b) AWS key management for managing encryption keys<br><br>c) CloudHSM hardware module | a) Stored data is encrypted using 256-bit AES algorithm<br><br>b) In case of distributed system data chunks are encrypted with AES 256 algorithm.<br><br>c) Databases and file storage is also protected using AES 128 and AES 256 algorithm. |
| **3.** | **DDoS Mitigation** | autoscaling, Amazon CloudFront and Amazon Route 53 | a) Use of GFE,<br><br>b) Google cloud virtual network |
| **4.** | **Network Security** | Network firewalls, Amazon VPC, and web application firewall. Customers can create their own private network using these. | Use of HTTPS protocol and certificate from a certificate authority(CA) for providing authentication , integrity and encryption |
| **5.** | **IAM** | AWS IAM allows for defining, and managing user access policies. | Google Cloud Identity and Access Management give granular access to resources |
| **5.** | **IAM** | AWS Identity and Access Management allow for defining, and managing user access policies. | Google Cloud Identity and Access Management give granular access to resources |

Cloud computing provides many advantages to users. But there are some major security threats associated with cloud computing. These organizations provide many tools for identifying various network attacks. Main traditional security threats and how these two organizations mitigate them are given below in the table:

Table 2

| **Main Security Threats** | **AWS** | **Google** |
|---|---|---|
| **MITM attack** | Using of SSL-protected endpoints , SSH host certificates Secure API | a) Encryption of Data during transmission.<br><br>b) HTTPS, TLS, BoringSSL |
| **DDoS** | Autoscaling, Amazon CloudFront and Amazon Route 53 | a) Google cloud virtual network, firewall rules, tags and Identity and Access Management (IAM).<br><br>b) GCP automatically provides isolation between virtual networks |
| **IP Spoofing** | Host-based firewall infrastructure | a) Filtering of traffic at various point of the network |

 

| | | |
|---|---|---|
| | | b) Google cloud virtual network<br><br>c) GCP provides anti-spoofing protection |

Main security issues in case of cloud and various methods used by these two organizations are given in the table below. Data integrity means protecting customer's data from deletion and modification. Only authorized users are allowed to modify the data. Data integrity in case of cloud means protection of data from unauthorized deletion and modification.

Data confidentiality means protection of user's sensitive data. In case of public cloud data confidentiality becomes very important because same hardware is used for storing the more than one user's data.

Data availability means data remains available to users under normal as well as under accidental situations.

Data Privacy means that personal information of the users and sensitive data of the users is not disclosed to unauthorized users [16].

Table 3

| S.N. | Main security Keys | AWS | Google Cloud |
|---|---|---|---|
| 1. | **Data Integrity** | a) Permissions with the help of IAM,<br><br>b) Various Integrity checks such as HMAC, MAC, Digital Signatures, | a) Secure Hardware structure<br><br>b) User identity<br><br>c) Secure storage services |
| 2. | **Data Confidentiality** | a) Proper infrastructure security<br><br>b)Different connectivity options,<br><br>c)Various data encryption method | a)Proper infrastructure security<br><br>b) Various data encryption method |
| 3. | **Data Availability** | a) Data is stored in different availability zones | a) Multi-tier and Multi Layer DoS protection |
| 4. | **Data Privacy** | a) Controlled Access to services and resources<br><br>b) Secure storage within AWS regions<br><br>c) Strong Encryption | a) Using Secure Infrastructure<br><br>b)Data encryption keys, Key encryption keys ,Google Key Management System |
| 5. | **Third Party Compliance audits** | Main players are ISO, PCI, HIPPA, FISMA,ITAR, NIST,MPAA, | ISO, SOC, FedRAMP, FISMA |

## VII. CONCLUSION

In case of AWS security is the shared responsibility of customer as well as service provider. AWS provides many different methods for the security of the data. In case of Google security is achieved by applying security at different layers. While cloud computing offers a lot of benefits but some security issues related to cloud are also there. Some important questions to be asked while using cloud computing are a) how stored data is protected by the cloud service provider. b) How the data is protected while it is transferred from the cloud. c) Does service provider is using strong authentication methods or not. d) Does the service provider is using proper law and regulation related to cloud computing or not. e) What kind of methods service provider will follow in case of accidental circumstances? f) What security tools are used to manage the cloud security? [17].

Customers should reevaluate the answers of these questions depending upon the sensitivity of the data before using a cloud.

## REFERENCES


[1] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski,G. Lee, D. Patterson, A. Rabkin, I. Stoica et al., "A view of cloud computing," Communications of the ACM, vol. 53, no. 4, pp. 50–58, 2010.

[2] Z. Xiao and Y. Xiao, "Security and privacy in cloud computing," IEEE Communications Surveys & Tutorials, vol. 15, no. 2, pp. 843–859, 2013.

[3] https://azure.microsoft.com/en-in/overview/what-is-cloud-computing/

[4] https://en.wikipedia.org/wiki/Cloud_computing

[5] http://en.wikipedia.org/wiki/Cloud_computing_architecture

[6] Hashizume, Keiko, et al. "An analysis of security issues for cloud computing." Journal of internet services and applications 4.1 (2013): 5.

[7] http://searchcloudcomputing.techtarget.com/definition/public-cloud

[8] Padhy, Rabi Prasad, Manas Ranjan Patra, and Suresh Chandra Satapathy. "Cloud computing: security issues and research challenges." International Journal of Computer Science and Information Technology & Security (IJCSITS) 1.2 (2011): 136-146.

[9] https://www.interoute.com/what-hybrid-cloud

[10] http://www.globaldots.com/cloud-computing-types-of-cloud/

[11] http://en.wikipedia.org/wiki/Cloud_computing_security

[12] https://www.linkedin.com/pulse/cloud-computing-security-sandesh-h-n

[13] https://aws.amazon.com/security/

[14] https://cloud.google.com/security/infrastructure/design/

[15] https://cloud.google.com/security/overview/whitepaper


 

[16] Sun, Yunchuan, et al. "Data security and privacy in cloud computing." International Journal of Distributed Sensor Networks 10.7 (2014): 190903.
[17] https://www.esds.co.in/blog/cloud-computing-security-questions/#sthash.JIZjE8JG.dpbs

**Authors Profile**

Rajinder Singh is an Assist. Professor in DCSA, PUSSGRC, Hoshiarpur, Punjab, India. He has more than fifteen years of experience of teaching post-graduate classes. His areas of interest are Wireless Network Security, Cyber Security, Artificial Intelligence and Android Security. He is currently pursuing His Ph.D. Degree from P.U. Chandigarh, India.

 